Primary User Emulation Attack Game in Cognitive Radio Networks: Queuing Aware Dogfight in Spectrum

Husheng Li[1], Vasu Chakravarthy[2], Sintayehu Dehnie[3], and Zhiqiang Wu[4]

[1] The University of Tennessee, Knoxville, TN
husheng@eecs.utk.edu
[2] Air Force Research Lab, Dayton, OH
Vasu.Chakravarthy@wpafb.af.mil
[3] Booz Allen Hamilton, Dayton, OH
Sintayehu.Dehnie.ctr@wpafb.af.mil
[4] Wright State University, Dayton, OH
zhiqiang.wu@wright.edu

Abstract. Primary user emulation attack, which targets distabilizing the queuing dynamics of cognitive radio networks, is studied using game theoretic argument. The attack and defense are modeled as a stochastic game. The Nash equilibrium of the game is studied. In particular, the Lyapunov drift is considered as the reward in each round. Explicit expressions of the Nash equilibrium strategies are obtained.

Keywords: primary user emulation, cognitive radio, stochastic game.

1 Introduction

Cognitive radio has attracted substantial studies since its birth in 1999 [14]. In cognitive radio systems, users without license (called secondary users) are allowed to use the licensed spectrum that licensed users (called primary users) are not using, thus improving the spectrum utilization efficiency. When primary users emerge, the secondary users must quit the corresponding channels. To ensure no interference to primary user traffic, the secondary user must sense the spectrum periodically to determine the existence of primary users.

Such a dynamical spectrum access mechanism, particularly the spectrum sensing mechanism, also incurs vulnerabilities for the communication system. One serious threat is the primary user emulation (PUE) attack [1], in which the attacker sends out signal similar to that of primary users during the spectrum sensing period such that the secondary users will be 'scared' away even if there is no primary user, since it is difficult to distinguish the signals from primary users and the attacker. Such an attack is very efficient since the attacker needs only very weak power consumption, due to the high requirement on the spectrum sensing sensitivity of secondary users.

Most existing studies on PUE attack fall in the topics of proactive detection of attacker [1] or passive frequency hopping [11]. Due to the difficulty of detecting

V. Krishnamurthy et al. (Eds.): GameNets 2012, LNICST 105, pp. 192–208, 2012.

the attacker, *we will focus on the frequency hopping for avoiding PUE, in which the secondary users randomly choose channels to sense such that the attacker cannot always block the traffic in the cognitive radio network.* Such an attack and defense procedure is essentially a game, which is coined 'dogfight in spectrum' in [11] and has been studied using game theoretic argument. In previous studies, only single hop communications, such as point to point communications or multiple access, are considered and total throughput is considered as the game reward (cost) for the defender (attacker). However, in many practical applications like sensor networks, the traffics are multihop and have constant average traffic volumes, thus forming a queuing dynamics since each secondary user has a buffer to store the received packets. Hence, the ultimate goal of the game is to stabilize / destabilize the queuing dynamics, thus making the game a *queuing aware* one. Note that the optimal scheduling strategy of stabilizing a queuing system in wireless communication network is obtained in the seminal work [20]. However, there has not been any study on the game for stabilizing/destabilizing queuing systems, which is of significant importance for the security of various queuing systems. In this paper, *we will model this queuing aware dogfight in spectrum as a stochastic game, in which the actions are the channels to sense/block and the rewards are the metrics related to the queue stability such as the Lyapunov drift and back pressure.* We will first study the centralized case, in which both the cognitive radio network and attackers are controlled by centralized controllers, thus making the game a two-player one. Then, we will extend it to the more practical situation, in which each player can observe only local system state, based on which it makes the decision of action. Different from graphical games in which each player has its own reward, in our situation, the attackers and secondary users form two coalitions whose rewards are the sum of the local rewards and each player devotes to increase the coalition reward. Such a 'local-decision-global-reward' brings significant difference from the graphical games. For both cases, we will provide the game formulation, the Nash equilibrium and value of the general situation, and discussions for special cases. Note that, for simplicity, we assume that the attackers know the queuing situation of the cognitive radio network, which can be realized by eavesdropping the control messages in the network.

In summary, our major contribution includes

– Study the network wide PUE attack with the awareness of queuing dynamics, which extends the PUE attack in single hop systems.
– Study the game of stabilizing/destabilizing queuing systems, which extends the decision problems of network stabilization.

The study will deepen our understanding on the security of cognitive radio networks, as well as that of general queuing systems. It will help the design of a robust cognitive radio network which can effectively combat the PUE attack in the network range.

The remainder of this paper is organized as follows. The existing work related to this paper will be introduced in Section 2. The system model will be explained in Section 3. The centralized and decentralized games will be discussed in Sections 4 and 5, respectively. Numerical results will be provided in Section 6. Finally, the conclusion will be drawn in Section 7.

2 Related Works

In this section, we provide a brief survey of the existing works related to this paper. Note that there are huge number of studies in each of the topics. Hence, the introduction is far from exhaustive.

2.1 Security Issues in Cognitive Radio Networks

In contrast to traditional wireless communication networks, two types of new attacks emerge in the context of cognitive radio network, namely the false report attack and PUE. The former one occurs only in collaborative spectrum sensing in which secondary users exchange information or send the observations to a fusion center in order to improve the performance of spectrum sensing. In such a collaboration, a malicious node can send faked report to the center or the neighbors. Hence, various approaches have been proposed to detect such an attack and the corresponding attacker. For example, a Bayesian framework is applied in [23] and [24] to detect the attacker. In [17], a trust system is used to evaluate the trustworthiness of each collaborating secondary user. We have explained the mechanism of PUE attack which also attracted significant studies. In [7], a mechanism is proposed to detect the PUE attack based on the approach proposed in [1]. In [21], the emulation attack is modeled as a Bayesian game and the Nash equilibrium is analyzed. In contrast to these studies, we study the attack and defense with multiple players in networks and the goal of destabilizing/stabilizing the queuing dynamics, instead of the spectrum sensing precision or the system throughput.

