A Bandwidth Monitoring Strategy Under Uncertainty of the Adversary's Activity

Andrey Garnaev and Wade Trappe, *Fellow, IEEE*

***Abstract*— When an adversary illicitly uses spectrum that it is not authorized for, it does so with a purpose in mind, such as to download a file or perhaps engage in a real-time communication session. In this paper, we examine how the incorporation of knowledge related to an adversary's purpose can improve the effectiveness of spectrum scanning protocols. First, we study the difference in the thief's behavior when considering throughput and delay as the two primary QoS parameters he is concerned with. Through our analysis, we show that the detection probability of unlicensed access to spectrum resources depends on the application type. Knowledge of the application type can be incorporated to spectrum scanning to tune better it to detect the thief. To illustrate this, we examine two Bayesian games. In the first game, the scanner wants to minimize the time needed to detect the invader. In the second game, the scanner wants to maximize the detection probability at each time slot by adapting its belief regarding the adversary's activity. In particular, it is shown in the minimizing detection time game that the equilibrium strategies are continuous with respect to priori knowledge of the invader's activity. Meanwhile, for the maximizing detection probability game, the strategies can have a jump discontinuity. This phenomena can be explained as the difference between tactical and strategic decision making: tactical decision making allows short-term, unpredictable moves, while strategic decision making is inclined to predictable moves. Finally, since the bandwidth model used in this paper is general, the conclusion as well as the approach provided can be applied to a variety of different network protection problems.**

***Index Terms*— Intrusion detection, wireless networks, Bayes methods.**

I. Introduction

THE OPENNESS of the lower-layer protocol stacks will enable cognitive radios (CR) to be an appealing platform for dynamic spectrum access (DSA). In spite of the potential benefits of dynamic spectrum access, the rewards are only possible if entities participate properly in the use of such spectrum. Unfortunately, the exposure of a cognitive radio's protocol stacks to the public makes it possible for CR platforms to be utilized for irresponsible behavior by secondary users [1]. A misuse of a CR can significantly compromise the benefits of DSA and threaten the privileges of incumbent users. Therefore, having the ability to enforce spectrum policies is an essential component to guaranteeing the correct operation of DSA and spectrum leasing.

The detection of unauthorized usage of spectrum is basically a problem of distinguishing bad (unauthorized) transmissions from good (authorized) ones, and there have been numerous signal processing techniques proposed for detecting unauthorized signals in the presence of authorized transmissions. Distinguishing unknown signals based on power (or energy) measurements is not a trivial issue, as illustrated by the brief survey we provide: The issue of detecting unknown signals in noise was addressed in [2] and in [3] for unknown signals over fading channels. The spectrum anomaly detection problem in a broader context, where the authorized transmitter can be mobile within the sensing area, was investigated in [4]. Methods for detecting spread-spectrum signals without prior knowledge of the signal structure were surveyed in [5], and expanded to noise of uncertain power in [6]. Factors like the channel fluctuating due to temperature changes were considered in [7], while energy detection of a signal with random amplitudes was studied in [8] and the impacts posed by quantization and dynamic range differences were surveyed in [9].

The research literature has tended to only examine the problem from a statistical detection perspective and fails to address the objective behind the thief's goal in using unauthorized spectrum. The real-world thief attempts to use spectrum for a purpose, say, to download a file or perhaps to watch streaming video. Clearly, the performance metrics associated with the thief's objective, carefully weighed with his/her likelihood of being detected by a spectrum scanner, would have an impact on how aggressively the thief attempts to utilize unauthorized spectrum. Incorporating knowledge of thief's objectives should also be leveraged by a spectrum scanner to improve detection performance. These simple and intuitive observations are generally lost in the formulations of DSA and the detection-theoretic formulations associated with identifying adversarial behavior.

In [10], a simple model was suggested with throughput and transmission delay as the Invader's utilities, and showed that the detection probability might depend on the type of Invader activity, such as whether the connection has delay constraints or not. Additionally, a scanning algorithm for a single time slot was developed to show that incorporating a pri-

Manuscript received April 29, 2015; revised October 2, 2015; accepted December 9, 2015. Date of publication December 22, 2015; date of current version February 1, 2016. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Negar Kiyavash.

A. Garnaev is with the Wireless Information Network Laboratory, Rutgers University, North Brunswick, NJ 08901 USA, and also with the Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University, Saint Petersburg 198504, Russia (e-mail: garnaev@yahoo.com).

W. Trappe is with the Department of Electrical and Computer Engineering, Rutgers University, Piscataway, NJ 08854-8058 USA, and also with the Wireless Information Network Laboratory, Rutgers University, North Brunswick, NJ 08901 USA (e-mail: trappe@winlab.rutgers.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2510959

ori knowledge of such activities could improve the efficiency of scanning efforts. The objective of this paper is to show how this knowledge could be incorporated into multi-time slot scanning strategies. To deal with this objective, two related problems of dynamic scanning are presented and solved. In the first problem, the Scanner wants to maximize the detection probability at each time slot by adapting its belief regarding the adversary's activity. In the second problem, the Scanner wants to minimize the time needed to detect the Invader. Solution of these problems, beyond improving the efficiency of scanning strategies, also gives an insight into the difference between tactical and strategic decision making associated with network protection. Finally note, that to keep presentation of this paper comprehensive, we briefly discuss the model presented in [10] to illustrate that detection probability might depend on the type of Invader's activity. Also, we have modified the proof of optimality for single time slot strategies to obtain their monotonicity properties. These properties have been applied to prove the convergence of the learning algorithm we present in this paper.

We note that, in the intrusion/scanning problem we consider, there are two agents having different goals associated with the set of frequency bands. Namely, the first agent is an IDS (Intruder Detection System, called the *Scanner*), who aims to detect illegal usage of spectrum. The second agent is the adversary (called the *Invader*) who intends to use the bandwidth illegally. Thus, the agent's goals are conflicting, and game theory is a proper framework for examining the problem, and hence we formulate a game between these two agents: the Scanner and the Invader. In [11] and [12], readers can find a structured and comprehensive survey of research contributions that analyze and solve security and privacy problems in computer networks and security systems. Here, as examples of game-theoretic approaches, we mention just a few such works: for modeling malicious users in collaborative networks [13], for adaptive packetized wireless communication [14], for attack-type uncertainty in a network [15], while the problem of fighting jamming with jamming was explored in [16]. A spectrum coexistence problem was investigated in [17]. The interactions between a user and a smart jammer regarding their respective choices of transmit power was explored in [18], while competitive interactions between a selfish secondary user transmitter-receiver pair and a jammer under incomplete knowledge of the jammer's location in the network was investigated in [19]. In [20] and [21] a tiling-based scanning algorithm (as well as an approach to find its optimal parameters) for detecting an intruder signal in a wide amount of bandwidth was proposed.

Because the information related to the intruder's goal is incomplete we apply a Bayesian approach, which is a powerful tool for updating the internal notion of an agent's knowledge related to another agent and allows us to update beliefs based on knowledge obtained during scanning. Bayesian approaches have been widely employed in dealing with different problems in networks, and notably have been used for devising intrusion detection mechanisms. For example, game theoretic models for decision and analysis in network intrusion detection were investigated in [22]. In [15], a problem of incorporating information related to different types of attack into a network protection strategy was studied. An intrusion detection problem in wireless ad hoc networks was explored in [23]. The impact of incomplete information regarding the other user's identities for the MAC layer networks being under DoS attacks was considered in [24]. A network's protection problem with unknown adversarial strategies was investigated in [25]. A problem where a jammer is unaware of the exact positions of the network nodes, but knows the prior distribution of their location was investigated in [26]. Anti-jamming strategy versus unknown type of low-power jamming attack was studied in [27].

The organization of this paper is as follows: in Section II, we first illustrate that the detection probability might depend on the application used. In Section III-A, we formulate a one shot maximizing detection probability (MaxDP) game (which is solved in closed form in Section V). In Section III-B, we formulate the minimizing detection time (MinDT) game (its explicit solution is given in Section IV). In Section VI, numerical illustrations comparing these solutions are presented. In Section VII, we deal with a problem regarding how the Scanner, to increase detection probability, can adapt its belief about the Invader's unlicensed activity if the adversary was not detected in the previous time slot. In Section VIII, conclusions are presented. Finally, in Appendix the proof of the obtained results is offered.

II. An Auxiliary Result: the Detection Probability Might Depend on the Application Used

In this section we study the unlicensed access of a user (called the secondary user *SU* or the adversary or the Invader) to a single band of spectrum that is owned by the primary user *PU*, who employs an IDS (called the Scanner) to scan/monitor the band with the purpose of detecting the intrusion. We have chosen to start with a single band to illustrate that the detection probability might depend on the application used by the Invader. In the next section we will show how this knowledge can be incorporated into the scanning protocol, first, with incomplete information about the application the Invader is using, and then how the Scanner can upgrade this information for further scanning if in the previous time slot the scanning failed.

The Invader may attempt to sneak usage of this single spectrum band for a variety of application purposes, e.g. file download/upload or streaming video to another recipient. These applications ultimately have different metrics associated with their success. To sneak usage the Invader applies a transmission power P. This activity is illegal from the viewpoint of the primary user. The Invader's satisfaction from illegally using this single band will be described by the Invader's utility function, U, which we assume depends on the signal-to-interference-ratio (SINR), as well as the type of application the Invader is engaged in. For example, the primary metric for data transmission might be throughput (which we shall quantify using the Shannon capacity for the channel), while for video streaming (particularly in the case of interactive video) the QoS metric of concern could be delay.

