This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE DySPAN 2010 proceedings

A Bayesian Game Analysis of Emulation Attacks in Dynamic Spectrum Access Networks

Ryan W. Thomas*, Ramakant S. Komali, Brett J. Borghetti, and Petri Mähönen

***Abstract*—Dynamic spectrum access has proposed tiering radios into two groups: Primary Users (PUs) and Secondary Users (SUs). PUs are assumed to have reserved spectrum available to them, while SUs (operating in overlay mode) must share whatever spectrum is available. The threat of *Emulation Attacks*, in which users pretend to be of a type they are not (either PU or SU) in order to gain unauthorized access to spectrum, has the potential to severely degrade the expected performance of the system. We analyze this problem within a Bayesian game framework, in which users are unsure of the legitimacy of the claimed type of other users. We show that depending on radios' beliefs about the fraction of PUs in the system, a policy maker can control the occurrence of emulation attacks by adjusting the gains and costs associated with performing or checking for emulation attacks.**

I. Introduction

Dynamic Spectrum Access (DSA) is an exciting new concept that promises to bring flexibility to spectrum management. Instead of relying on traditional spectrum licenses, in which licensees have exclusive rights to a fixed, static amount of spectrum, DSA schemes allow unused spectrum to be used opportunistically by other users. These opportunistic users are called Secondary Users (SUs), and must only use spectrum not in use by Primary Users (PUs), radios that have priority licenses for the spectrum. To operate in either a PU or SU role will require either a license or operating approval from a regulator such as the Federal Communications Commission (FCC). Radios holding a PU license have access to a reserved frequency band. Radios holding an overlay SU license have the ability to scavenge spectrum from whatever spectrum is sensed to be unused.

There may be times when radios do not want to use spectrum according to their license. Instead, the radio may pretend to hold a different license. The idea of such an Emulation Attack (EA) was first articulated by Chen in [1]. That work identified a specific kind of EA called the Primary User Emulation Attack (PUEA), in which a radio emulates a PU for either selfish or malicious reasons. When driven by selfishness, the radio emulates to maximize their spectrum usage; when driven by maliciousness, the radio emulates to degrade the DSA opportunities of the other spectrum users. Like any kind of illegal activity, deterring either kind of EA requires a combination of detection and punishment.

R. Thomas and B. Borghetti are with the Dept. of Electrical and Computer Engineering, The Air Force Inst. of Technology; R. Komali and P. Mähönen are with the Dept. of Wireless Networks, RWTH Aachen University, Germany. This research is funded in part by the Air Force Research Lab and by the Air Force Office of Scientific Research. This work also supported in part by European Union (ARAGORN project) and DFG through UMIC-research center facility. The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. This document has been approved for public release; distribution unlimited.

*Correspondence: R. Thomas, AFIT/ENG, 2950 Hobson Way, Wright-Patterson AFB, OH 45433. Phone: 937-255-3636 x4613, FAX: 937-656-7061, email: ryan.thomas@afit.edu

In this vein, the core contribution of this work is to investigate system-wide behaviors when the detection of selfish EAs leads to punishment. By proposing a Bayesian game framework where radios are unsure of the legitimacy of the claimed license of other radios, we identify conditions under which a Nash Equilibrium (NE) can exist. These conditions give insight into questions such as whether policy-abiding radios can coexist with selfish radios, with what probability selfish radios choose to launch EAs, and under what conditions selfish EAs are discouraged. The NE also reveal the probability of radios challenging the license of other radios to determine their legitimacy. These results can be used to determine appropriate policies to keep the rate of EA arbitrarily low, something of significant interest to regulatory agencies. Conversely, this information can be used by PU and SU licensees to determine how rampant EAs will be for their license type.

The remainder of the paper is organized as follows. Section II examines other work that uses Bayesian game theory to investigate the behavior of networks and malicious agents. Section III overviews Bayesian game theory. Section IV provides the DSA framework and a Bayesian game model for it. Section V and Section VI present a detailed equilibrium analysis of the interactions between SUs in the context of one-way and two-way EA games, respectively. Section VII provides concluding remarks and possible extensions of this work.

II. Related Work

Most work in emulation attacks has been focused on the detection aspect, primarily for the PUEA. Chen [1] suggests a location based authentication scheme called *LocDef*, in which the location (calculated from the Received Signal Strength (RSS) by a network of sensors) and waveform characteristics of a declared PU are compared against the known location and waveform characteristics for that transmitter. Particularly when the PUs consist of static, well-characterized users such as television broadcasters, this can be an effective scheme. A clustering approach is described in [2], in which waveform features are used to categorize a signal as being from a PU. More generally, in [3] and [4], various statistical tests are developed to determine whether it is likely that the measured RSS of the declared PU could have come from the actual PU. Unlike these works, which are primarily about detecting

978-1-4244-5188-3/10/$26.00 ©2010 IEEE

EAs, we focus on how to cope with these attacks once they are detected, and provide conditions for formulating an appropriate response mechanism system.

The idea of using game theory to investigate wireless engineering problems is well-accepted [5]. The works of [6], [7], [8] are most closely related to our work, and were among the few to use Bayesian games to investigate network behaviors under the threat of malicious users. In [6], an attacker/defender model is used for intrusion detection and a Bayesian game detection mechanism is proposed to make the monitoring process more energy efficient. This work complements our work which assumes that a detection and punishment mechanism is already in place, and then examines the impact of detection/punishment costs on network behavior, taking into account the benefit from acting maliciously. In [7], the synergy between malicious behavior and radio mobility is examined in the context of mobile ad-hoc networks. This work also examines effective strategies to negate advantages that malicious users have.

More recently, Bayesian games have been used to investigate malicious packet forwarding [8]. In this work, there are two types of radios: malicious radios, which can choose to forward packets or not, and regular radios that always forward packets. The sending radio has a belief about the distribution of these two types of radios in the system, but does not know initially what kind of radio it is sending to. The determination of the rate of misbehavior by malicious nodes is similar to the analysis done in this paper. However, the incentives for performing an attack in [8] are different than those for the EA; the model assumes that only the malicious radio has a choice of actions (to forward or not); and the authors only analyze the case in which a non-malicious radio meets a radio of unknown type. All three of these shortcomings will be addressed in this work.

III. Bayesian Games with Incomplete Information

Bayesian games, or games with incomplete information, are modeled as having players with different *types*. Knowledge of these types may or may not be extended to all players, meaning that some players may not know other player's types. In these games, random chance (called *nature*) selects types before the game is played according to some probability distribution (this uncertainty is known as incomplete knowledge). Strategy decisions in a Bayesian game are made based on a combination of players' type, their belief in the distribution of types from nature, the actions available to them and the payoffs under these combinations.

A Bayesian game contains several components with the following notations. A player set $\mathcal{N} = \{1, 2, \ldots, n\}$ consists of all players in the game. We use the identifier i to represent a particular player, and the identifier $-i$ to represent all players except for i. There is a set of types Θ_i for each player i, where a type represents a particular player's characteristics. For instance, in a fighting game, players might be of two types: $\Theta_i = \{strong, weak\}$. We use the notation $\theta_i \in \Theta_i$ to represent a particular player's actual type and $\Theta = \times_{i \in \mathcal{N}} \Theta_i$; the type profile of all players playing the game is denoted by $\theta \in \Theta$. Each player has an action set available to them $A_i = \{a_1, a_2, \ldots\}$, and a strategy set that is a mapping of their type to their actions, $S_i : \Theta_i \to A_i$. We use S to represent the space of strategy profiles (one action for each player), in other words $S = \times_{i \in \mathcal{N}} S_i$. Each player has a utility function $u_i : S \times \Theta \to \mathbb{R}$ that maps all players' chosen strategies and types to a real value, representing the preference of that particular combination (higher values are considered more desirable). Finally, each player has a distribution function $\rho_i : \Theta \to (0, 1)$ that represents their *beliefs* about nature's distribution of types. In a Bayesian game, it is assumed that S_i, $u_i(\cdot)$, Θ_i and ρ_i are "common knowledge," meaning that all players know them, know that all players know them, and so on. Any private information is a part of a player's particular type.

