SPECTRUM SCANNING WHEN THE INTRUDER MIGHT HAVE KNOWLEDGE ABOUT THE SCANNER'S CAPABILITIES

Andrey Garnaev, Wade Trappe, Dragoslav Stojadinovic, Ivan Seskar

WINLAB, Rutgers University, USA

ABSTRACT

Detecting malicious users in dynamic spectrum access scenarios is a crucial problem that requires an intrusion detection system (IDS) that scans spectrum for malicious activities. In this paper we design a spectrum scanning protocol that incorporates knowledge about the scanning effectiveness across different bands, which can increase scanning efficiency. The adversary, however, can also exploit such knowledge to its advantage. To understand the interplay underlying this problem, we formulate a Bayesian model, where the IDS faces a scanning allocation dilemma: if the intruder has no knowledge, then all the bands are under equal threat, while if the intruder has complete knowledge, then less-protected bands are more likely to be threatened. We solve this dilemma and show the optimal IDS strategy switches between the optimal response to these threats. Finally, we show that the strategy might be sensitive to prior knowledge, which can be corrected by adapted learning.

Index Terms— Spectrum scanning, Bayesian game, intrusion detection system

1. INTRODUCTION

Cognitive radio networks will support dynamic spectrum access (DSA). However, in spite of the potential benefits for DSA, the open nature of the wireless medium will make cognitive radios a powerful tool for conducting malicious activities or policy violations by secondary users [1]. Therefore, detecting malicious users or unlicensed activities is a crucial problem facing DSA. The challenge of enforcing the proper usage of spectrum requires an intrusion detection system (IDS) that will scan spectrum and identify anomalous activities [2]. Towards this objective, there have been several foundational efforts involving signal processing techniques that can be applied to spectrum scanning. For example, in [3], 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 [4]. Factors like noisy and fluctuating channels were considered in [5]. Energy detection of a signal with random amplitudes was studied in [6]. Even more, the impacts brought by quantization and dynamic range differences were surveyed in [7].

Since there are two agents with different goals (the IDS, which aims to detect illegal spectrum usage; and the adversary who intends to use the bands illegally), game theory is the ideal tool to employ. In [8], readers can find a comprehensive survey of research that examines security and privacy problems in computer networks via game-theoretic approaches. Some relevant work includes: the protection of a network under uncertain attack-type[9], jammer detection [10], detection of mobile intruder [11], self-adaptation mechanisms for IDS [12], for heterogeneous networks of nodes with non-correlated security assets [13], for detection of the intruder with uncertainty about used application [14], for dropping-packet attacks [15]. In [16] and [17], the authors present a tiling-based scanning algorithm for detecting an intruder signal in a wide amount of bandwidth, which is directly relevant to this paper.

The above literature, however, does not consider the dynamic interaction between the intruder, the IDS, and the technical characteristics of the spectrum scanner across the bands of interest. In particular, IDSs will have non-uniform detection characteristics across large swaths of bandwidth– a fact that can be exploited by both the intruder and the IDS. In this paper we examine the problem of how knowledge regarding the IDS detection capabilities across spectrum bands can be incorporated into scanning protocol to increase its efficiency. We also examine how such knowledge can be used by the adversary to arrive at two extreme cases for the knowledge the intruder might have: (a) complete knowledge on the IDS's technical characteristics (a smart intruder), and (b) no knowledge (naive intruder). Further, we examine how the IDS can adapt its belief about the intruder's knowledge during the scanning process.

The organization of this paper is as follows: in Section 2, we formulate and solve a single time-slot scanning problem. Then, in Section 3 we extend the formulation to incorporate repeated scanning, where the scanning and intrusion strategies are adapted through a Bayesian approach to incorporate the result of the previous time slot's scanning. In Section 4 implementation of the considered game is given using a testbed of USRP N210s and USRP X310s. In Section 5, we conclude the paper.

2. A SINGLE TIME SLOT SCANNING

We now formulate the problem of scanning and intruding over a large swath of bandwidth. We assume the total bandwidth consists of n bands. In our formulation, a signal can be transmitted in *one* of the n bands by the intruder. The IDS consists of a single sensor (scanner) that, at any time period, can only scan one of the n bands. In this subsection we assume that transmission and scanning are performed during a single time slot.