2.2 Stability of Queuing Systems

A key task in queuing systems is to stabilize the queuing dynamics; otherwise the buffers containing the packets will overflow, thus causing packet loss. In the seminal work [20], Tassiulas and Ephremides found a scheduling algorithm for wireless communication networks achieving the optimal throughput region. The algorithm was extended to the context of cognitive radio networks by incorporating impact of primary users [22]. In [15], a 'drift-plus-penalty' cost function is proposed to achieve the tradeoff between the queuing stability and other factors like delay. Note that the algorithm proposed in [20] is centralized, i.e., a center will make the decision of scheduling based on the queuing situations of each node, which is impractical in most applications. In recent years, the scheduling algorithm has been extended to the decentralized case at the cost of reasonable performance loss [25][27]. Although the scheduling algorithm and the corresponding queuing stability have been widely studied, there have been few studies on the queuing dynamics aware attack and defense using the tool of game theory.

2.3 Games

The analysis in this paper is based on game theory. Due to the features of the queuing aware dogfight in spectrum, our study concerns both stochastic games and graphical games since the reward is dependent on the system state and the players form a graph (network).

Stochastic Game. Many queuing systems can be modeled as Markov systems in which the future evolution of system is based on only the current system state. Hence, the corresponding game also requires a Markov framework, in which the reward is dependent on the system state. Games in a Markov system are called stochastic games and were studied by Shapley [19]. In stochastic games, the Nash equilibrium, or the game value, is characterized by the combination of dynamic programming and the value of one-snapshot games. A comprehensive introduction on stochastic games can be found in [5]. Note that the classical results in [5][19] are based on the assumption that all players have perfect information of the system state. In many situations, this assumption is invalid. For example, in the context of PUE attack on queuing dynamics in cognitive radio network, the attackers may not perfectly know the queuing situations of each secondary user. However, the computation of Nash equilibrium in stochastic games with partial observation is still an open problem. Hence, we focus on the case of perfect state information in this paper.

Graphical Game. As more studies are paid to various types of networks, such as social networks and communication networks, game theory is also extended from the traditional structureless setup (e.g., two players or multiple layers forming a complete graph) to the scenarios with network structures (called graphical game) [16]. In such games, the players form a graph or a network in which the corresponding topology plays an important role in the game. In one type of graphical game, each player has its own payoff. The algorithm for computing the Nash equilibrium has been studied in [4], [8] and [9]. In another type of graphical game, the players form two coalitions and each player aims to maximize the coalition reward equaling the sum of individual rewards. Such a game has been studied in [3] and [26]. An excellent summary can be found in [2].

3 System Model

The system model consists of the models of cognitive radio networks, data flows and primary user emulation attacks.

3.1 Network Model

We consider a cognitive radio network with N secondary users. The topology of the network can be represented by a graph with N nodes, in which two nodes adjacent to each other are able to communicate with each directly. We denote by $n \sim m$ if secondary users n and m are neighbors in the network. We assume that there are totally M licensed channels which may be used by K primary users. We denote by $\mathcal{N}_k$ the set of secondary users that may be affected by primary user k and denote by $\mathcal{M}_k$ the set of channels that primary user k occupies when it is active. For simplicity, we assume that the activities in different time slots of each primary user are mutually independent, and the probability of being active is denoted by p_k for primary user k.

The time is divided into time slots, each containing a spectrum sensing period followed by a data transmission period. At time slot t, the status of channel m is denoted by s_m; i.e., $s_m = 0$ when the channel is not being used by primary users and $s_m = 1$ otherwise. Due to the limited capability of spectrum sensing, we assume that each secondary user can sense only one channel during the spectrum sensing period. It is straightforward to extend to the more generic case in which multiple channels can be sensed simultaneously. For simplicity, we assume that the spectrum sensing is perfect; i.e., the output of spectrum sensing is free of errors.

3.2 Traffic Model

We assume that there are totally F data flows in the cognitive radio network. We denote by S_f and D_f the source node and destination node of flow f, respectively. We assume that the number of packets arriving at the source node of data flow f satisfies a Poisson distribution with expectation a_f. The routing paths of the F data flows can be represented by an $F \times N$ matrix $\mathbf{R}$ in which $R_{fn} = 1$ if data flow f passes through secondary user n and $R_{fn} = 0$ otherwise. We denote by $\mathcal{I}_n$ the set of flows passing through secondary user n.

The data flows are packetized using the same packet length. Each secondary user has one or more buffers to store the received packets. In each time slot, the secondary users will choose one packet, if there is any, and sense one or more channel for transmission. Suppose that one channel can support the transmission of only one data flow. We assume that, if two secondary users are close to each other, they are not allowed to sense the same channel due to the potential collision. We denote by $\mathcal{C}_n$ the set of other secondary users that have intolerable co-channel interference with secondary user n. We assume that there are sufficiently many channels such that any set of interfering secondary users can be assigned to different channels and all secondary users can transmit simultaneously by appropriately allocating the channels; i.e., $\max_n \mathcal{C}_n \ll M$.

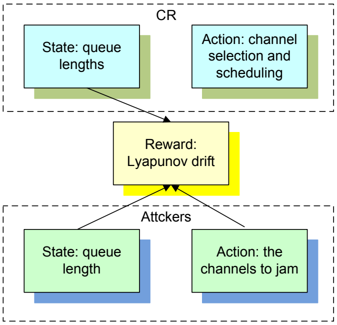

Fig. 1. Elements of the game

When secondary user n decides to transmit to the next hop neighbor j and an available channel, say m, is found, the packet can be delivered successfully with probability μ_{njm} which is determined by the channel quality.

