SPECTRUM ATTACKS AIMED AT MINIMIZING SPECTRUM OPPORTUNITIES

Andrey Garnaev[⋆] *Wade Trappe*[⋆] *Y. Thomas Hou*[†] *Wenjing Lou*[†]

[⋆] WINLAB, Rutgers University, North Brunswick, NJ USA
[†] Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA USA

ABSTRACT

Unutilized spectrum, i.e. spectrum holes, are opportunities that may be used for communication or other RF services. In this paper, we explore adversarial attacks that reduce the size of spectrum holes by showing their advantage compared to a random jammer. Using a game-theoretical approach, we design an optimal scanning strategy that provides an increased probability of detecting such an attack. The advantage of our strategy is achieved by focusing scanning efforts on bands that are more likely to be attacked, and neglecting the others. However, such focused scanning is a disadvantage since, if the adversary has a different objective, he can safely sneak usage of the bands neglected by such a specially-tuned spectrum scanner. To deal with this problem, we also derive the optimal scanning allocation that balances between applying the anti-spectrum holes attack scanning strategy and scanning the neglected bands so as to prevent the possibility of the adversary using those bands without being detected.

Index Terms— Spectrum scanning, spectrum holes, jamming, game theory

1. INTRODUCTION

The explosive growth of commercial wireless technologies will severely impact the operation of a wide array of radio frequency (RF) systems by reducing available radio spectrum. Since radio spectrum is a finite resource, and the gap between RF supply and demand will widen, there is a significant challenge that must be addressed in order to improve efficient spectrum utilization. One important approach to increase spectrum efficiency is to apply cognitive RF capabilities that locate spectrum opportunities (i.e., spectrum holes) that may be used for communication or adapting other services that use RF, such as position and navigation solutions. On the other hand, the open and dynamic nature of the wireless medium make such cognitive RF systems susceptible to malicious attacks, especially those involving jamming or interference. A reader can find comprehensive surveys of such threats in [1, 2]. Such threats can be quite simple, say, like a random jammer's attack or quite sophisticated, like ab *emulation* attack whereby a malicious user emulates a licensed primary user to obtain the resources of a given channel and wards-off other users from using the channels.

As new spectrum-adaptive wireless technologies are developed, there are new threats that arise associated with that wireless technology and can be tuned in a way to benefit the adversary. In particular, although a spectrum opportunity might open up and be utilized by a cognitive radio scanning spectrum, these spectrum holes can also be easily closed by an adversary that injects interference to *close* spectrum holes. Consequently, there are deep challenges associated with detecting an adversary attempting to make these spectrum opportunities unavailable. In this paper, to get insight into this problem, we *first* show by means of a simple model that an adversary's attack aimed to reduce the size of spectrum holes is more dangerous for spectrum utilization than a random jammer. *Secondly*, using a game-theoretical approach, we design the optimal spectrum scanning strategy as well as the optimal adversary's strategy for closing spectrum holes. We prove the efficiency of such scanning compared with random scanning. This efficiency is achieved by focusing scanning on the bands that will more probably be attacked and neglecting bands that might be unlikely to be attacked by an adversary intent on reducing the size of spectrum holes. Such focusing of the scanning strategy has its advantages and disadvantages: on the one hand, it is the best response against such "spectrum holes" attack; on the other hand, the spectrum scanner generally cannot know the true objective of the adversary. If the adversary has a different objective, he can take an advantage of such focused scanning and *sneak* usage of the other bands safely. To prevent the possibility of undetected sneaking, we further explore a model that allows one to find the optimal frequency with which to apply the suggested focused scanning strategy, while also scanning the rest of the bands to detect unauthorized usage of those bands.

