UC San Diego

UC San Diego Previously Published Works

Title

Optimal Sensing Disruption for a Cognitive Radio Adversary

Permalink

https://escholarship.org/uc/item/6d2395kg

Journal

IEEE Transactions on Vehicular Technology, 59(4)

ISSN

0018-9545 1939-9359

Authors

Peng, Qihang
Cosman, Pamela C
Milstein, Laurence B

Publication Date

2010-05-01

DOI

10.1109/TVT.2010.2043966

Peer reviewed

eScholarship.org Powered by the California Digital Library
University of California

Optimal Sensing Disruption for a Cognitive Radio Adversary

Qihang Peng, Pamela C. Cosman, *Fellow, IEEE*, and Laurence B. Milstein, *Fellow, IEEE*

***Abstract*—Spectrum sensing vulnerabilities in cognitive radio (CR) networks are being actively investigated, where most research focuses on mechanisms that deal with possible attacks without examining optimal sensing disruption strategies. This paper addresses the optimal design and analysis of a power-limited intelligent adversary to a CR network. The adversary targets unused bands and puts energy into them so that the number of unused bands appears reduced to secondary users. This is called *sensing disruption*. The optimal disruption strategy is obtained by maximizing the average number of false detections under the adversary's power constraint. It is shown that, for a CR network where energy detection is utilized by secondary users, the optimal sensing disruption strategy for noise spoofing for a CR adversary is equal-power partial-band spoofing. Numerical results and analyses of the optimal sensing disruption are provided.**

***Index Terms*—Cognitive radio (CR), disruption optimization, intelligent adversary, spectrum sensing.**

I. Introduction

STUDIES of usage patterns reveal that the most assigned spectrum experiences low utilization [1], [2]. Cognitive radio (CR) [3]–[5] allows for dynamic access of unused spectral bands with minimal interference to primary users, thereby ameliorating the contradiction between the spectrum shortage and low spectrum utilization. Spectrum sensing is one of the key enabling technologies for CR and has widely been studied.

Spectrum sensing techniques generally fall into two categories: local spectrum sensing and cooperative spectrum sensing. In local spectrum sensing, the sensing decision on whether the band is vacant is made individually by the secondary users. Local sensing algorithms include various approaches such as those described in [6]–[10]. Cooperative spectrum sensing algorithms have also been extensively studied, since they exploit spatial diversity among secondary users by combining local sensing information. Various cooperative sensing algorithms have been proposed [11]–[13] that are either based on local sensing data or local sensing decisions.

Manuscript received May 21, 2009; revised October 1, 2009 and January 8, 2010. First published February 25, 2010; current version published May 14, 2010. This work was supported by the Office of Naval Research under Grant N000140810081. The review of this paper was coordinated by Dr. O. Holland.

Q. Peng is with the School of Communications and Information Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China (e-mail: anniepqh@uestc.edu.cn).

P. C. Cosman and L. B. Milstein are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093 USA (e-mail: pcosman@ece.ucsd.edu; milstein@ece.ucsd.edu).

Digital Object Identifier 10.1109/TVT.2010.2043966

The motivation for using these sensing algorithms is the basic sensing-before-accessing paradigm. A spectral band is unavailable for use by secondary users if it is determined to be busy through sensing, while one judged to be vacant can be used until a primary user appears. This etiquette makes a CR network vulnerable to an attack by an intelligent adversary [14]–[21]. For a traditional radio, an adversary can interfere with reception by jamming the radio. For a cognitive radio, in addition to jamming, the adversary can interfere with reception or even prevent transmission by sensing disruption. The adversary emits signals in the unused bands, trying to deceive secondary users into thinking that the unused bands are occupied by primary users, thus preventing the secondary users from accessing the system, leading to reduced spectral efficiency of the CR system. Note that different vulnerabilities are exposed to the intelligent adversary for different sensing algorithms. In local spectrum sensing, since the decision on which band is available for use is made locally, emitting signals in the unused sensing bands can directly lower the probability of accessing by the secondary user. In cooperative sensing, in addition to transmitting spoofing signals in the unused bands, the adversary could also send malicious sensing data to mislead the global sensing decision. Based on the adversarial behavior, we categorize sensing disruption as either sensing link disruption or sensing cooperation disruption.

1) *Sensing link disruption*: The adversary launches electromagnetic signals in the spectral bands that the secondary user is observing. There are a variety of choices on the signal waveforms, e.g., Chen *et al.* [14] mentioned generating signals through primary user emulation.
2) *Sensing cooperation disruption*: When cooperative sensing is involved, there are two stages: local sensing and global decision. After local spectrum sensing, each secondary user broadcasts its sensing to all other secondary users so that a global decision on which bands are available can be made. Therefore, in the global decision stage, the adversary could act as a secondary user and send malicious data to mislead the global decision.

In our system, the adversary is neither a primary nor a secondary user. It is a rival entity of the secondary system, emitting spoofing signals in the allowable bands that can potentially be used by secondary users. We assume that the primary and secondary users are not malicious; this assumption makes sense, for example, in a military context where all the users are on the same side.

