Journal of Intelligent & Fuzzy Systems 28 (2015) 1281–1290
DOI:10.3233/IFS-141413
IOS Press

Game theoretic approach to optimize the throughput of cognitive radio networks in physical layer attacks

Arash Ahmadfard, Azizollah Jamshidi* and Alireza Keshavarz-Haddad
Electrical and Computer Engineering School, Communications and Electronics Department, Shiraz University, Shiraz, Iran

Abstract. Cognitive Radio (CR) is an adaptive, intelligent radio technology that can automatically detects available channels in a wireless spectrum and change transmission parameters to allow more concurrent wireless communications in a given spectrum band at a location. Physical layer attack is a common attack in these networks which can degrade the performance of cognitive radio networks severely. In this attack, the attacker mimics the signals of the Primary Users (PU) to mislead the cognitive users about the existence of the primary users. Two physical layer attack approaches are studied in this paper. First, we have considered the case that the cognitive users are united against the attacker to maximize the network total throughput. Second, we have studied the case that the cognitive users are selfish but have a common attacker. In both cases, we have assumed that the cognitive network employs carrier sense multiple access with collision avoidance (CSMA/CA) to prevent collisions. We use the game theory approach to model the optimization problem and then try to solve it. Some simulations are conducted to evaluate the cognitive network performances.

Keywords: Cognitive radio, intelligent systems, physical layer attack, game theory, optimization

1. Introduction

Cognitive radio is an intelligent radio that can be programmed and configured dynamically. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at a location [1]. This process is a form of dynamic spectrum management. The development of the cognitive radio is achieved by combining two main features: *cognitive capabilities* and *software-defined radio (SDR)*. Cognitive capabilities include signal processing and machine learning techniques which enable the cognitive users to find and exploit the spectrum opportunities. The intelligence techniques such as fuzzy approaches are used in these networks to control the power of CRs [2, 3]. The authors in [4] survey comprehensive game theoretic approaches for spectrum sharing in the CR networks.

As all of the wireless networks, security issues in cognitive networks are widely regarded in recent years [5–7]. Physical layer attack is one of the severest attacks on the cognitive radio systems. This attack is launched as follows: The frame structure of the cognitive users consists of two parts. In the first part, cognitive users sense the channels to avoid interference to the primary users and in the second part, cognitive users transmit data if no primary user activity is sensed. Both parts are vulnerable to attack. In the first part, an attacker

*Corresponding author. Azizollah Jamshidi, Electrical and Computer Engineering School, Communications and Electronics Department, Shiraz University, Shiraz, Iran. Tel./Fax: +98 71 36133060; E-mail: jamshidi@shirazu.ac.ir.

can send signals similar to those of the primary users to mislead the cognitive users about the existence of the primary activity in channels. Attack in this period is called Primary User Emulated (PUE) attack. This attack is also referred to as spoofing. Spoofing degrades the probability of false alarm in the detector of cognitive users. Moreover, the attacker can send signals in the data transmission period to degrade bit error rate of the cognitive users. Attack in the second period is called jamming. The impact of PUE attack on cognitive networks is studied in [8]. In [9], the tradeoff between spoofing and jamming is analyzed. Recently, some methods are proposed for the detection of PUE attacks. These works can be classified into two categories: location-based [10–13] and non location-based contributions [14, 15]. In [14], a transmitter verification scheme is proposed which verifies whether a signal is from a legitimate primary user or from a PUE attacker. This is accomplished by estimating the location of the transmitter and comparing the estimate with a list of locations of the primary users. Location-based contributions have a major shortcoming: Most of them need to know location and/or transmission power of the primary users a priori. These parameters change if the primary users are mobile or change their configurations. In [15], a method is proposed for identification of PUE attackers observing the received signals.

A traditional method for combating jamming attacks is frequency hopping (FH). In this method, the defender hops randomly over the channels to confuse the jammer. Several scenarios for mitigation of the PUE attack are considered in [16, 17]. In [16], in a first scenario, a system consisting of a single attacker and a single cognitive user is considered. The interactions between those two entities are modeled as a two-player zero-sum game. In a second scenario, a system consisting of a single attacker and multiple cognitive users is studied. The interactions between the attacker and the central controller are modeled as a two-player zero-sum game. In a third scenario, a system consisting of a single attacker and multiple cognitive users is considered. It is assumed that the cognitive network is distributed. In this paper, similar to [16], we have presented a passive approach for defending PUE attacks. A system consisting of a attacker and a distributed cognitive network with multiple users is studied. In a first scenario, we assume that the cognitive users are united against the attacker and follow a policy that maximizes the network total throughput. In a second scenario, we assume that the cognitive users are self-interested but they have a common enemy.

Compared to [16], our proposed approach has the following advantages:

– In [16], it is assumed that if two or more cognitive users select the same channel, they will collide and transmission will fail. In other words, there is no mechanism of collision avoidance like carrier sense multiple access (CSMA) or simultaneous multiple access like code division multiple access (CDMA) in the cognitive network. In this paper, we assume that the cognitive users employ carrier sense multiple access with collision avoidance (CSMA/CA) protocol to resolve the contention at the medium access control (MAC) layer on each channel. CSMA/CA protocol is a popular protocol which is used in IEEE 802.11 standard.
– In [16], in the case of a attacker and a distributed cognitive network, neither explicit expression nor iterative algorithm is proposed for obtaining NEP(s). In that case, due to complexity of the problem, only a proposition is provided which defines some necessary conditions for NEP(s) of the game. In this paper, we have overcome this problem. In particular, we have considered two cases: the case which the cognitive users are united against the attacker and the case that they are self-interested but have a common enemy. Not only we have studied the interactions between the attacker and the cognitive network for both scenarios, we have considered the competition or cooperation among the cognitive users.

