Optimal Sensing-Deception Strategy with Fading in Cognitive Radio Networks

Qihang Peng†, Dingyong Hu†, Qicong 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, Emails: {anniepqh, dyhu, qpeng}@uestc.edu.cn
‡Electrical and Computer Engineering Department, University of California, San Diego
San Diego, California 92093-0407, USA, Emails: {pcosman, milstein}@ucsd.edu

***Abstract*—The optimal sensing-deception strategy by a power-limited intelligent adversary of a cognitive radio network is analyzed in this paper. The average number of false detections of the secondary users is maximized when the adversary employs noise spoofing signals, and each such signal experiences multipath-induced fading. The global optimal solution to what turns out to be a nonlinear, non-convex optimization is obtained through a two-step transformation. Numerical results show that, under i.i.d. Rayleigh fading, the optimal sensing-deception strategy for the adversary corresponds to equal-power, partial-band spoofing.**

I. Introduction

Spectrum sensing [1], as one key technology of cognitive radio (CR) networks, can significantly increase spectral efficiency by exploiting available spectral bands for secondary users. However, it is noted that sensing has vulnerabilities [2], especially in a hostile or tactical environment.

If a CR network is exposed to an intelligent adversary, it can put spoofing signals into those bands that are available for secondary users, so that the secondary users are deceived into believing that these bands are occupied by primary users and should not be accessed. Therefore, available bandwidth for the CR network is reduced.

In [3], the authors analyzed the optimal sensing disruption strategy by maximizing the average number of false detections, i.e., minimizing the available bandwidth for the CR network. The optimal strategy for the adversary was shown to be an equal-power, partial-band spoofing. Further analyses in [4] showed that this worst-case spoofing was more effective than traditional jamming when most of the available bandwidth is required by the secondary users.

In [5], the authors analyzed the worst-case sensing deception with fading and showed that the performance asymptotically approaches that under AWGN. The model of [5] corresponds to worst-case results in the sense that it was obtained by assuming that the intelligent adversary had perfect knowledge of the fading coefficients at each sensing interval in each band. In this paper, we relax that assumption by requiring only that the second moment of the fading coefficients is known.

This research was partially supported by the Fundamental Research Funds for the Central Universities under grant number ZYGX2010J003, the Office of Naval Research under grant number N000140810081, and partially supported by the National Science Foundation under grant number CCF-0915727.

The average number of false detections is maximized, subject to a power constraint on the adversary. This is a nonlinear, non-convex optimization. It is difficult to get an analytical solution for how to allocate the adversary's power over the spectral bands of interest. However, we obtain the global optimal solution by a two-step transformation of the optimization: first converting the nonlinear non-convex objective into a piecewise linear function, and then introducing additional integer variables to replace the nonlinear constraints. Numerical results show that, under i.i.d. Rayleigh fading, the optimal sensing-deception strategy for the noise spoofing with fading once again corresponds to an equal-power, partial-band strategy.

The remaining parts of this paper are organized as follows. The system model is presented in Section II, and the globally optimal approach to the sensing-deception strategy is described in Section III. Numerical results and analysis are provided in Section IV, and we give our conclusions and future work in Section V.

II. System Model

In the spectral range of interest, some spectral bands are occupied by primary users (termed *busy bands*), as shown in Fig. 1. The others (termed *allowable bands*) that are not occupied by primary users are available for secondary users. We are interested in these allowable bands. The intelligent adversary puts spoofing signals into them, in order to deceive secondary users into believing that they are being occupied. The allowable bands that are chosen by the intelligent adversary to put spoofing signals in are called *spoofed bands*, while the allowable ones that are not spoofed are termed *vacant bands*. The allowable bands that are taken to be busy by secondary users are called *false detections*.

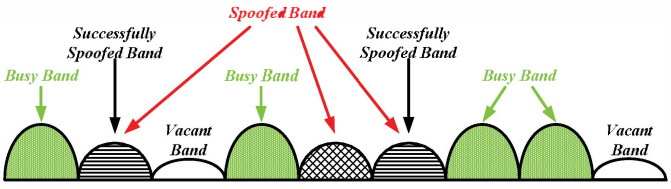

Fig. 1. Spectral band elaboration: Busy bands are ones used by primary users. All others are allowable bands.

For the kth allowable band, if it is spoofed, the received signal at a secondary user's receiver is composed of both the spoofing signal from the intelligent adversary and the additive noise, and is given by

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

where the subscript k indicates the kth allowable band, and $n_k(t)$ is the zero mean additive Gaussian noise, i.e., $n_k(t) \sim \boldsymbol{N}(0, \sigma_n^2)$. The noise spoofing signal emitted by the adversary in the kth band is denoted $j_k(t)$, which follows a Gaussian distribution, i.e., $j_k(t) \sim \boldsymbol{N}(0, P_k)$, where P_k is the spoofing power in the kth band. The parameter β_k in (1) represents flat fading within each subcarrier.