In this paper, we concentrate on sensing link disruption, since it applies to both local and cooperative spectrum sensing

0018-9545/$26.00 © 2010 IEEE

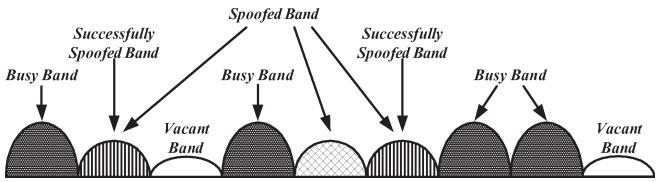


Fig. 1. Spectral band elaboration.

techniques. The feasibility of launching a sensing link disruption is analyzed in [22], and Chen *et al.* [23]–[25] studied mechanisms to combat such sensing attacks. Nevertheless, little is addressed in existing literature on sensing disruption design. That is, for a power-limited intelligent adversary, the adversary wants to distribute its power in the available bandwidth to induce the worst effect to the CR system.

Unused bands taken to be busy by secondary users are termed false detections. By maximizing the average number of false detections, we show that the optimal sensing disruption for noise spoofing is a partial-band strategy, with an equal power distribution. The remainder of this paper is organized as follows. The system model and general formulation are presented in Section II, and the optimal sensing disruption strategy is derived in Section III. Numerical results are provided in Section IV, and conclusions are presented in Section V.

II. System Model and General Formulation

The spectral range of interest is divided into multiple bands, each with identical bandwidth, as shown in Fig. 1. There are basically two types of bands: *busy bands* and *allowable bands*. Busy bands are those currently occupied by primary users, while allowable bands are those not currently used by primary users. The allowable bands can be accessed by secondary users through spectrum sensing.

However, it is likely that not all the allowable bands will be identified as such by the secondary user, due to the presence of background noise. The available bandwidth for secondary users is further reduced in a malicious sensing environment [26]. Note that the disruption that we consider in this paper applies only to secondary users and not primary users because primary users are not required to sense before accessing. The allowable bands in which the adversary chooses to launch signals are termed *spoofed bands*, while the allowable ones that are not spoofed are called *vacant bands*. The probability that an allowable band is determined by a secondary user to be busy is termed the *false detection probability*.

Assume that we have, at some instant of time, N allowable bands. Some of them are falsely detected to be busy. This number could vary over time, because of the stochastic wireless environment. The average number of false detections N_J is the focus of the adversary, who tries to minimize the available bandwidth for the CR system through maximizing N_J, subject to the adversary's power constraint.

Lemma: For a spectral range consisting of N allowable bands, N_J can be represented as the sum of the individual false detection probability on each band, i.e.,

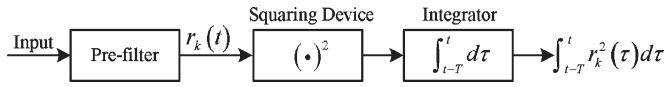


Fig. 2. Energy-detector diagram.

$$N_J = \sum_{k=1}^{N} p_k \tag{1}$$

where p_k is the false detection probability of the kth allowable band and is derived in the next section.

Proof: Let X_k $(k = 1, 2, \ldots, N)$ be variables such that $X_k = 1$ means that the kth band is sensed to be busy by the secondary user, while $X_k = 0$ indicates that this band is sensed to be vacant. Therefore, the number of false detections is the sum of X_k over all k. The expectation of this sum is the average number of false detections and is given by

$$N_J = E\left(\sum_{k=1}^{N} X_k\right) = \sum_{k=1}^{N} E(X_k) = \sum_{k=1}^{N} p_k. \tag{2}$$

■

The intelligent adversary having a power budget P has the goal of maximizing the average number of false detections. That is

$$\begin{aligned} \max \quad & \sum_{k=1}^{N} p_k \\ \text{s.t.} \quad & \sum_{k=1}^{N} P_k = P, \\ & P_k \geq 0, \qquad k = 1, 2, \ldots, N \end{aligned} \tag{3}$$

where P_k is the power the intelligent adversary emits on the kth allowable band.

III. Optimal Sensing Disruption for a Cognitive Radio Adversary

We consider a CR network where secondary users determine the availability of a spectral band through the use of a radiometer (i.e., energy detector).

A. Energy Detection at Secondary Users' Receivers

As shown in Fig. 2, the output of the integrator at any time is the energy of the input to the squaring device over a T second interval. The noise prefilter serves to limit the noise bandwidth to be the same as that of the allowable bands, which is denoted by W (in hertz). The decision on whether the observed band is vacant is made through comparing the output with a predetermined threshold. If it is greater than or equal to the threshold, a busy band is declared; otherwise, a vacant band is determined. In the absence of the adversary, allowable bands are vacant bands, that is, there is only thermal noise. We assume that the thermal noise power is identical across all allowable bands, and it is modeled as zero-mean additive

Gaussian noise $n_k(t)$ after the prefilter, i.e., $r_k(t) = n_k(t)$ and $n_k(t) \sim \mathcal{N}(0, \sigma_n^2)$.