3.3 PUE Attack Model

We assume that there are totally L PUE attackers distributed around the cognitive radio network. Each attacker chooses Q ($Q \leq M$) channels to attack. During each spectrum sensing period, each PUE sends interference in the Q channels such that the secondary users sensing these channels are scared away even if the channel is actually not being used by primary users. We denote by $\mathcal{V}_l$ the set of potential secondary user victims that could be jammed by attacker l. We assume that the attackers have certain knowledge about the current state of the cognitive radio network.

4 Centralized Game

In this section, we consider the centralized case, in which the actions of the attackers and secondary users are both fully coordinated. Hence, we can assume that there are two centers making the decisions for the attackers and secondary users, respectively, such that there are two players in the game.

4.1 Elements of Game

We define the following elements of the game. Obviously, this game is a stochastic one having the elements of reward, action and state.

- State: The system state, denoted by $\mathbf{s}$, includes the queue lengths of all flows and all secondary users which are denoted by $\{q_{fn}\}_{f=1,\ldots,F,n=1,\ldots,N}$. The state space is then denoted by $\mathcal{S}$ which consists of all possible $\mathbf{s}$. We assume that the system state is visible to both attackers and secondary users. Note that, since we assume that the primary users' activities are independent in time, the spectrum situation is memoryless. It is easy to extend to the case in which the spectrum has memory by incorporating the spectrum state into the system state.
- Actions: We denote by $\mathcal{A}_a$ and $\mathcal{A}_s$ the sets of actions of the attackers and secondary users, respectively. The actions of the attackers, denoted by $\mathbf{a}_a$, include the channels to jam, which are denoted by $\{\mathbf{c}_l^a\}_{l=1,\ldots,L}$ ($\mathbf{c}_l$ is a vector containing the Q channels to jam). The action of the secondary users, denoted by $\mathbf{a}_s$, includes the assignment of the channels, as well as the scheduled flow. We denote by $c_n(t)$ and $f_n(t)$ the assigned channel and scheduled flow at secondary user n at time slot t. To avoid co-channel interference, we have $c_n(t) \neq c_m(t)$ if $m \in \mathcal{C}_n$.

- Reward: The purpose of the attacker is to make the cognitive radio collapse, or equivalently destabilizing the queuing system, while the purpose of the secondary users is to stabilize the system. Hence, a quantity is needed to quantify the stability of the system. We define the following Lyapunov function, which is given by

$$V(\mathbf{s}(t)) = \sum_{f=1}^{F} \sum_{n=1}^{N} q_{fn}^2(t), \tag{1}$$

namely the square sum of all queue lengths. The larger the Lyapunov function is, the more unstable the system is since there are more packets staying in the network. Since $V(\mathbf{s}(t))$ can be rewritten as

$$V(\mathbf{s}(t)) = V(\mathbf{s}(0)) + \sum_{r=1}^{t} V(\mathbf{s}(r)) - V(\mathbf{s}(r-1)), \tag{2}$$

we define $d(t) = E\left[V(\mathbf{s}(t)) - V(\mathbf{s}(t-1)\right]$, namely the expected Lyapunov drift [15], as the reward of the attacker. When the Lyapunov drift is positive, the system becomes more unstable, thus benefiting the attackers. To define the reward of the secondary user system, we model the game as a zero-sum one and define $-d(t)$ as the reward of cognitive radio network. For simplicity, we add a discounting factor $0 < \beta < 1$ to the reward in each time slot such that the total reward of the attacker is given by

$$R = \sum_{t=0}^{\infty} \beta^t d(t), \tag{3}$$

which simplifies the analysis since it is much easier to analysis the game with a discounted sum of rewards. Note that this definition is motivated by the classical works on scheduling queuing network in which the scheduling tries to minimize the Lyapnov drift in order to stabilize the queues [15][20].

4.2 Attack/Defense Strategies

The attack strategy, denoted by π_a, is defined as the condition probability $P(\mathbf{a}_a|\mathbf{s})$; i.e., the probability of the action given the current system state. Similarly, we can also define the defense strategy, denoted by π_s, as $P(\mathbf{a}_s|\mathbf{s})$. We will first study the Nash equilibrium given the above game configuration via the Shapley's Theorem. Then, we will use a simpler definition of reward which simplifies the analysis.

Nash Equilibrium. First, we follow the standard solution of stochastic games. For a general stochastic game (not necessary zero-sum), the Nash equilibrium is defined as the pair of strategies (π_s^*, π_a^*), which satisfies

$$R(\pi_s^*, \pi_a^*) \geq R(\pi_s^*, \pi_a), \qquad \forall \pi_a, \tag{4}$$

$$R(\pi_s^*, \pi_a^*) \leq R(\pi_s, \pi_a^*), \qquad \forall \pi_s. \tag{5}$$

At the Nash equilibrium point, both players have no motivation to change the strategies specified the equilibrium point; any unilateral deviation from the equilibrium point can only incur performance degradation of itself.

