Secrecy in Cognitive Radio Networks: Turning Foes to Allies

Karim Khalil and Eylem Ekici
Department of Electrical and Computer Engineering
Ohio State University, Columbus, Ohio
Email: {khalilk, ekici}@ece.osu.edu

***Abstract*—We study a class of security problems in cognitive radio networks in which multiple half-duplex unlicensed (secondary) users independently eavesdrop the communications of licensed (primary) users unless granted access to communicate over the same spectrum band. The problem is to characterize the optimal rule for the primary system that grants spectrum access to selected secondary users and the optimal resource allocation for the secondary users. When granted access, the transmission of secondary users interferes with the eavesdropped primary signal at other eavesdropping users, possibly leading to improved primary secure rate. First, we formulate a simple game with only one secondary user and study its equilibria. The outcome presents optimality conditions to grant access to the secondary user as a function of channel conditions. Then, we study the game when multiple eavesdropping secondary users exist and show that it is not always optimal to grant access to the strongest eavesdropper. Interestingly, the outcome also reveals a recruiting process that turns selected eavesdroppers into helping jammers under certain conditions.**

I. Introduction

In this paper, we study security attacks in cognitive radio networks in which unlicensed (secondary) users compromise confidentiality of the transmission of licensed (primary) users by eavesdropping. Specifically, the eavesdropping secondary users threaten the primary system by eavesdropping primary traffic when not granted spectrum access to send their own information. Since secondary users have half-duplex transceivers, they can either transmit or eavesdrop at any given time. Thus, granting spectrum access to a selected secondary user to transmit its own information on the same spectrum band will neutralize its eavesdropping attack and may improve the achievable secrecy rate of the primary users.

The novel idea of "threaten-to-access" in Cognitive Radio Networks (CRNs) was recently introduced in our earlier work [1], [2]. In this work, secondary nodes that wish to transmit their own information to a base station serving the primary users, threaten primary nodes by eavesdropping primary traffic and hence decreasing primary secure rates. The main goal for the secondary users (SUs) is *communicating their own information* to the base station. This is in contrast to most of the works in the literature on security [3], where the only objective of attackers is to minimize the achievable confidential rates of primary users (PUs). In this paper, we seek to answer the following questions:

1) When is it optimal for the primary system to grant an eavesdropping secondary user (ESU) access to licensed spectrum?
2) When multiple ESUs exist, which ESU does the primary system select to grant spectrum access so that the primary secrecy rate is improved?
3) For each ESU, what is the optimal resource allocation in all cases?

To this end, we develop static non-cooperative games [4] that model interactions between half-duplex ESUs wishing to transmit their own information to a common destination (e.g., base station in a cellular system) and a PU, which is interested in maximizing its secure rate. We adopt the information theoretic secrecy notion [5], [6] as a measure of the confidentiality of the transmission of PU. In information theoretic secrecy schemes, security can be proven mathematically without imposing any restriction on the computational ability of the eavesdroppers, which is not possible in conventional cryptography. Its results are thus fundamental and independent on the state of technology. When an ESU is granted access and starts transmitting its own information, it is no longer an eavesdropper. In addition, when multiple ESUs exist, the transmission of the selected ESU causes interference on other ESUs and may limit their eavesdropping capabilities. Thus, the selected ESU may be considered as an ally in this case. We analyze equilibria and discuss their uniqueness properties. Moreover, we present interesting observations about some special cases and then provide a discussion on how our model can be implemented in cellular networks.

In [1], [2], we assumed coordination between PU and ESU (during transmission of ESU) such that an optimal multiple access coding scheme [7] can be used. We also considered a network with a single ESU. In this paper, we consider more practical level of coordination between PUs and ESUs, where the decoder treats signals other than the intended one as noise. In addition, we consider the case when multiple ESUs exist in the cognitive radio network and characterize the optimal ESU spectrum access rule the base station should employ to improve secure rate of the PU. We also show that this model bridges the gap between coordination models considered in [2] and conventional CRN models [8], where there is minimal interaction between PUs and SUs. Specifically, the scheme developed in this paper only requires changes to the admission control algorithms at the base station and the channel state feedback algorithm at PUs.

The rest of this paper is organized as follows. Section II presents our system model and our assumptions. In Section III, we formulate a 2-player game, characterize equilibria in different cases of channel conditions and study their uniqueness. In Section IV, we extend the game to multiple ESUs. In Section V, we discuss interesting properties of our scheme. We evaluate the performance of the primary system in Section VI. Finally, Section VII concludes the paper.

II. Preliminaries and Network Model

In this section, we review results and definitions from information theory and game theory that are essential in our analysis. Then, we introduce our network model and the assumptions we make in the paper.