If the band is not spoofed, there is only additive noise received at the secondary user in this band, that is,

$$r_k(t) = n_k(t) \tag{2}$$

The goal of the adversary is to make secondary users believe as many allowable bands as possible are occupied by primary users, thus minimizing the number of bands in which secondary users attempt to transmit. The aim of the intelligent adversary can be interpreted as maximizing the number of false detections. It is shown in [3] that the average number of false detections equals the sum of the false detection probability in each allowable band. If we consider a CR network where a radiometer is used to determine whether the observed band is available to access [6] [7], the conditional false detection probability in the kth allowable band, p_k, conditioned on β_k, can be obtained by using the techniques in [7], and results in

$$p_k = Q(\frac{a}{{\beta_k}^2 P_k + \sigma_n^2} + b) \tag{3}$$

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 is evaluated according to a predetermined false alarm probability [7], it is constant for all the allowable bands. If there is no spoofing signal launched in this band, i.e., $P_k = 0$, (3) reduces to $p_k = Q(a/{\sigma_n}^2 + b)$, which is in accordance with the false alarm probability in [7].

The conditional average number of false detections, $N_J^{(\boldsymbol{\beta})}$, conditioned on the fading coefficients, $\boldsymbol{\beta}$, is given by

$$N_J^{(\boldsymbol{\beta})} = \sum_{k=1}^{N} Q(\frac{a}{{\beta_k}^2 P_k + \sigma_n^2} + b) \tag{4}$$

where $\boldsymbol{\beta} = (\beta_1, \beta_2, ..., \beta_N)$, and N is the total number of allowable bands. By averaging over all β_k, we obtain the average number of false detections, N_J, given by

$$N_J = \sum_{k=1}^{N} \int_0^{+\infty} Q(\frac{a}{{\beta_k}^2 P_k + \sigma_n^2} + b) f_{\beta_k}(\beta_k) d\beta_k \tag{5}$$

where $f_{\beta_k}(\beta_k)$ is the probability density function of $\beta_k, k = 1, 2, ...N$. As mentioned previously, the intelligent adversary attempts to make as many allowable bands as possible seem busy to secondary users, thus maximally reducing available bandwidth for the CR system. However, as a practical matter, the adversary usually has a fixed power budget, and so it has to seek an optimal strategy. The optimal strategy can be formulated as follows:

$$\begin{aligned} &\max N_J \\ &s.t. \\ &\textstyle\sum_{k=1}^{N} P_k = P \\ &P_k \geq 0, \quad k = 1, 2, \ldots, N \end{aligned} \tag{6}$$

where P is the power budget of the intelligent adversary.

III. A Globally Optimal Approach to Sensing Deception With Fading

The objective is nonlinear and non-convex, but the concept of separable programming, where the objective and the constraint functions can be expressed as the sum of single-variable functions, is effective in allowing a convex nonlinear problem to be approximated with arbitrarily accurate piecewise linearization [8]. The global optimum can be obtained by any effective linear programming technique. For a nonlinear and non-convex problem, separable programming is also feasible, but additional processing is needed since, for a non-convex problem, there are possibly multiple local optima [9] [10]. We first transform the nonlinear problem in (6) into piecewise linear functions. Then we introduce additional integer constraints that lead to a mixed-integer linear optimization which can obtain the global optimum by using a standard branch and bound solver [11]. The two-step transformation approach is described below.

A. Piecewise Linearization

Note that the objective in (5) and (6) can be rewritten as

$$N_J = \sum_{k=1}^{N} f_k(P_k) \tag{7}$$

where $f_k(P_k) = \int_0^{+\infty} Q(\frac{a}{{\beta_k}^2 P_k + \sigma_n^2} + b) f_{\beta_k}(\beta_k) d\beta_k$. It is seen from (7) that N_J is a linear combination of $f_k(\cdot)$. We then need to transform each $f_k(\cdot)$ for $k = 1, 2, ..., N$ into a piecewise linear function.