The rest of paper is organized as follows: The network model is introduced in Section 1. Then, utility function of the cognitive network and attacker are discussed in Section 1. The best response of the cognitive network to the attacker is studied in Section 4. NEP of the game between cognitive network and attacker is discussed in Section 5. The performance results are presented in Section 6. Finally, conclusions are provided in Section 7.

2. Network Model

We consider a primary network with N channels. Primary users access the channels in a time-slotted fashion. The primary network traffic in each channel is modeled as a two state Markov model. The two states are: *no primary user activity* and *primary user exists*. c_i and θ_i denote the i^{th} channel and the probability that this channel is not used by the primary users.

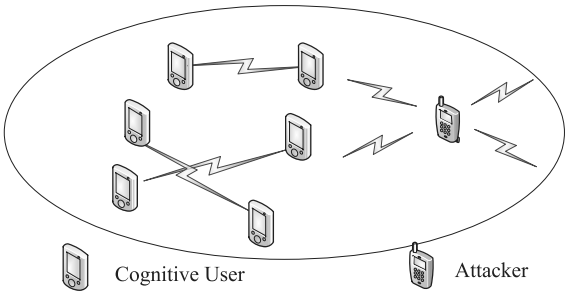

Fig. 1. Network Model.

We assume a distributed cognitive radio system consisting of M pairs coexists with the primary network. An attacker is also considered which jams the channel c_i with probability β_i, where $\sum_{i=1}^{N} \beta_i = 1$. We assume the attacker can only jam one channel at a time. Consequently, c_i is effectively idle with probability $\theta_{eff,i} = \theta_i(1 - \beta_i)$. Without loss of generality, we assume that $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$. From the cognitive users' point of view, there is no difference between the primary users and the attacker. Therefore, the cognitive users can only estimate $\theta_{eff,i}$. However, the attacker can estimate both θ_i and $\theta_{eff,i}$.

The cognitive users opportunistically utilize the channels whenever the channels are idle. To achieve this, cognitive users perform spectrum sensing. Each time slot is divided into two parts: In the first part, cognitive users select and sense the channels and in the second part, they transmit data if the channels are sensed to be idle. We assume that each cognitive user is able to sense only one channel at a time due to hardware limitations. Each cognitive user selects the channels based on a probability mass function. The probability that cognitive user i selects and senses channel j is denoted by α_{ij}. If the channels sensed to be idle, cognitive users access the channels using CSMA/CA protocol.

It is assumed that each device is able to hear the transmissions of other devices if they operate in the same channel. This assumption is made to avoid hidden terminal problem. It is true when the network scale is small. We assume that environment is roughly the same for the cognitive users. In this paper, we focus on symmetric strategies, i.e. we assume the cognitive users access the channel c_j with the same probability say α_j.

Let $\mathbf{z}_i(j)$ be a random variable that shows the status of channel i at time-slot j. This random variable equals 1 when the channel is idle and equals 0 when it is busy. If the channel is idle and the cognitive user sends information without collision with the other cognitive users, he can send B bits, otherwise he has to wait until the next time-slot. Therefore, the time average of the number of bits that a typical cognitive user sends during a block of T time-slots is

$$\mathbf{R} = \frac{1}{T} \sum_{j=1}^{T} B\, \mathbf{z}_i(j). \tag{1}$$

We assume that the discrete random process $\mathbf{z}_i(j)$ is a mean ergodic process [18], i.e. the time average is equal to the statistical average. Consequently, for large T, (1) is equivalent to

$$R = B\, \mathbb{E}\left\{\mathbf{z}_i(j)\right\}. \tag{2}$$

Apparently, R depends on many parameters like the probabilities that each user selects the channels, the traffic of primary network and medium access protocol employed.

The ultimate goal of the attacker is to degrade the throughput of cognitive network as much as possible. The interactions between the attacker and the cognitive network is modeled as a two-player zero-sum game.

We study two scenarios for the cognitive network: In the first scenario, the cognitive users become united against the attacker and follow a policy that maximizes the network total throughput. The whole cognitive users are taken as a unit which defends the attacker. In the second scenario, it is assumed that each cognitive user is only concerned about his own payoff and wants to maximize his own throughput. Although the cognitive users are self-interested, they have a common enemy. Modeling this situation is more difficult than the previous one. The interactions among the cognitive users are modeled as a multi-player mixed strategy game. Additionally, the interactions between the attacker and the cognitive network are modeled as two-player zero-sum game. Hence, in this situation, we have a game in another game.

3. Utility functions

In this section, the utility functions of the cognitive users and the attacker are derived.

3.1. Utility function of the cognitive users

We assume that cognitive users follow CSMA/CA protocol to access the channels. Let $\mathcal{K}_i(t)$ denote the random set of cognitive users who select the channel c_i at the time slot t. Cognitive users in the set $\mathcal{K}_i(t)$,

first sense the channel c_i at the beginning of the time slot. If no primary user activity is sensed, then they generate a random number according to a predefined rule and wait the time specified by that number. After the waiting period finished, the users in the set $\mathcal{K}_i(t)$ sense that channel again. If the channel remains idle, i.e. no cognitive user activity is detected, the users transmit their data. It is inferred that the user with the lowest random number wins the contention.

