Analysis and Simulation of Sensing Deception in Fading Cognitive Radio Networks

Qihang Peng[†‡], Pamela C. Cosman[‡], and Laurence B. Milstein[‡]
[†]School of Communication and Information Engineering
University of Electronic Science and Technology of China
Chengdu 610054, China, Email: anniepqh@uestc.edu.cn
[‡]Electrical and Computer Engineering Department, University of California, San Diego
San Diego, California 92093-0407, USA, Emails: {pcosman, milstein}@ece.ucsd.edu

***Abstract*—We are interested in determining the sensitivity of a tactical cognitive radio (CR) system to intentional spoofing. That is, we assume the existence of an intelligent adversary whose goal is to attack the CR system by deceiving the secondary users into believing that as many frequency bands as possible are occupied by primary users, thus minimizing the number of bands in which the secondary users attempt to transmit. We refer to this operation by the adversary as "spoofing", and the specific spoofing signal we choose is a partial-band noise waveform. That is, for a given total power level that is available to the adversary, we maximize the average number of false detections incurred by secondary users as a result of the spoofing.**

We consider a channel such that each band experiences flat Rayleigh fading, whereby the fading is independent from band to band, and derive the average number of false detections by the secondary users due to the spoofing. The results obtained for the fading channel are compared to similar results for an additive white Gaussian noise channel (AWGN). They are also compared to a physically unrealizable scenario whereby the spoofing knows the instantaneous fade gains of the spoofing waveform at the victim CR receiver. This latter result is presented as a "worst-case" perspective as to how well the spoofing operation can be expected to perform.

***Index Terms*—cognitive radio, fading, performance analysis, sensing deception.**

I. Introduction

COGNITIVE Radio (CR) [1] is one promising candidate in solving the contradiction between spectrum shortage and low utilization, by allowing secondary users to dynamically access unused spectral bands with only minimal degradation to primary users. A spectral band is accessed by secondary users if it is determined to be vacant through spectrum sensing. The band is unavailable if it is sensed to be busy.

However, this sensing-before-accessing paradigm poses a significant vulnerability in cognitive radio networks [2]. An intelligent adversary can transmit spoofing signals in the bands that are not used by primary users during the sensing interval, so secondary users can be deceived into thinking that these bands are occupied by primary users and should be avoided. These unused bands that are taken to be busy by secondary users are termed false detections. By maximizing the average number of false detections, an optimal noise-spoofing strategy has been derived under additive white Gaussian noise (AWGN) for a power-limited intelligent adversary in [3] and [4], which corresponds to an equal-power, partial-band attack. However, due to the stochastic wireless propagation environment, at any particular instant of time, it is possible that the spoofing signals of the adversary in different spectral bands fade differently. Intuitively, the performance of optimal spoofing by the adversary will be degraded in fading scenarios.

In this paper, the performance of worst-case sensing deception in fading cognitive radio networks is analyzed by maximizing the average number of false detections. The "worst-case" means that the optimal attack of the adversary is obtained based on perfect knowledge of fading coefficients in each band. Therefore, the results correspond to an upper bound on the performance that an intelligent adversary with noise spoofing could achieve in a fading environment, where a radiometer is used by the secondary users for spectrum sensing. Since the objective is non-convex and nonlinear, it is difficult to obtain an analytical solution for the optimal spoofing strategy. However, considering its separable structure, we transform the optimization into a mixed-integer programming problem, by introducing an additional set of constraints. Simulation results show that, with a limited power budget, the performance of the optimal sensing attack in a fading environment is degraded from that in AWGN when the number of allowable bands is so small that the adversary can spoof them all. When the number of allowable bands gets large, the performance of worst-case sensing deception under fading asymptotically approaches that under AWGN. Lastly, since the above results are unrealizable due to the assumption that the adversary knows the channel state information, we present results on the performance of an optimized partial-band noise spoofer, where no such assumption is required.

The remainder of this paper is organized as follows. The system model is presented in Section II, and the mixed-integer programming method is given in Section III. Simulation results and analysis are provided in Section IV, and conclusions are presented in Section V.

II. System Model

The spectral range of interest consists of two types of bands: *busy bands* and *allowable bands*. Busy bands are those

This research was supported by the Office of Naval Research under grant no. N000140810081.

978-1-4244-3709-2/10/$25.00 ©2010 IEEE

currently used by primary users, while the allowable bands are those not currently occupied by primary users. The focus of this paper is on the allowable bands. The allowable bands that the intelligent adversary chooses to put spoofing signals in are termed *spoofed bands*, while the allowable ones that are not spoofed are called vacant bands. The allowable bands that are taken to be busy by secondary users are called *false detections*.

