Optimal Scanning Bandwidth Strategy Incorporating Uncertainty about Adversary's Characteristics

Andrey Garnaev
WINLAB, Rutgers University
North Brunswick, USA
Email: garnaev@yahoo.com

Wade Trappe
WINLAB, Rutgers University
North Brunswick, USA
E-mail: trappe@winlab.rutgers.edu

Abstract—In this paper we investigate the problem of designing a spectrum scanning strategy to detect an intelligent Invader who wants to utilize spectrum undetected for his/her unapproved purposes. To deal with this problem we model the situation as two games, between a Scanner and an Invader, and solve them sequentially. The first game is formulated to design the optimal (in maxmin sense) scanning algorithm, while the second one allows one to find the optimal values of the parameters for the algorithm depending on parameters of the network. These games provide solutions for two dilemmas that the rivals face. The Invader's dilemma consists of the following: the more bandwidth the Invader attempts to use leads to a larger payoff if he is not detected, but at the same time also increases the probability of being detected and thus fined. Similarly, the Scanner faces a dilemma: the wider the bandwidth scanned, the higher the probability of detecting the Invader, but at the expense of increasing the cost of building the scanning system. The equilibrium strategies are found explicitly and reveal interesting properties. In particular, we have found a discontinuous dependence of the equilibrium strategies on the network parameters, fine and the type of the Invader's award. This discontinuity of the fine means that the network provider has to take into account a human/social factor since some threshold values of fine could be very sensible for the Invader, while in other situations simply increasing the fine has minimal deterrence impact. Also we show how incomplete information about the Invader's technical characteristics and reward (e.g. motivated by using different type of application, say, video-streaming or downloading files) can be incorporated into scanning strategy to increase its efficiency.

I. INTRODUCTION

Over the last few decades, the increasing demand for wireless communications has motivated the exploration for more efficient usage of spectral resources ([1], [2]). In particular, it has been noticed that there are large portions of spectrum that are severely under-utilized [3]. Recently, cognitive radio technologies (CR) have been proposed as a means to intelligently use such spectrum opportunities by sensing the radio environment and exploiting available

spectrum holes for secondary usage [4]. In CR systems, secondary users are allowed to "borrow (or lease)" the usage of spectrum from primary users (licensed users), as long as they do not hinder in the proper operation of the primary users' communications. Unfortunately, as we move to make the CR technologies commercial, which will allow secondary users to access spectrum owned by primary users, we will face the inevitable risk that adversaries will be tempted to use CR technology for illicit and selfish purposes [5]. If we imagine an unauthorized user (Invader) attempting to sneak usage of spectrum without obeying proper regulations or leasing the usage of the spectrum, the result will be that both legitimate secondary users and primary users will face unexpected interference, resulting in significant performance degradation across the system.

The challenge of enforcing the proper usage of spectrum requires the notion of a "spectrum policing agent", whose primary job is to ensure the proper usage of spectrum and identify anomalous activities occurring within the spectrum[5]. As a starting point to being able to police the usage of spectrum, we must have the ability to scan spectrum and effectively identify anomalous activities. Towards this objective, there have been several research efforts in signal processing techniques that can be applied to the spectrum scanning problem. For example, in [6], [7], the authors presented methods for detecting a desired signal contained within interference. Similarly, detection of unknown signals in noise without prior knowledge of authorized users was studied in [8], [9]. As another example, in [5], the authors proposed a method to detect anomalous transmission by making use of radio propagation characteristics. In [10], the authors investigated what impact on spectrum scanning can have information about the overarching application that a spectrum thief might try to run, while, in [11], a stationary bandwidth scanning strategy in a discounted repeated game was suggested.

However, these pieces of work tend to not examine the important "interplay" between the two participants inherent in the problem– the Invader, who is smart and will attempt to use the spectrum in a manner to minimize the chance of being detected and fined, while also striving to maximize the benefit he/she receives from illicit usage of this spectrum; and the Scanner, who must be smart

and employ a strategy that strategically maximizes the chance of detecting and fining the smart Invader, with minimal cost. This challenge is made more difficult by the complexity of the underlying scanning problem itself: there will be large swaths of bandwidth to scan, and the system costs (e.g., analog-to-digital conversion, and the computation associated with running signal classifiers) associated with scanning very wide bandwidth makes it impossible to scan the full range of spectrum in a single instance. Consequently, it is important to understand the strategic dynamics that exist between the Scanner and the Invader, while also taking into account the underlying costs and benefits that exist for each participant as well as information or its lack on the technical characteristics of the Invader and his object to intrude into the bandwidth. This paper[1] focuses on finding the optimal scanning strategy by selecting the scanned (and, similarly, the invaded) bandwidth that should be employed in spectrum scanning and examining how incorporating information or the lack of information about the technical characteristics of the Invader and his object can improve the scanning strategy. In order to solve this problem we will apply a Bayesian approach. Note that Bayesian approaches have been widely employed in dealing with different problems in networks, for example, intrusion detection [13], [14], [15], scanning bandwidth [10] and transmission under incomplete information [16], [17], [18], [19], [20], [21]. Finally note that the optimal scanning problem also relates the problem of designing security systems. Note that an extensive literature exists on the construction and modeling of different aspects of such security systems for communication and network security [22], [23], [24], [25], [26], [27], [13], [28], [29], security in wireless networks [30], [31] and cyber-security [32], [14], [16]. In [33], the readers can find a structured and comprehensive survey of the research contributions that analyze and solve security and privacy problems in computer networks via game-theoretic approaches.

The organization of this paper is as follows: in Section II, we first define the problem by formulating two games, which will be solved sequentially in terms of payoff and cost functions. In the first game, the Scanner looks for the maxmin scanning algorithm, if parameters (widths of used bandwidths) of scanning and intrusion are fixed and known. In the second game each player, using the first game's result, which supplies detection probability, looks for the optimal values of these parameters. To gain insight into the problem, in Section IV-A, we outline a linearized model for detection probability and arrive at the corresponding best response strategies for each player in Section IV-B. We then explicitly obtain the equilibrium strategies, in Section IV-C and Section IV-D, for cases involving complete and incomplete knowledge of the In-

vader's technical characteristics (radio's capabilities). In Section V, numerical illustrations are supplied. Finally, in Section VI, discussions and conclusions are supplied, and, in Appendix, the proofs of the announced results are offered to close the paper.

II. FORMULATION OF THE SCANNING PROBLEM

In this section, we set up our problem formulation. Our formulation of the spectrum scanning problem involves two players: the Scanner and the Invader. The Scanner, who is always present in the system, scans a part of the band of frequencies that are to be monitored, in order to prevent illegal usage by a potential Invader of the primary (Scanner) network's ownership of this band. We assume that the amount of bandwidth that needs to be scanned is much larger than is possible using a single scan by the Scanner, and hence the Scanner faces a dilemma: the more bandwidth that is scanned, the higher the probability of detecting the Invader, but at the expense of increasing the cost of the RF scanning system.