In our discussion, we shall use both of these two metrics for our analysis, though we note that similar formulations can hold for other utility functions. Thus, in this paper, we will be concerned with the following two choices for utility U. For Invader throughput we use

$$U(\text{SINR}) = W \ln(1 + \text{SINR}). \tag{1}$$

Since communication delay of a signal can be described as the time needed for its successful transmission, while throughput is the rate of successful signal delivery over a communication channel, the inverse value to throughput might be considered as an utility for communication delay:

$$U(\text{SINR}) = -\frac{1}{W \ln(1 + \text{SINR})}, \tag{2}$$

where the SINR for the Invader is given as follows:

$$\text{SINR} = \frac{hP}{W(\sigma^2 + g\overline{P})}. \tag{3}$$

Here, σ^2 is power for the underlying background noise, W is the bandwidth associated with the single band that the Invader is sneaking on, h is the channel gain associated with the channel from the Invader to its recipient, while g is the channel gain from the primary user transmitter to the Invader's recipient. $\overline{P}$ is power of the signal transmitted by the primary user. In all of the discussion that follows, we assume the values of g, h, σ^2, and $\overline{P}$ are known to the to the Invader. This assumption is easily plausible when communication systems involving transmitter-receiver feedback are employed (such feedback is common in cellular systems where downlink feedback is used to refine coding on uplink channels). Park and Wong [6] developed an information feedback scheme to approximately obtain the optimal training sequence set at the transmitter. Even without receiver feedback scheme, assuming isotropic noise conditions, the signal strength at the transmitter can be approximated by the assumption of channel reciprocity [28].

Unlicensed access to the network can be detected by the Scanner. For the sake of tractability, we assume that the detection probability depends on the SINR witnessed by the recipient of the Invader's transmission. We note that this assumption serves as a starting point for our discussion, and that this assumption is plausible since it is unlikely that the Invader would actually know the SINR at the Scanner, and hence the recipient's SINR acts as a proxy for the SINR at the Scanner. Further, we note that although detection is actually a function of SINR at the scanner, the scanner's SINR will be approximately proportional to the SINR at the Invader's recipient. For example, assuming simple quadratic pathloss in the environment, this proportionality would be the square of the ratio of the Invader-to-Scanner distance and the Invader-to-Recipient distance. Consequently, detection probability is a function $\gamma(\text{SINR})$ which is increasing in SINR such that $\gamma(0) = 0$ and $\gamma(\infty) = 1$. As a model case for detection probability we consider

$$\gamma(\text{SINR}) = 1 - \exp(-\alpha\,\text{SINR}) \tag{4}$$

with $\alpha > 0$ being the Scanner detection characteristics.

If the Invader is detected then he will be fined by F. Since we are focusing on *intrusion*, the Invader is not *paying* for access to the network, but he might instead be charged a fine F for violation if he is caught sneaking bandwidth. The payoff to the Invader is difference between the expected utility and expected fine. So, it is given as follows:

$$\upsilon_I(P) = (1 - \gamma(\text{SINR}))U(\text{SINR}) - F\gamma(\text{SINR}).$$

It is natural to assume that the Invader intrudes into the bandwidth if he can manage illegally to get acceptable quality of service. We can describe such quality by throughput or SINR. Say, the Invader might intrude into the bandwidth if his expected SINR is greater or equal to a threshold value ϵ, i.e.

$$\text{SINR} \geq \epsilon. \tag{5}$$

The Invader's objective is to find P maximizing his payoff $\upsilon_I(P)$ under condition (5).

The following theorem shows that the Invader's strategy as well as detection probability depend on the application he uses.

Theorem 1: The optimal power P^* for the Invader is given as follows:

$$P^* = \begin{cases} \dfrac{W(\sigma^2 + g\overline{P})}{h}\Psi^{-1}(F), & \Psi^{-1}(F) \geq \epsilon, \\ 0, & \Psi^{-1}(F) < \epsilon \end{cases}$$

with

$$\Psi(x) = \frac{1 - \gamma(x)}{\gamma'(x)}U'(x) - U(x). \tag{6}$$

The detection probability is given as follows:

$$\gamma^* = \begin{cases} \gamma(\Psi^{-1}(F)), & \Psi^{-1}(F) \geq \epsilon, \\ 0, & \Psi^{-1}(F) < \epsilon, \end{cases}$$

Since Ψ depends on the utility U and, so, on the application used by the Invader, then the detection probability also does these.

As a numerical illustration, we consider $W = 2$ and $\epsilon = 0.5$. Figures 1 and 2 illustrate SINR, detection probability and the Invader's payoff for both Invader utilities as a function of fine F and detection parameter α. It is quite natural that increasing fine F and improving detection's characteristics yields a reduction in malicious activity (which can be described by SINR) and the adversary's expected payoff for both utilities. Meanwhile the domain (α, F) of rejection from malicious activity (i.e., where SINR is equal to zero) essentially depends on the utility. For the delay utility it is drastically smaller than for the throughput utility. Increasing fine for both utilities leads to a slow reduction in detection probability due to the reduction in malicious activity. Increasing detection characteristics always leads to increasing the detection probability but only for the delay utility. For throughput utility, for a small fine the Invader deems it worthwhile to face the increasing probability detection, and only a large fine makes him reduce his activity to reduce his probability of being detected.

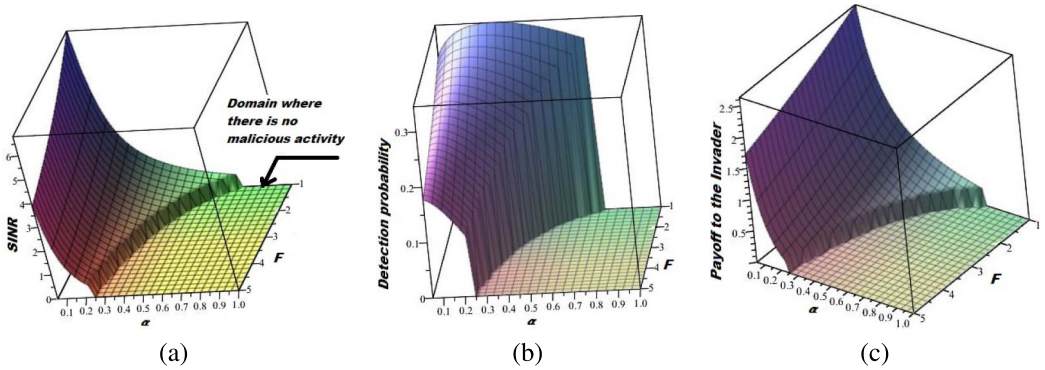


Fig. 1. (a) SINR, (b) detection probability, and (c) the Invader's payoff as functions of fine F and detection parameter α for throughput as the Invader's utility.

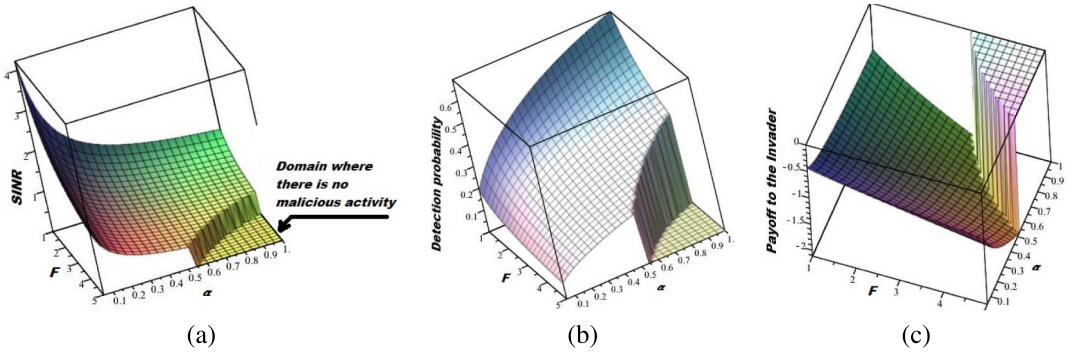


Fig. 2. (a) SINR, (b) detection probability, and (c) the Invader's payoff as functions of fine F and detection parameter α for delay as the Invader's utility.

III. Multiband Scanning With Incomplete Information on Adversary's Activity

In this section we relax the assumption of a single band. Namely, we assume that the PU owns n frequency bands $1, 2, \ldots, n$ of bandwidth W_1, W_2,..., W_n. These n bands will be scanned by the Scanner employed by the PU, and the Invader will only attempt to sneak usage on one of these bands in a single time slot. Then a natural question arises: what is the optimal strategy for sneaking (and, contrarily, the optimal strategy for scanning)? In particular, now note that by expanding the amount of opportunities for sneaking, we have increased the dimensionality associated with the interaction between the Invader and the Scanner.

As it was shown in Section II, the detection probability depends on the quality of the band being used (quantified by SINR) as well as the application the Invader attempts to use on that band.

We assume that the Invader can sneak usage of a band in support of an application of a specific type. The type of application cannot be chosen by the Invader, i.e. it is random (for example, it can be considered as chosen by nature). Namely, let with probability q^k the Invader sneaks to use application k, where $k = 1, 2$ (e.g., 1 for on-line video and 2 for data download). Let the detection probability be γ_i^k in band i for application k. We assume that the parameters of the network as well as probabilities q^k are known to the rivals. The Scanner does not know the application used by the Invader, while the Invader knows it. The action space

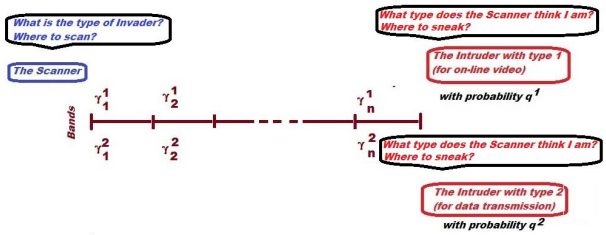


Fig. 3. The Scanner and the Invader.

(i.e. the set of (pure) strategies) for the rivals is the same, which is the set of bands $\{1, \ldots, n\}$ identified by indexes. With each application we associate an Invader type. Namely, we say that the Invader has type k, if he intends to sneak for using application k. Thus, the Scanner has to incorporate in its choice of which band to scan, the answer to the question - what is the type of Invader? The Invader has to incorporate in its choice of band to sneak, the answer to the question - what type does the Scanner think I am? (Figure3). To deal with this situation, a Bayesian approach will be applied.