In this paper, we use the term false alarm probability to denote the probability that a vacant band (one with thermal noise only and no spoofing power) is sensed by a secondary user to be busy. We use the term false detection probability to denote the probability that an allowable band is sensed by a secondary user to be busy. Therefore, the false detection probability includes false detections due to all causes (spoofing and thermal noise). Note that, on vacant bands, the false alarm probability and the false detection probability are equal. Using the results from Urkowitz in [6], the false alarm probability due to thermal noise is approximately given by

$$p_f = Q\left(\frac{K}{2\sqrt{TW}\sigma_n^2} - \sqrt{TW}\right) \tag{4}$$

where $Q(\cdot)$ is the Gaussian tail function, i.e.,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp(-t^2/2)\, dt \tag{5}$$

and the time–bandwidth product TW, as used in [6], refers to the product of the integration time interval and the bandwidth. The threshold for the kth allowable band is usually predetermined by the acceptable false alarm probability. Since the noise power is identical across all the allowable bands, it is reasonable to assume that the thresholds in (4) are identical and denoted by K.

B. False Detection Probability

In the presence of an intelligent adversary, the input $r_k(t)$ to the squaring device of a secondary user's receiver observing the kth allowable band consists of both thermal noise $n_k(t)$ and the spoofing signal $j_k(t)$. That is

$$r_k(t) = \beta j_k(t) + n_k(t) \tag{6}$$

where $j_k(t)$ is assumed to be Gaussian distributed with zero mean and power emitted P_k. The spoofing signal $j_k(t)$ and the noise $n_k(t)$ are assumed to be independent of each other. The path loss factor between the adversary and the secondary user's receiver is denoted as β, which is assumed to be constant across all bands.

Using the techniques from Urkowitz in [6], the test statistic u_k in the presence of the spoofing signal, that is, the sum of squared samples of received signals at the secondary user's receiver, is asymptotically normally distributed with zero mean and variance $P_k + \sigma_n^2$, and hence, the false detection probability p_k, which is the probability of determining that the kth allowable band is busy, is approximately given by

$$p_k(P_k) = Q\left(\frac{K}{2\sqrt{TW}\,(\beta^2 P_k + \sigma_n^2)} - \sqrt{TW}\right). \tag{7}$$

C. Optimal Sensing Disruption: A Partial-Band Strategy

Substituting the false detection probability (7) into (3), the optimal sensing disruption for a CR adversary can be formulated as

$$\begin{aligned} \max_{P_k} \quad & \sum_{k=1}^{N} Q\left(\frac{K}{2\sqrt{TW}\,(\beta^2 P_k + \sigma_n^2)} - \sqrt{TW}\right) \\ \text{s.t.} \quad & \sum_{k=1}^{N} P_k - P = 0, \\ & P_k \geq 0, \qquad k = 1, 2, \ldots, N. \end{aligned} \tag{8}$$

This optimization problem has a nonlinear objective with linear inequality and equality constraints. Using Lagrange multipliers and applying the Karush–Kuhn–Tucker (KKT) conditions [27], [28], we get the optimal spoofing power allocation as (see Appendix A), i.e.,

$$P_k^* = \begin{cases} P/n, & k \in \phi_{\lambda,N} \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

where $\phi_{\lambda,N} = \{k | \lambda_k^* = 0\}$ (λ_k^* is the Lagrange multiplier), and n is the number of bands that the adversary spoofs (termed spoofed bands in this paper). The optimal n, i.e., the optimal number of spoofed bands, is analyzed in Section III-D.

D. Optimal Number of Spoofed Bands N^*

The solution in (9) indicates the optimal sensing disruption strategy for the adversary corresponds to equal-power partial-band noise spoofing. However, it is not clear from (9) how many of the allowable bands should be targeted. In this section, we analyze the optimal number of bands that the adversary should spoof.

To find the value of n maximizing (8), we substitute (9) into (8). Denoting the result by $f(n)$, we have

$$\begin{aligned} f(n) = {} & nQ\left(\frac{K}{2\sqrt{TW}\,(\beta^2 P/n + \sigma_n^2)} - \sqrt{TW}\right) \\ & + (N-n)Q\left(\frac{K}{2\sqrt{TW}\sigma_n^2} - \sqrt{TW}\right). \end{aligned} \tag{10}$$

Substituting (4) into (10) yields

$$f(n) = n\left(Q\left(\frac{K - 2TW\left(\frac{\beta^2 P}{n} + \sigma_n^2\right)}{2\sqrt{TW}\left(\frac{\beta^2 P}{n} + \sigma_n^2\right)}\right) - p_f\right) + Np_f. \tag{11}$$

To optimize the problem, consider first replacing n with a real continuous variable x. We first find the extreme point $x = x^*$, where $f(x)$ reaches its maximum, and then consider the values at the two closest integers to x^*, i.e., $f(\lfloor x^* \rfloor)$ and $f(\lceil x^* \rceil)$. The optimal value of n, which is denoted as N^*, is $\lfloor x^* \rfloor$ or $\lceil x^* \rceil$