To find the Nash equilibrium, an auxiliary matrix game proposed by Shapley [19] is needed. We first define the matrix game conditioned on the system state s, which is given by

$$\mathbf{R}(\mathbf{s}) = \begin{pmatrix} d(\mathbf{s},1,1) & d(\mathbf{s},1,2) & \cdots & d(\mathbf{s},1,|\mathcal{A}_a|) \\ d(\mathbf{s},2,1) & d(\mathbf{s},2,2) & \cdots & d(\mathbf{s},2,|\mathcal{A}_a|) \\ \vdots & \vdots & \ddots & \vdots \\ d(\mathbf{s},|\mathcal{A}_s|,1) & d(\mathbf{s},|\mathcal{A}_s|,2) & \cdots & d(\mathbf{s},|\mathcal{A}_s|,|\mathcal{A}_a|) \end{pmatrix},$$

in which $d(\mathbf{s}, a_1, a_2)$ is the expected Lyapunov drift when the system state is $\mathbf{s}$ and the actions are a_1 and a_2 for the attackers and cognitive radio network, respectively.

We define the value vector of the attacker, denoted by $\mathbf{v}_a = (v_a(1), ..., v_a(|\mathcal{S}|)$, whose elements are given by

$$\mathbf{v}_a(\mathbf{s}) = R(\mathbf{s}), \qquad s = 1, ..., |\mathcal{S}|, \tag{6}$$

where $R(\mathbf{s})$ is the reward of the attackers given the initial state $\mathbf{s}$. Then, an auxiliary matrix game is defined with the following payoff matrices

$$\tilde{\mathbf{R}}(\mathbf{s}, \mathbf{v}_a) = \mathbf{R}(\mathbf{s}) + \beta \mathbf{T}(\mathbf{s}, \mathbf{v}_a), \qquad \mathbf{s} \in \mathcal{S}, \tag{7}$$

where the elements in the matrix $\mathbf{T}(\mathbf{s}, \mathbf{v}_a)$ are defined as

$$\mathbf{T}(\mathbf{s}, \mathbf{v}_a)_{ij} = \sum_{\mathbf{s}'} p(\mathbf{s}'|\mathbf{s}, i, j) v_a(\mathbf{s}'). \tag{8}$$

Similarly, we can also define the value vector for the cognitive radio network, which is denoted by $\mathbf{v}_c$.

The following theorem (Shapley, 1953, [19]) discloses the condition of the Nash equilibrium of the zero-sum stochastic game:

Theorem 1. *The value vector at the Nash equilibrium satisfies the following equations:*

$$v_a(s) = val\left[\mathbf{R}(s, \mathbf{v}_a)\right], \qquad s \in \mathcal{S}, \tag{9}$$

where the matrix game $\mathbf{R}(s, \mathbf{v}_a)$ *is in (7).*

Once the value vector $\mathbf{v}_a$ is obtained, the optimal action of the attackers is given by

$$\mathbf{a}_a(\mathbf{s}) = \arg\max_j \min_i \left(\tilde{\mathbf{R}}(\mathbf{s}, \mathbf{v}_a)\right)_{ij}, \tag{10}$$

while the optimal action of the cognitive radio is given by

$$\mathbf{a}_c(\mathbf{s}) = \arg\min_i \max_j \left(\tilde{\mathbf{R}}(\mathbf{s}, \mathbf{v}_a)\right)_{ij}. \tag{11}$$

Myopic Game for Back Pressure. Although the Nash equilibrium exists for the stochastic game formulation in the previous subsection, it is very difficult to obtain analytic expression for the equilibrium. We can only obtain the numerical solution for small systems. Moreover, it is still not clear whether defining the Lyapunov drift as the reward of each time slot is the optimal choice. In this subsection, we will study the myopic case in which the attackers and cognitive radio take myopic strategies by maximizing their rewards in each time slot, without considering the future evolution. Moreover, we will approximate the maximization of Lyapunov drift by maximizing the back pressure, which can simplify the stochastic game to a one-stage normal game.

It is well known that, when there is no attacker, the back pressure of flow f at secondary user n is given by [20]

$$D_{fn} = \begin{cases} (q_{fn} - q_{fj})\,\mu_{njm}, j \notin \mathsf{D}_f \\ q_{fn}\mu_{njm}, j \in \mathsf{D} \end{cases}, \tag{12}$$

where j is the next secondary user along flow f and m is the channel for the transmission from n to j (recall that $i \in \mathsf{D}_f$ means that node i is a destination node for flow f). [20] has shown that the scheduling algorithm minimizing the back pressure, which is tightly related to minimizing the Lyapunov drift, can stabilize the queuing system.

However, when attacks exist, the back pressure is dependent on the attackers' strategy since the channels selected by the attackers will change the transmission success probability μ_{njm}. Recall that the actions of attackers and cognitive radio network are denoted by $\mathbf{a}_a$ and $\mathbf{a}_c$, respectively. Then, the success probability, as a function of the actions, is given by (recall that $\mathcal{V}_l$ is the set of secondary user that attacker l can attack)

$$\tilde{\mu}_{njm}(\mathbf{a}_a, \mathbf{a}_c) = \mu_{njm} I(m \notin \mathbf{c}_l^a, \forall n \in \mathcal{V}_l), \tag{13}$$

where I is the characteristic function of the event that no attacker that can interfere secondary user n is attacking channel m. Then, the back pressure in the game is defined as a function of the actions $\mathbf{a}_a$ and $\mathbf{a}_c$, which is given by

$$\tilde{D}_{fn}(\mathbf{a}_a, \mathbf{a}_c) = \begin{cases} (q_{fn} - q_{fj})\,\tilde{\mu}_{njm}(\mathbf{a}_a, \mathbf{a}_c), j \notin \mathsf{D}_f \\ q_{fn}\tilde{\mu}_{njm}(\mathbf{a}_a, \mathbf{a}_c), j \in \mathsf{D}_f \end{cases}. \tag{14}$$