A. Payoffs and Strategies for one Shot MaxDP Game

In this section we describe one shot MaxDP game, i.e., the game played in a single time slot, where the Scanner wants to maximize detection probability. For such a game the payoff to the Scanner if the Scanner chooses band i to scan, and the Invader, using application k, chooses band j to sneak is γ_i^k for

$i = j$, and it is zero otherwise. The payoff to the Invader, using application k is $1-\gamma_i^k$ for $i = j$, and it is 1 otherwise. Hence, we have a matrix Bayesian game ([29]), which generally it does not have equilibrium in pure strategies. To deal with this situation randomized (mixed) strategies have to be introduced. A (mixed) strategy for the Scanner is $\boldsymbol{S} = (S_1, \ldots, S_n)$, where S_i is the probability that he scans at band i. So, $\sum_{i=1}^n S_i = 1$ and $S_i \geq 0$, $i \in [1, n]$. A (mixed) strategy for the Invader using application k is $\boldsymbol{T}^k = (T_1^k, \ldots, T_n^k)$, where T_i^k is the probability that he sneaks in band i. So, $\sum_{i=1}^n T_i^k = 1$ and $T_i^k \geq 0$, $i \in [1, n]$.

If the Scanner and the Invader apply strategies $\boldsymbol{S}$ and $(\boldsymbol{T}^1, \boldsymbol{T}^2)$, the (expected) payoff to the Scanner, which is the detection probability, is given as follows:

$$v_S(\boldsymbol{S}, (\boldsymbol{T}^1, \boldsymbol{T}^2)) = \sum_{i=1}^n S_i \left(\sum_{k=1}^2 q^k \gamma_i^k T_i^k \right). \tag{7}$$

The payoff to the the Invader using application k is the probability of non-detection and it is given as follows:

$$v_I^k(\boldsymbol{S}, \boldsymbol{T}^k) = 1 - \sum_{i=1}^n S_i \gamma_i^k T_i^k. \tag{8}$$

Recall that $(\boldsymbol{S}_*, (\boldsymbol{T}_*^1, \boldsymbol{T}_*^2))$ is an (Bayesian) equilibrium if and only if the following inequalities hold for any strategies $(S, (T^1, T^2))$:

$$\begin{aligned} v_S(\boldsymbol{S}, (\boldsymbol{T}_*^1, \boldsymbol{T}_*^2)) &\leq v_S(\boldsymbol{S}_*, (\boldsymbol{T}_*^1, \boldsymbol{T}_*^2)), \\ v_I^k(\boldsymbol{S}_*, \boldsymbol{T}^k) &\leq v_I^k(\boldsymbol{S}_*, \boldsymbol{T}_*^k) \text{ with } k = 1, 2. \end{aligned} \tag{9}$$

Note that, since the payoff v_S is linear in $\boldsymbol{S}$, and the payoff v_I^k is linear in $\boldsymbol{T}^k$, the considered game has an equilibrium [29]. Also, if $q^m = 0$, then the Invader of type m has not to be taken into account, and the equilibrium strategies turn into equalizing the rival's payoffs. Namely, the following result holds.

Remark 1: If $q^m = 0$ then the game is a non-zero sum matrix game between the Scanner and the Invader of type k. Their equilibrium strategies coincide and are given as follows:

$$S_i = T_i^k = (1/\gamma_i^k)/(\sum_{j=1}^n (1/\gamma_j^k)) \text{ for } i \in \{1, \ldots, n\},$$

where $k = 2$ if $m = 1$ and $k = 1$ if $m = 2$.

The payoffs to the Scanner and to the Invader of type k are given as follows:

$$v_S = 1/(\sum_{j=1}^n (1/\gamma_j^k)) \quad \text{and } v_I^k = 1 - 1/(\sum_{j=1}^n (1/\gamma_j^k)).$$

B. Payoffs and Strategies for MinDT Game

In this section we describe the MinDT game, i.e., the above considered game played repeatedly across time slots $t = 1, 2, \ldots$ until the Invader is detected. The cost function for the Scanner is the expected number of time slots until detection of the Invader. So, the Scanner wants to minimize expected detection time. The payoff to the Invader is number of time slots until his detection. The invader wants to maximize his detection time. We will solve the problem for stationary strategies, i.e., such strategies that do not depend on time slot. A stationary strategy for the Scanner is $\boldsymbol{S} = (S_1, \ldots, S_n)$, where S_i is the probability that he scans at band i. A stationary strategy for the Invader using application k is $\boldsymbol{T}^k = (T_1^k, \ldots, T_n^k)$, where T_i^k is the probability that he sneaks in band i. Note that, $1 - v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)$ is the detection probability of the Invader with type k at a time slot when the rivals use strategies $\boldsymbol{S}$ and $\boldsymbol{T}^k$. The expected detection time is given as follows:

$$\tau^k = \sum_{t=1}^{\infty} t \left(1 - v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)\right) \left(v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)\right)^{t-1} = \frac{1}{1 - v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)}.$$

Thus, the cost function to the Scanner is given as follows:

$$U_S(\boldsymbol{S}, (\boldsymbol{T}_*^1, \boldsymbol{T}_*^2)) = \sum_{k=1}^2 q^k/(1 - v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)).$$

The payoff to the Invader having type k is given by:

$$V_I^k(\boldsymbol{S}, \boldsymbol{T}^k) = 1/(1 - v_I^k(\boldsymbol{S}, \boldsymbol{T}^k)).$$

Unlike one-shot MaxDP game, in MinDT game, the cost function as well as the payoff function are nonlinear in $(\boldsymbol{S}, (\boldsymbol{T}^1, \boldsymbol{T}^2))$. The Scanner wants to minimize the expected cost function, and the Invader wants to maximize his payoff. Then, $\boldsymbol{S}$ and $(\boldsymbol{T}^1, \boldsymbol{T}^2)$ are the equilibrium strategies, if and only if they are the best response strategy to each other:

$$\boldsymbol{S}_* = \arg_{\boldsymbol{S}} \min U_S(\boldsymbol{S}, (\boldsymbol{T}_*^1, \boldsymbol{T}_*^2)), \tag{10}$$

$$\boldsymbol{T}_*^k = \arg_{\boldsymbol{T}^k} \max V_I^k(\boldsymbol{S}_*, \boldsymbol{T}^k) \text{ for } k = 1, 2. \tag{11}$$

Since $0 < v_I^k < 1$, U_S is convex in $\boldsymbol{S}$ as a linear combination of composition of convex function $1/(1-x)$ and linear functions v_I^k in $\boldsymbol{S}$. Similarly, V_I^k is convex in $\boldsymbol{T}^k$. Thus, we cannot apply straightforward the theorem of the existence of equilibrium [29], as it assumes that the cost function is convex, and the payoff function is concave. To deal with this snag, note that $\arg_{\boldsymbol{T}^k} \max U_I^k = \arg_{\boldsymbol{T}^k} \max v_I^k$, since $U_I^k = 1/(1 - v_I^k)$ and $0 < v_I^k < 1$. Thus, instead of the best response equation (11) we can consider the following equivalent equation:

$$\boldsymbol{T}_*^k = \arg_{\boldsymbol{T}^k} \max V_I^k(\boldsymbol{S}_*, \boldsymbol{T}^k) \text{ for } k = 1, 2. \tag{12}$$

The function v_I^k is linear in $\boldsymbol{T}^k$. Thus, by [29], the best response equations (11) and (12) have a solution, and the considered game has an equilibrium.

IV. Equilibrium Stationary Strategies for MinDT Game

In this Section, we will show that the MinDT game has a unique equilibrium, and we will find it explicitly. This allows us to show that the Invader's strategy has a band-sharing form, namely, all the bands are split into two groups, where each group is associated with a single type of Invader, and these groups either intersect at a single band, or do not intersect at all.

For the sake of simplicity, we assume that all the bands have different ratios for detection probabilities, i.e., $\gamma_i^1/\gamma_i^2 \neq \gamma_j^1/\gamma_j^2$ for any $i \neq j$. Without loss of generality

we can assume that the bands are arranged in decreasing order by ratio γ_i^1/γ_i^2, i.e.,

$$\gamma_1^1/\gamma_1^2 > \gamma_2^1/\gamma_2^2 > \ldots > \gamma_n^1/\gamma_n^2. \tag{13}$$

Theorem 2: The MinDT game has a unique equilibrium $(\boldsymbol{S}, (\boldsymbol{T}^1, \boldsymbol{T}^2))$.