(assuming that they do not exceed N), depending on whether $f(\lfloor x^* \rfloor)$ or $f(\lceil x^* \rceil)$ is larger. Let

$$f(x) = x\left(Q\left(\frac{K - 2TW\left(\beta^2 P/x + \sigma_n^2\right)}{2\sqrt{TW}\left(\beta^2 P/x + \sigma_n^2\right)}\right) - p_f\right) + Np_f \tag{12}$$

where $x \in R^+$. According to the extreme-value theorem [29], $f(x)$ must attain its maximum and minimum values in $[1, N]$. The first derivative of $f(x)$ with respect to x is

$$f'(x) = -\frac{ax\beta^2 P}{\sqrt{2\pi}(\beta^2 P + x\sigma_n^2)^2}\exp\left(-\left(\frac{ax}{\beta^2 P + x\sigma_n^2} + b\right)^2 \Big/ 2\right) + Q\left(\frac{ax}{\beta^2 P + x\sigma_n^2} + b\right) - p_f \tag{13}$$

where $a = K/2\sqrt{TW}$, and $b = -\sqrt{TW}$. In (13), setting $f'(x) = 0$ results in a nonlinear equation, and the expression of x^* can not directly be derived. However, defining a parameter V as $V \triangleq (TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2$, the following observations can be obtained (see Appendix B).

1) When $V < K$:

- There is *one* and *only one* point $x = x^*$ satisfying $f'(x^*) = 0$ and $0 < x^* < x_1$, where x_1 is defined in (49).
- $x = x^*$ is the *maximum* point of $f(x)$.

Since there are at most N bands to spoof, N^* is upper bounded by N. Therefore, N^* equals either $\lceil x^* \rceil$ or $\lfloor x^* \rfloor$, depending on whether $f(\lceil x^* \rceil)$ or $f(\lfloor x^* \rfloor)$ is larger, unless that value would cause N^* to exceed N, in which case $N^* = N$. This shows that when $V < K$, the optimal number of spoofed bands N^* is jointly determined by both x^* and N. When $\lceil x^* \rceil$ and $\lfloor x^* \rfloor$ are smaller than N, then N^* equals either $\lceil x^* \rceil$ or $\lfloor x^* \rfloor$, and $N^* < N$. In this case, the optimal sensing disruption is partial-band spoofing, that is, to identically distribute spoofing power over N^* out of N allowable bands. When $\lceil x^* \rceil$ and $\lfloor x^* \rfloor$ are both larger than or equal to N, this partial-band spoofing becomes full-band spoofing.

2) When $V \geq K$:

- $f'(x) > 0$, for *any* $0 \leq x < +\infty$, i.e., $f(x)$ *continuously* increases as x increases for any $x \geq 0$.

The monotonically increasing characteristic of $f(x)$ for $V \geq K$ indicates that the average number of false detections continuously increases as the number of spoofed bands increases. Therefore, the maximum of $f(x)$ is achieved when $x = x^*$ approaches positive infinity. In other words, the optimal sensing disruption in this case is to spoof as many bands as possible. Since there are N allowable bands, the optimal number of spoofed bands for $V \geq K$ is still upper bounded by N, that is, $N^* = N$. Hence, the optimal sensing disruption is full-band spoofing, i.e.,

$$P_k^* = P/N, \qquad k = 1, 2, \ldots, N. \tag{14}$$

Note that, while $V \geq K$ is a mathematically viable option, as a practical matter, it is an uninteresting case, since it approximately corresponds, for $TW \gg 1$, to $p_f \geq 0.5$. This can be seen as follows. Recall that $V = (TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2$. For $TW \gg 1$, it is approximately $2TW\sigma_n^2$. Therefore, if we rewrite (4) as

$$p_f = Q\left(\frac{K - 2TW\sigma_n^2}{2\sqrt{TW}\sigma_n^2}\right) \simeq Q\left(\frac{K - V}{2\sqrt{TW}\sigma_n^2}\right) \tag{15}$$

then $K = V$ corresponds to $p_f = 1/2$. Furthermore, if $K < V$, then $p_f > 1/2$. As a consequence of this observation, for the remainder of this paper, we only consider the case of $V < K$.

As shown in (1), the average number of false detections N_J is the sum of the false detection probability on each band, i.e., $N_J = \sum_{k=1}^{N} p_k$. Since the adversary spoofs N^* out of N allowable bands, the false detection probability p_k, as defined in (7), has two possible values: One is caused by both spoofing power and thermal noise and is given by

$$p = Q\left(\frac{K - 2TW\left(\beta^2 P/N^* + \sigma_n^2\right)}{2\sqrt{TW}\left(\beta^2 P/N^* + \sigma_n^2\right)}\right). \tag{16}$$

The other is solely generated by thermal noise, i.e., the false alarm probability p_f [as in (4)]. With this notation, N_J can be expressed as

$$N_J = N^* Q\left(\frac{K - 2TW\left(\frac{\beta^2 P}{N^*} + \sigma_n^2\right)}{2\sqrt{TW}\left(\frac{\beta^2 P}{N^*} + \sigma_n^2\right)}\right) + (N - N^*)p_f. \tag{17}$$

For $TW \gg 1$, we can approximate N_J as

$$N_J = N^* Q\left(\sqrt{TW}\frac{K - V - 2TW\frac{\beta^2 P}{N^*}}{2TW\left(\frac{\beta^2 P}{N^*} + \sigma_n^2\right)}\right) + (N - N^*)p_f. \tag{18}$$