We assume that if the Scanner scans a particular frequency band I_S and the Invader uses the band I_I then the invasion will be detected with certainty if $I_S \cap I_I \neq \emptyset$, and it will not be detected otherwise. Without loss of generality, we can assume that the size of the protected frequency band is normalized to 1. The Invader wants to use spectrum undetected for some illicit purpose. We consider two scenarios: (a) The reward for the Invader is related to the width of the frequency band he uses if he is undetected. If he is detected he will be fined. Thus, the Invader faces a dilemma: the more bandwidth he tries to use yields a larger payoff if he is not detected but also it increases the probability of being detected and thus to be fined, (b) The reward for the Invader is unknown to the Scanner: he only knows whether it is related to the width of the frequency band the Invader uses, or not. We formulate this problem as two games, which will be solved separately in the following two subsections.

A. Formulation of the first game - the scanning algorithm

In the first game, where we look for a maxmin scanning algorithm, the Scanner selects the band $B_S = [t_S, t_S + x] \subseteq [0, 1]$ with a fixed upper bound of frequency width x to scan i.e. $t_S \leq 1 - x$. The Invader selects the band $B_I = [t_I, t_I + y] \subseteq [0, 1]$ with a fixed upper bound frequency width y to intrude, i.e., $t_I \leq 1 - y$. Thus, B_S and B_I are pure strategies for the Scanner and the Invader. The Scanner's payoff $v(B_S, B_I)$ is 1 if the Invader is detected (i.e. $[t_S, t_S + x] \cap [t_I, t_I + y] \neq \emptyset$) and his payoff is zero otherwise. The goal of the Scanner is to maximize his payoff, while the Invader wants to minimize it. Thus, the Scanner and the Invader play a zero-sum game. The saddle point (equilibrium) of the game is a couple of strategies (B_{S*}, B_{I*}) such that for each couple of strategies (B_S, B_I) the following inequalities hold [34]:

$$v(B_S, B_{I*}) \leq v := v(B_{S*}, B_{I*}) \leq v(B_{S*}, B_I),$$

where v is the value of the game. It is clear that the game does not have a saddle point in the pure strategy if $x + y < 1$. To find the saddle point we have to extend the game by mixed strategies, where we assign a probability distribution over pure strategies. Then instead of the payoff v we have its expected value. The game has a saddle point in mixed strategies, and let $P(x, y)$ be the value of the game. Then $P(x, y)$ is the maximal detection probability of the Invader under worst conditions.

B. Formulation of the second game - the optimal parameters of the scanning algorithm

In the second game the rivals knowing their equilibrium strategies from the first game as well as detection probability $P(x, y)$, want to find the equilibrium frequency widths x and y. We here consider three sub-scenarios: (a) the Invader's type is known: namely, it is known how the reward for the Invader is related to the width of the frequency band he uses if he is undetected, (b) the technical characteristics of the Invader are known: namely, it is known which frequency band is available for him to use, (c) the Invader's type is unknown: instead, there is only a chance that the Invader reward is related to the width in use. Otherwise, it is not related. Different types of rewards can be motivated by using different types of applications (say, file-download or streaming video).

1) Invader reward is related to the bandwidth used: A strategy for the Scanner is to scan a width of frequency of size $x \in [a, b]$, and a strategy for the Invader is to employ a width of frequency of size $y \in [a, c]$, where $c \leq b < 1/2$. Thus, we assume that the Invader's technical characteristics (e.g., radio's capabilities) are not better than the Scanner's ones.

If the Scanner and the Invader use the strategies x and y, then the payoff to the Invader is the expected reward (which is a function $U(y)$ of bandwidth y illegally used by the Invader) minus intrusion expenses (which is a function $C_I(y)$ of bandwidth y) and expected fine F to pay, i.e.,

$$v_I(x, y) = (1 - P(x, y))U(y) - FP(x, y) - C_I(y). \quad (1)$$

The Scanner wants to detect intrusion taking into account scanning the expenses and damage caused by the illegal use of the bandwidth by the Invader. For detection, he is rewarded by a fine F imposed on the Invader. Thus, the payoff to the Scanner is the difference between the expected reward for detection, and the damage from intrusion into the bandwidth (which is a function $V(y)$ of bandwidth y illegally used by the Invader) with the scanning expenses (which is a function $C_S(x)$ of scanned bandwidth x),

$$v_S(x, y) = FP(x, y) - V(y)(1 - P(x, y)) - C_S(x). \quad (2)$$

Note that introducing transmission costs in such a formulation is common for CDMA [31], [35] and ALOHA networks ([36], [37]).

2) Incomplete information of the Invader's reward and technical characteristics: In this section we assume that the Invader's reward is defined by the reason he intruded into the bandwidth illegally for, and we consider two such reasons:

(a) With probability $1 - q_0$ for the Invader it is just important to work in the network without being detected. Thus, if he is not detected his reward is U which does not depend on the width of bandwidth employed for the intrusion. Then, of course, to minimize the probability of detection he will employ the minimal bandwidth allowed, thus, his strategy is $y = a$.

(b) With probability q_0 for the Invader the bandwidth he uses is important. Thus, his reward is the same as in Section II-B1. We assume that his technical characteristics can be different, the Invader knows his characteristics, but the Scanner does not know them. Under Invader's technical characteristics we assume an upper bound on the spectrum width he can employ. The Scanner knows only this upper bound on bandwidth as c with a conditional probability $q(c) \geq 0$ for $c \in [a, b]$, i.e., $\int_a^b q(c)\, dc = 1$.

To deal with this situation we are going to apply a Bayesian approach, namely, we introduce type $c \in [a, b]$ for the Invader related to the corresponding upper bounds (thus, we here deal with a continuum of Invader's types). The Invader knows his type, while the Scanner knows only its distribution. Denote by $\boldsymbol{y}(c) \in [a, c]$ the strategy of the Invader of type c. Then his payoff is given as follows:

$$\boldsymbol{v}_I^c(x, \boldsymbol{y}(c)) = (1 - P(x, \boldsymbol{y}(c)))U(\boldsymbol{y}(c)) \\ - FP(x, \boldsymbol{y}(c)) - C_I(\boldsymbol{y}(c)). \quad (3)$$

The payoff to the Scanner is the expected payoff taking into account the *type* of Invader:

$$\boldsymbol{v}_S^E(x, \boldsymbol{y}) = (1 - q_0)v_S(x, a) + q_0 \int_a^b q(c)v_S(x, \boldsymbol{y}(c))\, dc \quad (4)$$

with $v_S(x, \boldsymbol{y}(c))$ given by Eq. (2).