Since the considered problem has two agents (the spectrum scanner and the adversary) with different objectives, we apply game theory to model the problem as it provides a rich set of mathematical tools to analyze such conflicted multi-agents scenarios. In [3], readers can find a structured and comprehensive survey of research contributions that analyze and solve security and privacy problems using game theory. Here, as examples of game-theoretic approaches, we mention just a few such works: the problem of fighting jamming with jamming was explored in [4]. A spectrum coexistence problem was investigated in [5]. The interactions between a user and a smart jammer regarding their respective choices of transmit power was explored in [6], 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 [7], attack-type uncertainty on a network was investigated in [8], an optimal tiling-scanning strategy to detect an intruder in bandwidth was designed in [9], the competitive interactions in adaptive packetized wireless communications was studied in [10], and the uncertainty associated with the objective of ille-

gal spectrum activity was studied in [11, 12], while resilience of LTE networks and mobile devices against smart jamming attacks were modelled in [13] and in [14] correspondingly. 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 [15], anti-jamming strategies facing an unknown type of low-power jamming attack was studied in [16], and a network protection problem, where it is unknown whether an adversary is going to play Stackelberg equilibrium or Nash equilibrium, was solved in [17].

The organization of this paper is as follows: in Section 2 a model of adversary's attack on spectrum holes is presented. In Section 3, we formulate a scanning strategy (anti-spectrum hole attack scanning) that is designed to detect an adversary intent on closing spectrum holes. Next, in Section 4, we explore the optimal balance between random scanning and applying such an anti-spectrum hole attack scanning when the adversary might not be intent on attacking. Finally, in Section 5, conclusions and discussions are offered.

2. ADVERSARY'S ATTACK ON SPECTRUM HOLES

In this section, we describe a basic model for an attack that is intent on reducing opportunities associated with "spectrum holes" (i.e. periods of times for which spectrum bands are unused). For simplicity, we shall assume that this spectrum has been divided into n separate bands, and that each band may or may not be utilized at any instant by benign users. For example, a particular band might be allocated for continual DTV usage, while another band might be occasionally used in support of medical purposes. We assume that there is a probability p_i that band i is being used at any particular instant. Then, there is a probability $1-p_i$ that band i is not being used at any particular instant. An alternative view for this is that p_i describes the frequency with which band i is being used.

Due to the fact that p_i can be described as the frequency with which band i is being used, the expected time between signals being transmitted in band i is $T = \sum_{t=1}^{\infty} tp_i(1-p_i)^{t-1} = 1/p_i$. Thus, $1/p_i$ can be interpreted as a distance between two expected transmitted signals. Note that, if a band is in use all of the time, i.e., if $p_i = 1$, there are no spectrum holes in this band at all. In this case, $L_i(p_i) = 1/p_i - 1$ (thus, $L_i(1) = 0$) can be considered as a measure for spectrum hole size. The total size of the spectrum holes is given by $L(\boldsymbol{p}) = \sum_{i=1}^{n} L_i(p_i) = \sum_{i=1}^{n}(1/p_i) - n$. Thus, knowledge of p_i is important for technologies that scan in order to adapt RF usage. Bands with smaller frequencies p_i are more promising for spectrum utilization. On the other hand, such bands are also more plausible targets for malicious attacks aimed to reduce the possibility for such utilization. We assume that the adversary can choose, at any particular instant, to transmit on a single band. In this case, the adversary's strategy is represented as a probability vector $\boldsymbol{y} = (y_1, \ldots, y_n)$, where y_i is the probability that the adversary transmits in band i, i.e., $\sum_{i=1}^{n} y_i = 1$. Then, $q_i = p_i + y_i(1-p_i)$ is the probability that band i is either in use by legitimate users or by the adversary, or both. Thus,

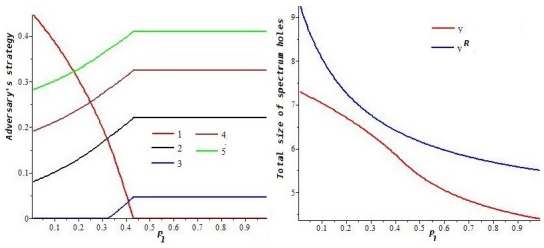


Fig. 1. The adversary's strategies (left) and the total spectrum hole size (right) as functions on probability p_1.

$$v_A(\boldsymbol{y}) = \sum_{i=1}^{n}(1/q_i - 1) = \sum_{i=1}^{n} 1/(p_i + y_i(1-p_i)) - n \qquad (1)$$

can be considered as a *measure for the total size of spectrum holes* of the bandwidth in the presence of the adversary. This measure is a cost function for the adversary. The adversary intends to minimize it, i.e., to find a strategy $\boldsymbol{y}$ such that $\boldsymbol{y} = \arg\min_{\boldsymbol{y}} v_A(\boldsymbol{y})$.