A. Wire-tap Channel

In the presence of an eavesdropper, the achievable secrecy rate of a transmitter is the rate at which the message of the sender is almost independent from the received signals at the eavesdropper. Achievability schemes (i.e., channel coding) are designed to maximize the confusion at the eavesdropper while maximizing the achievable rate at the legitimate receiver by exploiting the wireless channel characteristics such as noise and fading. A Gaussian wiretap channel model consists of a transmitter, a legitimate (intended) receiver and an eavesdropper, where the signals received at both the legitimate receiver and the eavesdropper are corrupted by additive white Gaussian noise (AWGN). The secrecy capacity of this channel, when noise variances are unity, is given by [9]

$$R_s(P) = \log_2(1 + aP) - \log_2(1 + bP), \quad (1)$$

for $a \geq b$ and $R_s(P) = 0$ otherwise, where $a, b > 0$ are the channel power gains of the legitimate (intended) receiver's channel and the eavesdropper channel, respectively, and P is the transmission power.

In our game, we assume that an ESU is equipped with a half duplex transceiver and can either transmit to the common destination D or eavesdrop the transmission of PU at any given time. Thus, the channel model during ESU's eavesdropping is a wiretap channel. Throughout the paper, we refer to the channel between PU and D as the primary channel, the channel between ESU and D as the secondary channel, and the channel between PU and ESU as the eavesdropper channel.

B. Game Theory Basics

Game theory provides an analytical framework to analyze situations of conflict between multiple decision makers that are ***rational, intelligent and selfish***. These attributes accurately characterize wireless devices designed to optimize their own performance. Here, we borrow definitions from [4] and [10] that are needed for equilibrium analysis in the following sections.

A strategic game is any $\mathcal{G}$ of the form $\mathcal{G} = (\mathcal{N}, (\mathcal{S}_i)_{i\in\mathcal{N}}, (u_i)_{i\in\mathcal{N}})$, where $\mathcal{N}$ is the set of players in the game. Let the utility of a player be given by $u_i(s_i, s_{-i})$ where $s_i \in \mathcal{S}_i$ is the strategy (or action) of player i chosen from the set of available strategies $\mathcal{S}_i$ and $\mathbf{s}_{-i}$ is the strategy profile of all other players except for player i chosen from $\times_{j\in\mathcal{N}-\{i\}}\mathcal{S}_j$. If strategy sets of all players in a game $\mathcal{G}$ are finite sets, the game is said to be finite game. A best response strategy s_i^* for player i is a strategy that maximizes $u_i(s_i, s_{-i})$ over $s_i \in \mathcal{S}_i$ given s_{-i}. In the following definitions, we focus on two-player games, i.e., $\mathcal{N} = \{1, 2\}$.

A Nash Equilibrium (NE) is the strategy profile at which no user has incentive to unilaterally deviate to other operating points.

Definition 1: An NE point is a strategy pair (s_1^*, s_2^*) such that

$$\begin{aligned} u_1(s_1^*, s_2^*) &\geq u_1(s_1, s_2^*), \forall s_1 \in \mathcal{S}_1, \\ u_2(s_1^*, s_2^*) &\geq u_2(s_1^*, s_2), \forall s_2 \in \mathcal{S}_2. \end{aligned} \quad (2)$$

Assume there exist two well defined unique mappings $T_1 : \mathcal{S}_2 \to \mathcal{S}_1$ and $T_2 : \mathcal{S}_1 \to \mathcal{S}_2$ such that for any fixed $s_2 \in \mathcal{S}_2$, $u_1(T_1(s_2), s_2) \geq u_1(s_1, s_2), \forall s_1 \in \mathcal{S}_1$ and for any fixed $s_1 \in \mathcal{S}_1$, $u_2(s_1, T_2(s_1)) \geq u_2(s_1, s_2), \forall s_2 \in \mathcal{S}_2$, i.e., T_i defines strategies that are best response to each strategy chosen by the other player. Let the set $D_i = \{(s_1, s_2) \in \mathcal{S}_1 \times \mathcal{S}_2 : s_i = T_i(s_j)\}$ for $i = 1, j = 2$ and $i = 2, j = 1$ be called the rational reaction set of player i and let $D_i(s_j) = \{s_i \in \mathcal{S}_i : (s_i, s_j) \in D_i\}$. Note that any pair in the set $D_1 \cap D_2$ is an NE according to Definition 1. Hence, a strategy profile $\mathbf{s}$ is an NE if and only if the strategy of every player in $\mathbf{s}$ is a best response to the other player's strategy.