Then, the reward of the attacker is given by (recall that f_n is the flow scheduled at secondary user n)

$$R(\mathbf{a}_a, \mathbf{a}_c) = -\sum_{n=1}^{N} \tilde{D}_{f_n,n}(\mathbf{a}_a, \mathbf{a}_c), \tag{15}$$

and the reward of the cognitive radio network is $\sum_{n=1}^{N} \tilde{D}_{f_n,n}$ since the game is modeled as a zero-sum one. Then, the strategy of the attackers at the Nash equilibrium is given by

$$\pi_a^* = \arg\max_{\pi_a} \min_{\pi_c} R(\pi_a, \pi_c), \tag{16}$$

and the corresponding action of the cognitive radio is given by

$$\pi_c^* = \arg\min_{\pi_c}\max_{\pi_a} R(\pi_a, \pi_c). \tag{17}$$

The actions at the Nash equilibrium point can be computed using linear programming. The challenge is the large number of actions when the network size or the number of channels is large. We will find the analytic expression for an example in the sequel. For large system size, we can only use approximations for exploring the Nash equilibrium.

4.3 Example

In this subsection, we use one example to illustrate the previous discussions, which also provides insights for networks with larger size. The example is illustrated in Fig. 2, in which there is one attacker and three secondary users. We assume that there are totally two channels over which two data flows are sent from secondary user 3 to secondary users 1 and 2, respectively. The attacker can only interfere secondary user 3. For simplicity, we assume that secondary user 3 can sense and transmit over both channels simultaneously; hence, there are only two possible actions for secondary user 3.

Stochastic Game for Lyapunov Drift. Due to its small size, the Nash equilibrium of the example can be obtained by solving equations. However, we are still unable to obtain the explicit expression. Below, we consider a more simplified case in which $\mu_{311} \gg \mu_{312}$ and $\mu_{322} \gg \mu_{321}$; i.e., secondary user 3 should use channel 1 to transmit data flow 1 and use channel 2 to transmit data flow 2. In this case, the strategy of the cognitive radio network is fixed; hence, the problem is converted from a game theoretic one to a single sided decision one. Then, the attacker needs to decide whether to jam data flow 1 (thus sending signal over channel 1) or jam data flow 2 (thus sending signal over channel 2). The following proposition provides the optimal strategy for the attacker.

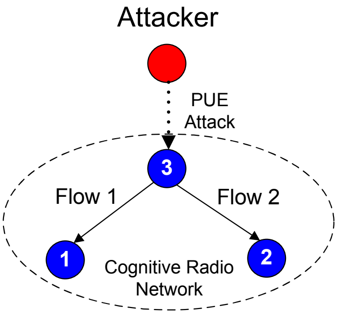

Fig. 2. An illustration of the example

Proposition 1. *Consider the above simplified case. We assume that the transmission success probability is μ and the new packet arrival rate is λ, both identical for the two data flows. The optimal strategy of the attacker to maximize the Lyapunov function is to choose the channel to jam the data flow having a larger queue length.*

One Stage Game for Back Pressure. Now we consider the one stage game for maximizing or minimizing the back pressure. Fix a certain time slot and drop the index of time for simplicity. It is easy to verify that the reward for the cognitive radio can be represented by a matrix, which is given by

$$\begin{pmatrix} q_{32}\mu_{322} & q_{31}\mu_{312} \\ q_{31}\mu_{311} & q_{32}\mu_{321} \end{pmatrix}. \tag{18}$$

The Nash equilibrium of this matrix game is provided in the following proposition. The proof is a straightforward application of the conclusion in [5]; hence, we omit the proof due to the limited space.

Proposition 2. *We denote by π_j^a the probability that the attacker attacks channel j, $j = 1, 2$, and by π_k^c the probability that secondary user 3 transmits data flow 1 over channel k while transmitting data flow 2 over the other channel, $k = 1, 2$. The Nash equilibrium of the matrix game in (18) is given by the following cases:*

- *If the following inequality holds; i.e.,*

$$\begin{cases} (q_{32}\mu_{322} - q_{31}\mu_{312})(q_{32}\mu_{321} - q_{31}\mu_{311}) > 0 \\ (q_{32}\mu_{322} - q_{31}\mu_{311})(q_{32}\mu_{321} - q_{31}\mu_{312}) > 0 \end{cases}, \tag{19}$$

  the equilibrium strategies are given by

$$\begin{cases} \pi_1^a = \frac{q_{32}\mu_{321} - q_{31}\mu_{311}}{q_{32}\mu_{322} - q_{31}\mu_{312} + q_{32}\mu_{321} - q_{31}\mu_{311}} \\ \pi_1^c = \frac{q_{32}\mu_{321} - q_{31}\mu_{312}}{q_{32}\mu_{322} - q_{31}\mu_{311} + q_{32}\mu_{321} - q_{31}\mu_{312}} \end{cases}. \tag{20}$$