Theorem 1 *The optimal adversary strategy $\boldsymbol{y}$ is unique, and it has a water-filling form given as follows:*

$$y_i = y_i(\omega) := \left\lfloor \left(\sqrt{(1-p_i)/\omega} - p_i \right) /(1-p_i) \right\rfloor_+, i = 1, \ldots, n, \quad (2)$$

where $\omega = \omega_*$ and $\omega_* \in (0, p_*)$ with $p_* = \max_i(1-p_i)/p_i^2$ is the unique root of the equation $\sum_{i=1}^{n} y_i(\omega) = 1$. Due to the left-side of this equation being continuous with respect to $\omega > 0$,and decreasing from infinity for $\omega \downarrow 0$ to zero for $\omega = p_*$, the root ω_* can be found uniquely by the bisection method.

Figure 1(top) illustrates the optimal strategy for the adversary as a function of the probability that band 1 is used by the users for $n = 5$ and $p = (p_1, 0.32, 0.41, 0.25, 0.18)$. The strategy has two switching points $p_1^1 = 0.32$ and $p_1^2 = 0.43$. For $p_1 < 0.32$ bands 1,2,3 and 4 are targets for attack by the adversary, while for $0.32 < p_1 < 0.43$ all five of the bands are under attack, and while for $0.43 < p_1$ bands 2,3,4 and 5 are targets for attack by the adversary. The adversary's strategy $\boldsymbol{y}$ is continuous with respect to p_1, which means it has a small sensitivity to small variations in the frequencies with which the bands are in use by legitimate users. Figure 1(bottom) illustrates that such an adversarial attack strategy is more efficient to achieve the goal of closing the size of spectrum holes than applying an uninformed, random jamming attack $\boldsymbol{y}^R = (1/n, \ldots, 1/n)$ in which the jamming attacks all of the bands with equal probability.

3. SPECTRUM SCANNER

In this section, we consider the situation when the spectrum is being monitored by some form of IDS (i.e. an intrusion detection system, the *spectrum scanner*), which scans the bands to detect malicious activity. We consider that the spectrum scanner can only scan a single band at any time. Then, the strategy for the spectrum scanner is represented by a probability vector $\boldsymbol{x} = (x_1, \ldots, x_n)$, where x_i is the probability

that the spectrum scanner scans band i. The adversary can be detected only if he transmits a signal in the same band i being scanned by the spectrum scanner. In this case, we assume then that the adversary's signal can be detected with certainty. Otherwise, the adversary's signal cannot be detected. The payoff to the scanner is detection probability, i.e., $v_S(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n} x_i y_i$, and the IDS goal is to maximize the payoff.

Then, if the spectrum scanner and the adversary apply strategies $\boldsymbol{x}$ and $\boldsymbol{y}$, we define the adversary cost function:

$$v_A(\boldsymbol{x},\boldsymbol{y}) = \sum_{i=1}^{n} \frac{1-x_i}{p_i+(1-p_i)y_i} - n, \tag{3}$$

which reflects the size of the spectrum holes if the adversary is not detected.

The adversary wants to minimize his cost, while the spectrum scanner wants to maximize his payoff $v_S(\boldsymbol{x},\boldsymbol{y})$. Thus a non zero-sum game arises [18], and we can look for (Nash) equilibrium strategies. Recall that a pair of strategies $(\boldsymbol{x}_*,\boldsymbol{y}_*)$ is a (Nash) equilibrium if and only if

$$v_A(\boldsymbol{x}_*,\boldsymbol{y}_*) \le v_A(\boldsymbol{x}_*,\boldsymbol{y}),\ v_S(\boldsymbol{x},\boldsymbol{y}_*) \le v_S(\boldsymbol{x}_*,\boldsymbol{y}_*)$$

for any $(\boldsymbol{x},\boldsymbol{y})$. Due to v_A being convex in $\boldsymbol{y}$, and v_S being linear in $\boldsymbol{x}$,there is at least one equilibrium [18]. The following theorem proves that the equilibrium is unique and gives it in closed form.