The other type of game formulations we employ is Stackelberg games. In a Stackelberg game, a leader makes a decision about its own strategy and followers then choose their strategies accordingly. In the following definitions, we fix player 1 as the leader and player 2 as the follower. The leader chooses the strategy that maximizes its utility from the rational reaction set of the follower [1].

Definition 2: A strategy $\tilde{s}_1 \in \mathcal{S}_1$ is a Stackelberg equilibrium strategy for the leader if

$$\inf_{s_2 \in D_2(\tilde{s}_1)} u_1(\tilde{s}_1, s_2) \geq \inf_{s_2 \in D_2(s_1)} u_1(s_1, s_2), \quad \forall s_1 \in \mathcal{S}_1. \quad (3)$$

The utility of the leader is a well defined quantity [4] and is given by

$$\tilde{u}_1 = \sup_{s_1 \in \mathcal{S}_1} \inf_{s_2 \in D_2(s_1)} u_1(s_1, s_2). \quad (4)$$

On important result about Stackelberg games is that every finite Stackelberg game admits a Stackelberg strategy for the leader [4].

C. Network Model

We consider an infrastructure-based wireless network where all users, both primary and secondary, are interested in communicating to a common destination (e.g., a base station). In this paper, we consider a system comprised of one PU

[1] In games with more than two players and with one leader, the followers choose their strategies simultaneously after the leader has chosen its strategy.

and N ESUs. We denote the PU as node 0 and ESUs as $\{1, 2, \cdots, N\}$.

We consider a time slotted system where channel gains are fixed during a time slot, and formulate one-shot games for each individual time slot. We also assume that channel gains are independent across users and symmetrical, i.e., the channel gain from node 1 to node 2 is identical to the channel gain from node 2 to node 1. Figure 1 shows an example of the considered network when $N = 2$ with different channel gains labeled.

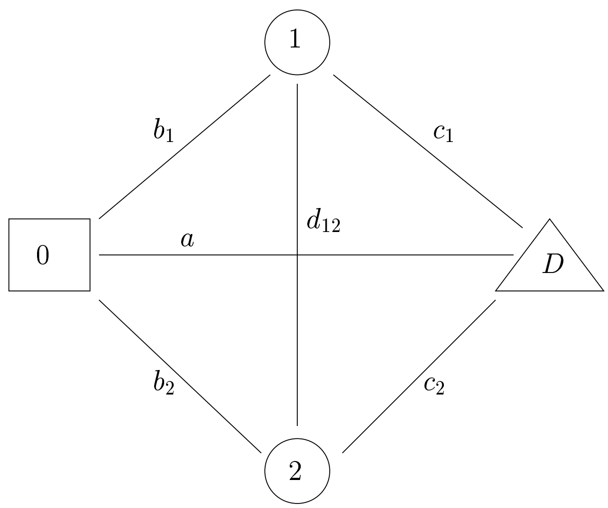

Fig. 1. System Model for $N = 2$.

In this paper, we employ an interference model in which the receiver D treats signals from unintended transmitters (i.e., interference signals) as noise. We assume half-duplex ESUs. Each ESU chooses either to transmit its own information or to receive signals. We also do not consider collusion; we assume that each ESU acts independent of other ESUs.

We model our problem as a non-cooperative game where the players are the base station D, the PU and the ESUs. Let $\mathcal{N} = \{1, \cdots, N\}$. In this paper, we consider discrete strategy sets. The strategy of the base station is to *select an ESU* $s_D \in \{0\} \cup \mathcal{N}$ for which the transmission is decoded in addition to transmission of PU, where $s_D = 0$ means no ESU is selected. The strategy of all other players is to transmit with a fixed power level $s_i = \{0, P_i^{\max}\}, i \in \{0, 1, \cdots, N\}$. When an ESU i chooses $s_i = 0$, then it eavesdrops the transmission of PU. Note that if an ESU is not selected by the base station, its transmission will not be decoded even if it chooses to transmit at a nonzero power level.

The players in this game are interested in maximizing their *net rate*, that is the achievable rate minus the transmission cost. Specifically, the base station is interested in maximizing the PU's net secure rate while the ESUs are interested in maximizing their net achievable rate. Let the strategy profile be defined as $\mathbf{s} = (s_D, s_1, s_2, \cdots s_N)$. Then, the utility function of the primary system is given by:

$$\begin{aligned} u_D(\mathbf{s}) = \Bigg[&\log_2\left(1 + \frac{aP_0}{1 + \sum_{i=1}^{N} c_i s_i}\right) \\ &- \log_2\left(1 + \max_{i \in \mathcal{N}} \left\{ \frac{b_i s_0 \mathbb{1}_{s_i=0}}{1 + \sum_{j \in \mathcal{N}-\{i\}} d_{ij} s_j} \right\}\right) \Bigg]^+ \\ &- \gamma_0 \log_2(1 + P_0), \end{aligned} \tag{5}$$

where P_0 is the fixed transmission power of the PU, $\mathbb{1}_x = 1$ when statement x is true and $\mathbb{1}_x = 0$ otherwise, d_{ij} is the channel gain between ESUs i and j, $[\cdot]^+ = \max\{\cdot, 0\}$ and γ_0 is the PU's transmission cost parameter.