Mixed strategies are probability distributions over all possible pure strategies $s_i \in S_i$. The set of all possible mixed strategies for player i is Σ_i, and we denote $\sigma_i(\theta_i) \in \Sigma_i$ to be a mixed strategy that player i chooses when its type is θ_i. Pure strategies are a degenerate case of mixed strategies, where particular strategies are chosen with a probability of 1.

One of the more useful game theoretic-concepts is the NE, which describes a state from which no rational player has any motivation to unilaterally change their chosen mixed or pure strategies (doing so would result in a equal or lower utility, thus giving the player no incentive to change). The Bayesian Nash Equilibrium (BNE) is an extension of the NE definition that incorporates the players' types and beliefs. In the mixed strategy space, the BNE is defined as the strategy profile $\hat{\sigma} = (\hat{\sigma}_1, \hat{\sigma}_2, \ldots, \hat{\sigma}_n)$ such that $\forall i \in \mathcal{N}$:

$$\hat{\sigma}_i(\theta_i) = \arg\max_{\sigma_i' \in \Sigma_i} \sum_{\theta_{-i}} \rho_i \left(\theta_{-i} | \theta_i\right) u_i \left(\sigma_i', \hat{\sigma}_{-i}, (\theta_i, \theta_{-i})\right) \quad (1)$$

In our analysis, we use the technique of iterated dominance which is one way of determining pure strategy BNE. Here, strategies which are dominated are iteratively deleted from the strategy set. The strategy set S_i^∞ includes strategies that survive this deletion process, where $S_i^\infty = \bigcap_{n=0}^{\infty} S_i^n$ and $S_i^0 = S_i$. If S_i^∞ is a singleton set for every player, then $\hat{s} = (s_1^\infty, s_2^\infty, \ldots, s_n^\infty)$ is a unique pure-strategy BNE. For further discussion of these and other concepts in Bayesian games (or for that matter, other topics in game theory), see [9].

IV. System Model

We assume that a network consists of multiple radios attempting to access (via PU and SU licenses) a shared block of spectrum. We assume that SU licenses are exclusive of PU licenses, meaning that radios can have one license or the other, but not both. Furthermore, we assume that interlopers (radios without a license) that use the spectrum frequently will be shut down or forced to get approval, making their presence uncommon. Therefore, this analysis ignores unlicensed radios and dual-licensed radios. We anticipate future work investigating the effect these users have on the system.

Without loss of generality, we suppose that all radios are within transmission range of one another and suffer from interference under the sub-bands that are in use by other radios. (Non-interfering radios can be disregarded in our spectrum sharing model because they do not influence each other's performance and therefore can coexist.) In this manner, the spectrum can be considered to be a common resource that all active radios are attempting to utilize some portion of. Figure 1 illustrates the interaction between the two radios of interest given other radios in the system.

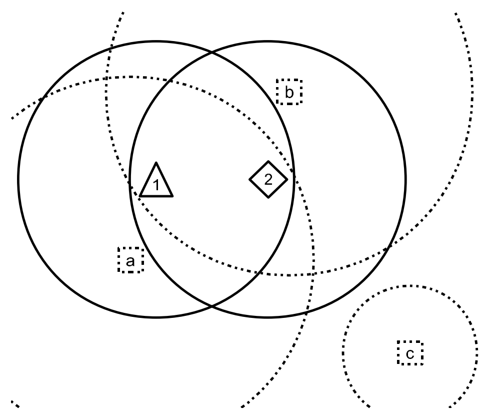

Fig. 1. Illustration of system model: Radio 1 and Radio 2 are the radios of interest. Circles represent regions of interference; radios a and b affect the available spectrum that Radios 1 and 2 observe; Radio c does not interfere and therefore is not considered.

The bandwidth that is available for a legitimate PU is considered to be a fixed and reserved quantity (of course, this assumption only holds when the bandwidth is legitimately used; when a radio performs an EA then more than one PU may be in a PU frequency band). In contrast, the bandwidth for SUs is dependent on the *available spectrum* (we use this term to describe all spectrum in a block not in use by a PU[1]) and the number of SUs sharing it. This forms a DSA system in which PUs have negotiated with the regulatory body a license that allows priority, interference-free access to a fixed subset of the spectrum block. Conversely, a SU license allows a radio to scavenge some amount of bandwidth from the spectrum that is unused by the PUs. Bandwidth for SUs is distributed among all SU radios as a function of the available free bandwidth and number of SUs. Although the process of negotiating spectrum allocation among SUs is beyond the scope of this work, we assume that all SUs receive an equal benefit from the process.

Although DSA proposes to relax the rules for how spectrum is accessed, it does not propose to eliminate regulation altogether. It is expected that radios will utilize the spectrum block in accordance with the license they hold. In support of this, we assume that there is some mechanism in place that allows the verification of a radio's PU or SU license. As discussed in Section I, several mechanism have been suggested in the literature for this, including location services, waveform identification (using either passive or active techniques) and certificates. In this work, we do not concern ourselves with the actual approach used, only assuming that there is one and it has some non-zero cost to perform (in terms of such resources as processing time, power consumption, and communication overhead).

Selfish radios (radios with the potential to perform a selfish EA) can either **emulate**, utilizing the spectrum in a manner of a license they do not hold, or use the spectrum **legitimately** and not perform an EA. Both types of licensees, PU and SU, if they are not policy-abiding, may choose to perform an EA. The idea of a Secondary User Emulation Attack (SUEA) is less discussed than the PUEA, but may occur when the available spectrum for SU use is more desirable than the spectrum reserved for PUs use (and SU and PU licenses are exclusive of one another). Other radios in the system can choose to either check the credentials of this radio (which we term **challenge**, since the selfish radio may or may not actually be emulating) and suffer the verification cost discussed above. Alternatively, these other radios can **accept** the stated role of the radio and allow the selfish radio to continue operating as it pleases.

Our model assumes the existence of a regulatory body (such as the FCC) with the authority to punish violators of policy. When a violation is detected (if a selfish radio's EA is challenged by another radio) the regulatory body has the capability to employ a punishment to the violator. The punishment cost can come in several possible forms, including financial penalties, bandwidth restrictions, time-outs or the forfeiture of other radio resources by the violator. For simplicity, we assume that punishments are fixed, meaning penalties do not change under repeated good or bad behavior. Furthermore, once punishments have been paid, violators are allowed to resume operations in the spectrum (under the terms of their correct license).

Finally, we assume that there are enough radios in the system that a radio knowing its own license type (SU or PU) will not have an effect on its belief of the distribution of the license types in the network. Furthermore, decisions to emulate and challenge are made simultaneously, preventing the decision of one radio from sequentially effecting the decision of the other.

The utility function for the radios is of the form

$$u_i(s,\theta) = r_i(s,\theta) - c_i(s,\theta)$$

where $r_i(s,\theta)$ is the *revenue* that a radio of type θ_i playing against other types θ_{-i} gets under a particular strategy profile s, and $c_i(s,\theta)$ is the *cost* assessed under that action (leaving the total utility as the *profit*). While the specific revenue values vary depending on the particular spectral scenario the radios are operating under, there are four types of revenue that are of interest. The first, r_p, is the revenue that a PU receives when it uses its reserved spectrum. Similarly, r_s is the benefit a SU receives when it shares available spectrum (spectrum that is not occupied by a PU) with some fixed number of other SUs. These two benefits are illustrated in Figure 2(a) and 2(b). When a radio has to share the available spectrum with one more radio than in the r_s case, it gets benefit r_s^*. This is illustrated in Figure 2(c). Finally, when two (emulating) PUs attempt to access reserved spectrum they receive benefit r_p^*. Figure 2(d) illustrates the case where the two PUs attempt to access two non-overlapping spectrum bands.