Theorem 2 *In the considered game, the equilibrium $(\boldsymbol{x},\boldsymbol{y})$ is unique and given as follows:*

$$x_i(\omega,\nu) = \begin{cases} 1-\omega\dfrac{(p_i+(1-p_i)\nu)^2}{1-p_i} & i \in I_{11}(\omega,\nu), \\ 0, & i \notin I_{11}(\omega,\nu), \end{cases} \tag{4}$$

$$y_i(\omega,\nu) = \begin{cases} \nu, & i \in I_{11}(\omega,\nu), \\ \dfrac{1}{1-p_i}\left(\sqrt{\dfrac{1-p_i}{\omega}} - p_i\right), & i \in I_{10}(\omega,\nu), \\ 0, & i \in I_{00}(\omega,\nu), \end{cases} \tag{5}$$

where

$$\begin{aligned} I_{00}(\omega,\nu) &= \left\{ i : \frac{1-p_i}{p_i^2} \le \omega \right\}, \\ I_{10}(\omega,\nu) &= \left\{ i : \frac{1-p_i}{(p_i+(1-p_i)\nu)^2} \le \omega < \frac{1-p_i}{p_i^2} \right\}, \\ I_{11}(\omega,\nu) &= \left\{ i : \omega < \frac{1-p_i}{(p_i+(1-p_i)\nu)^2} \right\}, \end{aligned} \tag{6}$$

where $\omega \in (0,p_*)$ and $\nu > 0$ are the unique solution of the equations

$$X(\omega,\nu) := \sum_{i=1}^{n} x_i(\omega,\nu) = 1,\ \ Y(\omega,\nu) := \sum_{i=1}^{n} y_i(\omega,\nu) = 1.$$

The value of the parameters ω and ν can be uniquely defined in two steps:

Step 1: *Since $Y(\omega,\nu)$ is decreasing in $\omega \in (0,p_*]$ for a fixed $\nu > 0$ from infinity for $\omega \downarrow 0$ to zero for $\omega = p_*$, and $Y(\omega,\nu)$ is increasing in ν for a fixed ω from zero for $\nu = 0$ to $\sum_{i=1}^{n} \frac{1}{1-p_i}\left[\sqrt{\frac{1-p_i}{\omega}} - p_i\right]_+$ for ν tending to infinity. Thus, for each $\omega \in (0,\omega_*]$ there exists $\nu(\omega)$ such that $Y(\omega,\nu(\omega)) = 1$. This $\nu(\omega)$ is continuous and increasing from $1/n$ for $\omega = 0$ to infinity while $\omega \uparrow \omega_*$.*

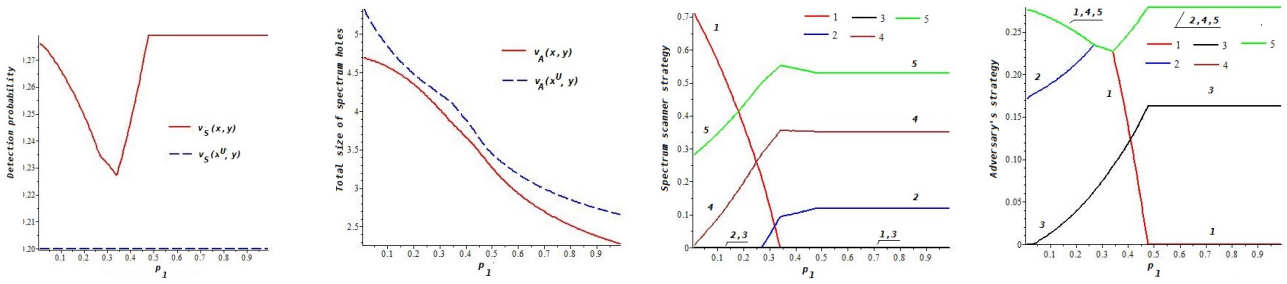
Step 2: *Since $X(\omega,\nu)$ is decreasing in ν and ω, then $X(\omega,\nu(\omega))$ is also decreasing, and ω is defined as the unique root in $(0,\omega_*)$ of the equation $X(\omega,\nu(\omega)) = 1$. Since all of the functions are monotonic, the bisection method can be applied to find $\nu(\omega)$ and ν. Since the suggested algorithm is a superposition of two bisection methods, the complexity of the algorithm is given by product of complexity of these bisection methods. This ν is detection probability of the adversary and $\nu > 1/n$. Thus, the scanning strategy $\boldsymbol{x}$ has higher efficiency compare with uniform scanning strategy $\boldsymbol{x}^U = (1/n,\ldots,1/n)$.*