Lemma 1. *For a typical cognitive user, the expected payoff obtained from the channel c_j is*

$$U_j = \frac{B\theta_{eff,j}}{M\alpha_j}\left(1-\left(1-\alpha_j\right)^M\right). \tag{3}$$

Proof. Suppose a typical user selects the channel c_j. The probability that l other cognitive users select that channel at the same time is

$$\binom{M-1}{l}\alpha_j^l\left(1-\alpha_j\right)^{M-l-1}. \tag{4}$$

In this situation, average number of bits transmitted in one time slot is $B\theta_{eff,j}/(l+1)$ because this channel is shared among $l+1$ users. As a result, the average number of bits a typical user sends is

$$U_j = \sum_{l=0}^{M-1}\binom{M-1}{l}\alpha_j^l\left(1-\alpha_j\right)^{M-l-1}\frac{B\theta_{eff,j}}{l+1} \tag{5}$$

$$= \sum_{l=0}^{M-1}\frac{B\theta_{eff,j}(M-1)!\alpha_j^l\left(1-\alpha_j\right)^{M-l-1}}{l!(l+1)(M-l-1)!} \tag{6}$$

$$= \frac{B\theta_{eff,j}}{M\alpha_j}\sum_{l=0}^{M-1}\binom{M}{l+1}\alpha_j^{l+1}\left(1-\alpha_j\right)^{M-l-1} \tag{7}$$

$$= \frac{B\theta_{eff,j}}{M\alpha_j}\left\{\sum_{l'=0}^{M}\binom{M}{l'}\alpha_j^{l'}\left(1-\alpha_j\right)^{M-l'}\right. \tag{8}$$

$$\left.-\left(1-\alpha_j\right)^M\right\}$$

$$= \frac{B\theta_{eff,j}}{M\alpha_j}\left(1-\left(1-\alpha_j\right)^M\right). \tag{9}$$

□

From Lemma 1, the expected payoff from the channel c_j is U_j. Therefore, the expected payoff from the whole channels is

$$R = \sum_{j=1}^{N}\alpha_j U_j \tag{10}$$

$$= \frac{B}{M}\sum_{j=1}^{N}\theta_{eff,j}\left(1-\left(1-\alpha_j\right)^M\right). \tag{11}$$

3.2. Utility function of the attacker

The attacker wants to degrade the performance of the cognitive network as much as possible. The higher the network total throughput, the lower the payoff of the attacker is. Since the interactions between the attacker and cognitive network are strictly competitive, it is reasonable to model the utility function of the attacker as $U_{attacker} = -R$. Therefore, we have a zero-sum game.

4. Best response of the cognitive users

In this section, we study the best response of the cognitive network to the attacker. Two cases are studied: the case that the cognitive users are united and the case that they are self-interest.

4.1. United cognitive users

In this subsection, we consider the situation in which the cognitive users are united against the attacker and their objective is to maximize the network total throughput.

Using (11), the following optimization problem obtains the best response of the cognitive users to the attacker:

$$\max_{\alpha_i} \quad R = \frac{B}{M}\sum_{j=1}^{N}\theta_{eff,j}\left(1-\left(1-\alpha_j\right)^M\right) \tag{12}$$

$$s.t. \quad \sum_{i=1}^{N}\alpha_i = 1$$

$$\alpha_i \geq 0$$

This optimization problem is equivalent to the following problem:

$$\min_{\alpha_i} \quad \sum_{j=1}^{N}\theta_{eff,j}\left(1-\alpha_j\right)^M \tag{13}$$

$$s.t. \quad \sum_{i=1}^{N}\alpha_i = 1$$

$$\alpha_i \geq 0$$

(13) is a convex optimization problem and the solution is easily obtained solving the KKT conditions. After some straightforward manipulations, the optimal access policy is

$$\alpha_i = \begin{cases} \left(1 - \left(\frac{\lambda}{M\theta_{eff,i}}\right)^{\frac{1}{M-1}}\right)^+ & \theta_{eff,i} > 0 \quad (14a) \\ 0 & \theta_{eff,i} = 0 \quad (14b) \end{cases}$$

where $(.)^+ = \max(0, .)$ and λ is the Lagrange dual multiplier that satisfies $\sum_{i=1}^{N} \alpha_i = 1$.

4.2. Selfish cognitive users

In this subsection, we study the best response of a cognitive network with self-interested users to the attacker. The interactions between the cognitive users can be modeled as a multi-player game. Since there is no central controller and they select the channels based on a probability mass function, we model the interactions between the cognitive users as a mixed strategy game. In the following, some lemmas are introduced and the NEP of this game is obtained.

Lemma 2. *As stated in Section 1, the channels are indexed such that $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$. At NEP, the cognitive users select the channels in the set $\mathcal{S} = \{c_1, c_2, \ldots, c_K\}$ with positive probability, where K will be obtained later. Moreover, the cognitive users do not select the other channels, i.e. they choose the channels in the set $\{c_{K+1}, c_{K+2}, \ldots, c_N\}$ with probability zero. We call the set $\mathcal{S}$ the support set.*

Proof. We prove this via contradiction. Suppose the support set is not of the aforementioned form. Therefore, the support includes a channel say c_h but not c_{h-1}. This means that at NEP, the cognitive users access channel c_{h-1} with probability zero. Hence, $U_{h-1} = B\theta_{eff,h-1}$ and $U_h = \frac{B\theta_{eff,h}}{M\alpha_h}\left(1-(1-\alpha_h)^M\right)$. By substituting $1-(1-\alpha_h)^M = \alpha_h \sum_{j=0}^{M-1}(1-\alpha_h)^j$ in U_h, it can be rewritten as $U_h = \frac{B\theta_{eff,h}}{M}\sum_{j=0}^{M-1}(1-\alpha_h)^j$. As can be seen, U_h is a decreasing function of α_h in the interval $0 < \alpha_h < 1$. Because $\lim_{\alpha_h \to 0} U_h = B\theta_{eff,h}$, it can be concluded that $U_h < B\theta_{eff,h}$. Therefore, the payoff obtained from the channel c_h is less than $B\theta_{eff,h}$. This contradicts the assumption that the cognitive network is operating in NEP. This results from the fact that $U_{h-1} = B\theta_{eff,h-1}$, $U_h < B\theta_{eff,h}$ and the assumption $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$. Since $U_{h-1} > U_h$, a rational cognitive user can increase his payoff by unilateral deviation from his strategy. □