Here we look for Bayesian equilibrium [34], i.e., for such couple of strategies $(x_*, \boldsymbol{y}_*)$ that for any $(x, \boldsymbol{y})$ the following inequalities hold:

$$\boldsymbol{v}_S^E(x, \boldsymbol{y}_*) \leq \boldsymbol{v}_S^E(x_*, \boldsymbol{y}_*), \\ \boldsymbol{v}_I^c(x_*, \boldsymbol{y}(c)) \leq \boldsymbol{v}_I^c(x_*, \boldsymbol{y}_*(c)), c \in \text{supp}(q), \quad (5)$$

with $\text{supp}(q) = \{c \in [a, b] : q(c) > 0\}$.

We assume that the Scanner and the Invader know (as in the case with complete information) the parameters F, C_I, C_S, V, U, a, b as well as the probabilities $q(c)$ ($c \in [a, b]$) and q_0.

III. Equilibrium strategies for the first game

In the following theorem we give the equilibrium strategies for the first game (thus, maxmin scanning algorithm) for fixed bound width of the rivals.

Theorem 1: In the first game with fixed width to scan x and to invade y, the rivals employ a uniform tiling behavior. Namely,

(a) Let $1 - (x + y)M \leq y$ with

$$M = \lfloor 1/(x + y) \rfloor, \tag{6}$$

where $\lfloor \xi \rfloor$ is the greatest integer less or equal to ξ. Then the Scanner and the Invader will, with equal probability $1/M$, employ a band of the set A_{-S} and A_{-I} correspondingly.

(b) Let $1 - (x + y)M > y$. Then the Scanner and the Invader will, with equal probability $1/(M + 1)$, employ a band of the set A_{+S} and A_{+I} correspondingly, where

$$
\begin{aligned}
A_{-S} &= \{[k(x+y) - x, k(x+y)], k = 1, ..., M\}, \\
A_{-I} &= \{[k(x+y) - y - \epsilon(M+1-k), k(x+y) - \epsilon(M-k)], \\
&\quad k = 1, ..., M\}, \quad 0 < \epsilon < x/M, \\
A_{+S} &= A_{-S} \cup [1 - x, 1], \\
A_{+I} &= \{[(k-1)(x+y+\epsilon), (k-1)(x+y+\epsilon) + y], \\
&\quad k = 1, ..., M\} \cup [1 - y, 1], \quad 0 < \epsilon < \frac{1 - y - M(x+y)}{M - 1}.
\end{aligned}
$$

The value of the game (detection probability) $P(x, y)$ is given as follows:

$$
P(x, y) = \begin{cases} 1/M, & 1 - (x+y)M \leq y, \\ 1/(M+1), & 1 - (x+y)M > y. \end{cases} \tag{7}
$$

IV. Equilibrium strategy for the second game

In this section, which is split into five subsections, we find the equilibrium strategies for the second game explicitly. First, in Subsection IV-A we linearize our model to get an explicit solution, then in Subsection IV-B the best response strategies are given, and they are employed in Subsections IV-C and IV-D to construct equilibrium strategies for known and unknown Invader's technical characteristics correspondingly.

A. Linearized model

In order to get an insight into the problem, we consider a situation where the detection's probability $P(x, y)$ for $x, y \in [a, b]$ is approximated by a linear function as follows:

$$P(x, y) = x + y. \tag{8}$$

Thus, Eq. (7) and Eq. (8) coincide for $x + y = 1/n, n = 2, 3, ...$ We assume that the scanning and intrusion cost as well as the Invader's and Scanner's utilities are linear in the bandwidth involved, i.e., $C_S(x) = C_S x$, $C_I(y) = C_I y$, $U(y) = Uy$, $V(y) = Vy$ where $C_S, C_I, U, V > 0$. Then the payoffs to the Invader and the Scanner, if they use strategies $x \in [a, b]$ and $y \in [a, c]$ ($\boldsymbol{y}(c) \in [a, c]$) respectively, become:

(i)   For the known Invader's reward:

$$
\begin{aligned}
v_I(x, y) &= U(1 - x - y)y - F(x + y) - C_I y, \\
v_S(x, y) &= F(x + y) - Vy(1 - x - y) - C_S x,
\end{aligned}
$$

(ii)   For the unknown Invader's reward and technical characteristics:

$$
\begin{aligned}
\boldsymbol{v}_I^c(x, \boldsymbol{y}(c)) &= U(1 - x - \boldsymbol{y}(c))\boldsymbol{y}(c) \\
&\quad - F(x + \boldsymbol{y}(c)) - C_I \boldsymbol{y}(c), \ \text{for } c \in \text{supp}(q), \\
\boldsymbol{v}_S^E(x, \boldsymbol{y}) &= q_0 \int_a^b \Big[F(x + \boldsymbol{y}(\xi)) \\
&\quad - V\boldsymbol{y}(\xi)(1 - x - \boldsymbol{y}(\xi)) \Big] q(\xi) \, d\xi \\
&\quad + (1 - q_0)\Big(F(x + a) - Va(1 - x - a) \Big) - C_S x.
\end{aligned}
$$

Note that linearized payoffs have found extensive usage for a wide array of problems in wireless networks [36], [38], [39], [40], [41]. Of course, such an approach simplifies the original problem and only gives an approximated solution. Meanwhile, it can also be very useful: sometimes it allows one to obtain a solution explicitly, and allows one to look inside of the structure of the solution as well as the correlation between parameters of the system.

B. The best response strategies

In this section, we give the best response strategies for the Scanner and the Invader when the Invader's reward and technical characteristics are unknown, i.e., such strategies that $\text{BR}_S^E(\boldsymbol{y}) = \arg\max_x v_S^E(x, \boldsymbol{y})$ and $\text{BR}_I^c(x) = \arg\max_{\boldsymbol{y}(c)} v_I^c(x, \boldsymbol{y}(c))$.