Let the intruder transmit a signal in band i. Then, if the sensor scans this band, the probability of the intruder's detection will be denoted q_i, which depends on the sensor and environment characteristics (e.g. non-uniform background interference, or non-uniform profile for the sensor's RF front-end). If the sensor scans a band different than the band being intruded upon, then the intruder is not detected (i.e. detection probability is 0). For the sake of tractability, we assume that the detection probability q_i depends on SINR (Signal-to-interference-plus-noise ratio) at the sensor. Further, we assume that we have an expected received power level associated with the intruder signal at the receiver (e.g. we assume the intruder uses a known power, and is located within a certain distance of the scanner). Thus, since SINR depends on background noise and interference levels, which can be different for different bands, the detection probability q_i also might vary with the band i.

The scanning strategy for the IDS may be thought of as a vector $\boldsymbol{x} = (x_1, \dots, x_n)$ assigning the probability that the scanner will scan each particular band. The strategy for the intruder depends on his type, which in this case corresponds to his knowledge about the IDS. If the intruder has no knowledge about the IDS (i.e., the probabilities q_i), then his optimal strategy is to intrude on the bands in a uniformly random way (i.e., with probability $1/n$ for each band). If the intruder has complete knowledge of the IDS's characteristics, then his strategy is the probability vector $\boldsymbol{y} = (y_1, \dots, y_n)$ assigning the probability (frequency) for the intruder to intrude in each of the bands. We assume that there is a priori knowledge on the intruder's type, namely, either the intruder might be a smart adversary with probability γ_1, or he might be naive with probability γ_0, or he might not be present at all in the total swath of bandwidth with probability γ_2. Thus, $\sum_{i=0}^{2} \gamma_i = 1$.

We assume that all these probabilities are known to the rivals. The payoff to the IDS is the detection probability, i.e., $v_{IDS}(\boldsymbol{x}, \boldsymbol{y}) = \gamma_1 v_{I1}(\boldsymbol{x}, \boldsymbol{y}) + \gamma_0 v_{I0}(\boldsymbol{x})$, where $v_{I1}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} q_i x_i y_i$ and $v_{I0}(\boldsymbol{x}) = \sum_{i=1}^{n} q_i x_i / n$ are the detection probability of the smart and naive types of the intruder. The detection probabilities for each type of intruder correspond to the intruder cost functions. The IDS wants to respond to each intruder's strategy by maximizing the detection probability (i.e., his payoff), while the intruder wants to respond to each IDS's strategy by minimizing the detection probability (i.e., his cost function). Such rivals strategies are called best response strategies, and the solution for the best response strategy equations yields equilibrium strategies. Also, note that a priori knowledge regarding the intruder type is employed, and thus the considered game is a Bayesian game [18].

For the sake of simplicity, we assume that all of the bands have different detection probabilities, i.e., $q_i \neq q_j$ for $i \neq j$. Without loss of generality, we can assume that the bands are arranged in decreasing order by their detection probabilities q_i, i.e., $q_1 > q_2 > \ldots > q_n$. The following theorem gives the equilibrium strategies explicitly. In particular, it shows that the IDS always, outside of a switching line Γ for probabilities (γ_0, γ_1) :

$$\Gamma = \{(\gamma_0, \gamma_1) : \; L(\gamma_0, \gamma_1) := \gamma_* \gamma_1 / (1 - \gamma_*) - \gamma_0 = 0\},$$

where $\gamma_* := n/(q_1 Q)$ with $Q = \sum_{j=1}^{n} (1/q_j)$, has a unique equilibrium strategy. The smart intruder has a unique equilibrium if the probabilities (γ_0, γ_1) are located above the switching line Γ. If these probabilities are located below the switching line Γ, then the smart intruder has a continuum of strategies equivalent to each other, i.e., they all return the same cost. On the switching line, Γ, the IDS has a continuum of equilibrium strategies that are all equivalent to each other, while the intruder has a unique strategy.

Theorem 1 *(a) If the probabilities (γ_0, γ_1) are located above the switching line, i.e.,*

$$L(\gamma_0, \gamma_1) > 0, \tag{1}$$

then there is a unique equilibrium $(\boldsymbol{x}, \boldsymbol{y})$ given as follows:

$$\begin{aligned} &x_i = 1/(q_i Q), \\ &y_i = (1/(q_i Q) - \gamma_0/n)/\gamma_1 \text{ for } i \in [1, n] \end{aligned} \tag{2}$$