Upon rewriting (18), we have

$$N_J = N^* Q\left(\sqrt{TW}\frac{(K - V)/\sigma_n^2 - 2TW\beta^2 P/\left(N^*\sigma_n^2\right)}{2TW\left(1 + \beta^2 P/\left(N^*\sigma_n^2\right)\right)}\right) + (N - N^*)Q\left(\sqrt{TW}\left(\frac{K}{2TW\sigma_n^2} - 1\right)\right). \tag{19}$$

We can see from (19) that, depending upon the ratio $\beta^2 P/N^*\sigma_n^2$ (i.e., the ratio of spoofer power per slot to thermal noise power), at times, partial-band spoofing is optimal, and at times, full-band spoofing is optimal. In particular, for a given N, if $\beta^2 P$ is sufficiently large, then full-band spoofing is optimal. Otherwise, the adversary's optimal strategy is partial-band spoofing.

E. Average Number of Additional False Detections ΔN_J

When there is no adversary, there are, in general, a nonzero number of bands determined to be busy by the secondary user, due to thermal noise, and this number is expressed as Np_f (by letting $P = 0$ in (19)). To isolate the effect of the spoofing from the thermal noise, we define the average number of *additional* false detections due to spoofing ΔN_J as

$$\Delta N_J = N_J - Np_f. \tag{20}$$

Substituting (17) into (20), ΔN_J is given by

$$\Delta N_J = N^*\left(Q\left(\frac{K}{2\sqrt{TW}\,(\beta^2 P/N^* + \sigma_n^2)} - \sqrt{TW}\right) - p_f\right). \tag{21}$$

When N is very large, we have the following result.

Remark: For $V < K$, ΔN_J is proportional to the spoofing power P with the following relationship:

$$\Delta N_J = \frac{a\beta^2 P}{\sqrt{2\pi}\,(\beta^2 c^* + \sigma_n^2)^2} \exp\left(-\frac{\left(a/\left(\beta^2 c^* + \sigma_n^2\right) + b\right)^2}{2}\right) \tag{22}$$

where c^* is a constant determined by the parameters a, b, σ_n^2, β, and p_f.

Proof: For partial-band spoofing, a very large N means that $N \gg x^*$. That is, N^* is only determined by the integer corresponding to x^*, which must satisfy $f'(x^*) = 0$ (as in (13)), i.e.,

$$-\frac{ax^*\beta^2 P}{\sqrt{2\pi}\,(\beta^2 P + x^*\sigma_n^2)^2} \exp\left(-\left(\frac{ax^*}{\beta^2 P + x^*\sigma_n^2} + b\right)^2 \Big/ 2\right) + Q\left(\frac{ax^*}{\beta^2 P + x^*\sigma_n^2} + b\right) - p_f = 0. \tag{23}$$

Let $c^* = P/x^*$ so that (23) can be rewritten as

$$-\frac{a\beta^2 c^*}{\sqrt{2\pi}\,(\beta^2 c^* + \sigma_n^2)^2} \exp\left(-\frac{\left(a/\left(\beta^2 c^* + \sigma_n^2\right) + b\right)^2}{2}\right) + Q\left(\frac{a}{\beta^2 c^* + \sigma_n^2} + b\right) - p_f = 0. \tag{24}$$

Equation (24) indicates that when a, b, σ_n^2, β, and p_f are fixed, c^* is constant. Ignoring the edge effects that come from the fact that the number of bands has to be an integer, c^* can be interpreted as the optimal amount of spoofing power to deploy in each slot. As spoofing power increases, the spoofer would not choose to use more power than c^* in a slot but would rather choose to spoof more bands, up to the point where all are spoofed. Since, for $V < K$, x^* is positive and finite, x^* can be represented as $x^* = P/c^*$. The average number of additional false detections due to spoofing ΔN_J is approximately

$$\begin{aligned}\Delta N_J &\approx x^*\left(Q\left(\frac{a}{\beta^2 c^* + \sigma_n^2} + b\right) - p_f\right) \\ &= \frac{P}{c^*}\left(Q\left(\frac{a}{\beta^2 c^* + \sigma_n^2} + b\right) - p_f\right).\end{aligned} \tag{25}$$

Substituting (24) in (25), ΔN_J can be represented as

$$\Delta N_J = \frac{a\beta^2 P}{\sqrt{2\pi}\,(\beta^2 c^* + \sigma_n^2)^2} \exp\left(-\frac{\left(a/\left(\beta^2 c^* + \sigma_n^2\right) + b\right)^2}{2}\right). \tag{26}$$

■

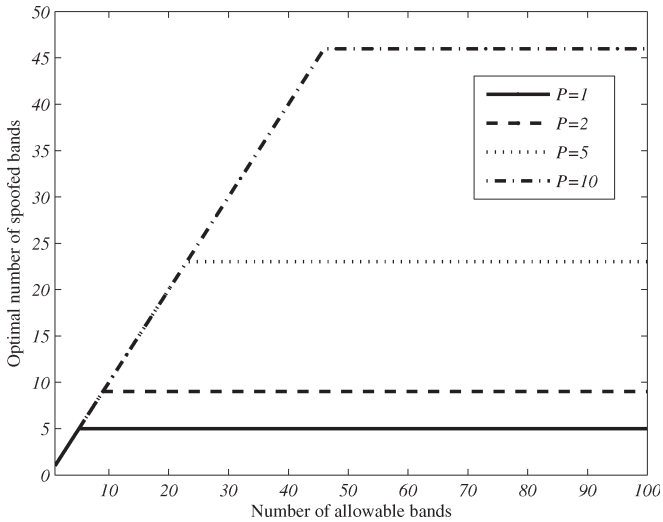


Fig. 3. Optimal number of spoofed bands versus number of allowable bands N with different spoofing powers P ($p_f = 0.05, \sigma_n^2 = 1, TW = 100$).