- *If the first equality in (19) does not hold, then we have the following possibilities:*
  - $q_{32}\mu_{322} \geq q_{31}\mu_{312}$ *and* $q_{32}\mu_{321} < q_{31}\mu_{311}$*, or* $q_{32}\mu_{322} > q_{31}\mu_{312}$ *and* $q_{32}\mu_{321} \leq q_{31}\mu_{311}$*: secondary user 3 should always transmit data flow 1 over channel 1; the attacker should attack channel 1 if* $q_{31}\mu_{311} > q_{32}\mu_{322}$ *and attack channel 2 otherwise.*
  - $q_{32}\mu_{322} < q_{31}\mu_{312}$ *and* $q_{32}\mu_{321} \geq q_{31}\mu_{311}$*, or* $q_{32}\mu_{322} \leq q_{31}\mu_{312}$ *and* $q_{32}\mu_{321} > q_{31}\mu_{311}$*: secondary user 3 should always transmit data flow 1 over channel 2; the attacker should attack channel 1 if* $q_{32}\mu_{321} > q_{31}\mu_{312}$ *and attack channel 2 otherwise.*
  - $q_{32}\mu_{322} = q_{31}\mu_{312}$ *and* $q_{32}\mu_{321} = q_{31}\mu_{311}$*: secondary user 3 can choose either action; the attacker should attack channel 1 if* $q_{32}\mu_{321} > q_{31}\mu_{312}$ *and attack channel 2 otherwise.*
- *If the second equality in (19) does not hold, then we have the following possibilities:*
  - $q_{32}\mu_{322} \leq q_{31}\mu_{311}$ *and* $q_{31}\mu_{312} < q_{32}\mu_{321}$*, or* $q_{32}\mu_{322} < q_{31}\mu_{311}$ *and* $q_{31}\mu_{312} \leq q_{32}\mu_{321}$*: the attacker should always attack channel 1; secondary user 3 should transmit data flow 1 over channel 1, if* $q_{32}\mu_{322} > q_{31}\mu_{312}$*, and transmit over channel 2 otherwise.*
  - $q_{32}\mu_{322} \geq q_{31}\mu_{311}$ *and* $q_{31}\mu_{312} > q_{32}\mu_{321}$*, or* $q_{32}\mu_{322} > q_{31}\mu_{311}$ *and* $q_{31}\mu_{312} \geq q_{32}\mu_{321}$*: the attacker should always attack channel 2; secondary user 3 should transmit data flow 1 over channel 1, if* $q_{31}\mu_{311} > q_{32}\mu_{321}$*, and transmit over channel 2 otherwise..*

- $q_{32}\mu_{322} = q_{31}\mu_{311}$ *and* $q_{32}\mu_{321} = q_{31}\mu_{312}$*: the attacker can attack any channel; secondary user 3 should transmit flow 3 over channel 1 if* $q_{32}\mu_{322} > q_{31}\mu_{312}$ *and attack channel 2 otherwise..*

Remark 1. We can draw the following conclusions from the Nash equilibrium:

- When all channels have the same quality, the attacker should attack each channel with probability 0.5, which is independent of the queue lengths.
- Suppose $\mu_{311} = \mu_{322} \gg \mu_{312} = \mu_{321}$; i.e., it is much desirable to transmit data flow 1 over channel 1 and data flow 2 over channel 2, the attacker should attack the channel more desirable for the data flow with more queue length. In this situation, the queue length information is useful.

4.4 Stability Analysis

Now we analyze the stability of the queuing dynamics. We first provide a brief introduction to the queuing stability when there is no attacker. Then, we consider the case when attacker exists.

Stability Without Attacker. When there is no attacker, the stability of queuing networks has been analyzed for single channel case in [20], which is easy to extend to the multichannel case. We denote by a L-dimensional vector $\mathbf{f}$ the sums of data flow rates of the links; i.e., f_l stands for the total data rates through link l, $l = 1, ..., L$. We denote by $\mathcal{S}$ the set of all vectors of transmission success probabilities, each dimension corresponding to a link and each vector corresponding to one possible channel assignment. Then, if we can find a vector $\mathbf{c} \in co(\mathcal{S})$ such that $\mathbf{f} < \mathbf{c}$, then the queue is stabilizable. When $\mathbf{f} > \mathbf{c}$, the queues cannot be stabilized. The proofs follow those of Lemma 3.2 and Lemma 3.3 in [20].

Stability Subject to Attacker. When attacker(s) exists, the capacity vector $\mathbf{c}$ is changed since the transmission success probability is decreased due to the PUE attack. Since the attack actions are dynamical, depending on the queue situations, each vector in $\mathcal{S}$ also becomes dynamical. Hence, it is difficult to analyze the stability analytically. Here we just provide a qualitative observation. For a certain link l, if the total flow rate f_l is close to the capacity c_l, then it is more possible that there is a long queue at the transmitter. As we have seen in the example, the attacker tends to attack secondary users with longer queues by jamming the channels more possibly available to the secondary user, given that the channel conditions are similar. Then, c_l is further decreased, thus making the attacker more focused on link l.

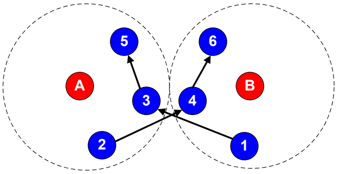

Fig. 3. An illustration of the decentralized game

For the simple example in Fig. 2, when the attacker and the network carry out the one-stage game, we have the following corollary of Prop. 1:

Corollary 1. *A necessary condition for $q_1 \to \infty$ and q_2 being finite is*

$$\left(\frac{\mu_{312}}{\mu_{311}+\mu_{312}}\right)^2 \mu_{311} + \left(\frac{\mu_{311}}{\mu_{311}+\mu_{312}}\right)^2 \mu_{312} < f_1, \tag{21}$$

and

$$\frac{\mu_{312}\mu_{311}\left(\mu_{321}+\mu_{322}\right)}{\left(\mu_{311}+\mu_{312}\right)^2} > f_2. \tag{22}$$

Proof. The proof is simple. We notice

$$c_1 = \left(1-\pi_1^a\right)\pi_1^c\mu_{311} + \pi_1^a\left(1-\pi_1^c\right)\mu_{312}, \tag{23}$$

and

$$c_2 = \pi_1^a\pi_1^c\mu_{321} + \left(1-\pi_1^a\right)\left(1-\pi_1^c\right)\mu_{322}. \tag{24}$$

Then, we simply substitute the conclusion in Prop. 1 into the above expressions of c_1 and c_2.