We select $L_k - 1$ line segments, so there are L_k endpoints. Let η_{ki} $(i = 1, 2, ..., L_k)$ denote the endpoints of the $L_k - 1$ line segments in the domain $[0, P]$. The optimization can be transformed into the following form:

$$\max \sum_{k=1}^{N} \sum_{i=1}^{L_k} q_{ki} \lambda_{ki} \tag{8}$$

s.t.

$$\sum_{k=1}^{N} \sum_{i=1}^{L_k} \eta_{ki} \lambda_{ki} = P \tag{9}$$

$$\sum_{k=1}^{N} \sum_{i=1}^{L_k} \eta_{ki} \lambda_{ki} \geq 0, k = 1, 2, ..., N \tag{10}$$

$$\sum_{i=1}^{L_k} \lambda_{ki} = 1, k = 1, 2, ..., N \tag{11}$$

$$\lambda_{ki} \geq 0, k = 1, 2, ..., N; i = 1, 2, ..., L_k \tag{12}$$

$$\lambda_{ki}\lambda_{kj} = 0, if |i - j| > 1 \tag{13}$$

where $q_{ki} = f_k(\eta_{ki}) = \int_0^{+\infty} Q(\frac{a}{\beta_k{}^2\eta_{ki}+\sigma_n^2} + b) f_{\beta_k}(\beta_k) d\beta_k$, and λ_{ki} are non-negative real variables in the domain $[0, 1]$.

Note that the constraint (13) is imposed to guarantee the accuracy of approximation, and ensures that only adjacent λ_{ki} can be nonzero. This constraint complicates the problem, since without (13) the optimization can be directly solved via a simplex method. So we need to find other linear expressions to replace the nonlinear constraint (13), which are described in the following subsection.

B. Mixed Integer Programming

For the L_k breakpoints, there are $L_k - 1$ linear segments. We assign a variable y_{ki} that corresponds to the i^{th} linear segment of the piecewise linear approximation such that [8] [11]

$$y_{ki} = \begin{cases} 1 & \text{if } \lambda_{ki} \neq 0 \text{ and } \lambda_{k,i+1} \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

for $i = 1, 2, ..., L_k - 1$. Then the constraint in (13) can be replaced as follows:

$$\lambda_{k1} \leq y_{k1}, k = 1, 2, ..., N \tag{15}$$

$$\lambda_{ki} \leq y_{k,i-1} + y_{k,i}, k = 1, 2, ..., N; i = 1, 2, ..., L_k \tag{16}$$

$$\lambda_{k,L_k} \leq y_{k,L_k-1}, k = 1, 2, ..., N \tag{17}$$

$$y_{kj} \in \{0, 1\}, k = 1, 2, ..., N \tag{18}$$

By transforming the constraint (13) into (15), (16), (17) and (18), the resulting optimization becomes a mixed-integer linear programming problem. The global optimum can be obtained by choosing from all the local optima via a branch and bound algorithm.

IV. Numerical Results And Analysis

In this section, we analyze the optimal sensing-deception strategies and corresponding performances under fading conditions with numerical examples. Each allowable band is assumed to experience i.i.d. Rayleigh fading.

In Fig. 2 to Fig. 3, we illustrate the optimal sensing-deception strategies for different second moments of the fading gain $\boldsymbol{\beta}$, and different receiver parameters at the radiometer. It is seen that, under various i.i.d. Rayleigh fading scenarios, the optimal sensing-deception strategies correspond to an equal-power, partial-band spoofing, meaning the adversary splits its power evenly across N^* allowable bands, where $1 \leq N^* \leq N$. N^* is called the *optimal number of spoofed bands* hereafter. Recall that the spoofing signal is fading independently and with identical statistics in each band, so, from the adversary's perspective, each allowable band behaves the same statistically. Thus, there is no bias for the adversary to spoof one band over another band. If the adversary has enough power, it can spread its power evenly over all the allowable bands, i.e., $N^* = N$.

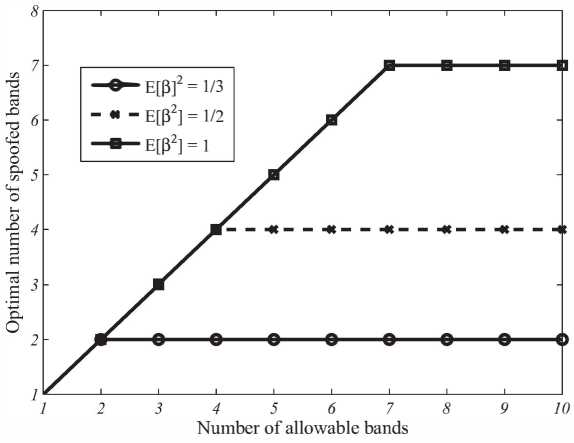

Fig. 2. Optimal number of spoofed bands versus number of allowable bands with different levels of fading (TW = 50, p_f = 0.05, and $P/\sigma_n{}^2$)