In other words, Lemma 2 states that self-interested cognitive users select the channels with lower primary plus attacker traffic and they have no incentive to select the channels which are too busy. This seems reasonable. It should be emphasized that we only know the form of the support set, i.e. K is not known at this point.

Lemma 3. *At NEP, cognitive users obtain the same payoff from the channels in the support set.*

Proof. Suppose this is not true. If the expected utility obtained from the channels in the support set are not the same, there is a channel with the highest expected payoff among them. This channel is the best channel. A selfish user can increase his utility by selecting the best channel with probability one and never selecting the other channels. This contradicts the assumption that the other channels are in the support set since the channels in the support set should be allocated nonzero access probabilities. □

Using Lemma 3, we know that the average payoff obtained from the channels in the support set are the same. As mentioned previously, the support set is not known exactly. If K were known, using Lemma 3, we could obtain NEP by solving the following simultaneous equation system:

$$\begin{cases} U_1 = \frac{\theta_{eff,1}}{M\alpha_1}\left(1-(1-\alpha_1)^M\right) = C & (15a) \\ \vdots & \\ U_i = \frac{\theta_{eff,i}}{M\alpha_i}\left(1-(1-\alpha_i)^M\right) = C & (15b) \\ \vdots & \\ U_K = \frac{\theta_{eff,K}}{M\alpha_K}\left(1-(1-\alpha_K)^M\right) = C & (15c) \\ \sum_{i=1}^{K} \alpha_i = 1, & (15d) \end{cases}$$

where C is an unknown constant. In the following, first we assume K is known and solve this equation system. The we obtain K precisely. This simultaneous equation system can be solved numerically. The Newton method is employed to achieve this target. In the Newton method, the unknown parameters are put into a vector $\mathbf{x}$, where

$$\mathbf{x} = [\alpha_1 \ \alpha_2 \ \ldots \ \alpha_K \ C]^T. \quad (16)$$

In every iteration, $\mathbf{x}$ is deviated in the direction $\Delta\mathbf{x}$ until $\Delta\mathbf{x}$ converges zero. For the previous equation system, $\Delta\mathbf{x}$ is obtained from the solution of the linear equation system $\Lambda\Delta\mathbf{x} = \mathbf{B}$, where

$$\Lambda = \left[\begin{array}{ccc|c} U_1' & & 0 & -1 \\ & \ddots & & \vdots \\ 0 & & U_K' & -1 \\ \hline 1 & \dots & 1 & 0 \end{array}\right] \tag{17}$$

and

$$\mathbf{B} = -\left[\begin{array}{c} U_1 - C \\ \vdots \\ \hline U_K - C \\ \hline \sum_{i=1}^{K} \alpha_i - 1 \end{array}\right], \tag{18}$$

where $U_i' = \frac{dU_i}{d\alpha_i}$. Because Λ is sparse, finding Λ^{-1} is a simple task. Hence, the Newton method seems to be an appropriate tool for solving the previous equation system.

In the following, K is determined. According to the definition, at NEP, the users can not increase their payoff by changing their strategy. The payoff obtained from the channels in the support set is C. C must be greater than the payoff obtained from the channels out of the support set, otherwise it is not NEP. Therefore, we must have

$$C \geq U_i = B\theta_{eff,i} \qquad \forall i \in \{K+1, K+2, \dots, N\} \tag{19}$$

Since $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$, (19) yields to

$$C \geq B\theta_{eff,K+1}. \tag{20}$$

Lemma 4. *For the scenario that we are talking about, if $\mathcal{S} = \{c_1, c_2, \dots, c_K\}$ is the support set and C is the expected payoff from the channels in the support set, at NEP we have: $C < B\theta_{eff,K}$.*

Proof. Considering the fact that U_i is a decreasing function of α_i in the interval $\alpha_i \in (0, 1)$ and $\lim_{\alpha_i \to 0} U_i = B\theta_{eff,i}$, we can write

$$0 < U_i < B\theta_{eff,i} \qquad i \in \{1, 2, \dots, K\}. \tag{21}$$

Moreover, because at NEP, the payoff obtained from the channels in the support set are the same and equals C, (21) yields to

$$0 < C < B\theta_{eff,i} \qquad i \in \{1, 2, \dots, K\}. \tag{22}$$

Due to the assumption $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$, (22) is equivalent to

$$0 < C < B\theta_{eff,K}. \tag{23}$$

Combining (20) and Lemma 4, it can be concludes that K is given by

$$K = \left\{k \,\middle|\, B\theta_{eff,k+1} \leq C < B\theta_{eff,k}\right\}. \tag{24}$$

For every k that satisfies (24), we have an NEP and this NEP is obtained by solving the equation system (15). Since we have assumed that the number of channels is N, $\theta_{eff,N+1}$ is undefined in (24). It should be mentioned that it is not necessary to check $C \geq B\theta_{eff,N+1}$ in (20). Thus for correctness of (24) for all cases, $\theta_{eff,N+1}$ is set zero. In this situation, C is always greater than $B\theta_{eff,N+1}$ and this inequality would be dummy.