5 Decentralized Game

As we have discussed in the previous section, the centralized game is difficult to analyze due to the large action space and state space; moreover, the centralized controls of the attackers and cognitive radio network are impractical in applications. Hence, we study the decentralized game for both attackers and cognitive radio network. An illustration is given in Fig. 3, in which we consider two attackers, namely A and B, and six secondary users, namely 1, 2, 3, 4, 5 and 6. A key feature for the decentralized game is that each attacker/secondary user is a player and each player makes decision based on the states of its neighbors/direct victims. For example, secondary user 2 makes its decision based on the state of secondary user 4, while attacker A makes its decision based on the states of secondary users 2 and 3.

Based on the big picture described above, we define the elements of the game as follows:

- System state: Due to the locality assumption, each player does not necessarily know the queue lengths of all secondary user and all flows. For attacker l, its state is $s_l^a = \{q_{fn}\}_{n\in\mathcal{V}_l, f\in\mathcal{I}_n}$, i.e., the queuing situations of all secondary users that it may attack. For secondary user n, its state is $s_l^a = \{q_{fm}\}_{n\sim m, f\in\mathcal{I}_m}$, i.e., the queuing situations of all neighboring secondary users.
- Strategy: As we have assumed, each player knows only the states of its neighbors. Hence, its action is also dependent on only the neighbors. We define the strategy of a player as the distribution of action given the states

of its neighbors and itself[1]. For each attacker, the strategy is given by $P(a|\left\{q_{fn}\right\}_{n\in\mathcal{V}_l,f\in\mathcal{I}_n})$, $a = 1,...,M$. For each secondary user n, the strategy is given by $P(a|\left\{q_{fn}\right\}_{m\sim n,f\in\mathcal{I}_m})$. The overall strategy of the cognitive radio network (attacker) is the product of the strategies of each secondary user (attacker); i.e.,

$$\begin{cases} \pi_a = \prod_{m=1}^{M} \pi_a^m \\ \pi_c = \prod_{n=1}^{N} \pi_c^n \end{cases}. \tag{25}$$

Note that the key difference between the decentralized game and the centralized one is the structure of the strategy; i.e., the decentralized game has a product space for the strategy while the centralized does not.

- Reward: Again, we consider the Laypunov drift as the reward. For secondary user n, its reward is given by

$$r_n(t) = \sum_{f\in\mathcal{I}_m} q_{fn}^2(t-1) - q_{fn}^2(t). \tag{26}$$

The total reward of the coalition of secondary users is then given by

$$\begin{aligned} R(t) &= \sum_{n=1}^{N} r_n(t) \\ &= V(t-1) - V(t), \end{aligned} \tag{27}$$

which is equal to the negative of the Laypunov drift.

The situation is slightly more complicated for the attacker coalition. Naturally, we can define the reward of attacker k as $-\sum_{n\in\mathcal{N}_k} r_n(t)$. However, if we simply add up the individual rewards of the attackers as the total reward of the attacker coalition, it may not be equal to the negative of $R(t)$, since the sets of secondary users affected by different attackers may overlap. Hence, we assume that, before launching the attack, the attacker divide the secondary users into disjoint sets and each attacker takes the rewards from only one set of secondary users, denoted by $\tilde{\mathcal{N}_k}$ for attacker k. Then, we define $-\sum_{n\in\tilde{\mathcal{N}_k}} r_n(t)$ as the reward of attacker k; thus, the total reward of the attacker coalition is equal to the negative of the reward of the secondary user coalition.

Then, the reward of the secondary user coalition is given by

$$R_s = E\left[\sum_{t=1}^{\infty} \beta^t R(t)\right], \tag{28}$$

[1] The more general strategy should include the history, namely the previous actions and previous system states, into the condition of the probability distribution of actions. It is still not clear whether the Markov assumption in the strategy loses any information. For the case of time average reward, it has been shown in [2] that, when the strategy of one coalition is fixed, the Markov strategy can achieve the optimal reward for the other coalition.

where β is the discounting factor. We can also consider the mean reward; however, it is much more complicated.

For the PUE attack game, we define the value of the game as follows [2].

Definition 1. *The value of the PUE attack game is given by*

$$\sup_{\pi_c} \inf_{\pi_a} R_c = \inf_{\pi_a} \sup_{\pi_c} R_c, \tag{29}$$

if both sides exist.

The following proposition shows the existence of the value of the decentralized stochastic game. The proof is similar to that of Theorem 4.16 in [2], where the reward is the average of rewards.

Proposition 3. *The value of the decentralized game, defined in (29) exists.*

The proof and more discussions will be made in the journal version.

6 Numerical Results

In this section, we use numerical results to demonstrate the theoretical analysis. In Fig. 4, we show the rate region subject to PUE attacks for the network in Fig. 2. The strategies are obtained by solving the equations in the Shapley's Theorem, using numerical approach [5]. Since there are infinitely many possible queue lengths, thus resulting in infinitely many system states, we merge all the cases with more than 9 packets in a queue into one state. We judge whether a given set of rates is stable by carrying out the simulation for the queuing dynamics; if one of the queues has more than 50 packets after 2000 time slots, we claim that the rates are unstable. We tested the case of Nash equilibrium, uniformly choosing the actions and no PUE attack. The region of each case is the area below the corresponding curve. We observe that the PUE attack can cause a significant reduction of the rate region.

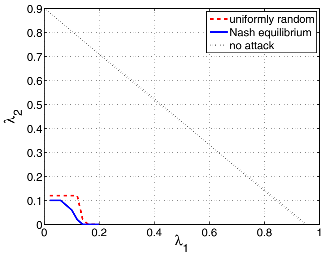

Fig. 4. Rate region subject to PUE attacks

7 Conclusions

In this paper, we have studied multiple attackers and an arbitrary cognitive radio network with multiple data flows, where the goal of the game is to stabilize (destabilize) the queuing dynamics by the secondary users (attackers). Both the centralized and decentralized cases of the game have been considered. The Lyapunov drift and the back pressure are considered as the game rewards for the stochastic game case and the myopic strategy case, respectively. The value functions and Nash equilibriums have been obtained for the general case, while the explicit expressions are obtained for simple but typical scenarios. Numerical simulations have been carried out to demonstrate the analysis.