IV. Results

In this section, we illustrate the optimal sensing disruption technique with some numerical examples.

A. Optimal Number of Spoofed Bands N^*

We first demonstrate how N^* varies with N. In Fig. 3, the optimal number of spoofed bands is plotted, where the curves are parameterized by the total spoofer power P. The threshold K corresponds to $p_f = 0.05$, noise power $\sigma_n^2 = 1$, and $TW = 100$. It is seen that each curve exhibits a knee, which corresponds to the transition from full-band spoofing to partial-band spoofing. To the left of the knee, the number of spoofed bands equals the number of allowable bands. 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. To the right of the knee, the number of allowable bands is large, and so, the optimal spoofer strategy is to spoof a fraction of them.

In Figs. 4 and 5, we assume that the number N of allowable bands is sufficiently large that the optimal number of spoofed bands N^* no longer depends on N. That is, we are operating to the right of the knee in Fig. 3. In Fig. 4, the optimal number of spoofed bands is plotted versus the spoofing-power-to-noise-power ratio $R = P/\sigma_n^2$ for a time–bandwidth product $TW = 100$. Different values of the threshold are used, with each one corresponding to a different false alarm probability. It is seen that N^* increases as R increases, which is reasonable since more spoofing power allows one to spoof more allowable bands. When the thermal noise power and TW are held constant, increasing p_f indicates a decrease in K (as seen in (4)). This allows a given level of spoofing power to be spread over a larger number of bands.

Consider now Fig. 5, where N^* versus the spoofing-power-to-noise-power ratio R is plotted for a threshold corresponding to $p_f = 0.05$, thermal noise power $\sigma_n^2 = 1$, and different values of TW. It is seen that, for fixed p_f and R, when TW increases, the optimal number of spoofed bands increases. That is, for

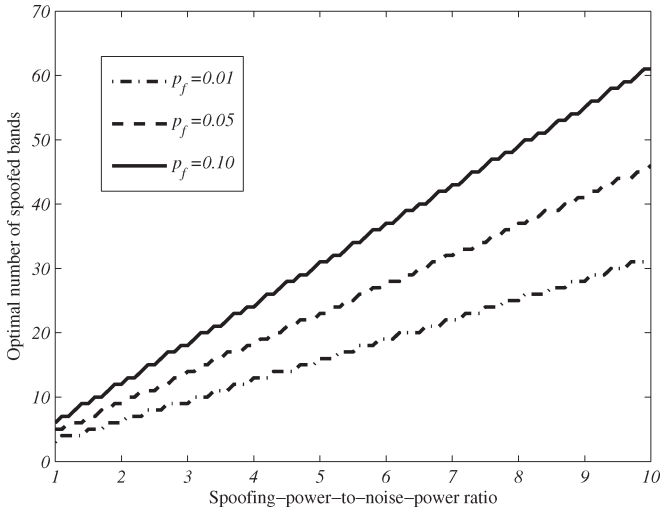


Fig. 4. Optimal number of spoofed bands N^* versus spoofing-power-to-thermal-noise-power ratio with different values of p_f. ($TW = 100$).

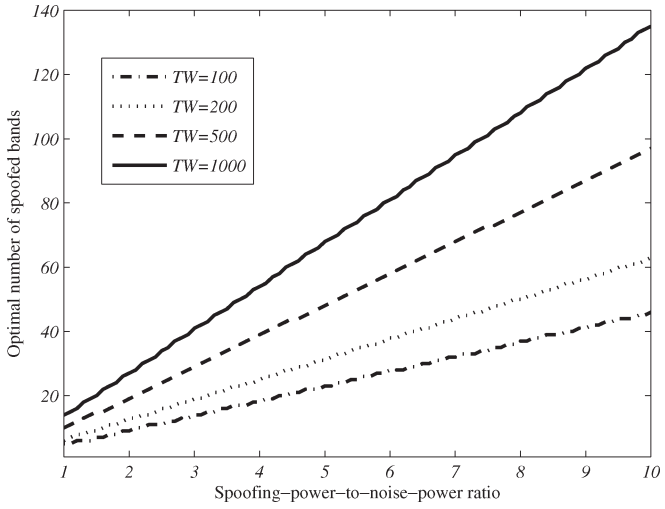


Fig. 5. Optimal number of spoofed bands N^* versus spoofing-power-to-thermal-noise-power ratio with different values of TW ($p_f = 0.05$).

the same spoofing power, an increase in TW increases the ability to spoof. This is reasonable because, for fixed W, a radiometer with a longer integration time can better determine whether the received power is below or above the threshold. When the integration time T is fixed, an increase in W increases the number of received signal samples to be accumulated. The energy on the observed band can more accurately be estimated when more samples are used; thus, the ability to distinguish whether the received signal power is above the threshold is increased.