(a) Let i_0 be such that

$$\psi_{i_0+1} \le \frac{q^1}{q^2}\left(\frac{\gamma_{i_0}^2}{\gamma_{i_0}^1}\right)^2 < \psi_{i_0} \tag{14}$$

with

$$\psi_m = \left(\sum_{i=m}^{n}\frac{1}{\gamma_i^1}\right)\Big/\left(\sum_{i=1}^{m-1}\frac{1}{\gamma_i^2}\right) \text{ for } m \in [1,n] \tag{15}$$

being decreasing sequence such that

$$\psi_1 = \infty \text{ and } \psi_{n+1} = 0. \tag{16}$$

Then

$$T_i^1 = \begin{cases} 0, & i < i_0, \\ 1 - \displaystyle\sum_{j=i_0+1}^{n} T_j^1, & i = i_0, \\ \dfrac{1}{q^1\gamma_i^1}\dfrac{q^1\gamma_{i_0}^1 + q^2\gamma_{i_0}^2\left(\frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}\right)^2}{\displaystyle\sum_{j=i_0+1}^{n}\frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0}\frac{\gamma_{i_0}^2}{\gamma_j^2}}, & i > i_0, \end{cases} \tag{17}$$

$$T_i^2 = \begin{cases} \dfrac{1}{q^2\gamma_i^2}\dfrac{q^1\gamma_{i_0}^1\left(\frac{\gamma_{i_0}^2}{\gamma_{i_0}^1}\right)^2 + q^2\gamma_{i_0}^2}{\displaystyle\sum_{j=i_0+1}^{n}\frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0}\frac{\gamma_{i_0}^2}{\gamma_j^2}}, & i < i_0, \\ 1 - \displaystyle\sum_{j=1}^{i_0-1} T_j^2, & i = i_0, \\ 0, & i > i_0, \end{cases} \tag{18}$$

$$S_i = \frac{1}{\displaystyle\sum_{j=i_0+1}^{n}\frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0}\frac{\gamma_{i_0}^2}{\gamma_j^2}} \times \begin{cases} \dfrac{\gamma_{i0}^1}{\gamma_i^1}, & i \in [i_0+1, n], \\ \dfrac{\gamma_{i0}^2}{\gamma_i^2}, & i \in [1, i_0]. \end{cases} \tag{19}$$

The payoff to the Invader of type 1 and 2 are given as follows:

$$V_I^1 = \sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1} + \frac{\gamma_{i_0}^2}{\gamma_{i_0}^1}\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}, \tag{20}$$

$$V_I^2 = \frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1} + \sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}. \tag{21}$$

The cost function to the Scanner is given as follows:

$$U_S = -\left(q^1 + q^2\frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}\right)\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1} - \left(q^1\frac{\gamma_{i_0}^2}{\gamma_{i_0}^1} + q^2\right)\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}. \tag{22}$$

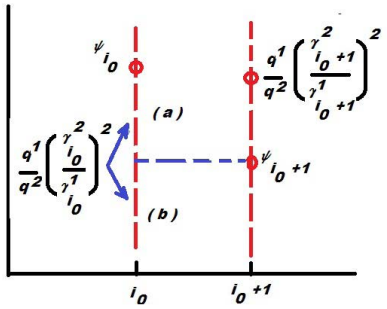


Fig. 4. Cases (a) and (b) of Theorem 2.

(b) Let i_0 be such that

$$\frac{q^1}{q^2}\left(\frac{\gamma_{i_0}^2}{\gamma_{i_0}^1}\right)^2 < \psi_{i_0+1} < \frac{q^1}{q^2}\left(\frac{\gamma_{i_0+1}^2}{\gamma_{i_0+1}^1}\right)^2. \tag{23}$$

Then

$$T_i^1 = \frac{1}{\displaystyle\sum_{j=i_0+1}^{n}(1/\gamma_j^1)} \times \begin{cases} 0, & i \le i_0, \\ 1/\gamma_i^1, & i > i_0, \end{cases}$$

$$T_i^2 = \frac{1}{\displaystyle\sum_{j=1}^{i_0}(1/\gamma_j^2)} \times \begin{cases} 1/\gamma_i^2, & i \le i_0, \\ 0, & i > i_0, \end{cases} \tag{24}$$

$$S_i = \begin{cases} \dfrac{1/\gamma_i^2}{\sqrt{\frac{q^1}{q^2\psi_{i_0+1}}}\displaystyle\sum_{j=i_0+1}^{n}\frac{1}{\gamma_j^1} + \sum_{j=1}^{i_0}\frac{1}{\gamma_j^2}}, & i \le i_0, \\ \dfrac{1/\gamma_i^1}{\displaystyle\sum_{j=i_0+1}^{n}\frac{1}{\gamma_j^1} + \sqrt{\frac{q^2\psi_{i_0+1}}{q^1}}\sum_{j=1}^{i_0}\frac{1}{\gamma_j^2}}, & i > i_0. \end{cases} \tag{25}$$

The payoffs to the Invaders are given as follows:

$$V_I^1 = \sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1} + \sqrt{\frac{q^2\psi_{i_0+1}}{q^1}}\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2},$$

$$V_I^2 = \sqrt{\frac{q^1}{q^2\psi_{i_0+1}}}\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1} + \sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}.$$

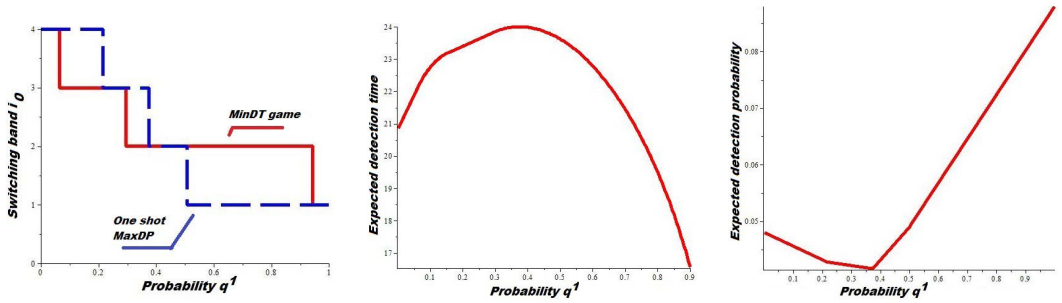
The cost function to the Scanner is $V_S = -q^1V_I^1 - q^2V_I^2$.

Since ψ_i is decreasing and γ_i^2/γ_i^1 is increasing, the switching band i_0 given by (14) and (23) (so, by cases (a) and (b) of Theorem 2) is uniquely defined (Figure 4).

By (17), (18) and (24), both types of Invader either do not employ the same band, or the band i_0 is the only band employed jointly by them. Thus, the Invader's strategies have an explicit band-sharing form.

V. Equilibrium Strategies in One Shot MaxDP Game

In this section, we find explicitly the equilibrium strategies for the rivals for the one shot MaxDP game. Based on the established properties of the equilibrium further explored in Section VII, a scanning learning algorithm will be designed for the MaxDP game played repeatedly.



(a) (b) (c)

Fig. 5. (a) Switching band, (b) the expected detection time for MinDT game, and (c) expected detection probability for one shot MaxDP game as functions of probability q^1.

Theorem 3: The one shot MaxDP game has a unique equilibrium $(\boldsymbol{S}, (\boldsymbol{T}^1, \boldsymbol{T}^2))$, where

$$T_i^1 = \begin{cases} 0, & i < i_0, \\ 1 - \sum_{j=i_0+1}^{n} T_j^1, & i = i_0, \\ \dfrac{1}{q^1 \gamma_i^1} \dfrac{q^1 \gamma_{i_0}^1 + q^2 \gamma_{i_0}^2}{\sum_{j=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_j^2}}, & i > i_0, \end{cases} \tag{26}$$

$$T_i^2 = \begin{cases} \dfrac{1}{q^2 \gamma_i^2} \dfrac{q^1 \gamma_{i_0}^1 + q^2 \gamma_{i_0}^2}{\sum_{j=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_j^2}}, & i < i_0, \\ 1 - \sum_{j=1}^{i_0-1} T_j^2, & i = i_0, \\ 0, & i > i_0, \end{cases} \tag{27}$$

$$S_i = \frac{1}{\sum_{j=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_j^1} + \sum_{j=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_j^2}} \times \begin{cases} \dfrac{\gamma_{i0}^1}{\gamma_i^1}, & i > i_0 \\ \dfrac{\gamma_{i0}^2}{\gamma_i^2}, & i \le i_0, \end{cases} \tag{28}$$

with i_0 given by the following conditions:

$$\psi_{i_0+1} \le \frac{q^1}{q^2} < \psi_{i_0}, \tag{29}$$

where ψ_m is given by (15) and (16).

The payoffs for the Scanner and the Invader corresponding to these equilibrium strategies are v_S, v_I^1 and v_I^2, where

$$v_S = \frac{q^1 \gamma_{i_0}^1 + q^2 \gamma_{i_0}^2}{\sum_{i=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_i^1} + \sum_{i=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_i^2}}, \tag{30}$$

$$v_I^1 = 1 - \frac{\gamma_{i_0}^1}{\sum_{i=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_i^1} + \sum_{i=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_i^2}}, \tag{31}$$

$$v_I^2 = 1 - \frac{\gamma_{i_0}^2}{\sum_{i=i_0+1}^{n} \frac{\gamma_{i_0}^1}{\gamma_i^1} + \sum_{i=1}^{i_0} \frac{\gamma_{i_0}^2}{\gamma_i^2}}. \tag{32}$$

Also, the Invader's payoffs have the following properties which will be applied in the next section.

Theorem 4: (a) There is an explicit threshold condition identifying the Invader's type with greater payoff, namely,

$$v_I^1 \{>, =, <\} v_I^2 \tag{33}$$

if and only if

$$q_{i0}^1 / q_{i0}^2 \{<, =, >\} 1. \tag{34}$$

(b) The Invader's payoff v_I^1 is piecewise constant, non-increasing in probability q^1, the Invader's payoff v_I^2 is piecewise constant, non-decreasing in probability q^1, and the ratio of the Invader's payoffs v_I^1 / v_I^2 is non-increasing in probability q^1.

The equilibrium scanning strategy (28) does not depend explicitly on the probabilities of using each application (i.e. q^1 and q^2) by the Invader. It depends only on the switching band i_0 which, by (29) and (15), depends on the ratio of these probabilities q^1/q^2. The Invader's equilibrium strategies (26) and (27) depend explicitly on the probabilities q^1 and q^2 as well as on the switching band i_0. Regarding payoffs, a symmetric situation arises. The Scanner's payoff (30) depends explicitly on the probabilities q^1 and q^2 as well as on the switching band i_0, while the Invader's payoffs (31) and (32) depend only on the switching band i_0, which depends on the ratio of these probabilities q^1/q^2. This leads to the Scanner's payoff as well as the Invader's strategies being continuous in the probability q^1, while the Invader's payoffs as well as the Scanner's strategy being discontinuous in the probability q^1.