From (5), it can be seen that only those ESUs that are not transmitting (i.e. with $s_i = 0$) can eavesdrop PU's transmission. Also the capability of reducing the confidential rate of PU is reduced by interference from other transmitting ESUs as shown by the denominator of the second term in (5).

The utility function of ESU i is given by:

$$\begin{aligned} u_i(\mathbf{s}) = &\log_2\left(1 + \frac{c_i s_i}{1 + aP_0 + \sum_{j \in \mathcal{N}-\{i\}} c_j s_j}\right) \mathbb{1}_{s_D=i} \\ &- \gamma_i \log_2(1 + s_i), i \in \mathcal{N}. \end{aligned} \tag{6}$$

where γ_i is the transmission cost parameter for ESU i. For our notion of net rate, we use a transmission cost function that increases logarithmically in the rate. The results in the paper also holds for more general increasing cost functions $f(s)$ with $f(0) = 0$.

In this model, we assume that the energy spent by ESUs during reception can be ignored. Also note that s_D affects the utility of PU only indirectly, where $s_i^*, i \in \mathcal{N}$ is function of s_D. In addition, since ESUs are interested in sending information to the base station, the base station can enforce its strategy s_D by decoding or ignoring transmission from certain ESUs, which is reflected by the identity function in (6). This fact motivates the Stackelberg equilibrium analysis in the next section.

III. Single ESU Games

In this section, we analyze the scenario when only one ESU is present in the network. We characterize the cases when it is beneficial for the primary system to allow the ESU to transmit its own information. The results in this section are then used in the more interesting scenario with multiple ESUs, which is addressed in the section IV.

Here, the strategy of the base station is either to allow the ESU to transmit its own information, by choosing $s_D = 1$, or block ESU traffic by choosing $s_D = 0$. When $s_D = 1$, the base station decodes PU's and ESU's signals, treating signals other than the intended one as noise. When $s_D = 0$, the base station just ignores ESU's transmission (if any), treating it as noise.

It is worth noting that a similar strategy set for ESU was considered in [2]. Specifically, a randomization strategy for ESU in our game here, where $s_1 = P_1^{\max}$ with probability α

and $s_1 = 0$ with probability $1-\alpha$, is equivalent to ESU's time fraction strategy considered in [2].

Since the transmission power of the PU is fixed and we have only one ESU, the utility functions in (5) and (6) can alternatively be rewritten as:

$$u_D(\mathbf{s}) = \left[\log_2\left(1+\frac{a'}{1+c's'_1}\right) - \log_2(1+b'\bar{s}'_1)\right]^+, \quad (7)$$

$$u_1(\mathbf{s}) = s'_1\left(\log_2\left(1+\frac{c'}{1+a'}\right)s_D - R_1^{\min}\right), \quad (8)$$

where $s'_1 \in \{0,1\}$ is the strategy of the ESU in this alternative formulation, $a' = aP_0^{\max}, c' = cP_1^{\max}, b' = bP_0^{\max}, \bar{s}'_1 = 1 - s'_1$, and $R_1^{\min} = \gamma_1 \log_2(1+P_1^{\max})$. In the following, we will use the $\tilde{s}$notation to denote the Stackelberg equilibrium strategy.

It can be seen that ESU only transmits when it is granted access (i.e., when $s_D = 1$) and when the achievable rate is above certain threshold $R_1^{\min}$. When ESU is not allowed to transmit (i.e., $s_D = 0$), however, ESU is better off not transmitting (i.e., chooses $s'_1 = 0$) to avoid negative utility. The base station decides whether it would tolerate interference if it allowed the ESU to transmit. If the effect of interference on PU's utility is less than the effect of eavesdropping, then D may choose $s_D = 1$.

As will be illustrated in Proposition 1, since the base station can enforce its strategy s_D, Stackelberg equilibrium will be the outcome of the game, with the base station as the leader. The outcome of the game has phase transition nature as follows.