In the following theorem, we prove that the NEP obtained in this section, is unique.

Theorem 1. *NEP is unique for the game among the cognitive users.*

Proof. Please refer to the Appendix I. □

5. NEP of the game between cognitive network and attacker

In the previous section, we studied the best response of the cognitive network to the attacker. In this section, we find the NEP(s) of the zero-sum game between the cognitive network and the attacker.

The throughput of the cognitive users depends on $\theta_{eff,i}$ which itself depends on two factors: the probability that cognitive users select each channel α_i and the probability that the attacker jams each channel β_i. In the previous section, we showed that how the cognitive users react to the attacker based on their preferences. We showed that the cognitive users adjust their access policy solving this optimization problem:

$$g(\beta) = \max_{\alpha_i} \quad R(\alpha, \beta) \tag{25}$$

$$\text{s.t.} \quad \textit{cognitive users' preferences} \tag{26}$$

$$\alpha_i \geq 0$$

$$\sum_{i=1}^{N} \alpha_i = 1$$

where by *cognitive users' preferences*, we mean whether the cognitive users are united or self-interested. (25) is simply obtains the best response of the cognitive network to the attacker considering the preferences of the cognitive users. This is discussed in detail in the previous section.

We consider the whole cognitive network as a unit which defends the attacker. The interactions between these two entities can be modeled as a two-player zero-sum game. The NEPs of such games can be obtained using *minmax theorem* [19]. Since the attacker is to launch the severest attack, finds β_i as follows:

$$\begin{aligned} \min_{\beta_i} \quad & g(\beta) \\ s.t. \quad & \beta_i \geq 0 \\ & \sum_{i=1}^{N} \beta_i = 1 \end{aligned} \tag{27}$$

Using (11), (27) can be rewritten as:

$$\begin{aligned} \min_{\beta_i} \quad & \frac{B}{M} \sum_{j=1}^{N} \theta_j (1-\beta_j) \left(1 - \left(1-\alpha_j^*\right)^M\right) \\ s.t. \quad & \sum_{i=1}^{N} \beta_i = 1 \\ & \beta_i \geq 0 \end{aligned} \tag{28}$$

where $\theta_{eff,j} = \theta_j(1-\beta_j)$ and α_j^* is the optimal cognitive users' access probabilities obtained from (25). Because the constraints in the aforementioned optimization problem builds a convex set, we can employ the gradient projection method [20] to solve the problem. In this method, β_i is obtained iteratively as detailed in Table 1.

In the following, we explain Table 1 in more detail. Let $\mathbf{b}_k = [\beta_1, \beta_2, \ldots, \beta_N]_k^T$ denote the access probabilities of the attacker at the k^{th} iteration. In gradient projection method, starting at point $\mathbf{b}_k$, we take a step $-\mu \mathbf{g}_k$ along the negative gradient of the objective function (28), where $0 < \mu < 1$ is step size. Since (28) is a constrained optimization problem, the point $\mathbf{b}_{k+1}^{'} = \mathbf{b}_k - \mu \mathbf{g}_k$ might be infeasible. To overcome this problem, in gradient projection method [20], we project $\mathbf{b}_{k+1}^{'}$ on the nearest point in the domain of the optimization problem to make it feasible, i.e. $\mathbf{b}_{k+1} = \left[\mathbf{b}_{k+1}^{'}\right]^*$. This procedure is repeated until $||\mathbf{b}_{k+1} - \mathbf{b}_k||^2 < \epsilon$, where ϵ is a small threshold.

Table 1
Attacker's access strategy

1)	**repeat**	
2)		Update α_j^* using (25)
3)		$\mathbf{g}_k = \nabla_{\beta_j} \left\{ \frac{B}{M} \sum_{j=1}^{N} \theta_j (1-\beta_j) \left(1 - \left(1-\alpha_j^*\right)^M\right) \right\}$
4)		$\mathbf{b}_{k+1}^{'} = \mathbf{b}_k - \mu \mathbf{g}_k$
5)		$\mathbf{b}_{k+1} = \left[\mathbf{b}_{k+1}^{'}\right]^*$
6)	**until**	$||\mathbf{b}_{k+1} - \mathbf{b}_k||^2 < \epsilon$

The projection is accomplished by solving the following convex optimization problem

$$\begin{aligned} \min_{\mathbf{b}_{k+1}} \quad & ||\mathbf{b}_{k+1} - \mathbf{b}_{k+1}^{'}||^2 \\ s.t. \quad & \mathbf{1}^T \mathbf{b}_{k+1} = 1 \\ & b_{i,k+1} \geq 0 \quad i \in \{1, 2, \ldots, N\} \end{aligned} \tag{29}$$

where $b_{i,k+1}$ is the i^{th} element of vector $\mathbf{b}_{k+1}$ and $\mathbf{1}$ denotes a column vector with all entities equal to one. As shown in (29), projection yields to a convex optimization problem. After some straightforward manipulations, the solution of this optimization problem can be obtained easily:

$$b_{i,k+1} = \left(b_{i,k+1}^{'} - \nu\right)^+ \tag{30}$$

where $(.)^+ = \max(0, .)$ and ν is the Lagrange dual multiplier that satisfies $\mathbf{1}^T \mathbf{b}_{k+1} = 1$.

In the following, we provide a theorem in which we prove that convergence of the procedure summarized in Table 1, yields to an NEP of the game between the cognitive network and attacker.