As stated earlier, algorithms for how the available spectrum is allocated amongst the SUs is beyond the scope of this

[1]This term is also referred in literature as "white space" or "spectrum holes."

work, as this is a field of active research in and of itself [10]. However, we present one simple scheme for SU spectrum allocation as an illustrative example. Under this scheme, the available spectrum is divided using an equal portioning rule. For instance, if there is F total spectrum in the block, a PU is taking up f spectrum and there are n other SU radios, then r_s is a function of $(F-f)/n$ and r_p is a function of f. If the PU decides to emulate and act as a SU, then r_s^* is a function of $F/(n+1)$. Finally, if two PUs decide to claim the same band of spectrum, and the result is that neither radio can use it because of interference, r_p^* would be 0. If they share the spectrum equally via some time or code division scheme, it is a function of $f/2$. If they access non-overlapping bands, r_p^* is a function of f.

If revenue for all radios increases monotonically with bandwidth, the ordering of r_s, r_p, and r_s^* is dependent on the number of other SUs, reserved PU bandwidth, available spectrum and frequency block bandwidth. In particular, the ordering $r_p < r_s^* < r_s$ occurs when $f < F/(n+1)$, which is when PUs take less than their "fair" allotment of the entire spectrum resource. The reverse ordering occurs when a PU takes more than their "fair" share. Other frequency allocation schemes and revenue functions would lead to different orderings.

Similar to the revenues, there are two types of costs that are of interest. The first is the regulatory body penalty for performing an EA, c_e. The other is the cost of challenging the other radio's license, c_c. As it is not clear that every time a violation is detected the regulatory body will be able to enact a punishment, without any loss of generality c_e can be considered an expected cost. Similarly, c_c may represent the expected cost to challenging a license if the scheme employed requires a dynamic amount of resources.

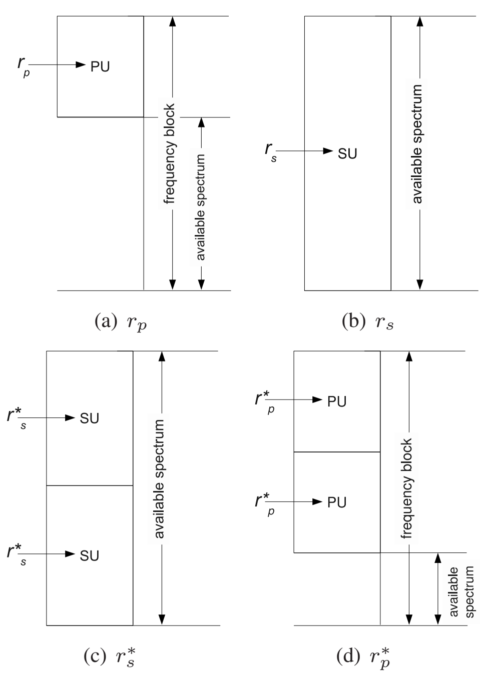

Fig. 2. Illustrations of the four revenue variables: 2(a), the revenue of the PU; 2(b), the revenue of the SU; 2(c), the revenue of a SU with an additional SU in the available spectrum; and 2(d), the revenue of a PU when it shares spectrum with an additional PU.

From this system model, we define two games that will drive our analysis in the rest of the paper. The first game is between a policy-abiding SU and a selfish radio holding either a SU or PU license and the second is between two selfish SUs that may perform an EA but are unsure if the other will challenge their license. We use two-player, one-shot Bayesian games to represent the interactions between radios. Modeling these games a two-player games is similar to the attacker/defender model used in [6], [7]. We assume that radios determine a strategy for dealing with other spectrum users and/or using the spectrum upon the decision to use the spectrum block, based only on their knowledge of radio utilities and their beliefs of type distributions. These strategies are applied immediately as other radios attempt to utilize the spectrum. These interactions occur quickly as compared to spectrum users arriving and leaving, so we approximate them as one-on-one, one shot events. Future work can relax these assumptions, providing insight into multi-stage, multi-radio interactions.

We determine the pure and mixed strategy BNE of these two games to gain insight into the steady-state rate of EAs in the system. We pursue an analytical approach here, where the values of the revenues and costs are not defined, allowing these results to be used by regulatory agencies for engineering DSA ecosystems.

V. The One-Way Emulation Attack Game

We now formally analyze the interaction between a policy abiding SU and a radio of unpredictable type (either SU or PU) that may choose to launch a selfish EA or act true to its type randomly (so as to reduce the probability of being detected).

A. Game Model

In this game, a radio willing to perform an EA interacts with a SU that is not going perform an EA but may or may not choose to challenge the license of the other radio. This game represents a scenario where policy dictates that radios can only be challenged at particular asymmetric times (such as when a radio enters into the spectrum for the first time); once radios have begun to utilize the spectrum, they are entrenched regardless of their legitimacy. This kind of policy might emerge if a certificate based scheme was used for authentication and certificates were only shared upon entry to a spectral band. Another scenario where this game could occur is when there are several licensees using a frequency block; some of these SUs are trustworthy and can be authenticated *a priori* via a negligible cost verification scheme, while the other radios are less trustworthy and require more costly verification.

The player set therefore consists of two radios: $\mathcal{N} = \{1, 2\}$. The type set for Radio 1, $\Theta_1 = \{p, s\}$ consists of two types, PU and SU, based on the license granted to the radio. Radio 2 is SU of type s. Both radios know their own type, however, Radio 2's type is known to Radio 1 while Radio 1's type is unknown to Radio 2. Due to the Radio 2's partial information about Radio 1, there are two actions that Radio 1 can take: either **emulate** and pretend it is the opposite of its type, or act **legitimately** and present itself without deception. The action set for Radio 1 is given as $A_1 = \{e, l\}$. Radio 2 has two actions available: either **challenge** Radio 1 and check its stated license or **accept** its claim. The action set for Radio 2 is given as $A_2 = \{c, a\}$. For both types, their strategy set S_i is their action set A_i. The game is considered to be played simultaneously; the normal form of the game for the two types of Radio 1 is shown in Figure 3 and the extensive form is given in Figure 4.

Radio 2

Radio 1		c	a
	e	$r_p - c_e$, $r_s - c_c$	r_s^*, r_s^*
	l	r_p, $r_s - c_c$	r_p, r_s

$\theta_1 = p$

Radio 1		c	a
	e	$r_s^* - c_e$, $r_s^* - c_c$	r_p, r_s
	l	r_s^*, $r_s^* - c_c$	r_s^*, r_s^*

$\theta_1 = s$

Fig. 3. The normal form one-way EA game, in which the selfish radio's (Radio 1's) type (p or s) is unknown to Radio 2, and Radio 2's type is known. Radio 1's utility is the top entry, Radio 2's the lower entry. Radio 1 is the row player and Radio 2 is the column player.

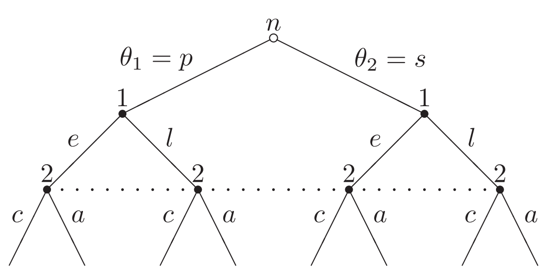

Fig. 4. The extensive form one-way EA game. Dotted lines represent information sets (states of game play that a player cannot differentiate between). Payoffs are in Figure 3, nature is represented by player n.