Theorem 2: In the second step of the considered game with unknown Invader's reward and technical characteristics the Scanner and the Invader have the best response strategies $\text{BR}_S^E(\boldsymbol{y})$ and $\text{BR}_I^c(x)$ given as follows:

$$
\text{BR}_S^E(\boldsymbol{y}) = \begin{cases} a, & \bar{\boldsymbol{y}} < R_{q_0}, \\ \text{any from } [a, b], & \bar{\boldsymbol{y}} = R_{q_0}, \\ b, & \bar{\boldsymbol{y}} > R_{q_0}, \end{cases} \tag{9}
$$

$$
\text{BR}_I^c(x) = \begin{cases} c, & c \leq L(x), \\ L(x), & a < L(x) < c, \\ a, & L(x) \leq a \end{cases} \tag{10}
$$

with

$$
\begin{aligned}
L(x) &= \frac{T - x}{2}, \\
T &= \frac{U - F - C_I}{U}, \\
R &= \frac{C_S - F}{V}, \\
R_{q_0} &= \frac{C_S - F - (1 - q_0)Va}{q_0 V} = \frac{R - a(1 - q_0)}{q_0}
\end{aligned} \tag{11}
$$

and

$$\bar{\boldsymbol{y}} = \int_a^b q(\xi)\boldsymbol{y}(\xi) \, d\xi.$$

C. Equilibrium strategies: the unknown Invader's reward and technical characteristics

The equilibrium for the game exists since the payoff to the Scanner is linear in x and the payoff to the Invader of type c is concave in $\boldsymbol{y}(c)$. The equilibrium can be found by Eq. (5) as a couple of strategies $(x, \boldsymbol{y})$ which are the best response to each other, i.e., $x = \mathrm{BR}_S^E(\boldsymbol{y})$ and $\boldsymbol{y}(c) = \mathrm{BR}_I^c(x)$, $c \in [a, b]$ and such a solution always exists and is unique as shown in the following theorem.

Theorem 3: The considered second game with unknown Invader's reward and technical characteristics has unique Bayesian equilibrium $(x, \boldsymbol{y})$, and it is given as follows:

$$
x = \begin{cases} b, & R_{q_0} \leq \overline{\mathbf{BR}}_I(b), \\ \overline{\mathbf{BR}}_I^{-1}(R_{q_0}), & \overline{\mathbf{BR}}_I(b) < R_{q_0} < \overline{\mathbf{BR}}_I(a), \\ a, & \overline{\mathbf{BR}}_I(a) \leq R_{q_0}, \end{cases}
$$

$$
\boldsymbol{y}(c) = \begin{cases} \mathrm{BR}_I^c(b), & R_{q_0} \leq \overline{\mathbf{BR}}_I(b), \\ \mathrm{BR}_I^c\left(\overline{\mathbf{BR}}_I^{-1}(R_{q_0})\right), & \overline{\mathbf{BR}}_I(b) < R_{q_0} < \overline{\mathbf{BR}}_I(a), \\ \mathrm{BR}_I^c(a), & \overline{\mathbf{BR}}_I(a) \leq R_{q_0}, \end{cases}
$$

$$(12)$$

where $c \in \mathrm{supp}(q)$ with

$$
\overline{\mathbf{BR}}_I(x) = \int_a^b q(\xi) \mathrm{BR}_I^\xi(x)\, d\xi \tag{13}
$$

and $\overline{\mathbf{BR}}_I^{-1}(x)$ is inverse function to $\overline{\mathbf{BR}}_I(x)$, i.e., $\overline{\mathbf{BR}}_I^{-1}\left(\overline{\mathbf{BR}}_I(x)\right) = x$.

D. Equilibrium strategies: the known Invader's technical characteristics and unknown reward

The equilibrium for the second game with complete information about the technical characteristics of the Invader and unknown reward can be presented explicitly as follows:

Theorem 4: Let the Invader's technical characteristics be known but his reward can be unknown. This second game has unique Nash equilibrium, and it is given by Table I.

Note that the Scanner's and Invader's equilibrium strategies can have sudden jumps (discontinuities) as one continuously varies the fine F and probability q_0 that the Invader's reward related bandwidth used. It is caused by the fact that R_{q_0} depends on these parameters, while L depends only on F. For example, (i_1)-(i_6) implies that the Invader's equilibrium strategy can jump while probability q_0 varies, and (i_2) and (i_6) yield about the possibility of such a jump by fine F. The possibility of jumps for the Scanner's equilibrium strategy follows from (i_2) and (i_5).

V. NUMERICAL ILLUSTRATIONS

As a numerical illustration of the scenario with complete information on the Invader's technical characteristics, we consider $U = V = 1$, $a = 0.01$, $b = 0.3$, $C_S = 0.4$, $C_I = 0.1$ and q is the uniform distribution in $[a_0, b_0] = [a + (b-a)/10, b] = [0.039, 0.3]$. Figure 1 demonstrates the Scanner's equilibrium strategy and payoff as functions of

the fine $F \in [0.1, 0.4]$ and the probability $q_0 \in [0.01, 0.99]$ that the Invader's reward related to bandwidth used. Increasing fine F and probability q_0 makes the Scanner employ a larger band and impacts the Scanner's payoff in a multi-directional way, namely, it increases F and decreases q_0. This is caused by the fact that the Invader, who wants to minimize his detection probability, causes less damage to the network than the one who benefits from using a larger bandwidth.

Figures 2 and 3 illustrate the Invader's equilibrium strategy and payoff if his reward is related to the bandwidth used for $c = a_0$ and $c = b_0$ respectively. Figure 4 demonstrates corresponding detection probabilities. The Invader of type $c = a_0$ employs a constant strategy $y(c) = a_0$ independent of the fine F and probability q_0. The Invader's payoff and detection probability vary in opposite directions while fine F and probability q_0 are increasing, namely, the Invader's payoff is decreasing, while the detection probability is increasing, since it also makes the Scanner to employ a larger bandwidth. What is interesting is that the Invader's payoff experiences a sudden drop and the detection probability experiences a sudden jump due to the Scanner's behaviour, who alters his strategy by a sudden jump at threshold values. For the Invader with a reward un-related to the bandwidth used, the payoff and detection behave similarly but with some shift since such an Invader also employs a constant strategy $y = a$ (Figure 5). The Invader of type $c = b_0$ uses a strategy depending on fine F and probability q_0. Increasing fine F and probability q_0 makes the Invader employ a smaller bandwidth and reduces his payoff. What is interesting that his detection probability is not monotonous by fine F and probability q_0 and increasing fine F and probability q_0 could even reduce the detection probability. It can be explained that at the threshold values of fine F and probability q_0 the Scanner already gets the upper band, while the Invader still does not get to the lower band, and further increasing of the fine and probability leads to continuous decreasing of the detection probability due to the smaller bandwidth employed by the Invader.