Theorem 2. *Convergence of the gradient-projection-based procedure studied in this section yields to an NEP of the zero-sum game between the cognitive network and attacker.*

Proof. According to the definition, a strategy profile is NEP iff no player can increase his payoff by unilateral deviation in his strategy. In other words, every player responds at his best to the other players. Since the cognitive network always responds best in every iteration, apparently, it is true at the convergence point. Moreover, the operating point of the attacker is obtained by solving the optimization problem (27). Two cases can be considered for the operating point of the attacker: First, the operating point is a local minimizer and second, it is a global minimizer of (27). Clearly, if the operating point of the attacker is a local minimizer, the attacker can improve his payoff. As a result, this point is not NEP. In the following, we prove this is not true at the convergence point. If we look more carefully at (28), we see that it is simply a linear programming (LP) problem for fixed α_j^*. LPs are convex and for convex optimization problems, any local minimum is also the

global minimum [21]. As can be seen in Table 1, in every iteration, we assume α_j^* is fixed and take a step towards the minimizer. At convergence point, we are at a global minimizer because as discussed before, for fixed α_j^*, (28) is convex. Therefore, attacker responds best to the cognitive network at the convergence point. Consequently, the operating point is an NEP. □

Remarks:

1. A major question arises as to whether or not the procedure summarized in Table 1 converges to the best NEP. A theorem by von Neumann [19] answers this question: In two-player zero-sum games, each player receives the same payoff in any NEP. The game studied in this section is a two-player zero-sum game between the attacker and cognitive network. Consequently, even if there are multiple NEPs, the payoff obtained in all of them are the same and there is no difference among them from a rational player's perspective.
2. Any time, the cognitive network responds to the environment at best. This is accomplished by solving (25). However, attacker does not necessarily launch the severest attack. To be more specific, attacker may not be smart enough to adjust his policy according to (27). If the attacker launches the severest attack, he forces the cognitive network to operate in an NEP. However, if he is not smart enough, the throughput of the cognitive network is higher. This is an important property of the proposed algorithm.

6. Simulation results

In this section, we have conducted numerical simulations to evaluate the proposed channel selection method.

A comparison between the performance of united and self-interested users is shown in Fig. 2. We have assumed that the network consists of 9 channels with effective probability of idleness $\theta_{eff,1} = 0.9$, $\theta_{eff,2} = 0.8$, $\theta_{eff,3} = 0.7$, …, and $\theta_{eff,9} = 0.1$. We assume B is 1 bit per time-slot. In this figure, the total throughput of the cognitive network is plotted as a function of the number of cognitive users. The achievable total throughput is $B\sum_{i=1}^{N}\theta_{eff,i} = 4.5$ bits per time slot. For both cases, the total throughput rises as the number of cognitive users increases because more spectrum opportunities are exploited. Obviously, unity results in higher performance in comparison to being selfish. This is easily seen in Fig. 2.

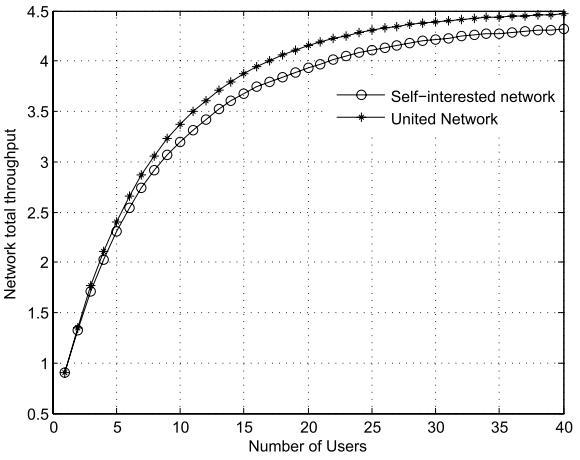

Fig. 2. Network total throughput.

The network studied in this paper was distributed. An important thing about distributed networks is that the users might not be willing to cooperate to fulfil network functions. This selfish misbehavior can cause severe performance degradation. Price of anarchy (PoA) can be employed as a factor for measurement of the performance loss owing to selfish misbehavior. By definition, PoA is defined as the ratio of maximum total utility to the total utility obtained from the worst case equilibrium. For the case in question, PoA is the ratio of throughput obtained by united users to the one obtained by self-interested users. A network consisting of 10 channels and 4 cognitive pairs is considered. The effective probability of idleness for these 10 channels are selected randomly and independently from a uniform distribution in the interval (0.1, 0.9). Figure 3 shows PoA for 100 random cases for the studied network. As can be seen, PoA is near 1 for many cases. This means that selfishness of cognitive users does not cause considerable drop in network total throughput.

Another performance metric simulated is antijamming efficiency (AJE). AJE is defined as the ratio of the expected throughput of a cognitive user when the attacker exists to the expected throughput of the cognitive user when no attacker exists. A cognitive network consisting of 10 channel and 4 users is simulated. The effective probability of idleness for these 10 channels are chosen randomly and independently from a uniform distribution in the interval (0.1, 0.9). An attacker is also considered which launches the severest attack. This scenario is repeated 100 times and for each one, AJE is simulated. Figure 4 plots AJE for each random scenario. Since we have assumed that attacker launches

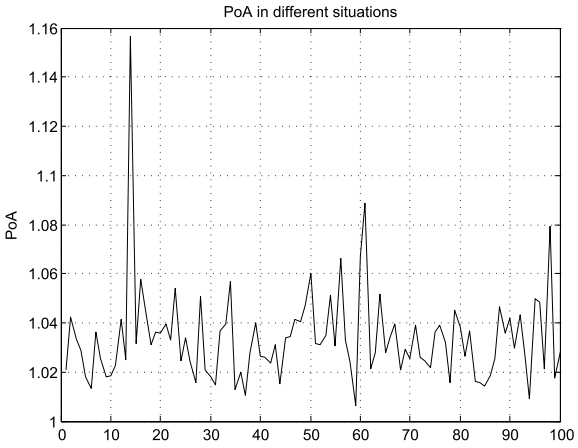

Fig. 3. PoA in 100 different random situations.