For the interaction in Figure 3, when Radio 1 is of type PU (top matrix), the utility outcomes are as follows: If Radio 1 decides to **emulate** and Radio 2 **challenges** it, the regulatory body ensures that Radio 1 only uses the PU spectrum (r_p) and pays the penalty (c_e). Under this scenario, Radio 2 gets the revenue of not sharing the available spectrum with an additional radio, but also must pay the cost (c_c) to challenge Radio 1's license. If instead of **challenge**, Radio 2 had **accepted** Radio 1's emulation, then both radios will share the available spectrum with the other radio (r_s^*). If Radio 1 does not **emulate**, it receives the benefit of the PU spectrum. If Radio 2 decides to **challenge** when Radio 1 has acted **legitimately**, Radio 1 has committed no wrong doing and will still get the revenue from the PU spectrum, while Radio 2 will still have to pay for **challenging** (c_c) and get the same revenue (r_s). Similarly, if Radio 1 acts **legitimately** and Radio 2 **accepts**, then both radios receive their appropriate spectrum revenues without any costs. Similar logic is used to determine the payoff matrix when Radio 1 is of type SU (bottom matrix).

B. Pure and Mixed Strategy Analysis

To determine the pure strategy BNE of the one-way EA game, we begin by calculating the expected utility for Radio 2 when faced with an unknown Radio 1. We define Radio 2's beliefs as $\rho_2\{\theta_1 = p\} = \phi$ and thus $\rho_2\{\theta_1 = s\} = 1 - \phi$ (Radio 1's beliefs are not interesting, since Radio 2's type is known to all). From this, we can transform the one-way EA normal form of Figure 3 into the expected one-way EA normal form shown in Figure 5, where Radio 2's expected utility is given for each possible combination of pure strategy pairs by both types of Radio 1. For brevity, we adopt the notation $\Delta_{xy} = r_x - r_y$ (likewise, $\Delta_{xy^*} = r_x - r_y^*$).

Radio 2

Radio 1		c	a
	(e, e)	$r_p - c_e, r_s^* - c_e$, $r_s^* + \phi\Delta_{ss^*} - c_c$	r_s^*, r_p, $r_s - \phi\Delta_{ss^*}$
	(e, l)	$r_p - c_e, r_s^*$, $r_s^* + \phi\Delta_{ss^*} - c_c$	r_s^*, r_s^*, r_s^*
	(l, e)	$r_p, r_s^* - c_e$, $r_s^* + \phi\Delta_{ss^*} - c_c$	r_p, r_p, r_s
	(l, l)	r_p, r_s^*, $r_s^* + \phi\Delta_{ss^*} - c_c$	r_p, r_s^*, $r_s^* + \phi\Delta_{ss^*}$

Fig. 5. The expected one-way EA game, the top left utility is Radio 1 type PU, top right is Radio 1 type SU, and bottom is expected utility for Radio 2. The labeling for Radio 1's row entries is $(s_1(p), s_1(s))$.

We begin by examining Figure 5 to see under what circumstances Radio 2's strategies of **challenge** or **accept** dominate each other. We also use the notation $(s_1(p), s_1(s))$ to represent the pure strategies played by Radio 1's two types.

Remark 1: When $c_c > 0$, **challenge** ($s_2 = c$) can never be a dominant strategy for Radio 2.

Proof: The proof is straightforward and follows from the observation from Figure 5 that when neither type of Radio 1 **emulate** but play the strategy (l, l) instead, **challenge** and **accept** have the following dominance relationship[2] based on c_c:

$$c_c \underset{s_2=a}{\overset{s_2=c}{\lessgtr}} 0 \tag{2}$$

■

For the converse case, the following proposition holds:

Remark 2: There always exists a belief threshold ϕ_0 for which **accept** ($s_2 = a$) is a dominant strategy for Radio 2.

Proof: We analyze the four possible scenarios to determine the dominance relationship. When Radio 1 plays (e, e), then **challenge** and **accept** have the following relationship:

$$\begin{array}{lll} \phi \underset{s_2=a}{\overset{s_2=c}{\lessgtr}} & \frac{1}{2} + \frac{c_c}{2\Delta_{ss^*}} & \text{if } \Delta_{ss^*} > 0 \\ \phi \underset{s_2=a}{\overset{s_2=c}{\gtrless}} & \frac{1}{2} + \frac{c_c}{2\Delta_{ss^*}} & \text{if } \Delta_{ss^*} < 0 \end{array} \tag{3}$$

[2]The notation $x \underset{s_i=b}{\overset{s_i=a}{\lessgtr}} y$ indicates player i's strategy a dominates b when $x < y$ and b dominates a when $x > y$.

When Radio 1 plays (e, l), then **challenge** and **accept** have the following dominance relationship:

$$\begin{aligned} \phi &\underset{s_2=a}{\overset{s_2=c}{\gtrless}} \frac{c_c}{\Delta_{ss^*}} \quad \text{if } \Delta_{ss^*} > 0 \\ \phi &\underset{s_2=a}{\overset{s_2=c}{\lessgtr}} \frac{c_c}{\Delta_{ss^*}} \quad \text{if } \Delta_{ss^*} < 0 \end{aligned} \tag{4}$$

Radio 1 playing (l, e) leads to the following dominance relationship:

$$\begin{aligned} \phi &\underset{s_2=a}{\overset{s_2=c}{\gtrless}} 1 + \frac{c_c}{\Delta_{ss^*}} \quad \text{if } \Delta_{ss^*} > 0 \\ \phi &\underset{s_2=a}{\overset{s_2=c}{\lessgtr}} 1 + \frac{c_c}{\Delta_{ss^*}} \quad \text{if } \Delta_{ss^*} < 0 \end{aligned} \tag{5}$$

From Remark 1, we know that when $c_c > 0$, $s_2 = a$ dominates $s_2 = c$ when Radio 1 plays (l, l) strategy. Thus, **accept** $(s_2 = a)$ is a dominant strategy under all Radio 1 strategies when it is dominant in Equations (3), (4) and (5). Solving these three inequalities for $c_c > 0$ gives us the following conditions under which **accept** is dominant:

$$\begin{array}{lll} \text{for} & \Delta_{ss^*} < -c_c & \phi > 1 + c_c/\Delta_{ss^*} \\ \text{for} & \Delta_{ss^*} \in (-c_c, c_c) & 0 < \phi < 1 \\ \text{for} & \Delta_{ss^*} > c_c & \phi < c_c/\Delta_{ss^*} \end{array} \tag{6}$$

Thus, for each of the three case we have a ϕ_0 for which $s_2 = a$ is a dominant strategy. ■

Remark 2 tells us that no matter what the revenue and costs, if the policy-abiding radios believe that there are more or less than a certain fraction of PUs in the system, they will not challenge licenses.

Proposition 1: For the one-way EA game, there exists at least two pure strategy BNE.

Proof: The above conditions in Equations (3), (4) and (5) identify when Radio 2's **challenge** strategy can be eliminated by iterated dominance. Going back to Figure 3, once **challenge** has been eliminated, either Radio 1's strategy of **emulating** or acting **legitimately** can be eliminated depending on Δ_{ps^*}.

If $\Delta_{ps^*} < 0$, the PUs will **emulate** (because it dominates **legitimate** operation) and SUs will do the opposite. Thus, the BNE in this case is $((\hat{s}_1(p) = e, \hat{s}_1(s) = l), \hat{s}_2 = a)$. When $\Delta_{ps^*} > 0$, the opposite dominance relations hold: PUs won't **emulate** and SUs will. The BNE in this case is $((\hat{s}_1(p) = l, \hat{s}_1(s) = e), \hat{s}_2 = a)$.