with the expected payoff to the IDS given as follows

$$v_{IDS} = 1/Q,$$

and the same costs for either the smart or naive intruder, i.e.,

$$v_{I1} = v_{I0} = 1/Q.$$

(b) If the probabilities (γ_0, γ_1) are located below the switching line, i.e.,

$$L(\gamma_0, \gamma_1) < 0, \tag{3}$$

then there is a unique equilibrium scanning strategy $\boldsymbol{x}$, and a continuum of the smart intruder strategies $\boldsymbol{y}$, where

$$\boldsymbol{x} = (1, 0, \dots, 0),$$

$$y_i \begin{cases} = 0, & i = 1, \\ \leq \dfrac{\gamma_0 (q_1 - q_i)}{n \gamma_1 q_i} \text{ such that } \sum_{j=2}^{n} y_j = 1, & i \in [2, n], \end{cases}$$

with the expected payoff to the IDS

$$v_{IDS} = \gamma_0 q_1 / n,$$

and the costs to the smart and naive types of invader:

$$v_{I1} = 0,$$

and

$$v_{I0} = q_1 / n,$$

correspondingly.

(c) If the probabilities (γ_0, γ_1) are located on the switching line, i.e., $L(\gamma_0, \gamma_1) = 0$, then there is a unique smart intruder's strategy $\boldsymbol{y}$ given by (2), and a continuum of IDS scanning strategies

$$x_i = \begin{cases} 1 - \epsilon \sum_{j=2}^{n} (1/q_j), & i = 1, \\ \epsilon / q_i, & i \in [2, n], \end{cases}$$

for any positive ϵ such that $\epsilon < 1/Q$.

3. REPEATED SCANNING WITH ADAPTING BELIEFS

In this section we extend the single time slot scanning problem to the case of multiple time slots as a *repeated* game in time slots $t = 1, 2, \ldots$. At the beginning of each time slot the rivals can adapt their a priori probabilities. Denote by γ_i^t, $i \in [0, 2]$ for the time slot t, the adapted probabilities associated with the belief that there is either a smart or naive intruder, or he is not present in the network, where $\gamma_i^1 = \gamma_i$,

$i \in [0,2]$. Let $(\boldsymbol{x}^t, \boldsymbol{y}^t)$ be a pair of equilibrium strategies at time slot t, where $(\boldsymbol{x}^1, \boldsymbol{y}^1) = (\boldsymbol{x}, \boldsymbol{y})$ is given by Theorem 1. The probability that the invader is not detected at time slot t, if he is a smart adversary, is $1 - v_{I1}(\boldsymbol{x}^t, \boldsymbol{y}^t)$. Similarly, the probability that the invader is not detected at time slot t, when he is a naive adversary, is $1 - v_{I0}(\boldsymbol{x}^t, \boldsymbol{y}^t)$. Then, by Bayes' theorem, the adapted beliefs for the time slot $t+1$ are given as follows:

$$\begin{aligned}
\gamma_i^{t+1} &= \frac{\gamma_i^t(1 - v_{Ii}(\boldsymbol{x}^t, \boldsymbol{y}^t))}{\gamma_2^t + \gamma_1^t(1 - v_{I1}(\boldsymbol{x}^1, \boldsymbol{y}^1)) + \gamma_0^1(1 - v_{I0}(\boldsymbol{x}^t, \boldsymbol{y}^t))}, i = 0, 1,\\
\gamma_2^{t+1} &= \frac{\gamma_2^t}{\gamma_2^t + \gamma_1^t(1 - v_{I1}(\boldsymbol{x}^1, \boldsymbol{y}^1)) + \gamma_0^1(1 - v_{I0}(\boldsymbol{x}^t, \boldsymbol{y}^t))}.
\end{aligned} \tag{4}$$

By (4), the inequality $\gamma_2^{t+1} > \gamma_2^t$ is equivalent to the following inequality $\gamma_2^t + \gamma_1^t(1 - v_{I1}(\boldsymbol{x}^1, \boldsymbol{y}^1)) + \gamma_0^t(1 - v_{I0}(\boldsymbol{x}^t, \boldsymbol{y}^t)) < 1$. This inequality clearly holds for any t. Thus, γ_2^t is increasing and upper-bound by 1. Thus, it converges, and, by (4), it converges to 1 and, hence, γ_0^t and γ_1^t converge to zero, if the a priori probability that the invader might not be present is positive.