Proposition 1: ESU is granted spectrum access and transmits its own information if and only if

$$\log_2\left(1+\frac{c'}{1+a'}\right) > R_1^{\min}, \quad (9)$$

and

$$\frac{a'c'}{1+a'+c'} < b'. \quad (10)$$

Proof: To prove the proposition, we will characterize the Stackelberg equilibrium of the game, with the base station as the leader and other nodes as followers, for all ranges of the parameters $a', b', c', R_1^{\min}$ and show that the profile $(s_D, s'_1) = (1,1)$ is the only equilibrium if and only if (9), (10) are true.

First, we find the best response of the ESU. It can be easily seen that

$$T_1(s_D) = \begin{cases} s_D; & \text{if } \log_2(1+c'/(1+a')) > R_1^{\min}, \\ 0; & \text{if } \log_2(1+c'/(1+a')) \le R_1^{\min}. \end{cases} \quad (11)$$

Now, for the case when $\log_2(1+c'/(1+a')) > R_1^{\min}$, the ESU is willing to switch from eavesdropping to transmission if it is granted spectrum access by the base station. In this case, the solution of the game in pure Stackelberg equilibrium strategy depends on the relative advantage the PU will gain, in terms of secure rate, if the ESU is granted spectrum access. Specifically, if $b' > a'c'/(1+a'+c')$, then $\tilde{s}_D = 1$ and the solution of the game is $(\tilde{s}_D, \tilde{s}'_1) = (1,1)$. However, if $b' \le a'c'/(1+a'+c')$, then the solution is $(0,0)$.

On the other hand, when $\log_2(1+c'/(1+a')) \le R_1^{\min}$, $s'_1 = 1$ is a strictly dominated strategy for the ESU and $\tilde{s}'_1 = 0$, independent of s_D. Thus, both the strategy profiles $(0,0)$ and $(1,0)$ are pure strategy Stackelberg equilibria in this case. The non-uniqueness here does not create a problem since the utility of the primary system (leader) is unique. This concludes the proof. ■

The equilibrium analysis of the discrete game considered in this section suggests that ESU is willing to switch from eavesdropping to transmission only if the PU channel (i.e., a') is weak enough with respect to its rate requirement $R_1^{\min}$. In this case, the primary system will grant ESU spectrum access if the effect of ESU's eavesdropping threat is worse than its noise effect on the transmission of PU. Otherwise, ESU will only eavesdrop PU traffic.

The analysis also reveals the fact that sometimes the primary system prefers to tolerate noise from ESU than to tolerate eavesdropping. In the following section, we study the multiple-ESU scenario and investigate how noise from one ESU can even improve the secure rate of the PU by interfering with PU's signals at other eavesdroppers.

IV. The Multiple-ESU Game

In this section, we extend the game in Section III-A to mutliple ESUs. Here, we consider a 3-player static game with one the base station and two[2] ESUs (nodes 1 and 2) all transmitting to a common destination (D) as shown in Fig. 1.

In this game, the strategy set of the base station is $s_D \in \{0,1,2\}$ while the strategy set of each ESU is $s'_i \in \{0,1\}$, $i \in \{1,2\}$, as in the previous section. Utility functions are given as follows.

$$\begin{aligned} u_D =& \Bigg[\log_2\left(1+\frac{a'}{1+c'_1s'_1+c'_2s'_2}\right) \\ &- \log_2\left(1+\max\left\{\frac{b'_1\bar{s}'_1}{1+d'_2s'_2}, \frac{b'_2\bar{s}'_2}{1+d'_1s'_1}\right\}\right)\Bigg]^+, \quad (12) \\ u_i =& s'_i\left(\log_2\left(\frac{c'_i}{1+a'+c'_{3-i}s'_{3-i}}\right)\mathbb{1}_{s_D=i} - R_i^{\min}\right), \\ & i \in \{1,2\}, \quad (13) \end{aligned}$$

where $d'_i = dP_i^{\max}$ and $R_i^{\min} = \gamma_i \log_2(1+P_i^{\max})$. Now, we define multiple quantities that will help us characterize equilibrium points for the game. Let

[2]Noting that only one ESU is granted spectrum access, it can be seen that the extension to larger number of ESUs is straight forward.

$$R_0^0 = [\log_2(1+a') - \log_2(1+\max\{b_1', b_2'\})]^+ , \quad (14)$$

$$R_0^1 = \left[\log_2\left(1+\frac{a'}{1+c_1'}\right) - \log_2\left(1+\frac{b_2'}{1+d_1'}\right)\right]^+ , \quad (15)$$

$$R_0^2 = \left[\log_2\left(1+\frac{a'}{1+c_2'}\right) - \log_2\left(1+\frac{b_1'}{1+d_2'}\right)\right]^+ , \quad (16)$$

$$\Delta R_i = \log_2\left(\frac{c_i'}{1+a'}\right) - R_i^{\min}. \quad (17)$$

where R_0^0 is PU's achieved utility when both ESUs are eavesdropping, $R_0^1(R_0^2)$ is PU's achieved utility when ESU 1 (ESU 2) is transmitting and and ESU 2 (ESU 1) is eavesdropping, and ΔR_i is the slope of the utility function of ESU i. The primary system offers spectrum access to an ESU i only if $R_0^i > R_0^0$. In addition, an ESU i accepts spectrum access offer and switch from $s_i' = 0$ to $s_i' = 1$ only if $\Delta R_i > 0$.