VI. DISCUSSION

In this paper, we suggest a simple model for designing a maxmin scanning algorithm for detection of an Invader with incomplete information about the Invader's reward and technical characteristics and we find the optimal parameters (width of bandwidth to scan) for this algorithm. We have shown that this optimal width essentially depends on the network's and agent's characteristics and under some conditions a small variation of network parameters and fine could lead to jump changes in the optimal strategies, as well as in the payoffs of the rivals. This mixture between continuous and discontinuous behavior of the Invader under the influence of fine implies that the network provider has to carefully make a value judgement: some threshold values of fine could have a huge impact on

Case	Condition	Condition	x	y	P_R	P_U
i_1	$R_{q_0} < a$	$L(b) < a$	b	a	$a + b$	$2a$
i_2	$R_{q_0} < a$	$a \leq L(b) \leq c$	b	$L(b)$	$b + L(b)$	$b + a$
i_3	$R_{q_0} < a$	$c < L(b)$	b	c	$b + c$	$b + a$
i_4	$c < R_{q_0}$	$L(a) < a$	a	a	$2a$	$2a$
i_5	$c < R_{q_0}$	$a \leq L(a) \leq c$	a	$L(a)$	$a + L(a)$	$2a$
i_6	$c < R_{q_0}$	$c < L(a)$	a	c	$a + c$	$2a$
i_7	$a \leq R_{q_0} \leq c$	$L(b) \leq R_{q_0} \leq L(a)$	$L^{-1}(R_{q_0})$	R_{q_0}	$L^{-1}(R_{q_0}) + R_{q_0}$	$L^{-1}(R_{q_0}) + a$
i_8	$a \leq R_{q_0} \leq c$	$L(a) \leq a$	a	a	$2a$	$2a$
i_9	$a \leq R_{q_0} \leq c$	$a < L(a) < R_{q_0}$	a	$L(a)$	$a + L(a)$	$2a$
i_{10}	$a \leq R_{q_0} \leq c$	$c < L(b)$	b	c	$b + c$	$b + a$
i_{11}	$a \leq R_{q_0} \leq c$	$R_{q_0} < L(b) < c$	b	$L(b)$	$b + L(b)$	$b + a$

TABLE I

THE EQUILIBRIUM STRATEGIES (x, y) WITH $L^{-1}(R_{q_0}) = T - 2(C_S - F - (1 - q_0)V)/(q_0V)$ AND P_R AND P_U ARE DETECTION PROBABILITIES OF THE INVADER WITH REWARD RELATED AND UN-RELATED TO THE BANDWIDTH USED.
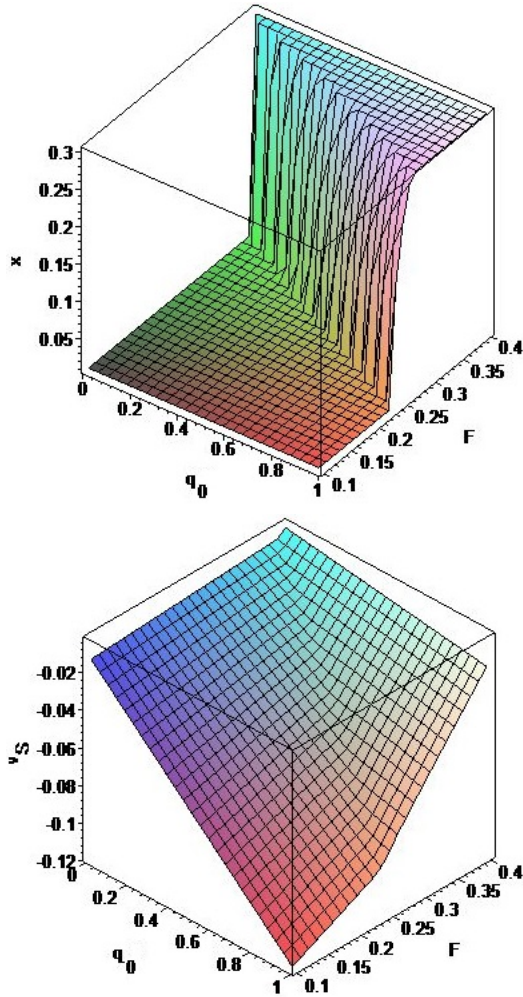

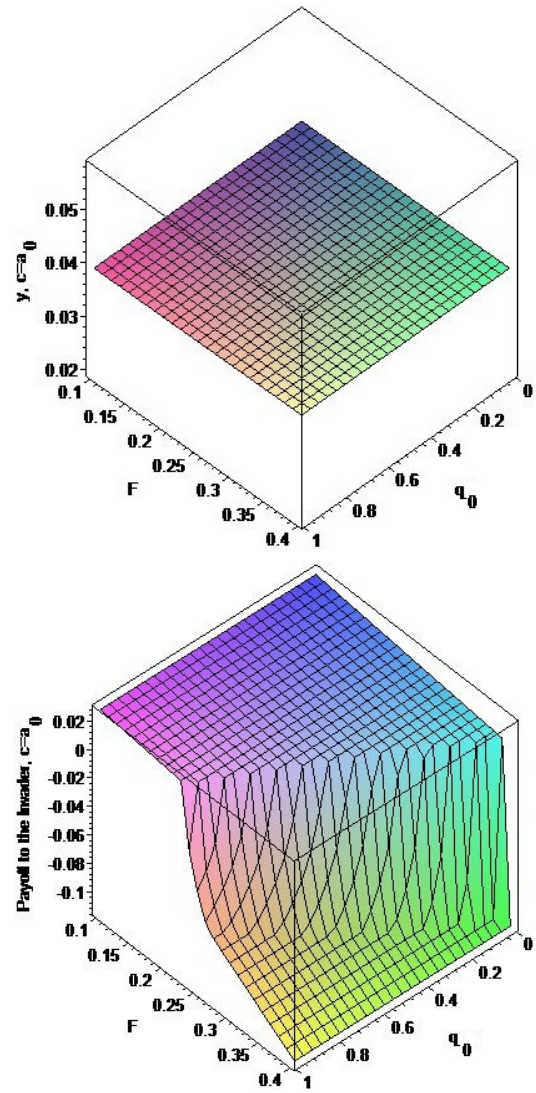Fig. 1. Equilibrium strategy x (upper) and payoff (bottom) to the Scanner.