VI. Numerical Illustration

As an illustration we consider a situation with $n = 4$ bands and the detection probabilities $\gamma^1 = (0.9, 0.8, 0.25, 0.1)$ and $\gamma^2 = (0.1, 0.2, 0.3, 0.4)$. Then $\gamma^1/\gamma^2 = (9, 4, 0.83, 0.5)$ and the condition (13) holds. Figure 5(a) and 6(a) illustrates the switching band i_0 for the one shot MaxDP game as well as for the MinDT game, and the domain of applying cases (a) and (b) of Theorem 2 for the MinDT game. It is interesting to note that the payoffs for the Scanner for both games are continuous in q^1 (Figure 5(b) and (c)). In the MinDT game, the payoff for the Invader still is continuous. Meanwhile, in the one shot MaxDP game the payoff for the Invader is piecewise-constant in q^1, and thus discontinuous in q^1 (Figure 6(b) and (c)). The payoff to the Invader of type 2 is increasing, while the payoff

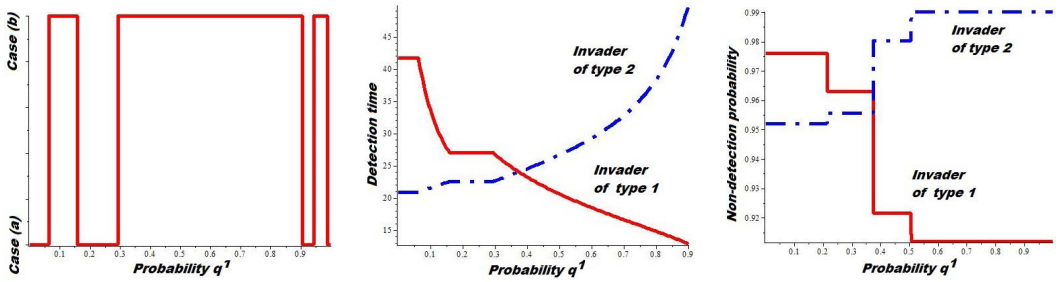


Fig. 6. (a) Cases of Theorem 2, and the payoffs to the Invader of both types for (b) MinDT game and (c) one shot MaxDP game as functions of the probability q^1.

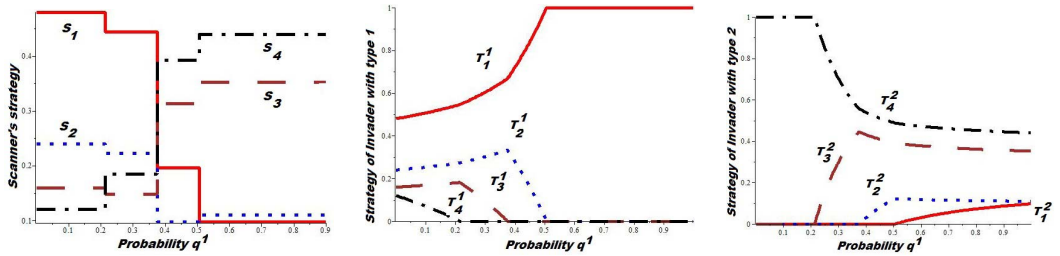


Fig. 7. The equilibrium strategies for one shot MaxDP game as functions of probability q^1.

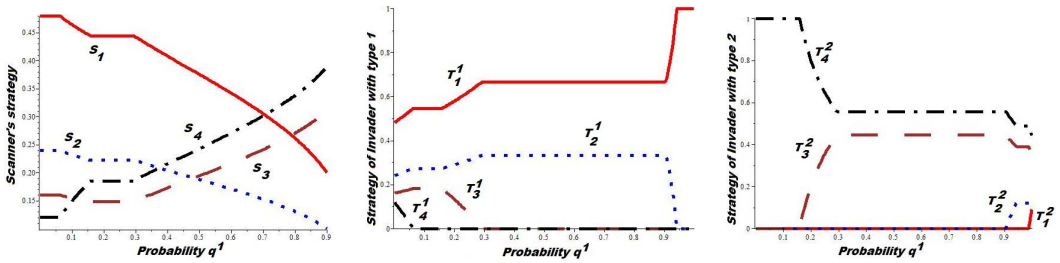


Fig. 8. The equilibrium strategies for MinDT game as functions of probability q^1.

to the Invader of type 1 is decreasing in q^1, due to the Scanner re-allocates scanning efforts as a response to a more probable malicious activity. In the one shot MaxDP game, the Scanner's payoff has a threshold value of probability q^1 returning the minimal payoff. In the MinDT game, the Scanner's cost function has a threshold value of probability q^1 returning the maximal cost. Such threshold probability q^1 can aid in designing a maxmin scanning algorithm for a one shot MaxDP game and a minmax algorithm in the MinDT game, if the Invader and its application is considered.

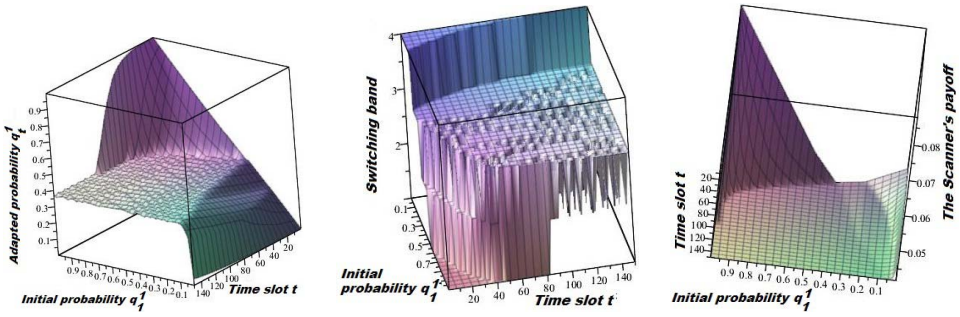
Regarding the strategies, the Invader's strategies for both games are continuous in probability q^1, while the Scanner's strategy continuity exists only for the MinDT game (Figures 7 and 8). The Scanner's strategy does not miss any band, allocating efforts among all of them, which allows it to maintain a positive probability to detect any type of the Invader. The Invader's strategy is quite different: when the Invader understands that the Scanner is focused on a specific Invader type, then the Invader would switch his sneaking effort to use the band that is best for his purpose. If the a priori probability does not push the Scanner to focus on a specific Invader's type, then the Invader would spread its sneaking effort amongst several bands.

VII. How to Update the Belief on Invader's Unlicensed Activity

In this section, we consider the scanning problem, where at the beginning of each time slot the Scanner adapts his belief regarding the Invader's unlicensed activity if the scanning during the previous time slot failed. The Invader does not change its type of activity, but can choose a different band to intrude upon at the beginning of the next time slot after taking into account any perception it might have regarding the adjusted Scanner's belief.

To get insight into the problem here, we consider the rule, where the adapting the belief takes into account the result of the scanning only from the previous time slot (i.e., does not upon any other previous time slot). Since q^k is a priori probability that the Invader of type k was present in the bands, then at the beginning of the first time slot the Scanner's belief about the Invader's type k' presence will be denoted as $q_1^k = q^k$. Denote by $i_{01} = i_0$ the corresponding switching band given by (29).

At the first time slot, the rivals apply the equilibrium strategy $(\boldsymbol{S}_1, (\boldsymbol{T}_1^1, \boldsymbol{T}_1^2))$ given by Theorem 3 according to the original belief. The probability that the Invader is not detected, if he is of type k, is $v_I^k(\boldsymbol{S}_1, \boldsymbol{T}_k)$. Then, by Bayes' theorem,



(a) (b) (c)

Fig. 9. (a) The adapted probability q_t^1, (b) the switching band i_{0t} and (c) the expected payoff to the Scanner v_S as functions of initial probability q_1^1 and time slot t for oscillatory learning.

the revised probability for the Invader of type k being in the bands is given as follows:

$$q_2^k = \frac{q_1^k v_I^k(\boldsymbol{S}_1, \boldsymbol{T}_1^k)}{q_1^1 v_I^1(\boldsymbol{S}_1, \boldsymbol{T}_1^1) + q_1^2 v_I^2(\boldsymbol{S}_1, \boldsymbol{T}_1^2)}. \tag{35}$$

Thus, here we deal with the simplest learning mechanism with adapting the belief. As examples of more advanced learning mechanisms, say, reinforcement learning, see, [30]. Taking into account this updated belief, the rivals repeat the game in the second time slot, and so on. By Theorem 3 the strategies $(\boldsymbol{S}_1, (\boldsymbol{T}_1^1, \boldsymbol{T}_1^2))$ are uniquely defined by a threshold band $i_{01} = i_0$ given by (29). By (35) we have that

$$\frac{q_2^1}{q_2^2} = \frac{q_1^1}{q_1^2} \frac{v_I^1(\boldsymbol{S}_1, \boldsymbol{T}_1^k)}{v_I^2(\boldsymbol{S}_1, \boldsymbol{T}_2^k)}.$$

Thus, by (33) and (34),

$$\frac{q_2^1}{q_2^2}\{<, =, >\}\frac{q_1^1}{q_1^2}$$

if and only if

$$\frac{\gamma_{i_{01}}^1}{\gamma_{i_{01}}^2}\{>, =, <\}1.$$

Let i_{02} be the switching band for the second time slot, so, by (14), it is given as follows:

$$\psi_{i_{02}+1} \le \frac{q_2^1}{q_2^2} < \psi_{i_{02}}.$$

The property that ψ_m is decreasing in m yields that, if

$$\frac{\gamma_{i_{01}}^1}{\gamma_{i_{01}}^2}\{>, <\}1, \tag{36}$$

then

$$i_{02}\{\ge, \le\}i_{01}. \tag{37}$$

Let $(\boldsymbol{S}_t, (\boldsymbol{T}_t^1, \boldsymbol{T}_t^2))$ and q_t^k be the equilibrium strategies and the adapted belief for time slot k. Then, for the next time slot the adapted belief is given by

$$q_{t+1}^k = \frac{q_t^k v_I^k(\boldsymbol{S}_t, \boldsymbol{T}_t^k)}{q_t^1 v_I^1(\boldsymbol{S}_t, \boldsymbol{T}_t^1) + q_t^2 v_I^2(\boldsymbol{S}_t, \boldsymbol{T}_t^2)}. \tag{38}$$

Then,

$$\frac{q_{t+1}^1}{q_{t+1}^2}\{<, =, >\}\frac{q_t^1}{q_t^2} \tag{39}$$

if and only if

$$\frac{\gamma_{i_{0t}}^1}{\gamma_{i_{0t}}^2}\{>, =, <\}1, \tag{40}$$

with i_{0t} being such that

$$\psi_{i_{0t}+1} \le \frac{q_t^1}{q_t^2} < \psi_{i_{0t}}.$$

Finally, note that, (36) implies

$$i_{0(t+1)}\{\ge, \le\}i_{0t}. \tag{41}$$

This, jointly with (13), implies the following result.