We now characterize equilibrium points for the multiple-ESU game. In this game, the base station is the leader who chooses its strategy first then announces it to the followers. ESUs then play a Nash game by taking simultaneous decisions, given the strategy announced by the base station. The following results can be easily derived based on the equilibrium analysis in Section III.

First, the best response of ESU i, $i \in \{1, 2\}$ is given by:

$$T_i(s_D) = \begin{cases} 1; & \text{if } \Delta R_i > 0 \ \& \ s_D = i \\ 0; & \text{otherwise .} \end{cases} \quad (18)$$

Given the knowledge of the best response of ESUs, the base station now decide its strategy then announces it. Given the strategy of the leader in the Stackelberg game, both ESUs then react by playing a 2-player Nash game. We now check the outcome of the 3-player non-cooperative game, depending on the network model parameters:

1) When $\Delta R_1, \Delta R_2 > 0$ (all ESUs are motivated to transmit), then:
   a) If $R_0^0 > R_0^1, R_0^2$ (if spectrum cannot be granted to either ESU), then $\tilde{s}_D' = 0$ and the solution of the game is $(0, 0, 0)$.
   b) If $R_0^1 < R_0^2$ (if spectrum can be granted to ESU 2), then the solution is $(2, 0, 1)$. The solution is $(1, 1, 0)$ otherwise.
2) When $\Delta R_1 < 0 < \Delta R_2$ (if only ESU 2 is motivated to transmit), then the solution depends on the value of R_0^2. If $R_0^0 < R_0^2$ (if spectrum can be granted to ESU 2), the solution is $(2, 0, 1)$. Otherwise, it is $(0, 0, 0)$. A similar result holds when only ESU 1 is motivated to transmit.
3) When $\Delta R_1, \Delta R_2 < 0$ (no ESU is motivated to transmit), the points $(0, 0, 0)$, $(1, 0, 0)$ and $(2, 0, 0)$ all represent the solutions to the non-cooperative game. However, at each of the three points, the outcome of the utility of the primary system is the same.

The equilibrium analysis shown above suggests the following ESU spectrum access algorithm, to be implemented at the base station. Let $\mathcal{W}$ be the set of ESUs such that for all $i \in \mathcal{N}$, $i \in \mathcal{W}$ if $\Delta R_i > 0$. Also let $\mathcal{F}$ be the set such that for all $i \in \mathcal{N}$, $i \in \mathcal{F}$ if $R_0^i > R_0^0$. $\mathcal{W}$ represents the set of ESUs in $\mathcal{N}$ that can tolerate noise from PU's transmission and are willing to switch from eavesdropping mode to transmission mode, while $\mathcal{F}$ represents the set of ESUs that can improve the secure rate of PU if granted spectrum access. It is then the duty of the base station to select an ESU from $\mathcal{W} \cap \mathcal{F}$ such that the utility u_0 is maximized. If the intersection of $\mathcal{W}$ and $\mathcal{F}$ is empty in a certain time slot, then no ESU is granted spectrum access in that time slot.

V. Discussion

In this section, we present some interesting observations on the outcome of the multiple-ESU game.

A. Interference vs. Eavesdropping

When an ESU is selected to transmit and d_{12} is large, the negative term in the achievable PU secrecy rate expression becomes small. The decision is then based mainly on how interference affects the achievable PU rate at D. This models, for example, the case when ESUs are very near to each other geographically. When d_{12} is small (e.g., far apart ESUs), both interference effect at D and eavesdropping effect are significant in the decision of PU. In this case, our model complements the model in [2] which focused only on the eavesdropping effect.

Now, consider the scenario where $b_1' > b_2'$ and $R_1^{\min}$ is large. This implies that $\Delta R_1 < 0$, $\Delta R_2 > 0$ and $R_0^2 > R_0^0$ implying the solution $(2, 0, 1)$. So even though ESU 1 has better eavesdropping capabilities than ESU 2, ESU 2 is granted access since the relative advantage gained by PU from interference on ESU 1 (specified by d) is larger than the relative disadvantage of interference on D (specified by c_2'). In addition, it shows that its not always optimal to select ESU with the largest eavesdropping capabilities.