Using Theorem 1, the adapted probabilities (4) can be given explicitly as follows:

(i) if $L(\gamma_0^t, \gamma_1^t) > 0$ then

$$\begin{aligned}
\gamma_i^{t+1} &= \frac{\gamma_i^t(1 - 1/Q)}{\gamma_2^t + (\gamma_1^t + \gamma_0^t)(1 - 1/Q)}, i = 0, 1,\\
\gamma_2^{t+1} &= \frac{\gamma_2^t}{\gamma_2^t + (\gamma_1^t + \gamma_0^t)(1 - 1/Q))},
\end{aligned} \tag{5}$$

(ii) if $L(\gamma_0^t, \gamma_1^t) < 0$ then

$$\begin{aligned}
\gamma_0^{t+1} &= \frac{\gamma_0^t(1 - q_1/n)}{\gamma_2^t + \gamma_1^t + \gamma_0^t(1 - q_1/n)},\\
\gamma_i^{t+1} &= \frac{\gamma_i^t}{\gamma_2^t + \gamma_1^t + \gamma_0^t(1 - q_1/n)}, i = 1, 2.
\end{aligned} \tag{6}$$

We separately consider two cases: (a) $\gamma_2 = 0$, and (b) $\gamma_2 > 0$.

Case (a): Let $\gamma_2 = 0$, then, by (5), if (1) holds, then scanning does not allow one to improve their knowledge regarding the intruder's type, since $\gamma_i^{t+1} = \gamma_i^t$ for $i = 0, 1$ and any t. Let (6) hold. By (6), $\gamma_0^{t+1} < \gamma_0^t$ and $\gamma_1^{t+1} > \gamma_0^t$, and if the condition of (ii) holds for any i, then γ_1^t tends to 1, and γ_0^t tends to zero. Since $\gamma_2 = 0$, the condition of (ii) is equivalent to $\gamma_0^t > \gamma_*$. Thus, there is a t_* such that $\gamma_0^{t_*-1} > \gamma_* \geq \gamma_0^{t_*}$, and the IDS can adapt his belief on the intruder's type until time slot t_*, after that his belief stabilizes.

Case (b): Let $\gamma_2 > 0$. Then, while the condition of (i) holds, the updates to both probabilities γ_i^t for $i = 0, 1$ are decreasing, i.e. $\gamma_i^{t+1} < \gamma_i^t$ for $i = 0, 1$. While if the condition of (ii) holds, the updated probability γ_0^t is decreasing, and the updated probability γ_1^t is increasing in such a way that the sum $\gamma_0^t + \gamma_1^t$ is decreasing.

Further, we note that, although the scanning parameters depend continuously on the a priori probabilities, the sensor's optimal strategy consists only of two modes, and each of them is the optimal response to a specific intruder type. Thus, the IDS manages to solve this "running after two hares" problem by scanning according to the most likely intruder type for the current time slot, and then switching its scanning at an appropriate time when the most-likely intruder type changes.

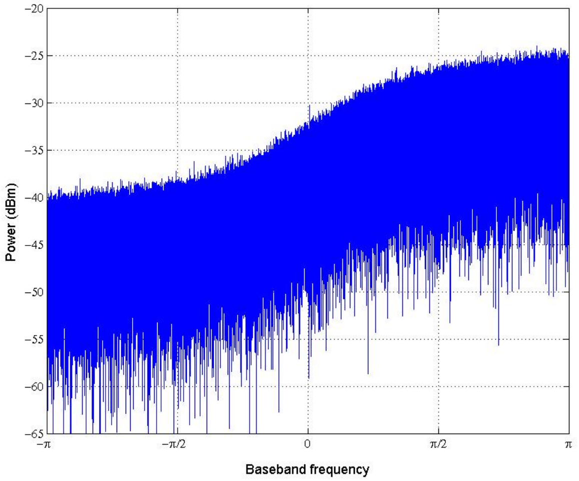

Fig. 1. Power versus frequency profile for the artificial interference signal used to control the detection probabilities in our scanning experiment. The frequency axis is presented in normalized baseband frequency $[-\pi, \pi]$. The actual bandwidth spanned was 200 MHz.

4. SCANNING EXPERIMENT RESULTS

In order to explore the behavior of our scanning strategies in a realistic setting, we implemented the game using the ORBIT wireless testbed[20]. Specifically, we used the ORBIT grid nodes equipped with USRP software defined radio devices for creating the intruding signal transmission as well as for implementing the IDS.