Figure 2(a) and (b) illustrate an increase in the detection probability as well as an increase in the size of spectrum holes that arises when applying the equilibrium scanning strategy $\boldsymbol{x}$ compared with a uniform scanning strategy $\boldsymbol{x}^U$. This effect is achieved by focusing the scanning efforts on the bands where the spectrum scanner can detect the adversary with largest probability, while neglecting the other bands due to their low contribution in the expected payoff. Namely, for $p_1 < 0.28$ only bands 1,4, and 5 are scanned, for $0.28 < p_1 < 0.33$ bands 1,2, 4, and 5 are scanned, and for $0.33 < p_1$ bands 2,4, and 5 are scanned (Figure 2(c)). We note the interesting phenomena that the adversary uses more bands to attack than the spectrum scanner to scan. Namely, for $p_1 < 0.48$ all of the bands are under attack, while for $p_1 > 0.48$ all of the bands except band 1 are being attacked. This explains why for $p_1 > 0.48$, the adversary's attack strategy is constant.

4. HOW OFTEN TO SCAN THE NEGLECTED BANDS

The advantage of the scanning strategy $\boldsymbol{x}$ is that it is tuned for a jamming attack that seeks to close spectrum holes. This efficiency is achieved by focusing the scanning efforts on the bands that are more likely to be attacked, and neglecting the others. Such focused efforts are also a disadvantage, since the adversary could safely use bands that were neglected by such a tuned strategy. To reduce this disadvantage, the scanning strategy should, from time to time, also scan the remainder of the bands that aren't being scanned by the tuned strategy. Then, a question arises: how often should the revised strategy scan these other bands? To explore this, we consider that the adversary is attempting to sneak usage of the spectrum (and not necessarily to close the spectrum holes), and thus introduce a new type of the adversarial strategy, a *sneaking* strategy $\boldsymbol{y}^S$, by which the adversary randomly uses bands $I_{10} \cup I_{00}$ that are not being scanned by the scanning strategy $\boldsymbol{x}$. To meet this new challenge, the (revised) spectrum scanner should employ both strategy $\boldsymbol{x}$ as well as a new strategy $\boldsymbol{x}^S$ (like an ambush strategy [19]) that scans the bands $I_{10} \cup I_{00}$ with uniform probability.

At any instant, the adversary does not know what type of adversarial mode the spectrum scanner is scanning against; similarly, at any instant, the spectrum scanner does not know what type of attack mode the adversary will actually employ. Thus, the rivals face a dilemma in choosing the proper strategies. This dilemma can be described by the following zero-sum 2×2 matrix game



(a) (b) (c) (d)

Fig. 2. (a) Detection probabilities, (b) total spectrum hole size, (c) the spectrum scanner's strategy and (d) the adversary's strategy as functions of the probability p_1.