In the spoofed bands, the received signal at a secondary user is composed of both the spoofing signal from the adversary and additive noise, given by

$$x_k(t) = \beta_k j_k(t) + n_k(t) \tag{1}$$

where the subscript k refers to the kth band, $n_k(t)$ is the additive Gaussian noise in the kth band, i.e., $n_k(t) \sim \mathcal{N}(0, \sigma_n^2)$, and $j_k(t)$ is the noise spoofing signal emitted by the adversary in the kth band and has a Gaussian distribution, i.e., $j_k(t) \sim \mathcal{N}(0, \sigma_{J,k}^2)$, where $\sigma_{J,k}^2 = P_k$ and P_k is the spoofing power in the kth band. The signal $j_k(t)$ is attenuated by the channel gain β_k, which is assumed to be constant during the sensing interval. It is assumed that $n_k(t)$ and $j_k(t)$ are independent of each other.

We consider a cognitive radio network where secondary users determine the availability of a spectral band through a radiometer. Using the techniques in [5], the conditional false detection probability in the kth allowable band, p_k, conditioned on β_k, is given by

$$p_k = Q\left(\frac{a}{\beta_k^2 P_k + \sigma_n^2} + b\right) \tag{2}$$

where $a = K/2\sqrt{TW}$, and $b = -\sqrt{TW}$. TW is the integration-time-bandwidth product of the radiometer, and K is the threshold used by the secondary user to declare that a band is busy. Since K results from a predetermined false alarm probability, it is constant for all the allowable bands. Therefore, the conditional average number of false detections, $N_J^{(\beta)}$, conditioned on channel fading coefficients, β, is given by [4]

$$N_J^{(\beta)} = \sum_{k=1}^{N} Q\left(\frac{a}{\beta_k^2 P_k + \sigma_n^2} + b\right) \tag{3}$$

where $\beta = (\beta_1, \beta_2, \cdots, \beta_N)$, and N is the total number of allowable bands. The average number of false detections, N_J, is given by

$$N_J = \sum_{k=1}^{N} \int_0^{+\infty} Q\left(\frac{a}{\beta_k^2 P_k + \sigma_n^2} + b\right) f_{\beta_k}(\beta_k)\, d\beta_k \tag{4}$$

where $f_{\beta_k}(\beta_k)$ is the probability density function of β_k, $k = 1, 2, \ldots, N$.

The performance of the worst-case sensing deception of the intelligent adversary with a power budget P can be obtained by using the following steps:

Step I: Maximizing the conditional average number of false detections, $N_J^{(\beta)}$, for each β, that is

$$\begin{aligned} \max \quad & N_J^{(\beta)} \\ s.t. \quad & \sum_{k=1}^{N} P_k = P \\ & P_k \geq 0 \end{aligned} \tag{5}$$

Step II: Averaging $N_J^{(\beta)}$ over β.

III. Mixed-Integer Programming Approach

It is seen from (2) and (5) that the objective is non-convex and nonlinear. Interestingly, it is separable in the optimization variables P_k. With this specific structure, we can approximate the nonlinear function $N_J^{(\beta)}$ by a piecewise linear function [6]. The optimization in (5) is transformed into the following form:

$$\max \quad \sum_{k=1}^{N} \sum_{i=1}^{L_k} q_{ki} \lambda_{ki} \tag{6}$$

subject to

$$\sum_{k=1}^{N} \sum_{i=1}^{L_k} \eta_{ki} \lambda_{ki} = P \tag{7}$$

$$\sum_{i=1}^{L_k} \eta_{ki} \lambda_{ki} \geq 0 \quad k = 1, 2, \ldots, N \tag{8}$$

$$\sum_{i=1}^{L_k} \lambda_{ki} = 1 \quad k = 1, 2, \ldots, N \tag{9}$$

$$\lambda_{ki} \geq 0 \quad k = 1, 2, \ldots, N;\ i = 1, 2, \ldots, L_k \tag{10}$$

$$\lambda_{ki} \lambda_{kj} = 0 \quad if\ \ |i - j| > 1 \tag{11}$$

where $q_{ki} = Q\left(\frac{a}{\beta_k^2 \eta_{ki} + \sigma_n^2} + b\right)$, where $\eta_{ki}\,(i = 1, 2, \ldots, L_k)$ are the end points of the $L_k - 1$ line segments in the domain $[0, P]$. Note that the constraint (11) is imposed to guarantee the accuracy of approximation, which ensures that only adjacent λ_{ki} can be positive. This constraint complicates the problem, since without (11) the optimization can be directly solved by a simplex method. Now we assign a variable y_{ki} that corresponds to the ith linear segment of the piecewise linear approximation such that [7]