Our IDS scanned a total bandwidth consisting of 200 MHz, starting from 600 MHz and ending at 800 MHz. The IDS scanning and the intruding signal transmission were performed using USRP N210 devices. Given the hardware limitations associated with the USRP N210's, the scan bandwidth we used was 20 MHz, and thus the total bandwidth of 200 MHz was divided into ten 20 MHz wide bands, with different probabilities of detection for each band. In order to emulate a non-homogenous RF environment, we introduced artificial background interference (i.e. noise) so that we could effectively control the detection probabilities across the different bands. Due to the bandwidth limitations associated with the USRP N210 radio device, it was necessary for us to implement our 200 MHz of artificial interference using a different radio device. In this experiment, we decided to use a USRP X310 software-defined radio to transmit our interference into the environment. The frequency-response profile for our interference, in dBm scale, is shown on Figure 1. Here we note that x-axis corresponds to 200 MHz of baseband frequency, which has been normalized to $[-\pi, \pi]$. Using this interference signal as the background interference, we effectively controlled the detection probabilities for our 200 MHz

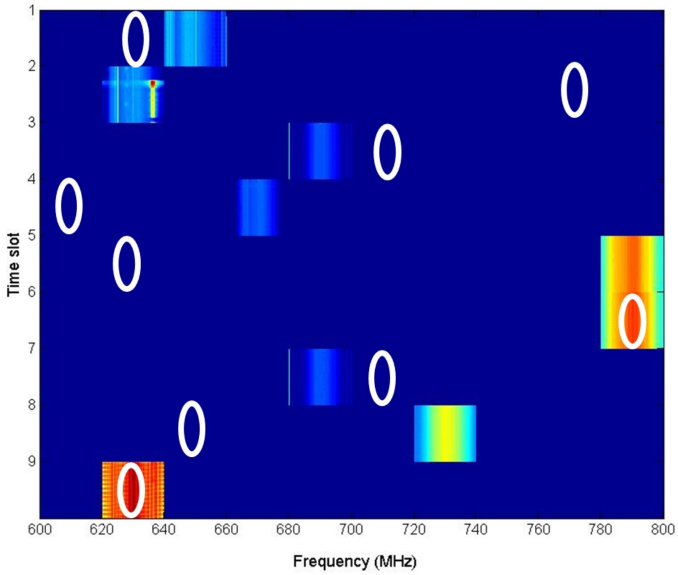

Fig. 2. An example run of the repeated spectrum game that was implemented using USRP N210s and a USRP X310 on the ORBIT wireless testbed. In the spectrum scanning game presented, the white ovals illustrate the band associated with the intruder's location.

of interest. In particular, to estimate the detection probabilities q_i used in our formulation from Section 3, we determined the signal-to-interference levels (SINR) by separately measuring the background interference alone, and the interference with the intruder signal present. In order to arrive at detection probabilities, we used the formula given in [19]:

$$P_D \approx Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{\frac{N}{2}}10^{\frac{SINR}{10}}}{10^{\frac{SINR}{10}}+1}\right), \tag{7}$$

where N is the number of time samples taken into the calculation of SINR, and P_{FA} is the desired probability of false alarm, which in our case was 0.05. The resulting detection probabilities ranged from 0.32 up to 0.76 in the less-interfered bands.

In Figure 2, we present both the intruder and scanner behavior for a short run of a repeated scanning game where the beliefs regarding the intruder being present were adapted. In this short experiment, the time slot duration was taken to be 1 second. For each 20 MHz band that was scanned by the IDS, a moving average 64-point FFT was performed. The figure shows the total 200 MHz of bandwidth used in the example game, where only the scanned bands and their associated smoothed spectrum are presented with nonzero power in the corresponding time slots. We have also depicted, using white ovals mark, the bands that were chosen at each time slot by the intruder. In particular, in the run of this game that we present, during time slot 6 the intruder and the IDS chose the same band, but the detection failed due to the high levels of background interference present in that band. Later, in time slot 9, the intruder and the IDS used the same band, but in this case the intruder was caught in the band centered around 630 MHz, which had less background interference.

5. CONCLUSIONS

In order to support the scanning of large amounts of bandwidth, we have outlined a new scanning paradigm that incorporates knowledge regarding the technical specifications (i.e. detection probabilities) associated with a spectrum scanning intrusion detection system. Since the adversary can also leverage knowledge of the IDS technical characteristics to its advantage, there is an inherent tradeoff between the benefits that such knowledge provides the IDS and the benefits to the intruder. To illustrate this tradeoff, we have formulated a Bayesian game theoretical model between an intruder and the scanner, where the knowledge the intruder has about the IDS is associated with the knowledge of the IDS detection probabilities.