$$M = \begin{matrix} \boldsymbol{x} \\ \boldsymbol{x}^S \end{matrix} \begin{pmatrix} \boldsymbol{y} & \boldsymbol{y}^S \\ v_S(\boldsymbol{x},\boldsymbol{y}) & 0 \\ v_S(\boldsymbol{x}^S,\boldsymbol{y}) & v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) \end{pmatrix},$$

where the rows correspond to the spectrum scanner's strategies, and the columns correspond to the adversary's strategies. This payoff matrix reflects two cases of Theorem 2: (a) if $I_{10} \neq \emptyset$ then $v_S(\boldsymbol{x}^S,\boldsymbol{y}) > 0$, and (b) $v_S(\boldsymbol{x},\boldsymbol{y}^S) = 0$. This matrix game has an equilibrium (see [18]). Moreover, this equilibrium involves randomized (mixed) strategies due to $v_S(\boldsymbol{x}^S,\boldsymbol{y}) < v_S(\boldsymbol{x}^S,\boldsymbol{y}^S)$ (since support of $\boldsymbol{y}$ is $I_{10} \cup I_{11}$ while $\boldsymbol{x}^S$ and $\boldsymbol{y}^S$ are uniform strategies in $I_{10} \cup I_{00}$) and $v_S(\boldsymbol{x}^S,\boldsymbol{y}) < v_S(\boldsymbol{x},\boldsymbol{y})$ (since $(\boldsymbol{x},\boldsymbol{y})$ is the equilibrium).

Theorem 3 *The considered game has a unique equilibrium. Namely, with probability, α (α^S), the spectrum scanner should use strategy $\boldsymbol{x}$ ($\boldsymbol{x}^S$), and with probability, β (β^S), the adversary should use strategy $\boldsymbol{y}$ ($\boldsymbol{y}^S$), where*

$$\alpha = \frac{v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) - v_S(\boldsymbol{x}^S,\boldsymbol{y})}{v_S(\boldsymbol{x},\boldsymbol{y}) + v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) - v_S(\boldsymbol{x}^S,\boldsymbol{y})}, \ \alpha^S = 1-\alpha,$$

$$\beta = \frac{v_S(\boldsymbol{x}^S,\boldsymbol{y}^S)}{v_S(\boldsymbol{x},\boldsymbol{y}) + v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) - v_S(\boldsymbol{x}^S,\boldsymbol{y})}, \ \beta^S = 1-\beta.$$

The detection probability is

$$D = \frac{v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) v_S(\boldsymbol{x},\boldsymbol{y})}{v_S(\boldsymbol{x},\boldsymbol{y}) + v_S(\boldsymbol{x}^S,\boldsymbol{y}^S) - v_S(\boldsymbol{x}^S,\boldsymbol{y})}.$$

Figure 3, illustrates some interesting properties of the strategies. The spectrum scanner can maintain a permanent level of security (detection probability) by a strategy that combines the robustness to the environment's parameters (as reflected by the probabilities p_i associated with bands being used by benign users) with sensitivity to its critical values. In other words, it has piece-wise constant structure. Namely, $\alpha = 0.6$ for $p_1 < 0.26$ and $p_1 > 0.32$ while $\alpha = 0.8$ for $0.26 < p_1 < 0.32$. Thus, in each of these intervals the strategy is robust to varying in environment's parameters (as well as in related varying in the adversary's attack). While, at the critical points $p_1 = 0.26$ and $p_1 = 0.32$, it becomes very sensitive and it changes by a jump discontinuity. Although, the adversary strategy is continuous in p_1 (so, less sensitive to such varying), in contrast, the spectrum strategy requires very precise (i.e., small) tuning to each small variation of the environment's parameters. The adversary, with higher probability, applies a minimize spectrum hole attack than it chooses

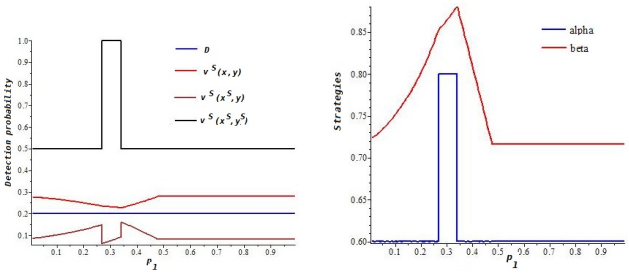


Fig. 3. Detection probabilities (left) and the spectrum scanner's strategy (right) as functions of the probability p_1.

to sneak usage of the bandwidth. The spectrum scanner, in response, also with higher probability tries to meet such an attack instead of responding to sneaking usage. Is it quite an interesting and surprising result that it is possible that the spectrum scanner cares about the sneaking attack (and, so, about the neglected bands) with higher probability than the adversary intends to actually attack them, namely, $\alpha^S > \beta^S$ due to $\alpha < \beta$.