$$y_{ki} = \begin{cases} 1 & \text{if } \lambda_{ki} \neq 0 \text{ and } \lambda_{k,i+1} \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

for $i = 1, 2, \ldots, L_k - 1$. Then the constraint (11) can be replaced as follows:

$$\lambda_{k1} \leq y_{k1}, \quad k = 1, 2, \ldots, N \tag{13}$$

$$\lambda_{ki} \leq y_{k,i-1} + y_{ki}, k = 1, 2, \ldots, N;\ i = 1, 2, \ldots, L_k \tag{14}$$

$$\lambda_{k,L_k} \leq y_{k,L_k-1}, k = 1, 2, \ldots, N \tag{15}$$

$$\sum_{i=1}^{L_k - 1} y_{ki} = 1, \quad k = 1, 2, \ldots, N \tag{16}$$

$$y_{ki} \in \{0, 1\}, \quad k = 1, 2, \ldots, N;\ i = 1, 2, \ldots, L_k \tag{17}$$

By transforming the constraint (11) into constraints from (13) to (17), the resulting optimization becomes a mixed-integer linear programming problem that can be solved using a standard method.

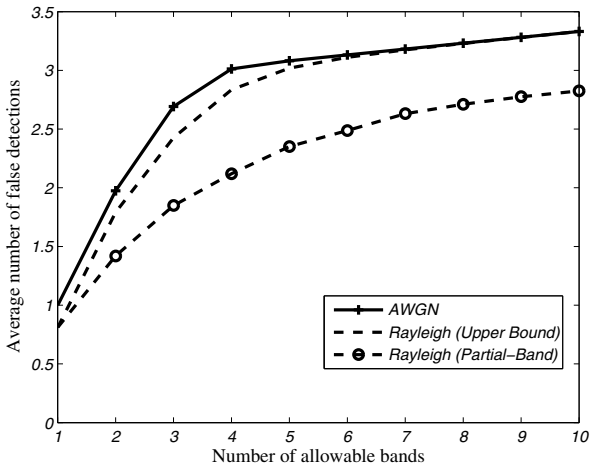

Fig. 1. Average number of false detections versus the number of allowable bands ($E\left[\beta_k^2\right] = 1$, $TW = 100$, $p_f = 0.05$, and $P = 1$)

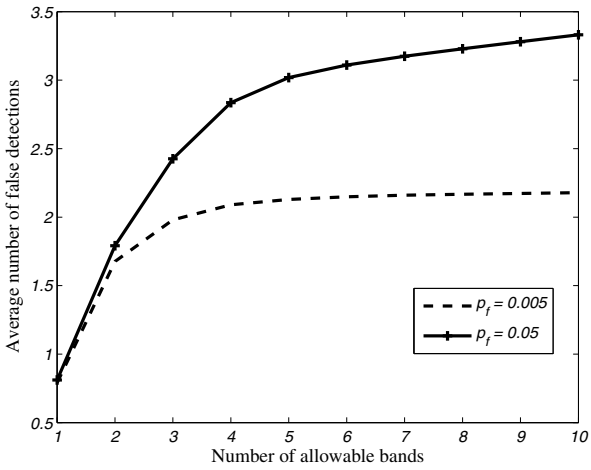

Fig. 2. Average number of false detections versus the number of allowable bands ($E\left[\beta_k^2\right] = 1$, $TW = 100$, and $P = 1$)

IV. Simulation Results and Analysis

In this section, we present the performance of worst-case sensing deception obtained through the algorithm in Section III, as well as the performance of an optimal partial-band noise spoofing strategy [4].

The average number of false detections versus the number of allowable bands is plotted in Fig. 1, where spoofing signals experience i.i.d. Rayleigh fading in each band, with a unit second moment. The thermal noise power is normalized to unity, the integration-time-bandwidth product $TW = 100$, and the false alarm probability $p_f = 0.05$. It is seen from Fig. 1 that, when the number of allowable bands is small, for example $N \leq 5$, the performance of worst-case sensing deception under AWGN is better than that under Rayleigh fading. This is because under this regime, the adversary has enough power to spoof all allowable bands. Under AWGN, the spoofing signals will be received at the secondary user with identical power. However, under Rayleigh fading, the spoofing signals will often be attenuated such that the probability of successful spoofing is reduced. On the other hand, when the number of allowable bands increases, the adversary can spoof only a portion of them, denoted as N^*. Under the fading environment, the intelligent adversary will choose those bands that are not severely faded to spoof. When N increases, the probability that N^* bands are not seriously faded increases. Hence, the performance of worst-case sensing deception with fading asymptotically approaches that under AWGN as N increases.