Thus, we have found two pure-strategy BNE, hinging on the signs of Δ_{ss^*} and Δ_{ps^*}. ■

Under static, one-shot games, whether the radio's beliefs actually reflect reality is immaterial to the behavior of the radios; they never get a chance to verify their beliefs and thus operate as if their beliefs were reality. To determine the system-wide behaviors of the radios, we will assume that these beliefs are correct, in other words, we assume that the belief distribution is the actual distribution.

A regulatory agency may be concerned how likely it is that radios will perform EAs under various revenue and cost scenarios. We term this the EA *rate* of the system or $p[EA]$ – the probability that a randomly encountered radio will choose to **emulate**. We investigate the *worst case* EA rate, which is defined as

$$p_{\max}[EA] = \max_{\phi \in (0,1)} p[EA]$$

As discussed and shown above, under pure strategy equilibria, either the PUs or the SUs will **emulate** (but not both), meaning that $p[EA] = \phi$ if PUs **emulate** or $p[EA] = 1 - \phi$ if SUs **emulate**. When $\Delta_{ss^*} \in (-c_c, c_c)$, any value of ϕ admits a pure strategy equilibria (see Equation (6)); outside this range ϕ must meet one of the two constraints given in Equation (6). When any value of ϕ admits a pure strategy equilibria, $p_{\max}[EA]$ is 1, and when ϕ is constrained, the ϕ at the constraint maximizes $p[EA]$. Table I summarizes the worst case EA rates in the system under the pure strategy BNE.

	$\Delta_{ss^*} \in (-\infty, -c_c)$	$(-c_c, 0)$	$(0, c_c)$	(c_c, ∞)
$\Delta_{ps^*} > 0$	$-\frac{c_c}{\Delta_{ss^*}}$	1	1	1
$\Delta_{ps^*} < 0$	1	1	1	$\frac{c_c}{\Delta_{ss^*}}$

TABLE I
SUMMARY OF WORST-CASE EA RATES FOR THE ONE-WAY EA GAME UNDER PURE STRATEGY BNE.

The mixed strategy NE exists when neither radio has any incentive to change its mixing probabilities. For the special case of two player games in which each player has only two pure strategies, under the NE each radio selects a mixed strategy so that the other player is indifferent (in an expected utility sense) to either of the two pure strategies it can employ. In other words, each player selects a mixing probability $p[s_i = s_i^1] = p_i$ such that

$$\begin{aligned} & p_i u_{-i}(s_{-i}^1, s_i^1) + (1 - p_i) u_{-i}(s_{-i}^1, s_i^2) \\ = \; & p_i u_{-i}(s_{-i}^2, s_i^1) + (1 - p_i) u_{-i}(s_{-i}^2, s_i^2) \end{aligned} \tag{7}$$

It is difficult to create an analytical solution to the mixed BNE for the one-way EA game because there are three mixed strategies that must be simultaneously solved for: $\sigma_1(p)$, $\sigma_1(s)$ and σ_2, leading to three mixing probabilities: p_p, the probability that PUs **emulate** p_s, the probability that SUs **emulate** and q, the probability that Radio 2 **challenges**. In a BNE, each of these mixed strategies must simultaneously be best responses to each other.

To reduce the degrees of freedom, we observe that the value of Δ_{ps^*} determines whether **emulate** will be a strictly dominated strategy for either the PU or SU type: for $\Delta_{ps^*} > 0$, PU types will act **legitimately**, and the same holds for SUs under $\Delta_{ps^*} < 0$. When this occurs, either p_p or p_s becomes 0, and there are only two remaining mixing parameters: q and the remaining p_i, which can be solved according to Equation (7).

First, we examine the case in which $\Delta_{ps^*} > 0$, meaning only SUs have reason to select between **emulate** or acting **legitimately**. Under this scenario, we solve for q to make SUs indifferent to either action:

$$\begin{aligned} & q\,(r_s^* - c_e) + (1 - q)\,(r_p) \\ = \; & q\,(r_s^*) + (1 - q)\,(r_s^*) \end{aligned}$$

Solving for q, we get:

$$q = \frac{\Delta_{ps^*}}{\Delta_{ps^*} + c_e} \quad (8)$$

Similarly, under this scenario, SUs must choose a p_s to make Radio 2 indifferent to either **challenge** or **accept** under the knowledge that PUs will be acting **legitimately**.

$$\begin{aligned} & \phi\left(r_s - c_c\right) + (1-\phi)\left(r_s^* - c_c\right) \\ = \;& \phi\left(r_s\right) + (1-\phi)\left(p_s\left(r_s\right) + (1-p_s)\left(r_s^*\right)\right) \end{aligned}$$

Solving this for p_s, we get:

$$p_s = \frac{-c_c}{(1-\phi)\,\Delta_{ss^*}} \quad (9)$$

Repeating the process for the other case, $\Delta_{ps^*} < 0$, in which PUs have both strategies undominated (and SUs are dominated such that they will only act **legitimately**), the following values of q and p_p are obtained:

$$q = \frac{\Delta_{ps^*}}{\Delta_{ps^*} - c_e} \quad (10)$$

$$p_p = \frac{c_c}{\phi \Delta_{ss^*}} \quad (11)$$

The mixed strategies for q given in Equations (8) and (10) ensure that $q \in (0, 1)$. However, we see there exists ranges of Δ_{ss^*} so that both Equations (9) and (11) produce values of p_i that are invalid. In particular, p_s exceeds 1 when:

- $\Delta_{ps^*} > 0$ and $\Delta_{ss^*} \in (-c_c/(1-\phi), 0)$ or
- $\Delta_{ps^*} < 0$ and $\Delta_{ss^*} \in (0, c_c/\phi)$

and p_s under-runs 0 when:

- $\Delta_{ps^*} > 0$ and $\Delta_{ss^*} > 0$ or
- $\Delta_{ps^*} < 0$ and $\Delta_{ss^*} < 0$.

In these cases, whatever mixed strategy chosen will either be too small or too big to make the other radio indifferent to its two strategies, and the other radio will respond with a pure strategy (in other words, the expected utility for one strategy will be larger than the other). The radio with the ineffective mixed strategy will respond to this pure strategy with another pure strategy, making the BNE a pure rather than mixed strategy pair. For all four cases above, any mixed strategy chosen by Radio 1 type leads to Radio 2 choosing **accept** as a best response, to which Radio 1's types will have best responses of **emulating** or acting **legitimately**, depending on the sign of Δ_{ps^*}.

From these observations, the following proposition can be summarized:

Proposition 2: For $\Delta_{ps^*} > 0$, $(\hat{\sigma}_1, \hat{\sigma}_2) = ((l, \hat{p}_s), \hat{q})$ is a BNE, whereas for $\Delta_{ps^*} < 0$, $(\tilde{\sigma}_1, \tilde{\sigma}_2) = ((\tilde{p}_p, l), \tilde{q})$ is a BNE, where $\hat{q}$, $\hat{p}_s$, $\tilde{q}$ and $\tilde{p}_p$ are given by Equations (8), (9), (10) and (11), respectively.

From the above results, it is possible to determine the worst-case mixed strategy EA rates. Under mixed strategy equilibria, the EA rate is given by:

$$p[EA] = \phi p_p + (1-\phi) p_s \quad (12)$$

Given that one of Radio 1's types will always be acting **legitimately** (depending on the sign of Δ_{ps^*}), there are three regions that the EA region goes through: the region where it mixes between **emulate** and **legitimate**, the region where it always **emulates**, and the region where it always acts **legitimately**. In the first region, the EA rate is not a function of ϕ (because ϕ cancels out when p_p and p_s are plugged into Equation (12)), and thus the worst case EA rate is a function of Δ_{ss^*}. In the second region, $p[EA]$ is a function of ϕ, and $\phi = 1$ maximizes this to $p[EA] = 1$. Finally, in the third region, neither radio is **emulating**, so $p[EA] = 0$. These worst-case EA rates are summarized in Table II.