B. Average Number of False Detections N_J

In Fig. 6, the average number of false detections is plotted for $V < K$. The time–bandwidth product $TW = 100$, the thermal noise power $\sigma_n^2 = 1$, and the threshold K corresponds to $p_f = 0.05$ and $p_f = 0.005$ in Fig. 6(a) and (b), respectively. For a given P, the average number of false detections increases as the number of allowable bands increases. Each curve exhibits a knee, and the interpretation of the knee is the same as that for Fig. 3. The loss of secondary bandwidth could be either due to both spoofing and thermal noise power [as in (7)] or only due to thermal noise power, that is, with false alarm probability p_f (as in (4)). When the number of allowable bands $N > N^*$, then some of those $N - N^*$ bands might not be used by a secondary user due to false alarms caused by thermal noise. Given that we are in the region where $N > N^*$, when the number of allowable bands increases by ΔN, the average number of false detections increases by $\Delta N \cdot p_f$, resulting in a linear increase, and the slope is equal to p_f. Comparing Fig. 6(b) with Fig. 6(a), we see that, for the same spoofing power, the average number of false detections is larger in Fig. 6(a) than it is in Fig. 6(b). This shows that a lower threshold increases the probability of false detection for a given level of spoofing power.

C. Average Number of Additional False Detections Due to Spoofing

With the same parameters as in Fig. 6, the average number of additional false detections due to spoofing ΔN_J versus the number of allowable bands is plotted in Fig. 7. Note that ΔN_J becomes constant when the number of allowable bands N becomes large, because when $N > N^*$, there will be no spoofing power put into more than N^* bands.

Fig. 8 shows ΔN_J versus spoofing power when N is very large ($N = 1000$), with the same parameters as in Fig. 7(a) and (b). Both curves are linear, i.e., ΔN_J linearly increases when spoofing power increases.

D. Available Bandwidth under Sensing Disruption

The expected percentage of available bands (i.e., $100(N - N_J)/N$) under different spoofing powers is illustrated in Fig. 9, parameterized by the number of allowable bands. The time–bandwidth product $TW = 100$, the thermal noise power $\sigma_n^2 = 1$, and the threshold K corresponds to $p_f = 0.05$. All the curves start from the available bandwidth at a percentage of 95% instead of 100%, as a result of the nonzero false alarm probability, which initially results in some of the allowable bands being classified as busy. The expected percentage of available bands first sharply decreases as the spoofing power increases. The decrease becomes slower as spoofing power further increases, due to the fact that the Q function in (7) saturates for large negative values of its argument.

V. Conclusion

An analysis of optimal sensing disruption by noise spoofing in a CR network has been presented in this paper. A general formulation of the optimal sensing disruption has been given by maximizing the average number of false detections by an intelligent adversary, subject to a power constraint. In particular, for a CR network where energy detection is used by the secondary users, the optimal strategy has been derived and shown to correspond to equal-power partial-band spoofing. From our analysis, the following observations are made: 1) More spoofing power allows the adversary to spoof more bands, up to the point where all bands are spoofed, at which point additional spoofing power serves to increase the