In this game, the IDS has to solve a scanning allocation dilemma: if the intruder is naive and has no knowledge of the IDS's capabilities, then all of the spectral bands are under an equal threat (probabilistically); while, if the intruder is smart and has complete knowledge of the IDS's capabilities across spectrum bands, then less-effective bands are under higher threat of intrusion. We solve this problem for a scanning game involving a single time slot, as well as for a repeated scanning game in which the knowledge the intruder has regarding the IDS is adaptively updated. For the single time slot scanning game, the equilibrium strategies are found explicitly, and it was shown that the IDS always, outside of a switching line for probabilities (γ_0, γ_1) has a unique equilibrium, where γ_0 is the IDS's a priori probabilistic belief that the intruder is naive, and γ_1 is the IDS's a priori probabilistic belief that the intruder is smart. The smart intruder has a unique equilibrium if probabilities (γ_0, γ_1) are located above the switching line. If these probabilities are located below the switching line, the smart intruder has a continuum of strategies equivalent to each other, i.e., they all return the same cost. On the switching line, the IDS has a continuum of equilibrium strategies, while the intruder has a unique strategy, which also equivalent to each other. The optimal IDS strategy switches between the optimal response to each of these threats, while the intruder can act more flexibly by tuning his strategy continuously with respect to his knowledge of the IDS characteristics. Due to its discontinuity, the strategy might be sensitive to a priori knowledge, which can be corrected by further adapted learning.

For the repeated, multiple time slot game, we provided an explicit formulation for updating the IDS's knowledge regarding the type of intruder it is facing using a Bayesian approach. We also proved the convergence of our adaptive learning strategies. We then demonstrated the implementation of our scanning game and the associated adaptive-learning scanning strategies using a testbed of software-defined radios. A goal of our on-going work is to develop the suggested approach for an IDS consisting of multiple spectrum sensors, where the detection probability can depend on both the characteristics of each spectral band as well as on the mutual geographical locations of the sensors and the intruder.

Acknowledgements: This material is based upon work supported by the National Science Foundation under ECCS-1247864.

6. REFERENCES

[1] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A trusted radio infrastructure for enforcing spectrum etiquettes," in *Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, 2006, pp. 101–109.

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

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

[4] 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.

[5] K. Cai, V. Phan, and R. O'Connor, "Energy detector performance in a noise fluctuating channel," in *Proceedings of Military Communications Conference (MILCOM '89)*, 1989, vol. 1, pp. 85Ű–89.

[6] V. Kostylev, "Energy detection of a signal with random amplitude," in *Proceedings of IEEE International Conference on Communications (ICC 2002)*, 2002, vol. 3, pp. 1606–1610.

[7] S. Koivu, H. Saarnisaari, and M. Juntti, "Quantization and dynamic range effects on the energy detection," in *Proceedings of the 6th Nordic Signal Processing Symposium (NORSIG 2004)*, 2004, pp. 264–267.

[8] 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.

[9] 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.

[10] A. Garnaev, Y. Hayel, and E. Altman, "A jammer's dilemma: where and how to jam," in *Proceedings of 2012 6th International Conference on Network Games, Control and Optimization (NetGCooP)*, 2012, pp. 69–73.

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

[12] J. Stiborek, M. Grill, M. Rehak, K. Bartos, and J. Jusko, "Game theoretical adaptation model for intrusion detection system," in *Proceedings of 10th International Conference on Practical Applications of Agents and Multi-Agent Systems*, 2012, pp. 201–210.

[13] L. Chen, "A game theoretical framework on intrusion detection in heterogeneous networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 165–178, 2009.

[14] 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)*, 2012, pp. 1054–1059.

[15] M. Estiri and A. Khademzadeh, "A game-theoretical model for intrusion detection in wireless sensor networks," in *Proceedings of 2010 23rd Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2010, pp. 1–5.

[16] 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 (CROWNCOM)*, 2013, pp. 148–153.

[17] A. Garnaev and W. Trappe, "Stationary equilibrium strategies for bandwidth scanning," in *Proceedings of MACOM 2013*, M. Jonsson and et al, Eds. 2013, vol. 8310 of *LNCS*, pp. 168–183, Springer.

[18] G. Owen, *Game theory*, Emerald Group Publishing Limited, 1995.

[19] S.M Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*, Prentice Hall, 1998.

[20] "Orbit: Open access research testbed for next-generation wireless networks," http://www.orbit-lab.org.