	$\Delta_{ss^*} \in$ $\left(-\infty, \frac{-c_c}{1-\phi}\right)$	$\left(\frac{-c_c}{1-\phi}, 0\right)$	$\left(0, \frac{c_c}{\phi}\right)$	$\left(\frac{c_c}{\phi}, \infty\right)$
$\Delta_{ps^*} > 0$	$\frac{-c_c}{\Delta_{ss^*}}$	1	1	0
$\Delta_{ps^*} < 0$	0	1	1	$\frac{c_c}{\Delta_{ss^*}}$

TABLE II
SUMMARY OF WORST-CASE EA RATES OF THE ONE-WAY EA GAME UNDER MIXED STRATEGY BNE.

C. Summary of results

There are several important findings in the analysis of this game. Both pure and mixed strategy equilibria are defined by Δ_{ps^*} and Δ_{ss^*}. The first parameter relates to Radio 1, and reflects the difference in revenue the radio gets from acting as a PU versus sharing the available spectrum as a SU with the other player. This parameter captures the revenue gained (or lost) from emulating. The second parameter relates to Radio 2, and reflects the difference in revenue the radio gets from acting as a SU without sharing the available spectrum versus as a SU and having to share. This parameter captures the revenue gained (or lost) from challenging.

Under the pure strategy equilibria, the first important result is that the rate of EA is not correlated with the cost of emulating. In other words, no matter what the magnitude of the penalty that the regulatory agency places on emulating, there is no pure strategy profile that would incentivize Radio 2 to challenge. Because of this, Radio 1 decides whether to emulate or not simply based off of whether it will benefit from the change in spectrum usage from switching type. Whichever license provides higher revenue is selected, whether that requires emulating or not.

However, accept is not always a pure strategy equilibria for Radio 2. As identified earlier, there are two general regions where accept is a pure equilibrium strategy for Radio 2: The first occurs when the revenue gained from challenging is less than cost of challenging. The second occurs when Radio 2 believes there are fewer emulating radios (i.e. PUs, since all PUs will emulate in this case) than the ratio of the cost of challenging to revenue gained from a successful challenge. In other words, accept is a pure strategy when the expected gain from challenging is less than the cost of challenging.

For the mixed strategy equilibria, the cost of emulating affects the rate of challenging. For a fixed amount of revenue gained from emulating, higher costs of emulating leads to lower rates of challenging. In other words, as the penalties increase on emulating, Radio 2 has to challenge less frequently to maintain Radio 1's indifference to either emulating or acting legitimately. This makes sense, as the cost of emulating acts to counter the incentive of emulating, and the greater the cost, the less often challenge has to be played to make the expected utilities the same for legitimate operation and emulation. Radio 1 emulates with a probability that makes the expected gain for Radio 2 from challenging equal to the cost of challenging. The expected gain from challenging is the product of the probability the radio *may* emulate (recall in the mixed strategy, only one type of Radio 1 will emulate at a time), the probability this radio *will* emulate (their mixing strategy) and the gain from challenging.

For both pure and mixed strategies, the beliefs that Radio 2 has about the distribution of types have a larger impact on both the rate of EA and the worst case rate of EA than the cost of emulating. Rather than focus on penalties, regulators would be wise to ensure that the gain from challenging is significant and the cost of challenging is small, as this reduces the rate of emulating. In summary, EAs are better controlled via the carrot of Radio 2's revenue than from the stick of Radio 1's EA punishment penalties.

VI. The Two-Way Emulation Attack Game

We now explore a different game in which each radio has partial knowledge about the type of the other. In this game, both radios are SUs that will potentially commit an EA but do not know if the other radio will challenge them. In this game every claimed PU license represents an EA, however not all radios will take the effort to verify the attack and report it to the regulatory agency.

A. Game Model

The two-way game may manifest in a scenario where a subset of the SUs have the capability to report EAs and will therefore challenge all licenses, while others do not have this capability (perhaps they are not able to communicate with the regulatory body) and never challenge. Alternatively, it represents a scenario in which the challenge/accept mixed strategy is dictated by policy, rather than the radio itself.

In this game, the player set consists of two SU radios. However, the type set is different than in one-way EA game (since both radios here are SUs), and consist of radios that always *challenge* the claimed license type of other radios and radios that always *accept* the claimed license, $\Theta_i = \{c, a\}$. Both radios know their own type but are unaware of the other radio's type. Each type has the same action set, **emulate** or act **legitimately**, $A_i = \{e, l\}$. The game is played simultaneously; the normal form of the game for the four possible combinations of types is shown in Figure 6 and the extensive form in Figure 7.

In this game, some of the more interesting payoffs pairs include: When both radios **emulate** and are both of type *challenge*, the radios share the available spectrum (r_s^*) and pay both the punishment cost and the cost of checking the license credentials; when both radios **emulate** and both radios are of type *accept*, the radios share the same PU spectrum (r_p^*) (which, as discussed earlier, may be equal to or less than r_p, depending on the scenario); and when one radio performs an EA and is of type *accept* while the other radio doesn't and is of type *challenge*, it leads to both radios sharing the available spectrum (r_s^*) and paying either the punishment cost (c_e) or the cost to challenge (c_c).

	e	l
e	$r_s^* - c_e - c_c$, $r_s^* - c_e - c_c$	$r_s^* - c_e - c_c$, $r_s^* - c_c$
l	$r_s^* - c_c$, $r_s^* - c_e - c_c$	$r_s^* - c_c$, $r_s^* - c_c$

$\theta_1 = c, \theta_2 = c$

	e	l
e	$r_p - c_c$, $r_s - c_e$	$r_p - c_c$, r_s
l	$r_s^* - c_c$, $r_s^* - c_e$	$r_s^* - c_c$, r_s^*

$\theta_1 = c, \theta_2 = a$

	e	l
e	$r_s - c_e$, $r_p - c_c$	$r_s^* - c_e$, $r_s^* - c_c$
l	r_s, $r_p - c_c$	r_s^*, $r_s^* - c_c$

$\theta_1 = a, \theta_2 = c$

	e	l
e	r_p^*, r_p^*	r_p, r_s
l	r_s, r_p	r_s^*, r_s^*

$\theta_1 = a, \theta_2 = a$

Fig. 6. The normal form two-way EA game, in which both radios' type (a or c) is unknown to the other. Radio 1's utility is the top entry, Radio 2's the lower entry. Radio 1 is the row player and Radio 2 is the column player.

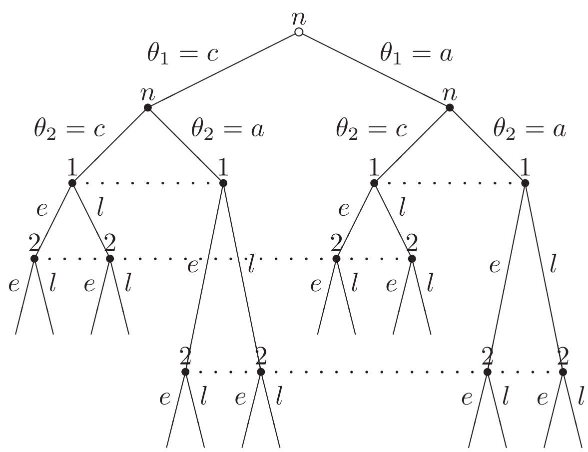

Fig. 7. The extensive form two-way EA game. Dotted lines represent information sets (states of game play that a player cannot differentiate between). Payoffs are shown in Figure 6, nature is represented by player n.

B. Pure and Mixed Strategy Analysis

In determining the pure strategy BNE of the two-way EA game, we immediately identify from Figure 6 (under our standard assumptions that $c_e > 0$ and $c_c > 0$) that if $\Delta_{sp^*} > 0$ and $\Delta_{ps^*} < 0$, the strategy of acting **legitimately** is dominant for both types of radios – *challenge* and *accept* – regardless of their beliefs about the distribution of types. However, if these conditions do not hold, there are no easily identifiable pure strategy BNE and we must look for a mixed strategy equilibrium.