It is, of course, unrealistic to assume that the adversary knows the fading coefficients and therefore knows which bands to spoof. As a consequence, the performance of the optimal equal-power partial-band noise spoofing with fading is also included in Fig. 1. The optimal number of allowable bands to spoof is obtained numerically by finding the minimum of the average numbers of false detections (averaged over 1000 realizations) when spoofing power is equally spread over n allowable bands, where n varies from 1 to N. It is seen that the

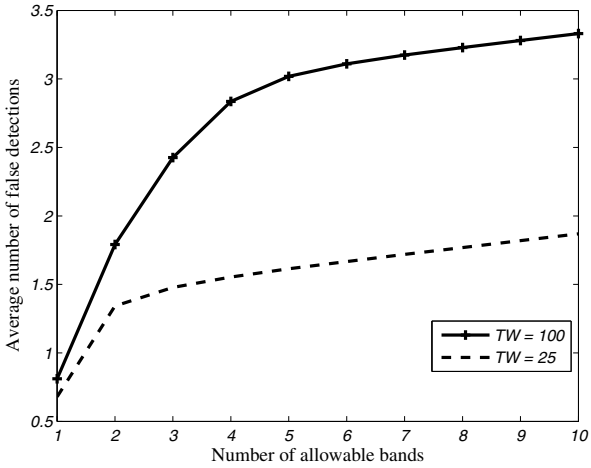

Fig. 3. Average number of false detections versus the number of allowable bands ($E\left[\beta_k^2\right] = 1$, $p_f = 0.05$, and $P = 1$)

average number of false detections under partial-band spoofing is roughly 80% of that under worst-case sensing deception with fading. This performance loss is due to the fact that we have removed the ideal assumption that the adversary knows the instantaneous fading coefficients in each spoofed band. Instead of knowing which bands to spoof, the adversary knows the optimal number to spoof, and then randomly chooses that number of allowable bands out of all the possible choices.

In Fig. 2, the average number of false detections versus the number of allowable bands is plotted, parameterized by the false alarm probability. It is seen that, under i.i.d. Rayleigh fading in each band, the sensing deception performance is improved when the false alarm probability is increased. This is due to the fact that when a secondary user adjusts his threshold to allow a higher false alarm probability, this will allow both a higher false alarm probability due to noise and also a higher rate of success for the adversary.

The average number of false detections parameterized by

TW is illustrated in Fig. 3. It is seen that, when TW increases, the sensing deception performance is improved. This is because, for a fixed bandwidth, an increase in TW means an increase in the integration time of the radiometer, which leads to a more accurate estimation on how much energy is received in this band. Hence, the probability of successful spoofing is increased. On the other hand, for a fixed integration time, an increase in TW means an increase in the bandwidth, which leads to an increase in the number of received samples to be accumulated. Therefore, the ability to distinguish whether the received signal is above the threshold is increased. In either case, an increase in TW means a secondary user will be more likely to correctly detect the existence of a primary user, but will also be more likely to be deceived by the spoofer.

V. Conclusions

In this paper, we consider a "worst-case" sensing deception for a power-limited intelligent adversary under independent fading channels, by maximizing the average number of false detections. The performance of the worst-case sensing deception is obtained by transforming the non-convex, nonlinear optimization into a mixed-integer programming problem, through introducing an additional set of constraints. Simulations show that, when the number of allowable bands is smaller than the optimal number of spoofed bands under AWGN, the worst-case sensing deception performance under AWGN is better than that under fading channels. As N increases, the worst-case sensing deception performance asymptotically approaches that under AWGN.

More realistically, we show the performance of equal-power partial-band spoofing. The average number of false detections under partial-band spoofing with fading is roughly 80% of that under worst-case sensing deception with fading. Under Rayleigh fading, an increase in either the false alarm probability or the integration-time-bandwidth product will increase the probability of successful spoofing for a given level of spoofing power.

References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE JSAC*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[2] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," *IEEE International Conf. on Cognitive Radio Oriented Wireless Networks and Communications*, Aug. 2007, pp. 456-464.

[3] Q. Peng, P. C. Cosman, and L. B. Milstein, "Worst-case sensing deception in cognitive radio networks," *IEEE Globecom*, 2009.

[4] Q. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," *IEEE Transactions on Vehicular Technology*, accepted for publication.

[5] H. Urkowitz, "Energy detection of unknown deterministic signals," in *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523-531, Apr. 1967.

[6] S. S. Rao, *Optimization: Theory and Applications*, 2nd edition, John Wiley and Sons, 1983.

[7] M. A. Bolender and D. B. Doman, "Non-linear control allocation using piecewise linear functions: A linear programming approach," *AIAA Guidance, Navigation, and Control Conference and Exhibit*, Aug. 2004.