5. CONCLUSIONS

In this paper, we showed that a specially-aimed attack can be devised that reduce the availability of spectrum holes, and thus could present a dangerous attack for spectrum utilization. To reduce the impact of such an attack, we used a game-theoretical approach to arrive at a scanning strategy that gives an increase in efficiency in detecting such an attack. This improvement is achieved by focusing the scanning on the most bands that are most promising from the adversary's point of view. However, an adversary might have other objectives in mind and could exploit the bias of the scanning strategy to instead sneak usage of (or even interfere with) bands being neglected by the best response algorithm. We thus found a revised scanning strategy that combines the possibility of the adversary trying to close spectrum holes with the possibility that it is merely trying to use the spectrum bands. The goal of our future work is to advance the formulation for more sophisticated adversarial behaviour when the adversary could have more nuanced objectives, and to incorporate more general detection rules associated with the scanner detecting an adversarial transmission.

6. REFERENCES

[1] A.G. Fragkiadakis, E.Z. Tragos, and I.G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 15, pp. 428–445, 2013.

[2] J. Marinho, J. Granjal, and E. Monteiro, "A survey on security attacks and countermeasures with primary user detection in cognitive radio networks," *EURASIP Journal on Information Security*, vol. 4, pp. 1–14, 2015.

[3] 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.

[4] L. Chen and J. Leneutreb, "Fight jamming with jamming - a game theoretic analysis of jamming attack in wireless networks and defense strategy," *Computer Networks*, vol. 55, pp. 2259–2270, 2011.

[5] A. Garnaev and W. Trappe, "One-time spectrum coexistence in dynamic spectrum access when the secondary user may be malicious," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 1064–1075, 2015.

[6] L. Xiao, J. Liu, Q. Li, N.B. Mandayam, and H.V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 2578–2590, 2015.

[7] R. El-Bardan, S. Brahma, and P.K. Varshney, "Power control with jammer location uncertainty: A game theoretic perspective," in *Proc. 48th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, 2014.

[8] 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.

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

[10] K. Firouzbakht, G. Noubir, and M. Salehi, "On the performance of adaptive packetized wireless communication links under jamming," *IEEE Trans. on Wireless Communications*, vol. 13, pp. 3481–3495, 2014.

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

[12] A. Garnaev and W. Trappe, "A bandwidth monitoring strategy under uncertainty of the adversary's activity," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 837–849, 2016.

[13] F.M. Aziz, J.S. Shamma, and G.L Stuber, "Resilience of LTE networks against smart jamming attacks," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp. 734–739, 2014.

[14] L. Xiao, C. Xie, T. Chen, H. Dai, and H.V. Poor, "A mobile offloading game against smart attacks," *IEEE Access*, vol. 4, pp. 2281–2291, 2016.

[15] M. Scalabrin, V. Vadori, A.V. Guglielmi, and L. Badia, "A zero-sum jamming game with incomplete position information in wireless scenarios," in *Proc. 21th European Wireless Conference*, pp. 1–6, 2015.

[16] 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 Transactions on Signal and Information Processing over Networks*, vol. 2, pp. 49–56, 2016.

[17] A. Garnaev, M. Baykal-Gursoy, and H.V. Poor, "Security games with unknown adversarial strategies," *IEEE Transactions on Cybernetics*, vol. 46, pp. 2291–2299, 2016.

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

[19] A.Y. Garnaev, "On a Ruckle problem in discrete games of ambush," *Naval Research Logistics*, vol. 44, pp. 353–364, 1997.