Proposition 3: The two-way EA game admits at least one pure strategy BNE.

From the discussion above, we observe from Figure 6 that, when $\Delta_{sp^*} > 0$ and $\Delta_{ps^*} < 0$, (l,l) is a pure strategy BNE.

To investigate the mixed-strategy BNE, we use similar notation as before; the mixed strategy for a radio of type *challenge* $\sigma_i(c)$ is probability p_c that they **emulate** and $1-p_c$ that they act **legitimately**. For radios of type *accept* the mixed strategy is $\sigma_i(a)$ and p_a denotes the probability of **emulating**. All radios are assumed to have the same beliefs about the distribution of types; in other words, $\rho_1 = \rho_2$ for all types. The beliefs about the type distribution is given by $\rho_i(\theta_{-i} = c) = \phi$ (and thus $\rho_i(\theta_{-i} = a) = 1 - \phi$). This game has perfect symmetry, meaning there are no distinguishing characteristics to separate Radio 1 from Radio 2 removing the need to have separate mixing parameters for the radios (i.e. q_c and q_a).

Furthermore, it turns out that p_c is not a necessary variable, since there is no need for radios of type *challenge* to mix strategies; for these radios ϕ alone determines which strategies dominate. When a radio of type *challenge* faces a radio also of type *challenge*, no matter what mixed strategy either radio selects, the utility is either $r_s^* - c_e - c_c$ if it **emulates** or $r_s^* - c_c$ if it acts **legitimately**. In the same manner, if a radio of type *challenge* faces a radio of type *accept*, no matter what mixed strategy the *accept* radio selects, the utility of the *challenge* radio is either $r_p - c_c$ if it **emulates** or $r_s^* - c_c$ if it acts **legitimately**. In this manner, no mixed strategy from either type can make radios of type *challenge* indifferent.

Remark 3: Radios of type *challenge* will always play a pure strategy (**emulate** or **legitimate**), regardless of the mixed or pure strategies of the radio types they face.

Thus, there will always exist a dominance relationship based only on the *challenge* radio's belief about the distribution of types in the system. We can define this dominance relationship as:

$$\begin{array}{c} \phi\left(r_s^* - c_e - c_c\right) + (1-\phi)\left(r_p - c_c\right) \\ \underset{s_i(c)=l}{\overset{s_i(c)=e}{\gtrless}} \\ \phi\left(r_s^* - c_c\right) + (1-\phi)\left(r_s^* - c_c\right) \end{array}$$

which can be re-written in terms of ϕ as:

$$\begin{array}{lll} \phi \underset{s_i(c)=l}{\overset{s_i(c)=e}{\lessgtr}} \frac{\Delta_{ps^*}}{c_e + \Delta_{ps^*}} & \text{if } (c_e + \Delta_{ps^*}) > 0 \\ \phi \underset{s_i(c)=l}{\overset{s_i(c)=e}{\gtrless}} \frac{\Delta_{ps^*}}{c_e + \Delta_{ps^*}} & \text{if } (c_e + \Delta_{ps^*}) < 0 \end{array} \qquad (13)$$

Equation (13) reveals that when $\Delta_{ps^*} < 0$, **legitimate** behavior always dominates **emulating**, regardless of the player's beliefs. Note that under this condition, the right hand side of the top equation is always less than 0 and the right hand side of the bottom equation is always greater than 1. Since $\phi \in (0,1)$, this means that all values of ϕ will satisfy one of these equations in which legitimate operation is the dominant strategy. For values of $\Delta_{ps^*} > 0$, the dominance relation depends on the top equation, since $c_e + \Delta_{ps^*} > 0$ always holds (assuming $c_e > 0$).

When radios of type *accept* mix their strategies (we call this the mixing radio), they are trying to make other radios of type *accept* (we call this the opponent radio) indifferent to either strategy choice. The opponent radio knows it can face one of three things: a *challenge* radio playing a pure strategy, the mixing radio acting **legitimately**, or the mixing radio **emulating**. Thus, the mixing radio must choose a mixed strategy so that the expected utility for the opponent radio is the same whether it **emulates** or acts **legitimately**. If we assume that radios of type challenge are acting **legitimately**, then this relationship between the expected utilities for each strategy leads to the following:

$$\begin{array}{rl} & \phi\left(r_s^* - c_e\right) + (1-\phi)\left(p_a r_p^* + (1-p_a)\, r_p\right) \\ = & \phi\left(r_s^*\right) + (1-\phi)\left(p_a r_s + (1-p_a)\, r_s^*\right) \end{array}$$

which gives the following probability of **emulating** for radios of type *accept*:

$$p_a = \frac{\Delta_{ps^*}}{\Delta_{ps^*} + \Delta_{sp^*}} - \frac{\phi c_e}{(1-\phi)\left(\Delta_{ps^*} + \Delta_{sp^*}\right)} \qquad (14)$$

When we assume that radios of type challenge are **emulating**, we get the same mixing strategy as in Equation (14). When *challenge* radios act **legitimately**, *accept* radios receive r_s^* revenue under either strategy choice the *challenge* radio chooses. Similarly, when the *challenge* radio **emulates**, the *accept* radios receive r_s under either strategy choice. In both cases, these terms cancel out, leaving radios of type *accept* with an expected difference in utility of ϕc_e between *challenge* radios acting **legitimately** or **emulating**. Thus, the mixed strategy given by Equation (14) holds for either pure strategy played by radios of type *challenge*. These observations can be summarized in the following proposition.

Proposition 4: For the two-way EA game, there exists two mixed-strategy BNE:

- $(\hat{\sigma}_1, \hat{\sigma}_2) = ((l, \hat{p}_a), (l, \hat{p}_a))$ when $\Delta_{ps^*} < 0$ or when $\Delta_{ps^*} > 0$ and $\phi > \Delta_{ps^*}/(c_e + \Delta_{ps^*})$; and
- $(\hat{\sigma}_1, \hat{\sigma}_2) = ((e, \hat{p}_a), (e, \hat{p}_a))$ when $\Delta_{ps^*} > 0$ and $\phi < \Delta_{ps^*}/(c_e + \Delta_{ps^*})$

where $\hat{p}_a$ is given by (14).

The EA rates under these mixed strategies as a function of ϕ can be calculated as

$$p[EA] = \phi p_c + (1-\phi) p_a$$

. This function has three possible regions: the region where p_a under-runs 0 (leading to a pure strategy BNE); the region where $p_a \in (0,1)$ (leading to a mixed strategy BNE for radios of type *accept*); and the region where p_a overruns 1 (also leading to a pure strategy BNE).

For the valid range of p_a, the EA rate depends on the whether radios of type *challenge* are **emulating** (determined by Equation (13)). When they are acting **legitimately**, the EA rate changes linearly with ϕ according to

$$p[EA] = \frac{\Delta_{ps^*}}{\Delta_{ps^*} + \Delta_{sp^*}} + \phi \frac{-c_e - \Delta_{ps^*}}{\Delta_{ps^*} + \Delta_{sp^*}}$$

When radios of type *challenge* are **emulating**, the EA rate changes according to:

$$p[EA] = \frac{\Delta_{ps^*}}{\Delta_{ps^*} + \Delta_{sp^*}} + \phi \frac{-c_e + \Delta_{sp^*}}{\Delta_{ps^*} + \Delta_{sp^*}}$$

Note that these are lines in the form $y = mx + b$ parameterized on ϕ.