Fig. 2. Equilibrium strategy y (upper) and payoff (bottom) to the Invader for $c = a_0$.
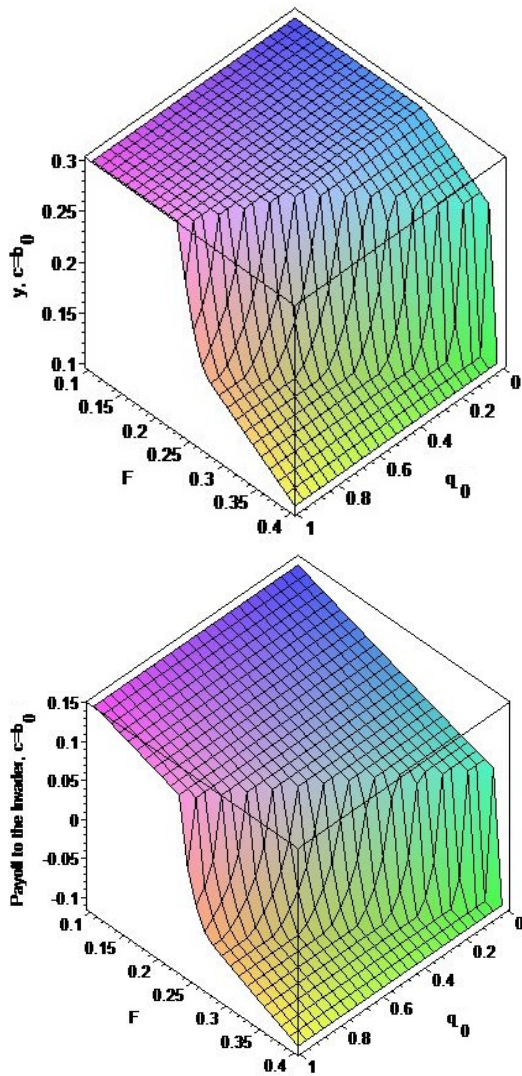
Fig. 3. Equilibrium strategy y (upper) and payoff (bottom) to the Invader for $c = b_0$.

Fig. 4. Detection probability of the Invader with $c = a_0$ (upper) and $c = b_0$ (bottom).

the Invader, while in the other situations a small increase will have a minimal impact on the strategies used. A goal for our future investigation is to investigate the non-linearized detection probability. Also, we intend to extend our model to the case of multi-step scanning algorithms with learning.

VII. APPENDIX

A. Proof of Theorem 1

Suppose that the Invader uses a band B_I with width y and the Scanner with equal probability employ a band from the set A_{-S} (A_{+S}) for $1 - (x + y)M \leq y$ (for $1 - (x + y)M > y$). The intervals composing A_{-S} and A_{+S} are separated from each other by at most y. So, at least one band from A_{-S} for $1 - (x + y)M \leq y$ and from A_{+S} for $1 - (x + y)M > y$ intersects with B_I. So, detection probability is greater or equal to $1/M$ for $1 - (x+y)M \leq y$
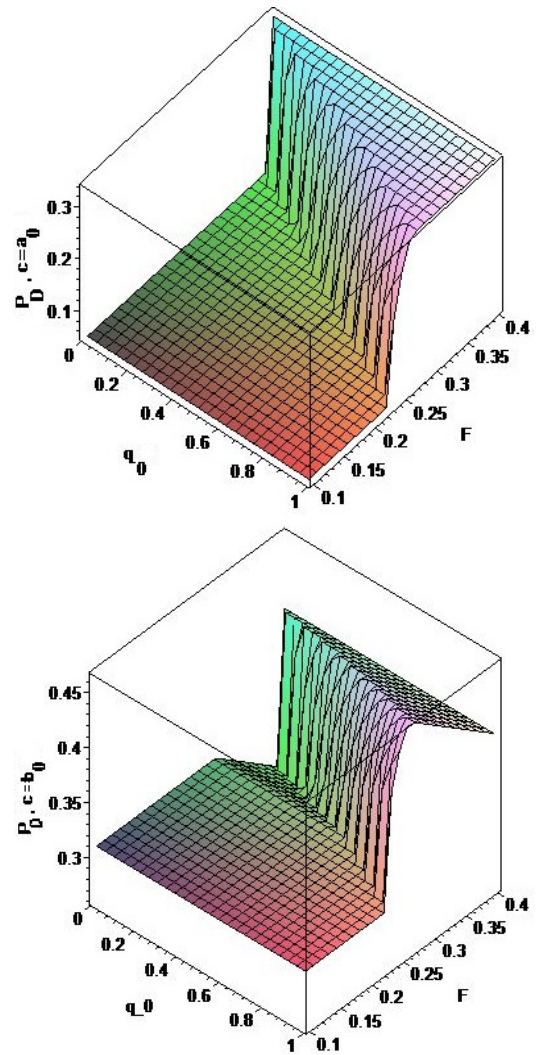
and it is is greater or equal to $1/(M+1)$ for $1 - (x+y)M > y$.

Suppose that the Scanner uses a band B_S with width x and the Invader with equal probability employ a band from the set A_{-I} (A_{+I}) for $1 - (x + y)M \leq y$ (for $1 - (x + y)M > y$). The intervals composing A_{-I} and A_{+I} are separated from each other by more that x. So, at most one band from A_{-I} for $1 - (x + y)M \leq y$ and from A_{+I} for $1 - (x + y)M > y$ intersects with B_S. So, detection probability is less or equal to $1/M$ for $1 - (x + y)M \leq y$ and it is is less or equal to $1/(M+1)$ for $1 - (x+y)M > y$ and the result follows. ∎
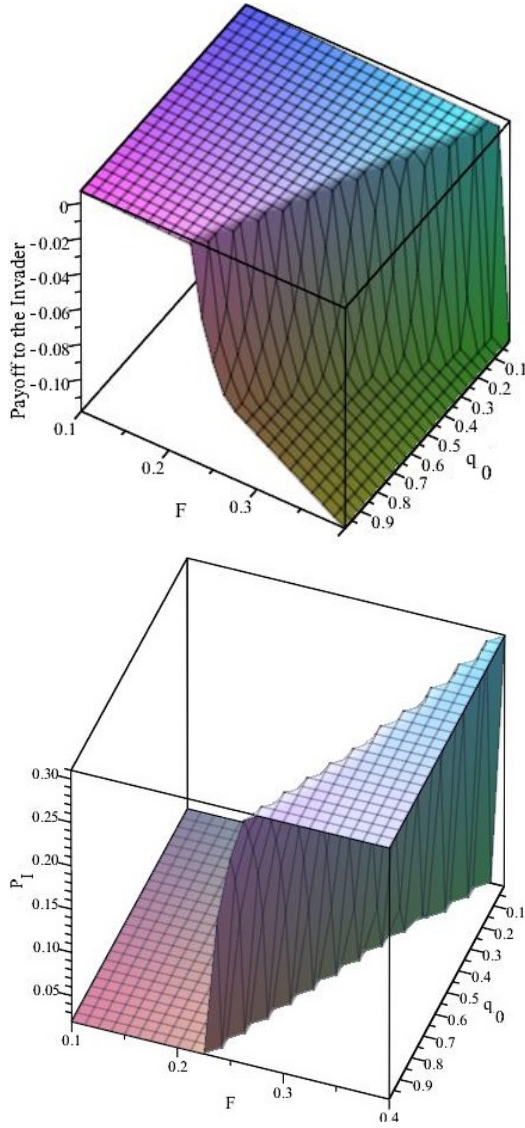
Fig. 5. Payoff (upper) and detection probability (bottom) of the Invader with reward un-related to the bandwidth used.