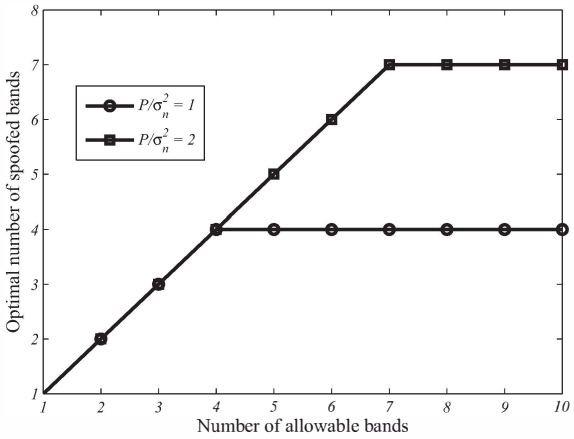

Fig. 3. Optimal number of spoofed bands versus number of allowable bands with different spoofing powers (TW = 50, p_f = 0.005, and $E[\beta^2]$ = 1)

In Fig. 2, the optimal number of spoofed bands N^* versus the number of allowable bands N is plotted. The integration-time-bandwidth product TW = 50, the threshold K corresponds to p_f = 0.05, and the power budget of the intelligent adversary P is set such that $P/\sigma_n{}^2$ = 1. Three fading scenarios are considered, where $E[\beta^2]$ = 1, 1/2, and 1/3. It is seen in Fig. 2 that, for each curve, the optimal number of spoofed bands first increases, up to a certain point, and then becomes constant. For example, for the curve where the second moment of the fading coefficient is normalized to unity, when the total number of allowable bands $N \leq 7$, the optimal number of bands that the adversary should spread its power into is equal to N. This is because, when the number of allowable bands is small, the adversary has enough power to spoof all of them with a high probability of success in each band. So the strategy in this case corresponds to a full-band spoofing. However, when N continues to increase, the adversary could not achieve a satisfactory probability of success in each band if he spreads his power over all allowable bands, so it is better

to spoof only a fraction of them. When N further increases, the optimal number of spoofed bands N^* stays constant. With the other parameters unchanged, when the the number of allowable bands is sufficiently large such that N^* no longer depends on N, the optimal sensing-deception strategy for the adversary is always to spoof the same number of bands. Further, comparing the three curves in the region where N is large enough so that N^* is constant, N^* decreases when $E[\beta^2]$ decreases. Specifically, N^* is larger when $E[\beta^2] = 1$ than when $E[\beta^2] = 1/2$ or $1/3$. This is reasonable because the spoofing signal fades more severely when $E[\beta^2]$ is smaller, resulting in a lower probability of successful spoofing. In other words, fading will decrease the adversary's capability of spoofing.

Further, similar observations to those in [3] can be obtained from Fig. 3, where the optimal number of spoofed bands N^* versus N under i.i.d. Rayleigh fading is plotted, with the curves parameterized by spoofing power P, integration-time-bandwidth product TW, and the threshold for sensing, respectively. It is seen that, under i.i.d. Rayleigh fading, in the region where N is sufficiently large such that N^* stays constant, the optimal number of spoofed bands N^* increases when

1) the power budget P of the adversary increases,
2) TW increases,
3) p_f increases (corresponding to a decrease in the threshold for sensing).

This is reasonable because, although fading will decrease the probability of successful spoofing, it does not change how different parameters affect the consequence of spoofing: increasing either P, TW, or p_f leads to an increase in the spoofing capability.

V. Conclusions And Future Work

The optimal sensing-deception strategy by noise spoofing in a CR network has been analyzed in this paper. With a fixed power constraint, the formulation of the optimal sensing-deception strategy has been given for the intelligent adversary, whose goal is to maximize the average number of false detections. A global optimal approach has been proposed to solve the nonlinear, non-convex optimization problem via a two-step transformation. Numerical results have shown that, under i.i.d. Rayleigh fading, the optimal sensing-deception strategy corresponds to an equal-power, partial-band noise spoofing. Continuing research is being conducted to analyze the optimal sensing-deception strategy under other fading scenarios, such as Rician fading, and non-identical but independent fading in each band.

References

[1] R. Tandra, S. M. Mishra, and A. Sahai, "What is a spectrum hole and what does it take to recognize one?" *Proceedings of IEEE*, vol. 97, no. 5, pp. 824-848, May 2009.

[2] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," *in Proc. IEEE 3rd Intl. Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, pp. 1-7, May 2008.

[3] Q. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary," *IEEE Trans. on Vehicular Technology*, vol. 59, no. 4, pp. 1801-1810, 2010.

[4] Q. Peng, P. C. Cosman, and L. B. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE Journal on Selected Areas in Communications*, accepted for publication.

[5] Q. Peng, P. C. Cosman, and L. B. Milstein, "Analysis and simulation of sensing deception with fading in cognitive radio networks," *IEEE Wicom*, 2010.

[6] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28-40, Feb. 2008.

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

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

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[10] M. S. Bazaraa, H. D. Sherali, C. M. Shetty, *Nonlinear Programming Theory and Algorithms, second edition*, Wiley, New York.

[11] 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.