Theorem 5: Let the learning algorithm be given by (38).

(i) Let $\gamma_n^1/\gamma_n^2 > 1$. Then the switching band i_{0t} monotonically converges to n, the adapted probabilities (q_t^1, q_t^2) monotonically converges to $(0, 1)$, and the scanning strategy converges to $\boldsymbol{S}$ with $S_i = (1/\gamma_i^2)/(\sum_{j=1}^n (1/\gamma_j^2))$.

(ii) Let $\gamma_1^1/\gamma_1^2 < 1$. Then the switching band i_{0t} monotonically converges to 1, the adapted probabilities (q_t^1, q_t^2) monotonically converges to $(1, 0)$, and the scanning strategy converges to $\boldsymbol{S}$ with $S_i = (1/\gamma_i^1)/(\sum_{j=1}^n (1/\gamma_j^1))$.

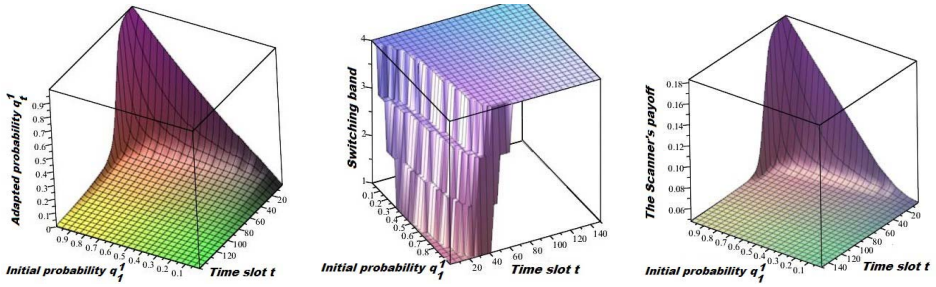
(iii) Let $\gamma_1^1/\gamma_1^2 > 1 > \gamma_n^1/\gamma_n^2$. Thus, there exists an i_* such that $\gamma_{i*}^1/\gamma_{i*}^2 \ge 1 > \gamma_{i_*+1}^1/\gamma_{i_*+1}^2$. Then, the switching bands oscillate around bands i_* and $i_* + 1$.

(iv) The detection time τ^k of the Invader of type k is given as follows:

$$\tau^k = \sum_{t=1}^{\infty} t \left(1 - v_I^k(\boldsymbol{S}_t, \boldsymbol{T}_t^k)\right) \prod_{j=1}^{t-1} v_I^k(\boldsymbol{S}_j, \boldsymbol{T}_j^k).$$

An oscillatory effect in the scanning strategy is expected, and we note that such oscillatory strategies are often used to optimize searching, c.f. naval search operations [31], [32].

Figure 9 illustrates the oscillatory learning for $\gamma^1 = (0.9, 0.8, 0.25, 0.2)$ and $\gamma^2 = (0.1, 0.2, 0.3, 0.4)$. Thus, $\gamma^1/\gamma^2 = (9, 4, 0.83, 0.5)$, and $\gamma_2^1/\gamma_2^2 > 1 > \gamma_3^1/\gamma_3^2$. So, condition (iii) of Theorem 5 with $i_* = 2$ holds. The Scanner's strategy oscillates around bands 2 and 3.



(a) (b) (c)

Fig. 10. (a) The adapted probability q_t^1, (b) the switching band i_{0t} and (c) the Scanner's v_S as functions of initial probability q_1^1 and time slot t for monotonic learning.

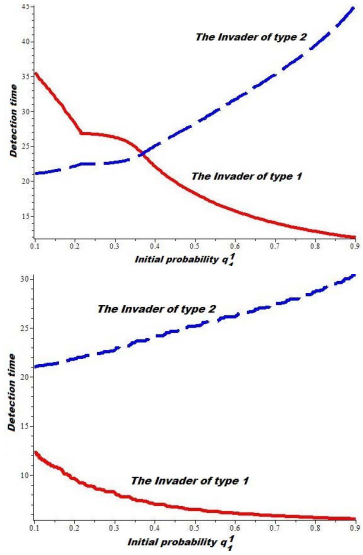


Fig. 11. Expected detection time for oscillatory (top) and monotonic (bottom) learning as functions of initial probability q_1^1.

The adapted probability to belief that the Invader has type 1 oscillates around 0.36. It is interesting that switching from monotonic to an oscillatory learning mode occurs, for small initial probability q_1^1, slower then for the others.

Figure 10 illustrates monotonic learning for $\gamma^1 = (0.9, 0.8, 0.7, 0.6)$ and $\gamma^2 = (0.1, 0.2, 0.3, 0.4)$. Thus, $\gamma^1/\gamma^2 = (9, 4, 2.3, 1.5)$, and $\gamma_4^1/\gamma_4^2 > 1$. So, condition (i) of Theorem 5 holds, and the switching point i_{0t} converges in a non-decreasing manner to 4. By getting this value, the adapted probability q_t^1 becomes equal to zero, and the Scanner's payoff stabilizes on the value 0.48.

Figure 11 illustrates that detection time is decreasing in q_1^1 for type 1 and is increasing in q_1^1 for type 2 of the Invader. It is interesting that for oscillatory learning there is a switching point ($q^1 = 0.37$), where detection time coincide for both Invader's types, while for monotonic learning detection time for type 2 is greater than for type 1.

VIII. Conclusion

In this paper, we have examined the relationship between an illegitimate user attempting to sneak usage of bandwidth owned by others, which is being monitored by a Scanner, and with the underlying application that the Invader is attempting to employ. First, we showed that the QoS requirements for the application plays a critical role in how the thief should attempt to sneak usage of spectrum and, consequently, a critical role in how the spectrum monitoring infrastructure should scan spectrum. Then, we have put forward a question: how can a priori knowledge of the application type be incorporated into spectrum scanning to tune it for better detecting the thief. Using two game-theoretic models (minimizing detection time and maximizing detection probability at each time slot) we have shown how the Scanner can gain using this a priori knowledge. We note that these two models allow also us to demonstrate the difference between tactical and strategic decision making. Maximizing detection probability at each time slot game might be associated with tactical decision making which allows short-term, unpredictable moves. Meanwhile, the minimizing detection time game might be associated with strategic decision making, which involves longer-term, more predictable moves. We further analyzed the behavior of belief probabilities in the maximizing detection game played repeatedly, and found that the optimal learning scanning protocol can be either monotonic or oscillatory, and explicit criteria for such protocol was established. A goal of our future research is to develop a scanning protocol for detecting more sophisticated Invader behaviour where the Invader can combine silent and active modes as well as change between types of illegal activity.

Appendix

A. Proof of Theorem 1

First note that

$$\frac{d\, v_I(P)}{d\, P} = \frac{\mathrm{SINR}}{d\, P}(U'(\mathrm{SINR})(1-\gamma(\mathrm{SINR})) - (U(\mathrm{SINR})+F)\gamma'(\mathrm{SINR})).$$

Since $\frac{d\,\mathrm{SINR}}{d\,P} > 0$, the optimal power P is a solution of the equation

$$\Psi(\mathrm{SINR}) = F$$

with Ψ given by (6). For the considered detection probability (4) we have that

(a) for the throughput utility

$$\Psi(x) = \frac{W}{\alpha(1+x)} - W\ln(1+x)$$

(b) for the delay utility

$$\Psi(x) = \frac{1}{\alpha W \ln^2(1+x)(1+x)} + \frac{1}{W\ln(1+x)}.$$

It is clear that $\Psi(x)$ is decreasing for both utilities, and the result follows. ∎

B. Proof of Theorem 2

Recall that all the equilibrium are solutions of equations (10) and (12).

Since U_S is convex on $\boldsymbol{S}$, the strategy $\boldsymbol{S}$ is the best response to $(\boldsymbol{T}^1, \boldsymbol{T}^2)$ if and only if there is an ω such that

$$\sum_{k=1}^{2} \frac{q^k \gamma_i^k T_i^k}{\left(\sum_{i=1}^n \gamma_i^k S_i T_i^k\right)^2} \begin{cases} = \omega, & S_i > 0, \\ \le \omega, & S_i = 0. \end{cases} \tag{42}$$

The function v_I^k is linear in $\boldsymbol{T}^k$. Thus, $\boldsymbol{T}^k$ is the best response to $\boldsymbol{S}$ if and only if there is a ν^k such that

$$\gamma_i^k S_i \begin{cases} = \nu^k, & T_i^k > 0, \\ \ge \nu^k, & T_i^k = 0. \end{cases} \tag{43}$$

By (43), $S_i > 0$ for any i. Also, by (42), there is no i such that $T_i^1 = T_i^2 = 0$. We consider separately two cases: (a) there is an i such that $T_i^1 > 0$ and $T_i^2 > 0$, (b) there is no i such that $T_i^1 > 0$ and $T_i^2 > 0$.