Appendix

Note that

$$\boldsymbol{v}_S^E(x, \boldsymbol{y}) = \left(F - C_S + q_0 V \bar{\boldsymbol{y}} + (1 - q_0) V a\right) x$$

$$+ q_0 \left[(F - V)\bar{\boldsymbol{y}} + V \int_a^b \boldsymbol{y}^2(\xi) q(\xi) \, d\xi \right]$$

$$+ (1 - q_0)(F - V + V a)a.$$

So, for a fixed $\boldsymbol{y}$ the payoff $\boldsymbol{v}_S^E(x, \boldsymbol{y})$ is linear on x. Thus, $\mathrm{BR}_S^E(\boldsymbol{y}) = \arg\max_x \boldsymbol{v}_S^E(x, \boldsymbol{y})$ is defined by sign of $F - C_S + q_0 V \bar{\boldsymbol{y}} + (1 - q_0) V a$ as it is given by (9).

Note that, the Invader's payoff has the following form:

$$\boldsymbol{v}_I^c(x, \boldsymbol{y}(c)) = (U(1 - x) - F - C_I)\boldsymbol{y}(c) - U\boldsymbol{y}^2(c) - xF.$$

So, for a fixed x the payoff $\boldsymbol{v}_I^c(x, \boldsymbol{y}(c))$ is a concave quadratic polynomial on $\boldsymbol{y}(c)$ getting its absolute maximum at $\boldsymbol{y}(c) = (U(1 - x) - F - C_I)/(2U)$. Thus, the

maximum of $\boldsymbol{v}_I^c(x, \boldsymbol{y}(c))$ by $\boldsymbol{y}(c)$ within $[a, c]$ is reached either on its bounds $\boldsymbol{y}(c) = a$ and $\boldsymbol{y}(c) = c$ or at $\boldsymbol{y}(c) = (U(1 - x) - F - C_I)/(2U)$ if it belongs to $[a, c]$ as it is given by (10). ∎

A. Proof of Theorem 3

First note that $(x, \boldsymbol{y})$ is a Nash equilibrium if and only if it is a solution of equations $x = \mathrm{BR}_S^E(\boldsymbol{y})$ and $\boldsymbol{y}(c) = \mathrm{BR}_I^c(x)$, $c \in [a, b]$ with $\mathrm{BR}_S^E(\boldsymbol{y})$ and $\mathrm{BR}_I^c(x)$ given by Theorem 2.

By (11) we have that (9) in equilibrium point is equivalent to

$$x = \begin{cases} a, & \overline{\mathbf{BR}}_I(x) < R_{q_0}, \\ \text{any from } [a, b], & \overline{\mathbf{BR}}_I(x) = R_{q_0}, \\ b, & \overline{\mathbf{BR}}_I(x) > R_{q_0} \end{cases} \quad (14)$$

with $\overline{\mathbf{BR}}_I(x)$ given by (13).

Note that $\overline{\mathbf{BR}}_I(x)$ is non-increasing on x. Thus, if $\overline{\mathbf{BR}}_I(a) < R_{q_0}$, then $\overline{\mathbf{BR}}_I(x) < R_{q_0}$ for any x and (14) yields that x has to be equal to a. If $\overline{\mathbf{BR}}_I(b) > R_{q_0}$, then $\overline{\mathbf{BR}}_I(x) > R_{q_0}$ for any x and (14) yields that x has to be equal to b. If $\overline{\mathbf{BR}}_I(b) \le R_{q_0} \le \overline{\mathbf{BR}}_I(a)$ then $x = \overline{\mathbf{BR}}_I^{-1}(R_{q_0})$ and the result follows. ∎

B. Proof of Theorem 4

For the situation with complete information of the Invader's technical characteristics the best response strategies turn into

$$\mathrm{BR}_S(y) = \begin{cases} a, & y < R_{q_0}, \\ \text{any from } [a, b], & y = R_{q_0}, \\ b, & y > R_{q_0}, \end{cases} \quad (15)$$

$$\mathrm{BR}_I(x) = \begin{cases} a, & L(x) \le a, \\ L(x), & a < L(x) < c, \\ c, & c \le L(x) \end{cases}$$

$$= \begin{cases} a, & x \le T - 2c, \\ L(x), & T - 2c < x < T - 2a, \\ c, & T - 2a \le x. \end{cases} \quad (16)$$

Thus, the equilibrium can be described as an intersection of the best response curves (Figure 6). Such intersection always exists.

Let $a > R_{q_0}$. By (15), $\mathrm{BR}_S(y) \equiv b$. This, jointly with (16), implies (i_1)-(i_3).

Let $R_{q_0} > c$. By (15), $\mathrm{BR}_S(y) \equiv a$. Then, (16) implies (i_4)-(i_6).

Let $a \le R_{q_0} \le c$. First note $L(x)$ is linear decreasing function from $L(a)$ for $x = a$ to $L(b)$ for $x = b$.

(a) Let $L(b) \le R_{q_0} \le L(a)$. Then the equation $L(x) = R_{q_0}$ has the unique root within $[a, b]$. Thus, (15) and (16) yield (i_7).
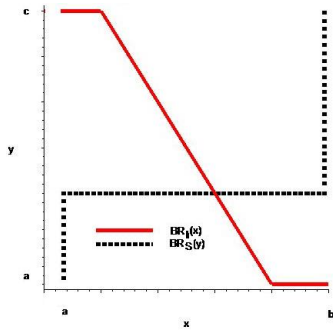
Fig. 6. The Nash equilibrium as an intersection of the best response curves

    (b)   Let $L(a) \leq R_{q_0}$. Then, $L(x) < R_{q_0}$ for $x \in (a, b]$. So, by (16), $BR_I(x) < c$ for $x \in [a, b]$. Besides, by the assumption, the equation $L(x) = R_{q_0}$ does not has root in $[a, b]$. Thus, by (15), $BR_S(y) \equiv a$. So, (16) implies (i_8) and (i_9).

    (c)   Let $R_{q_0} < L(b)$. Then $L(x) > R_{q_0}$ for $x \in [a, b)$. Thus, by (16), $BR_I(x) > a$ for $x \in [a, b]$. Besides, by the assumption, the equation $L(x) = R_{q_0}$ does not has root in $[a, b]$. So, by (15), $BR_S(y) = b$, and, (16) implies (i_{10}) and (i_{11}).

∎

REFERENCES

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, 2005.

[2] J. Mitola, "Cognitive radio: brain-empowered wireless communications," in *Proceedings of IEEE International Workshop on Mobile Multimedia Communications (MoMuC '99)*, pp. 3–10, 1999.