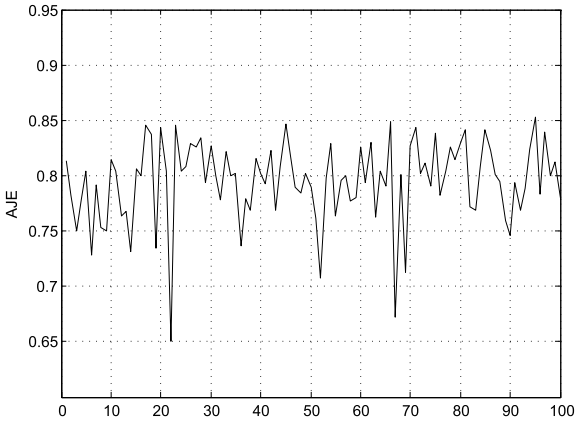

Fig. 4. Effect of attacker on united cognitive network in 100 different random situations.

the severest attack, the obtained AJE relates to the worst case.

7. Conclusions

A severe attack on cognitive radio systems is PUE attack. In this attack, the attacker mimics the signals of the primary users to mislead the cognitive users about the existence of the primary users. Two passive approaches, similar to frequency hopping (FH) in traditional anti-jamming schemes, are studied in this paper. First, we have considered the case that the cognitive users are united against the attacker and adjust their access policy such that the network total throughput is maximized. Second, we have studied the case that the cognitive users are selfish but have a common enemy. In both cases, we have assumed that the cognitive network is distributed and users employ carrier sense multiple access with collision avoidance (CSMA/CA) to prevent collisions. Simulation results are presented to show the performance of the proposed methods.

References

[1] Q.H. Mahamound, Cognitive Networks: Towards Self-Aware Networks, Wiley Press, 2007, Ch. 11, pp. 271–289.

[2] M.-L. Ku and J.-C. Lin, Cognitive radio and interference management: Technology and strategy, Hershey, PA: Information Science Reference, 2013, Ch. 6.

[3] A. ur Rahman, I. Qureshi, A. Malik and M. Naseem, Dynamic resource allocation for ofdm systems using differential evolution and fuzzy rule base system, *Journal of Intelligent and Fuzzy Systems (JIFS)*, IOS Press.

[4] M.M. Halldorson, J.Y. Halpern, L. Li and V.S. Mirrokni, On spectrum sharing games, in: ACM on Principles of distributed computing, 2004, pp. 107–114.

[5] A. Fragkiadakis, E. Tragos and I. Askoxylakis, A survey on security threats and detection techniques in cognitive radio networks, *IEEE Communications Surveys and Tutorials* **15**(1) (2013), 428–445.

[6] Y. Zhang and L. Lazos, Vulnerabilities of cognitive radio mac protocols and countermeasures, *IEEE Network* **27**(3) (2013), 40–45.

[7] M. Jo, L. Han, D. Kim and H. In, Selfish attacks and detection in cognitive radio ad-hoc networks, *IEEE Network* **27**(3) (2013), 46–50.

[8] Z. Jin, S. Anand and K.P. Subbalakshmi, Impact of primary user emulation attacks on dynamic spectrum access networks, *IEEE Transactions on Communications* **60**(9) (2012), 2635–2643.

[9] Q. Peng, P. Cosman and L. Milstein, Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary, *IEEE Journal on Selected Areas in Communications* **29**(4) (2011), 903–911.

[10] R. Chen, J.-M. Park and J. Reed, Defense against primary user emulation attacks in cognitive radio networks, *IEEE Journal on Selected Areas in Communications* **26**(1) (2008), 25–37.

[11] Z. Jin, S. Anand, K.P. Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in: Communications, 2009. ICC '09. *IEEE International Conference on*, 2009, pp. 1–5.

[12] Z. Yuan, D. Niyato, H. Li, J.B. Song and Z. Han, Defeating primary user emulation attacks using belief propagation in cognitive radio networks, *IEEE Journal on Selected Areas in Communications* **30**(10) (2012), 1850–1860.

[13] Z. Jin, S. Anand and K.P. Subbalakshmi, Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, *Sigmobile Mob Comput Commun Rev* **13**(2) (2009), 74–85.

[14] Z. Chen, T. Cooklev, C. Chen and C. Pomalaza-Raez, Modeling primary user emulation attacks and defenses in cognitive radio networks, *in: Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International*, 2009, pp. 208–215.

[15] N. Nguyen, R. Zheng and Z. Han, On identifying primary user emulation attacks in cognitive radio systems using

nonparametric bayesian classification, *IEEE Transactions on Signal Processing* **60**(3) (2012), 1432–1445.
[16] H. Li and Z. Han, Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part I: Known channel statistics, *IEEE Transactions on Wireless Communications* **9**(11) (2010), 3566–3577.
[17] H. Li and Z. Han, Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part II: Unknown channel statistics, *IEEE Transactions on Wireless Communications* **10**(1) (2011), 274–283.
[18] A. Papoulis and S. Pillai, Probability, Random Variables, and Stochastic Processes, McGraw-Hill, 2002.
[19] M. Osborne and A. Rubinstein, A Course in Game Theory, MIT Press, 1994, pp. 21–24.
[20] D. Bertsekas, Nonlinear Programming, 2nd Edition, *Athena Scientific*, 1995, Ch. 2, pp. 223–243.
[21] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004, p. 138.