References

1. Chen, R., Park, J.-M., Reed, J.H.: Defense against primary user emulation attacks in cognitive radio networks. IEEE J. on Select. Areas in Commun. Special Issue on Cognitive Radio Theory and Applications 26(1) (2008)
2. Chornei, R.K., Daduna, H., Knopov, P.S.: Control of Spatially Structured Random Processes and Random Fields with Applications. Springer (2006)
3. Daskalakis, C., Papadimitriou, C.: Computing pure Nash equilibria in graphical games via Markov random fields. In: Proc. of the 7th ACM Conferene on Electrionic Commerce (2006)
4. Elkind, E., Goldberg, L., Goldberg, P.: Graphical games on tree revisited. In: Proc. of the 7th ACM Conferene on Electrionic Commerce (2006)
5. Filar, J., Vrieze, K.: Competitive Markov Decision Processes. Springer (1997)
6. Han, Z., Pandana, C., Liu, K.J.R.: Distributive opportunistic spectrum access for cognitive radio using correlated equilibrium and no-regret learning. In: Proc. of IEEE Wireless Communications and Networking Conference, WCNC (2007)
7. Jin, Z., Anand, S., Subbalakshmi, K.P.: Detecting primary user emulation attacks in dynamic spectrum access networks. In: Proc. of IEEE International Conference on Communications, ICC (2009)
8. Kakade, S., Kearns, M., Langford, J., Ortiz, L.: Correlated equilibria in graphical games. In: Proc. of the 4th ACM Conference on Electronic Commerce, EC (2003)
9. Kakade, S.M., Kearns, M., Ortiz, L.E.: Graphical Economics. In: Shawe-Taylor, J., Singer, Y. (eds.) COLT 2004. LNCS (LNAI), vol. 3120, pp. 17–32. Springer, Heidelberg (2004)
10. Korilis, Y.A., Lazar, A.A.: On the existence of equlibria in noncooperative optimal flow control. Journal of the ACM 42, 584–613 (1995)
11. Li, H., Han, Z.: Dogfight in spectrum: Jamming and anti-jamming in cognitive radio systems. In: Proc. of IEEE Conference on Global Communications, Globecom (2009)
12. Li, H., Han, Z.: Blind dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems with unknown channel statistics. In: Proc. of IEEE International Conference on Communications, ICC (2010)
13. Li, H., Han, Z.: Competitive spectrum access in cognitive radio networks: Graphical game and learning. In: Proc. of IEEE Wireless Communication and Networking Conference, WCNC (2010)
14. Mitola, J.: Cognitive radio for flexible mobile multimedia communications. In: Proc. IEEE Int. Workshop Mobile Multimedia Communications, pp. 3–10 (1999)
15. Neely, M.J.: Stochastic Network Optimization with Application to Communication and Queuing Systems. Morgan&Claypool Press (2010)
16. Nisan, N., Roughgarden, T., Tardos, E., Vazirani, V.V. (eds.): Algorithmic Game Theory. Cambridge University Press (2007)
17. Qin, T., Yu, H., Leung, C., Sheng, Z., Miao, C.: Towards a trust aware cognitive radio architecture. ACM SIGMOBILE Newsletter 13 (April 2009)

18. Sampath, A., Dai, H., Zheng, H., Zhao, B.Y.: Multi-channel jamming attacks using cognitive radios. In: Proc. of IEEE Conference on Computer Communications and Networks, ICCCN (2007)
19. Shapley, L.S.: Stochastic games. In: Proceedings Nat. Acad. of Science USA, pp. 1095–1100 (1953)
20. Tassiulas, L., Ephremides, A.: Stability properties of constrained queuing systems and scheduling for maximum throughput in multihop radio networks. IEEE Trans. Automat. Control 37, 1936–1949 (1992)
21. Thomas, R.W., Komali, R.S., Borghetti, B.J., Mahonen, P.: A Bayesian game analysis of emulation attacks in dynamic spectrum access networks. In: Proc. of IEEE International Symposium of New Frontiers in Dynamic Spectrum Access Networks, DySPAN (2008)
22. Urgaonkar, R., Neely, M.J.: Opportunistic scheduling with reliability guarantees in cognitive radio networks. IEEE Trans. Mobile Computing 8, 766–777 (2009)
23. Wang, W., Li, H., Sun, Y., Han, Z.: Attack-proof collaborative spectrum sensing in cognitive radio networks. In: Proc. of Conference on Information Sciences and Systems, CISS (2009)
24. Wang, W., Li, H., Sun, Y., Han, Z.: CatchIt: Detect malicious nodes in collaborative spectrum sensing. In: Proc. of IEEE Conference on Global Communications, Globecom (2009)
25. Wu, X., Srikant, R.: Regulated maximal matching: A distributed scheduling algorithm for multihop wireless networks with node-exclusive spectrum sharing. In: Proc. of 44th IEEE Conference on Decision and Control (2005)
26. Yao, D.: S-modular games, with queuing applications. Queuing Systems and Their Applications 21, 449–475 (1995)
27. Ying, L., Srikant, R., Eryilmaz, A., Dullerud, G.E.: Distributed fair resource allocation in cellular networks in the presence of heterogeneous delays. In: Proc. of IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, WIOPT (April 2005)