B. Distributed Property

The strategies developed in this paper are distributed in nature since they are based on equilibrium concepts of game theory. However, knowledge of different channel parameters is assumed at each node, which limits the distributed decision making process. Nevertheless, this complete information assumption can be justified in a practical scenario that guarantees knowledge of different channel parameters at different nodes as follows.

For a wireless cellular network, PU transmits to the base station. Each ESU that wishes to transmit its own information to the base station announces its presence by transmitting its minimum rate requirement. After an announcement by ESA i, all other nodes in the network can measure their channel gain from node i. Recall that we assume reciprocal channels. Then, PU reports the values of eavesdropper channel gain b_i to the base station, since it is the actual decision maker in the game on behalf of the PU. Since each ESU is actually interested to access the channel, each ESU sends channel gain with other ESUs to PU to show its jamming capabilities. Note that cheating in reporting jamming capabilities can be detected at the base station by comparing channel gains reported from different ESUs. The base station then will have all the necessary information to decided whether it will grant access to an ESU and the index of that ESU.

C. A Comment on Implementation

The parameter s_D in the games we developed is decided by the base station. Consequently, when P_0 is fixed in the discrete game, there will be no involvement of PUs in the selection algorithm other than reporting eavesdropper channel gain, which make this scheme suitable for practical applications with simple modifications to current cellular networks that assign one PU per resource (time or frequency slot). Research in CRNs is usually classified either in commons model, where the primary system is oblivious to secondary users activity, or property rights model where primary users get paid by secondary users (e.g., using cooperative communications techniques) to be granted spectrum access [11], [12]. Consequently, this can be considered as an intermediate case between commons model cognitive radio networks with no interaction between the two systems and property rights model where there is full interaction.

VI. Performance Evaluation

In this section, we evaluate the performance of the primary network and compare the achievable utility when spectrum access is not granted to ESUs versus when access is granted based on the outcome of the multiple ESU game presented in Section IV. The comparison is done for varying average of PU channel gain and varying number of ESUs.

First, we present an example of a one-shot game, i.e., a single time slot. Consider the scenario when $N = 3$. Let $\gamma_0 = 0.1, P_0^{\max} = 1, \gamma_i = 0.2, P_i^{\max} = 1, i \in \mathcal{N}$. We generate a sample of the channel gains $a, b_i, c_i, d_{ij}, i, j \in \mathcal{N}, i \neq j$, according to an exponential distribution with unit mean. In this example, $a = 0.8253, b = [1.1219\ 2.24087\ 0.2103], c = [0.9174\ 0.4226\ 0.5677], d_{12} = d_{21} = 5.7693, d_{13} = d_{31} = 0.4287$ and $d_{23} = d_{32} = 1.1485$. Given theses, values, it is easy to see that $R_0^0 = 0, R_0^1 = 0.0773, R_0^2 = 0.4388$ and $R_0^3 = 0$. For the ESUs, only $\Delta R_1 > 0$. Thus, only ESU 1 is willing to switch to transmit mode. Since $R_0^1 > R_0^0$, the base station grants ESU 1 access to spectrum by choosing $s_D = 1$. Note that ESU 2 is the most capable eavesdropper in this example.

Next, we evaluate the performance over many time slots. We focus on Rayleigh fading channels, where the channel gains are exponentially distributed. We calculate the average utility over a simulation period of 100000 time slot, where we assume channel gains to be i.i.d across time slots. In this case, we assume that the number of ESUs is fixed during the entire simulation period to $N = 3$. In addition, we consider the uniform case across ESUs where average channel gains are set to $\mathbb{E}[b_i] = \mathbb{E}[c_i] = \mathbb{E}[d_{ij}] = 1, i, j \in \mathcal{N}, i \neq j$. Power cost parameters are set to $\gamma_0 = 1$, $\gamma_i = 0.2, i \in \mathcal{N}$ and unit transmission power is assumed for all nodes in the network. In Fig. 2, the utility of the primary system is plotted against $\mathbb{E}[a]$ when the base station grants spectrum access to a selected ESU according to the algorithm in Section IV. The dashed curve shows the utility achieved by the primary system when ESUs are not granted access. It is clear that granting access to SUs yields improved primary utility for all values of PU average channel gain.