Appendix I: Proof of Theorem 1

Uniqueness of NEP for the game among cognitive users is proved via contradiction. Suppose this game has two NEPs. Let $\mathcal{S}' = \{c_1, c_2, \ldots, c_{K'}\}$ and $\mathcal{S}'' = \{c_1, c_2, \ldots, c_{K''}\}$ represent the corresponding support sets. Let C' and $\left(\alpha_1^{'}, \alpha_2^{'}, \ldots, \alpha_{K'}^{'}\right)$ denote the expected payoff from the channels in the support set $\mathcal{S}'$ and the strategy corresponding to that NEP, respectively. Also C'' and $\left(\alpha_1^{''}, \alpha_2^{''}, \ldots, \alpha_{K''}^{''}\right)$ denote the expected payoff from the channels in the support set $\mathcal{S}''$ and the strategy corresponding to that NEP, respectively. Without loss of generality, let $K^{''} > K^{'}$. To prove the uniqueness of NEP, we introduce the following lemma first.

Lemma 5. *For the scenario that is been discussed, we have* $\alpha_i^{'} > \alpha_i^{''} \quad \forall i \in \{1, \ldots, K'\}$.

Proof. Suppose this is not true. Therefore, we can write $\exists j \in \{1, \ldots, K'\} : \alpha_j^{'} \leq \alpha_j^{''}$. Since U_i is a decreasing function of α_i, we have: $U_j^{'} = \frac{B\theta_{eff,j}}{M\alpha_j^{'}}\left(1-\left(1-\alpha_j^{'}\right)^M\right) \geq U_j^{''} = \frac{B\theta_{eff,j}}{M\alpha_j^{''}}\left(1-\left(1-\alpha_j^{''}\right)^M\right)$. At NEP, the payoff obtained from all the channels in the support set is same. Because $U_j^{'} = C^{'}$ and $U_j^{''} = C^{''}$, we have $C^{'} \geq C^{''}$. Again, using the fact that the payoff from all the channels in the support set is the same, we can write: $U_i^{'} = \frac{B\theta_{eff,i}}{M\alpha_i^{'}}\left(1-\left(1-\alpha_i^{'}\right)^M\right) \geq U_i^{''} = \frac{B\theta_{eff,i}}{M\alpha_i^{''}}\left(1-\left(1-\alpha_i^{''}\right)^M\right) \quad \forall i \in \{1, \ldots, K'\}$. Again, using the fact that U_i is a decreasing function of α_i, we can write: $\alpha_i^{'} \leq \alpha_i^{''} \ \forall i \in \{1, \ldots, K'\}$. Hence, $\sum_{i=1}^{K^{'}} \alpha_i^{'} \leq \sum_{i=1}^{K^{'}} \alpha_i^{''}$. Therefore, $\sum_{i=1}^{K^{'}} \alpha_i^{''} \geq 1$. In the following, we show that this is not true and lemma is proved.

Because $K^{''} > K^{'}$ and $\sum_{i=1}^{K^{''}} \alpha_i^{''} = 1$, we have $\sum_{i=1}^{K^{'}} \alpha_i^{''} + \sum_{i=K'+1}^{K''} \alpha_i^{''} = 1$. According to the definition of the support set, all the channels in the support set $\mathcal{S}^{''}$ are allocated positive probability, i.e. $\alpha_j^{''} > 0 \forall j \in \{1, \ldots, K^{''}\}$. Using this and the equation $\sum_{i=1}^{K^{'}} \alpha_i^{''} + \sum_{i=K'+1}^{K''} \alpha_i^{''} = 1$, we can write $\sum_{i=1}^{K^{'}} \alpha_i^{''} < 1$. This is in direct contradiction to $\sum_{i=1}^{K^{'}} \alpha_i^{''} \geq 1$. This concludes the proof of Lemma 5. □

Using the previous Lemma, we know that if $K^{'} > K^{''}$ we have $\alpha_i^{'} > \alpha_i^{''} \ \forall i \in \{1, \ldots, K^{'}\}$. Since U_i is a decreasing function of α_i, we have $U_i^{'} = \frac{B\theta_{eff,i}}{M\alpha_i^{'}}\left(1-\left(1-\alpha_i^{'}\right)^M\right) < U_i^{''} = \frac{B\theta_{eff,i}}{M\alpha_i^{''}}\left(1-\left(1-\alpha_i^{''}\right)^M\right) \ \forall i \in \{1, \ldots, K^{'}\}$. Since at NEP, the payoff from all channels in the support set is same, we can write $C^{'} < C^{''}$.

In the following we show that this contradicts the assumption $K^{''} > K^{'}$ and as a result, the uniqueness of NEP is proved. From (24) we can write

$$\theta_{eff,K''+1} \leq \frac{C^{''}}{B} < \theta_{eff,K''} \tag{31}$$

and

$$\theta_{eff,K'+1} \leq \frac{C^{'}}{B} < \theta_{eff,K'}. \tag{32}$$

Combining (31) and (32) and the assumption $\theta_{eff,1} \geq \theta_{eff,2} \geq \cdots \geq \theta_{eff,N}$, we have

$$\theta_{eff,K''+1} \leq \frac{C^{''}}{B} < \theta_{eff,K''} \leq \theta_{eff,K'+1} \leq \frac{C^{'}}{B} < \theta_{eff,K'} \tag{33}$$

Hence, $C^{'} > C^{''}$ which is in direct contradiction to $C^{'} < C^{''}$. Consequently, the uniqueness of NEP is proved.