(a) Let there exist an i such that $T_i^1 > 0$ and $T_i^2 > 0$. By (43), we have that for such i the following relation has to hold:

$$\gamma_i^1 / \gamma_i^2 = \nu^1 / \nu^2. \tag{44}$$

By (13), there is at most one such i. Denote this i by i_0. Also, By (43), $S_i > 0$ for any i. Then, by (42), either $T_i^1 > 0$ or $T_i^2 > 0$ for any i, and both of them can be positive for the only i. Thus, by (43), if $i \in I^1$ where $I^1 = \{i : T_i^1 > 0\}$ then $\gamma_i^1 S_i = \nu^1$ and $\gamma_i^2 S_i \ge \nu^2$. Thus, $\gamma_i^1 / \gamma_i^2 \le \nu^1 / \nu^2$ for $i \in I^1$. Similarly, $\gamma_i^1 / \gamma_i^2 \ge \nu^1 / \nu^2$ for $i \in I^2 = \{i : T_i^2 > 0\}$. Then, by (13), $I^1 = [i_0, n]$ and $I^2 = [1, i_0]$ and

$$S_i = S_i(\nu^1, \nu^2) := \begin{cases} \nu^1 / \gamma_i^1, & i \in I^1, \\ \nu^2 / \gamma_i^2, & i \in I^2. \end{cases} \tag{45}$$

Also, since $\boldsymbol{T}^k$ is a probability vector, (43) implies that

$$\sum_{i=1}^{n} S_i \gamma_i^k T_i^k = \nu^k. \tag{46}$$

Let $I_0^k = I^k \backslash \{i_0\}$. Thus, by (42) and (46), we have

$$T_i^k = T_i^k(\omega) := \begin{cases} \dfrac{\omega \left(\nu^k\right)^2}{q^k \gamma_i^k}, & i \in I_0^k, \\ T_{i_0}^k(\omega), & i = i_0, \\ 0, & \text{otherwise} \end{cases} \tag{47}$$

and

$$\frac{q^1 \gamma_{i_0}^1 T_{i_0}^1(\omega)}{\left(\nu^1\right)^2} + \frac{q^2 \gamma_{i_0}^2 T_{i_0}^2(\omega)}{\left(\nu^2\right)^2} = \omega. \tag{48}$$

Since $\boldsymbol{T}^k$ has to be a probability vector, by (47), we have that

$$T_{i_0}^k(\omega) = 1 - \sum_{i \in I_0^k} \frac{\omega \left(\nu^k\right)^2}{q^k \gamma_i^k}. \tag{49}$$

Substituting these both $T_{i_0}^k$ into (48) implies that

$$\frac{q^1 \gamma_{i_0}^1}{\left(\nu^1\right)^2} \left(1 - \sum_{i \in I_0^1} \frac{\omega \left(\nu^1\right)^2}{q^1 \gamma_i^1}\right) + \frac{q^2 \gamma_{i_0}^2}{\left(\nu^2\right)^2} \left(1 - \sum_{i \in I_0^2} \frac{\omega \left(\nu^2\right)^2}{q^2 \gamma_i^2}\right) = \omega. \tag{50}$$

Thus,

$$\omega = \frac{q^1 \gamma_{i_0}^1 / \left(\nu^1\right)^2 + q^2 \gamma_{i_0}^2 / \left(\nu^2\right)^2}{1 + \sum_{i \in I_0^1} \frac{\gamma_{i_0}^1}{\gamma_i^1} + \sum_{i \in I_0^2} \frac{\gamma_{i_0}^2}{\gamma_i^2}}. \tag{51}$$

This allows us, by using (47) and (49), to get $\boldsymbol{T}^k$ in closed form as a function on i_0.

How can i_0 be found? It is defined by the condition that $\boldsymbol{T}^k$ is a strategy (a probability vector). Definition of ω implies that $\sum_{j=1}^n T_j^k = 1$. Since $\omega > 0$ then, by (47), $T_i^k > 0$ for $i \in [1, n] \backslash \{i_0\}$. So, i_0 has to be defined from the conditions that $T_{i_0}^k$ must be non-negative, and $T_{i_0}^k > 0$ for at least one k, which is, by (49), equivalent to

$$\frac{q^1 \gamma_{i_0}^1 / \left(\nu^1\right)^2 + q^2 \gamma_{i_0}^2 / \left(\nu^2\right)^2}{1 + \sum_{i \in I_0^1} \frac{\gamma_{i_0}^1}{\gamma_i^1} + \sum_{i \in I_0^2} \frac{\gamma_{i_0}^2}{\gamma_i^2}} \le \frac{1}{\sum_{i \in I_0^k} \frac{\left(\nu^k\right)^2}{q^k \gamma_i^k}}, \tag{52}$$

and at least one on these inequalities has to be strong. This expression can be simplified as follows:

$$\sum_{i \in I_0^k} \frac{\left(\nu^{k'}\right)^2}{q^k \gamma_i^k} \le \sum_{i \in I^{k'}} \frac{\left(\nu^k\right)^2}{q^{k'} \gamma_i^{k'}}, \quad \{k', k\} = \{1, 2\}. \tag{53}$$

Taking the ratio of probabilities q_1/q_2 as a threshold value allows us to present the conditions (53) in the following form:

$$\frac{\sum_{i \in I_0^1} \frac{1}{\gamma_i^1}}{\sum_{i \in I^2} \frac{1}{\gamma_i^2}} \le \frac{q^1}{q^2} \left(\frac{\nu^2}{\nu^1}\right)^2 = \frac{q^1}{q^2} \left(\frac{\gamma_{i0}^2}{\gamma_{i0}^1}\right)^2 \le \frac{\sum_{i \in I^1} \frac{1}{\gamma_i^1}}{\sum_{i \in I_0^2} \frac{1}{\gamma_i^2}}. \tag{54}$$

In (15) and (16), the inequalities (54) are equivalent to (14) with ψ_i given by (15).

Note that

$$\psi_m - \psi_{m+1} = \frac{\sum_{i=m}^{n} \frac{1}{\gamma_i^1} \sum_{i=1}^{m} \frac{1}{\gamma_i^2} - \sum_{i=m+1}^{n} \frac{1}{\gamma_i^1} \sum_{i=1}^{m-1} \frac{1}{\gamma_i^2}}{\sum_{i=1}^{m} \frac{1}{\gamma_i^2} \sum_{i=1}^{m-1} \frac{1}{\gamma_i^2}} > 0.$$

So, ψ_m is decreasing. By (13), γ_m^2 / γ_m^1 is increasing. Thus, i_0 is uniquely defined by (14).

To complete our investigation we have to define only ν^1 and ν^2. Summing up (45) and taking into account that $\boldsymbol{S}$ is a probability vector implies

$$\sum_{i=i_0+1}^{n} \frac{\nu^1}{\gamma_i^1} + \sum_{i=1}^{i_0} \frac{\nu^2}{\gamma_i^2} = 1. \tag{55}$$

Then,

$$\nu^2\left(\frac{\nu^1}{\nu^2}\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1}+\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}\right)=1. \tag{56}$$

Also, by (44) with $i=i_0$, we have that

$$\nu^1=\frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}\nu^2. \tag{57}$$

Substituting this ν^1 into (56) yields

$$\nu^2=\frac{\gamma_{i_0}^2}{\sum_{i=i_0+1}^{n}\frac{\gamma_{i_0}^1}{\gamma_i^1}+\sum_{i=1}^{i_0}\frac{\gamma_{i_0}^2}{\gamma_i^2}}. \tag{58}$$

Thus, ν^1 and ν^2 are obtained explicitly, and (a) follows.

(b) Let there not exist an i such that $T_i^1>0$ and $T_i^2>0$. Following the proof of (a), we obtain that there is an i_0 such that

$$\frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}>\frac{\nu^1}{\nu^2}>\frac{\gamma_{i_0+1}^1}{\gamma_{i_0+1}^2}. \tag{59}$$

Also, for such i_0 the relation (45) has to hold for strategy $\boldsymbol{S}$, and

$$T_i^1\begin{cases}=0, & i\le i_0,\\ >0, & i>i_0,\end{cases}\qquad T_i^2\begin{cases}>0, & i\le i_0,\\ =0, & i>i_0.\end{cases} \tag{60}$$

Then, (42) and (60) yield

$$T_i^1=\frac{\omega(\nu^1)^2}{q^1}\times\begin{cases}0, & i\le i_0,\\ \frac{1}{\gamma_i^1}, & i>i_0,\end{cases}$$
$$T_i^2=\frac{\omega(\nu^2)^2}{q^2}\times\begin{cases}\frac{1}{\gamma_i^2}, & i\le i_0,\\ 0, & i>i_0.\end{cases} \tag{61}$$

Since $\boldsymbol{T}^1$ and $\boldsymbol{T}^2$ are probability vectors, (61) implies

$$\frac{\omega(\nu^1)^2}{q^1}\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1}=1, \tag{62}$$

$$\frac{\omega(\nu^2)^2}{q^2}\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}=1, \tag{63}$$

and $\boldsymbol{T}^1$ and $\boldsymbol{T}^2$ have to be given by (24).

Dividing (62) by (63) yields

$$\left(\frac{\nu^1}{\nu^2}\right)^2\frac{q^2}{q^1}=\frac{\sum_{i=1}^{i_0}(1/\gamma_i^2)}{\sum_{i=i_0+1}^{n}(1/\gamma_i^1)}=\frac{1}{\psi_{i_0+1}}. \tag{64}$$

This, jointly with (59), implies (23).