[3] I.F. Akyildiz, W.Y. Lee, M.C. Vuran, and S. Mohanty, "Next generation /dynamic spectrum access/ cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, pp. 2127–2159, 2006.

[4] B.A. Fette, *Cognitive radio technology*. Burlington, MA: Academic Press, 2009.

[5] S. Liu, Y. Chen, W. Trappe, and L.J. Greenstein, "ALD: An anomaly detection framework for dynamic spectrum access networks," in *Proceedings of IEEE INFOCOM 2009*, pp. 675–683, 2009.

[6] S. Verdu, *Multiuser detection*. Boston, MA: Cambridge University Press, 1998.

[7] H. V. Trees, *Detection, Estimation, and Modulation Theory, Radar-Sonar Signal Processing and Gaussian Signals in Noise*. Wiley-Interscience, 2004.

[8] F.F. Digham, M.S. Alouini, and M.K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Transactions on Communications*, vol. 55, pp. 21–24, 2007.

[9] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, pp. 523–531, 1967.

[10] A. Garnaev, W. Trappe, and C.-T. Kung, "Dependence of optimal monitoring strategy on the application to be protected," in *Proceedings of 2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 1054–1059, 2012.

[11] A. Garnaev and W. Trappe, "To eavesdrop or jam, that is the question," in *Proceedings of ADHOCNETS 2013* (M. Sherif and et al., eds.), vol. 129 of *LNICST*, pp. 146–161, Springer, 2014.

[12] A. Garnaev, W. Trappe, and C.-T. Kung, "Optimizing scanning strategies: Selecting scanning bandwidth in adversarial RF environments," in *Proceedings of the 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWN-COM)*, pp. 148–153, 2013.

[13] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless Ad Hoc networks," in *Proceedings of the 2006 Workshop on Game Theory for Communications and Networks*, pp. 1–12, 2006.

[14] A. Agah, S.K. Das, K. Basu, and M. Asadi, "A Bayesian game approach for intrusion detection in wireless Ad Hoc networks," in *Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA 2004)*, pp. 243–346, 2004.

[15] A. Garnaev, M. Baykal-Gursoy, and H.V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 1278–1287, 2014.

[16] Z. Han, N. Marina, M. Debbah, and A. Hjrungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP Journal on Wireless Communications and Networking*, 2009. Article ID 452907.

[17] E. Altman, K. Avrachenkov, and A. Garnaev, "Fair resource allocation in wireless networks in the presence of a jammer," *Performance Evaluation*, vol. 67, pp. 338–349, 2010.

[18] G. He, M. Debbah, and E. Altman, "k-player Bayesian waterfilling game for fading multiple access channels," in *Proceedings of the 3rd IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP 2009)*, pp. 17–20, 2009.

[19] T. Heikkinen, "A minmax game of power control in a wireless network under incomplete information," Tech. Rep. 99–43, DIMACS, New Brunswick, NJ, 1999.

[20] S. Jean and B. Jabbari, "Bayesian game-theoretic modeling of transmit power determination in a self-organizing CDMA wireless network," in *Proceedings of 60th IEEE Vehicular Technology Conference (VTC)*, vol. 5, pp. 3496–3500, 2004.

[21] S. Adlakha, R. Johari, and A. Goldsmith, "Competition in wireless systems via bayesian inference games." http://arxiv.org/abs/0709.0516, 2007.

[22] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proceedings of IEEE CDC 2003*, pp. 2595–2600, 2003.

[23] K.C. Nguyen, T. Alpcan, and T. Basar, "Security games with incomplete information," in *Proceedings of IEEE ICC 2009*, pp. 1–6, 2009.

[24] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks: The case of several jammers," in *Proceedings of International Conference on Game Theory for Networks (GameNets '09)*, pp. 585–592, 2009.

[25] S.N. Hamilton, W.L. Miller, A. Ottand, and O.S. Saydjari, "Challenges in applying game theory to the domain of information warfare," in *Proceedings of ISW 2002*, pp. 1–6, 2002.

[26] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proceedings of HICSS 2010*, pp. 1–10, 2010.

[27] A. Garnaev, G. Garnaeva, and P. Goutal, "On the infiltration game," *International journal of game theory*, vol. 26, pp. 215–221, 1997.

[28] C. Comaniciu, N.B. Mandayam, and H.V. Poor, *Wireless Networks Multiuser Detection in Cross-Layer Design*. New York: Springer, 2005.

[29] V.J. Baston and A.Y. Garnaev, "A search game with a protector," *Naval Research Logistics*, vol. 47, no. 2, pp. 85–96, 2000.

[30] A. Mukherjee and A.L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proceedings of MILCOM 2010*, pp. 1695–1700, 2010.

[31] Q. Zhu, W. Saad, Z. Han, H.V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: a game-theoretic approach," in *Proceedings of Military communications conference (MILCOM)*, pp. 119–124, 2011.

[32] L. Kong-wei and J. Wing, "Game strategies in network security,"

International journal of information security, vol. 4, pp. 71–86, 2005.

[33] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Survey*, vol. 45, no. 3, 2013.

[34] D. Fudenberg and J. Tirole, *Game theory.* Boston, MA: MIT Press, 1991.

[35] E. Altman, K. Avrachenkov, and A. Garnaev, "Taxation for green communication," in *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt 2010)*, pp. 108–112, 2010.

[36] Y.E. Sagduyu and A. Ephremidess, "A game-theoretic analysis of denial of service attacks in wireless random access," *Journal of Wireless Networks*, vol. 15, pp. 651–666, 2009.

[37] A. Garnaev, Y. Hayel, E. Altman, and K. Avrachenkov, "Jamming game in a dynamic slotted ALOHA network," in *Game Theory for Networks* (R. Jain and R. Kannan, eds.), vol. 75 of *LNICST*, pp. 429–443, Springer, 2012.

[38] E. Altman, K. Avrachenkov, and A. Garnaev, "Jamming in wireless networks under uncertainty," *Mobile Networks and Applications*, vol. 16, pp. 246–254, 2011.

[39] S.L. Kim, Z. Rosberg, and J. Zander, "Combined power control and transmission rate selection in cellular networks," in *Proceedings of 50th IEEE Vehicular Technology Conference (VTC)*, vol. 3, pp. 3 –10, 1999.

[40] I. Koo, J. Ahn, H.A. Lee, and K. Kim, "Analysis of Erlang capacity for the multimedia DS-CDMA systems," *IEICE Trans. Fundamentals*, vol. E82-A, no. 5, pp. 849–855, 1999.

[41] A. Garnaev and W. Trappe, "The eavesdropping and jamming dilemma in multi-channel communications," in *Proceedings of 2013 IEEE International Conference on Communications (ICC)*, pp. 753–757, 2013.