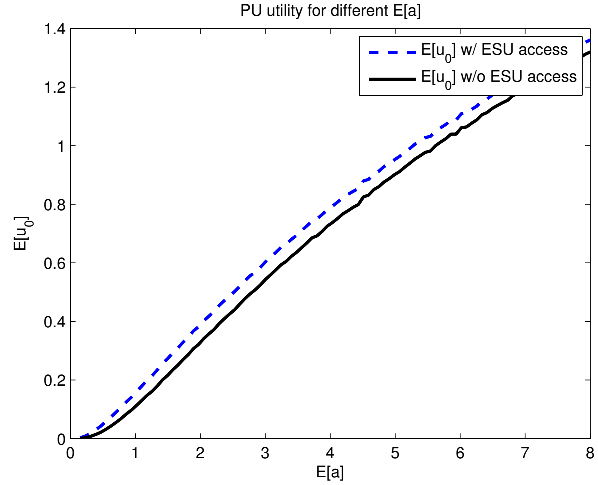

Fig. 2. PU utility v.s. average channel gain.

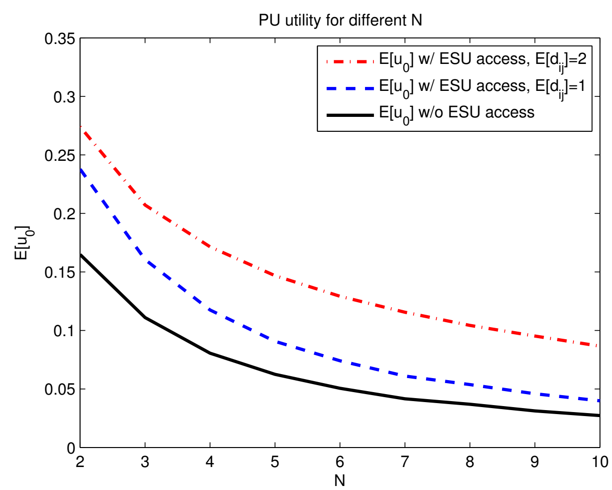

Fig. 3. PU utility v.s. number of ESUs.

Finally, we study how PU utility vary with the number of ESUs in the network for the same value of parameters considered in the previous part. In Fig. 3, we plot $\mathbb{E}[u_0]$ against a varying number of ESUs for two different values of $\mathbb{E}[d_{ij}]$. It is shown that the advantage of granting spectrum access to ESUs diminishes for large number of ESUs. However, this advantage diminishes at a lower rate if $\mathbb{E}[d_{ij}]$ is increased (e.g., for nearby ESUs).

VII. Conclusion

We presented a non-cooperative game theoretical formulation that models eavesdropping threat of secondary users to primary systems. In the presented games, the primary system allows one ESU to transmit its information, simultaneously with the primary user's transmission, to improve its secure rate. Equilibria of the game, in which the base station is the leader and ESUs are the followers, were characterized and their uniqueness was discussed. The outcome of the game with multiple eavesdropping ESUs implies a recruiting process, where the primary system selects an ESU that effectively jam other ESUs while having minimum interference effect on the signal of PU. In our future work, we will study more general selection schemes that can allow multiple ESUs to transmit simultaneously, and study the tradeoff between complexity and optimality. In addition, we will investigate the multiple-ESU game with continuous strategy sets and study cases when the restriction to simple discrete strategies does not degrade performance of different users. Finally, we will study how much performance improvement our spectrum access scheme can offer to the primary system when ESUs collude.

References

[1] K. Khalil and E. Ekici, "Multiple access game with a cognitive jammer," in *Proc. 46th Asilomar Conf. on Signals, Systems and Computers*, 2012.

[2] ——, "Multiple access games with a cognitive eavesdropper," *arXiv preprint arXiv:1211.4053*, 2012.

[3] K. J. R. Liu and B. Wang, *Cognitive radio networking and security*. Cambridge University Press, 2011.

[4] T. Basar and G. J. Olsder, *Dynamic noncooperative game theory*. Academic Press, 1995.

[5] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4, pp. 355–580, Apr. 2009. [Online]. Available: http://dx.DOI.org/10.1561/0100000036

[6] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[7] T. M. Cover and J. A. Thomas, *Elements of information theory*. Wiley-Interscience, 1991.

[8] I. F. Akyildiz, W. Y. Lee, M. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[9] I. Csiszar and J.Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, 1978.

[10] M. Simaan, "Equilibrium properties of the nash and stackelberg strategies," *Automatica*, vol. 13, pp. 635–636, 1977.

[11] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 203 –213, Jan. 2008.

[12] K. Khalil, M. Karaca, O. Ercetin, and E. Ekici, "Optimal scheduling in cooperate-to-join cognitive radio networks," in *Proc. 30th IEEE International Conf. on Computer Communications (INFOCOM 2010)*, Apr. 2011, pp. 3002 –3010.