Where do the transitions occur between the mixed strategies and the pure strategies? Based on whether $p_a = 1$ or $p_a = 0$, Equation (14) reveals two key ϕ thresholds:

$$\phi_0^* = \frac{\Delta_{ps^*}}{\Delta_{ps^*} + c_e} \tag{15}$$

$$\phi_1^* = \frac{\Delta_{sp^*}}{\Delta_{sp^*} - c_e} \tag{16}$$

Whether a particular ϕ value admits valid mixed strategy p_a depends on whether ϕ is greater than or less than ϕ_0^* and ϕ_1^* and the following three conditions:

- $\Delta_{ps^*} + \Delta_{sp^*} \lessgtr 0$
- $\Delta_{ps^*} + c_e \lessgtr 0$
- $\Delta_{sp^*} - c_e \lessgtr 0$

For a continuum of ϕ values, there are 8 combinations that the above conditions can take on. Two of these conditions are impossible to satisfy for $c_e > 0$. Examples of the remaining 6 are shown in Figure 8. Note that the shape of $p[EA]$ varies significantly depending on these parameters. In particular, for certain threshold levels ϕ_0^* and ϕ_1^*, radios will always choose to **emulate** or never **emulate**. For other threshold values, the rate of emulation in the system is observed to be high or low depending on the gains (or lack thereof) from **emulate** or **challenge**. Thus, the perceived distribution of types has a large effect in keeping EAs in check.

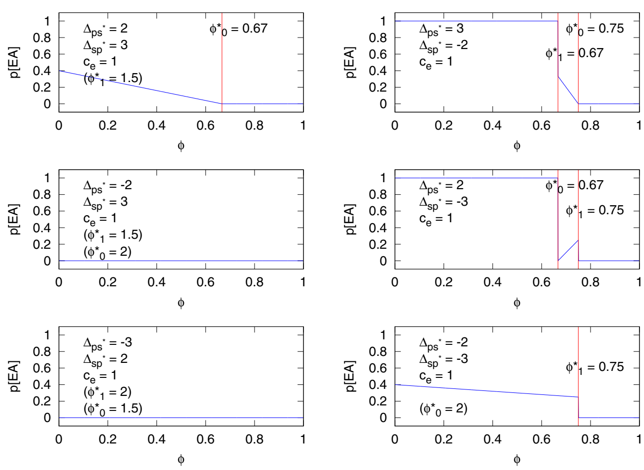

Fig. 8. Typical plots of $p[EA]$ versus ϕ when radios of type *challenge* are acting legitimately ($p_c = 0$). The relations between Δ_{ps^*}, Δ_{sp^*} and c_e represent the 6 possible combinations of conditions identified from thresholds in Equations (15) and (16).

C. Summary of results

In the two-way EA game, two parameters control the pure and mixed strategies – Δ_{ps^*} and Δ_{sp^*}. The first represents the revenue gained (or lost) between sharing the SU spectrum and having the exclusive access to PU spectrum. Similarly, the second parameter represents the revenue gained (or lost) between potentially sharing the PU spectrum and not having to share the SU spectrum. For mixed strategies, the radio's beliefs and the cost of emulating also come into play.

We observe that the cost of emulation has no effect on some of the pure strategy equilibrium. The first pure strategy equilibrium identified, in which all types of radios act legitimately, occurs when radios receive less revenue using the spectrum as a PU than sharing the spectrum as a SU and less revenue from sharing the spectrum as a PU than not sharing the spectrum as a PU. Under these conditions, the pure strategy of acting legitimately is chosen because there is no benefit to emulating under these conditions. Since both the *challenge* and *accept* types are SUs, if one SU emulates and the other SU doesn't, the radio that chose to emulate receives less revenue because of their decision. If they both emulate, each will receive less revenue than had one of them unilaterally decided not to. Acting legitimately is self-enforcing because their is no spectral incentive to perform an EA. Under the equal portioning scheme described in Section IV, this scenario would occur when the PU spectrum is less than their "fair" portion of the spectrum block.

When playing a mixed strategy, the probability of emulating given in Equation (14) increases proportionally to the expected revenue from getting PU spectrum without being challenged and decreases proportionally to the expected cost of getting caught. In other words, the radios of type accept don't like emulating when the cost of emulating goes up or the benefit of emulating goes down. Furthermore, because of the game symmetry, all mixed and pure BNE strategies are the same for Radio 1 and Radio 2.

In general, regulatory agencies will have a harder time creating good "rules of thumb" for dealing mixed strategy BNE in this game, as the BNE behavior of the system under mixed strategies is strongly dictated by the relative magnitudes of the revenue gained and lost under different spectral use cases. However, under all mixed strategies, increasing the cost of emulating will decrease the propensity for radios to emulate.

VII. Conclusions and Future Work

Opening up the spectrum to allow different licensees to coexist in a DSA network may encourage selfish activity. In this work, we examine one such manifestation of selfish behavior, namely *Emulation Attacks*. Selfish radios may choose to emulate (and conceal their true type) or act legitimately from time to time, so as to increase the expected benefit they obtain from the spectrum, thereby giving rise to uncertainty in the system. We model the interactions between a selfish radio and policy-abiding radio (one-way EA game) and between two selfish radios (two-way EA game) as Bayesian games.

Both one-way and two-way EA games are games of imperfect information that admit BNE in pure and mixed strategies. For these games, we show that, under different conditions on system parameters (representing the expected gain/cost of sharing spectrum, expected gain/cost from verifying radio licenses, and beliefs radios have about each other), different BNE arise. In addition to establishing stability of the system, these conditions also identify the worst case rate of EAs in DSA networks, and provide limits that discourage selfish policy-breaking behavior (by making the legitimate action dominate over emulate). Additionally, these conditions also serve as a guideline for regulatory agencies and policy makers to ensure that the rate of EA in the system are kept arbitrarily small. Of particular interest to regulators, we find that the penalties levied against violators do not always have an effect on the BNE and that the belief that radios have on the type distribution will often dictate the BNE strategy. This implies that the fraction of user types may be as important a parameter for regulatory agencies to control as the penalties.

Our future work entails analysis of multi-stage multi-radio interaction games, where multiple selfish radios are encountered repeatedly over time. This is a generalization of the two-player one-shot games presented in this work and will allow beliefs to change over time. Furthermore, we are interested in exploring what happens when all four combinations of strategies are available to both PUs and SUs – emulate/legitimate combined with accept/challenge.

REFERENCES

[1] R. Chen, J.-M. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan 2008.

[2] T. R. Newman and T. C. Clancy, “Security threats to cognitive radio signal classifiers,” *Proc. of Wireless@VT 2009*, 2009.

[3] S. Anand, Z. Jin, and K. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” *Proc. of IEEE DySPAN 2008*, 2008.

[4] Z. Jin, S. Anand, and K. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” *Proc. of IEEE ICC 2009*, pp. 1–5, June 2009.

[5] A. B. MacKenzie and L. A. DaSilva, *Game Theory for Wireless Engineers*. Morgan & Claypool, 2006.

[6] Y. Liu, C. Comaniciu, and H. Man, “A bayesian game approach for intrusion detection in wireless ad hoc networks,” in *GameNets ’06: Proceeding from the 2006 workshop on Game theory for communications and networks*, 2006.

[7] F. Li and J. Wu, “Hit and Run: A Bayesian Game Between Malicious and Regular Nodes in MANETs,” *Proc. of IEEE SECON*, pp. 432–440, 2008.

[8] W. Wang, M. Chatterjee, and K. Kwiat, “Coexistence with malicious nodes: A game theoretic approach,” *Proc. of IEEE GameNets 2009*, 2009.

[9] D. Fudenberg and J. Tyrole, *Game Theory*. MIT Press, 1991.

[10] J. Suris, L. DaSilva, Z. Han, A. MacKenzie, and R. Komali, “Asymptotic optimality for distributed spectrum sharing using bargaining,” *IEEE Transactions on Wireless Communications*, Oct. 2009.