By (45) and (55), ν^2 and ν^1/ν^2 are correlated by (56). By (64),

$$\frac{\nu^1}{\nu^2}=\sqrt{\frac{q^1}{q^2\psi_{i_0+1}}}.$$

Substituting this ν^1/ν^2 into (56) yields

$$\nu^2=\frac{1}{\sqrt{\frac{q^1}{q^2\psi_{i_0+1}}}\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1}+\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}}. \tag{65}$$

Similarly, we can obtain that

$$\nu^1=\frac{1}{\sum_{i=i_0+1}^{n}\frac{1}{\gamma_i^1}+\sqrt{\frac{q^2\psi_{i_0+1}}{q^1}}\sum_{i=1}^{i_0}\frac{1}{\gamma_i^2}}, \tag{66}$$

and the result follows. ■

C. Proof of Theorem 3

First note that, since v_S is linear in $\boldsymbol{S}$, then $\boldsymbol{S}$ is the best response to $\boldsymbol{T}^1$ and $\boldsymbol{T}^2$ if and only if there is an ω such that

$$\sum_{k=1}^{2}q^k\gamma_i^kT_i^k\begin{cases}=\omega, & S_i>0,\\ \le\omega, & S_i=0.\end{cases} \tag{67}$$

Similarly, since v_I^k is linear in $\boldsymbol{T}^k$, then $\boldsymbol{T}^k$ is the best response to $\boldsymbol{S}$ if and only if there is a ν^k such that $\gamma_i^kS_i=\nu^k$ for $T_i^k>0$ and $\gamma_i^kS_i\ge\nu^k$ for $T_i^k=0$. Then, following the proof of Theorem 2(a), the result follows. ■

D. Proof of Theorem 4

(a) By (31) and (32),

$$\frac{1-v_I^1}{1-v_I^2}=\frac{\gamma_{i_0}^1}{\gamma_{i_0}^2}. \tag{68}$$

Since

$$\frac{1-v_I^1}{1-v_I^2}=\frac{1/v_I^2-v_I^1/v_I^2}{1/v_I^2-1}$$

and $0<v_I^1,v_I^2<1$, (68) implies (a).

(b) Let

$$s_m:=\sum_{i=m+1}^{n}\frac{1}{\gamma_i^1}+\frac{\gamma_m^2}{\gamma_m^1}\sum_{i=1}^{m}\frac{1}{\gamma_i^2}.$$

Then, (13) implies that

$$\begin{aligned}s_m-s_{m+1}&=\frac{1}{\gamma_{m+1}^1}-\frac{\gamma_m^2}{\gamma_m^1}\frac{1}{\gamma_{m+1}^2}+\left(\frac{\gamma_m^2}{\gamma_m^1}-\frac{\gamma_{m+1}^2}{\gamma_{m+1}^1}\right)\sum_{i=1}^{m+1}\frac{1}{\gamma_i^2}\\&=\left(\frac{\gamma_m^2}{\gamma_m^1}-\frac{\gamma_{m+1}^2}{\gamma_{m+1}^1}\right)\sum_{i=1}^{m}\frac{1}{\gamma_i^2}<0.\end{aligned} \tag{69}$$

Thus, s_m is increasing in m. Since $q^1/(1-q^1)$ is increasing in q^1 and ψ_m, given by (15), is decreasing in m, (29) implies that i_0 is non-increasing in q^1. By (31), $v_I^1=1-1/s_{i_0}$. Thus, v_I^1 is non-increasing in q^1. The payoff v_I^2 can be considered similarly. ■

REFERENCES

[1] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A trusted radio infrastructure for enforcing spectrum etiquettes," in *Proc. 1st IEEE Workshop Netw. Technol. Softw. Defined Radio Netw.*, Sep. 2006, pp. 101–109.

[2] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[3] F. F. Digham, M.-S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," *IEEE Trans. Commun.*, vol. 55, no. 1, pp. 21–24, Jan. 2007.

[4] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 675–683.

[5] R. A. Dillard, "Detectability of spread-spectrum signals," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 15, no. 4, pp. 526–537, Jul. 1979.

[6] B. Park and T. F. Wong, "Optimal training sequence in MIMO systems with multiple interference sources," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, vol. 1. Nov./Dec. 2004, pp. 86–90.

[7] K. V. Cai, V. Phan, and R. J. O'Connor, "Energy detector performance in a noise fluctuating channel," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, vol. 1. Oct. 1989, pp. 85–89.

[8] V. I. Kostylev, "Energy detection of a signal with random amplitude," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 3, Apr. 28–May 2, 2002, pp. 1606–1610.

[9] S. Koivu, H. Saarnisaari, and M. Juntti, "Quantization and dynamic range effects on the energy detection," in *Proc. 6th Nordic Signal Process. Symp. (NORSIG)*, Jun. 2004, pp. 264–267.

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

[11] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Survey*, vol. 45, no. 3, 2013, Art. ID 25.

[12] M. Tambe, A. X. Jiang, B. An, and M. Jain, "Computational game theory for security: Progress and challenges," in *Proc. AAAI Spring Symp. Appl. Comput. Game Theory*, 2012, pp. 1–6. [Online]. Available: http://teamcore.usc.edu/papers/2014/AAAISS14.pdf

[13] G. Theodorakopoulos and J. S. Baras, "Game theoretic modeling of malicious users in collaborative networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1317–1327, Sep. 2008.

[14] K. Firouzbakht, G. Noubir, and M. Salehi, "On the performance of adaptive packetized wireless communication links under jamming," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3481–3495, Jul. 2014.

[15] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Incorporating attack-type uncertainty into network protection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1278–1287, Aug. 2014.

[16] L. Chen and J. Leneutre, "Fight jamming with jamming—A game theoretic analysis of jamming attack in wireless networks and defense strategy," *Comput. Netw.*, vol. 55, no. 9, pp. 2259–2270, 2011.

[17] A. Garnaev and W. Trappe, "One-time spectrum coexistence in dynamic spectrum access when the secondary user may be malicious," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 1064–1075, May 2015.

[18] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2578–2590, Dec. 2015.

[19] R. El-Bardan, S. Brahma, and P. K. Varshney, "Power control with jammer location uncertainty: A game theoretic perspective," in *Proc. 48th Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2014, pp. 1–6.

[20] A. Garnaev, W. Trappe, and C.-T. Kung, "Optimizing scanning strategies: Selecting scanning bandwidth in adversarial RF environments," in *Proc. 8th Int. Conf. Cognit. Radio Oriented Wireless Netw. (CROWNCOM)*, Jul. 2013, pp. 148–153.

[21] A. Garnaev and W. Trappe, "Stationary equilibrium strategies for bandwidth scanning," in *Multiple Access Communcations* (Lecture Notes in Computer Science), vol. 8310, M. Jonsson, A. Vinel, B. Bellalta, N. Marina, D. Dimitrova, and D. Fiems, Eds. New York, NY, USA: Springer, 2013, pp. 168–183.

[22] A. Agah, S. K. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach," in *Proc. 3rd IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, Aug./Sep. 2004, pp. 343–346.

[23] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," in *Proc. Workshop Game Theory Commun. Netw.*, 2006, pp. 1–12.

[24] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 112–118, Aug. 2011.

[25] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "Security games with unknown adversarial strategies," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2015.2475243.

[26] M. Scalabrin, V. Vadori, A. V. Guglielmi, and L. Badia, "A zero-sum jamming game with incomplete position information in wireless scenarios," in *Proc. 21st Eur. Wireless Conf.*, May 2015, pp. 1–6.

[27] A. Garnaev, Y. Liu, and W. Trappe, "Anti-jamming strategy versus a low-power jamming attack when intelligence of adversary's attack type is unknown," *IEEE Trans. Signal Inf. Process. Over Netw.*, to be published, doi: 10.1109/TSIPN.2015.2506038.

[28] M.-H. Lu, P. Steenkiste, and T. Chen, "Design, implementation and evaluation of an efficient opportunistic retransmission protocol," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, vol. 1. 2009, pp. 73–84.

[29] D. Fudenberg and J. Tirole, *Game Theory*. Boston, MA, USA: MIT Press, 1991.

[30] G. C. Chasparis, J. S. Shamma, and A. Rantzer, "Nonconvergence to saddle boundary points under perturbed reinforcement learning," *Int. J. Game Theory*, vol. 44, no. 3, pp. 667–699, 2015.

[31] B. O. Koopman, *Search and Screening: General Principles With Historical Applications*. New York, NY, USA: Pergamon, 1980.

[32] A. Y. Garnaev, "Search game in a rectangle," *J. Optim. Theory Appl.*, vol. 69, no. 3, pp. 531–542, 1991.

Andrey Garnaev received the M.Sc. degree in mathematics, the Ph.D. degree in applied mathematics, and the D.Sc. degree in computer science and applied mathematics from Saint Petersburg State University, Saint Petersburg, Russia, in 1982, 1987, and 1997, respectively. He is currently a Researcher with WINLAB, Rutgers University, USA, and a Professor with the Department of Computer Modelling and Multiprocessor Systems, Saint Petersburg State University, Russia. He has published in leading journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *Telecommunication Systems Journal*, *Performance Evaluation*, and the *Journal of Optimization Theory and Applications*. His current research interests are in applications of game theory and optimization theory in network security, wireless communication, and related fields.

Wade Trappe (F'14) is a Professor with the Electrical and Computer Engineering Department, Rutgers University, and the Associate Director of the Wireless Information Network Laboratory (WINLAB), where he directs WINLAB's research in wireless security. He has led several federally funded projects in the area of cybersecurity and communication systems, projects involving security and privacy for sensor networks, physical-layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources (the ORBIT testbed), and new RFID technologies. His experience in network security and wireless spans over 15 years, and he has coauthored a popular textbook on security, *Introduction to Cryptography with Coding Theory*, as well as several monographs on wireless security, including *Securing Wireless Communications at the Physical Layer* and *Securing Emerging Wireless Systems: Lower-layer Approaches*. He served as an Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the *IEEE Signal Processing Magazine*, and the IEEE TRANSACTIONS ON MOBILE COMPUTING. He served as the Lead Guest Editor of the 2011 Special Issue of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY on Using the Physical Layer for Securing the Next Generation of Communication Systems and served as the IEEE Signal Processing Society Representative to the Governing Board of the IEEE TMC. He is the IEEE SPS Regional Director for Region 1-6.