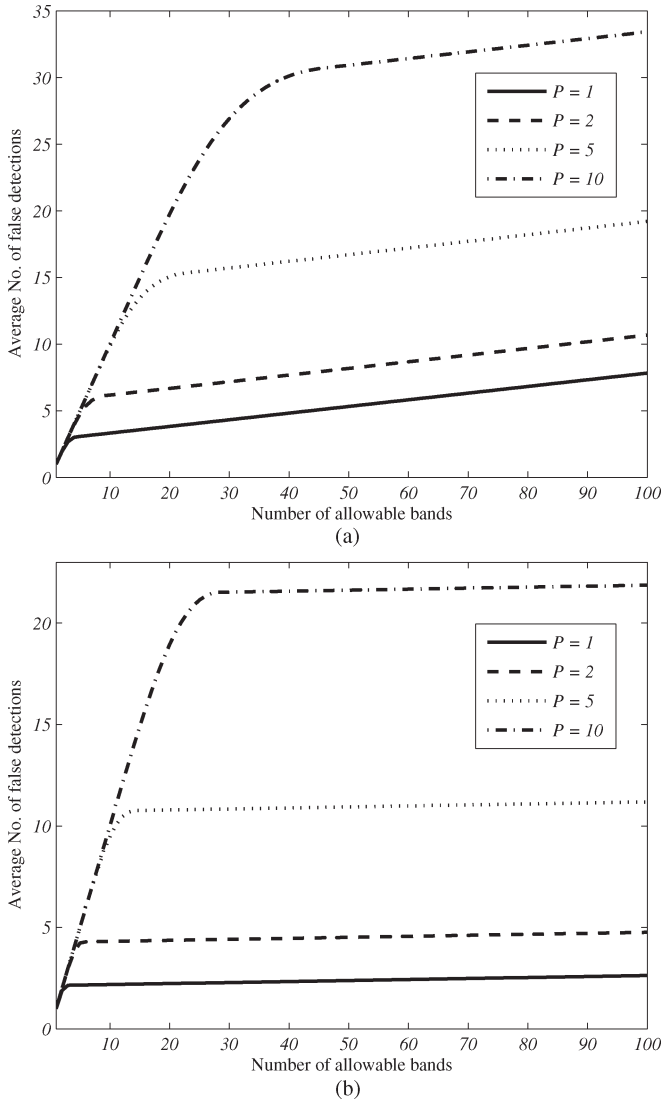


Fig. 6. Average number of false detections N_J versus number of allowable bands N with different spoofing powers P ($\sigma_n^2 = 1, TW = 100$). (a) $p_f = 0.05$. (b) $p_f = 0.005$.

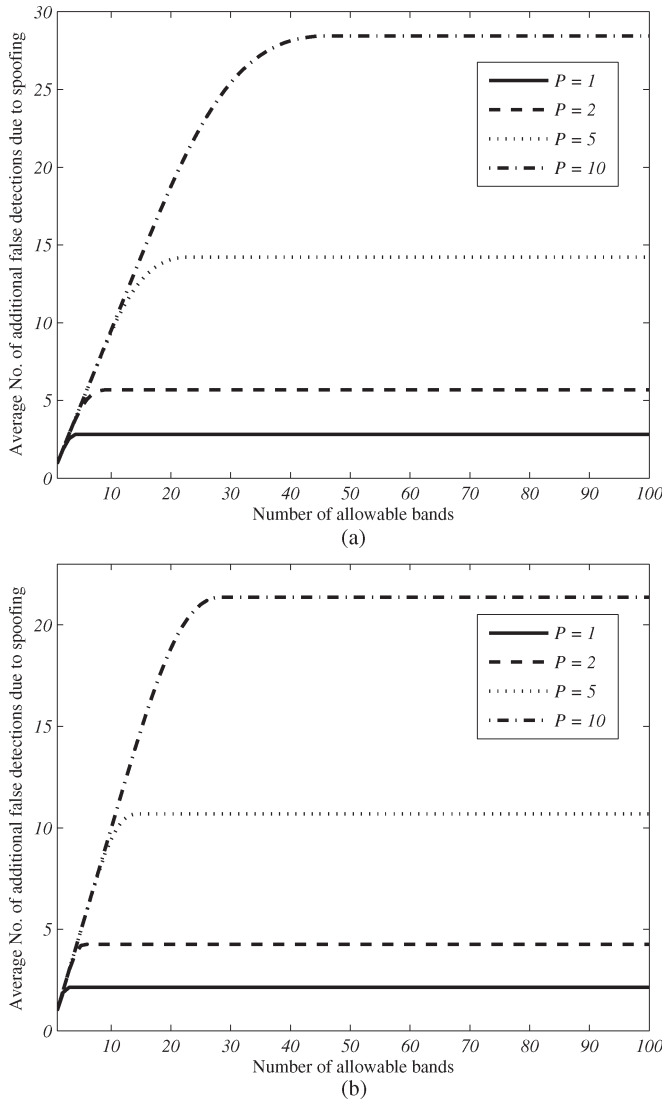


Fig. 7. Average number of additional false detections due to spoofing ΔN_J versus number of allowable bands N with different spoofing powers P ($\sigma_n^2 = 1, TW = 100$). (a) $p_f = 0.05$. (b) $p_f = 0.005$.

probability of successful disruption. 2) A decrease in the threshold leads to an increase in the probability of successful disruption. 3) An increase in the time–bandwidth product will increase the spectrum sensing performance of secondary users in a noise-only environment, and it will also boost the probability of successful disruption. 4) For a given set of system parameters (time–bandwidth product TW, thermal noise power σ_n^2, and false alarm probability p_f), the average number of additional false detections due to spoofing is proportional to the spoofing power.

APPENDIX A
OPTIMIZATION DERIVATIONS

Equation (8) can be rewritten as

$$\min_{P_k} \quad f_0(\vec{P}) = -\sum_{k=1}^{N} Q\left(\frac{K}{2\sqrt{TW}\,(\beta^2 P_k + \sigma_n^2)} - \sqrt{TW}\right)$$

$$\text{s.t.} \quad f_k(\vec{P}) = -P_k \le 0, \qquad k = 1, 2, \ldots, N$$

$$h(\vec{P}) = \mathbf{1}^T \vec{P} - P = 0. \tag{27}$$

The Lagrangian $L : R^N \times R^N \times R \to R$ associated with (27) is

$$L(\vec{P}, \vec{\lambda}, v) = f_0(\vec{P}) + \sum_{k=1}^{N} \lambda_k f_k(\vec{P}) + v h(\vec{P}) \tag{28}$$

where $\vec{\lambda} = (\lambda_1, \ldots, \lambda_k, \ldots, \lambda_N) \in R^N$ and $v \in R$ are the Lagrange multipliers. Letting $\vec{P}^*$, $\vec{\lambda}^*$, and v^* be the optimal set of points, we obtain the KKT conditions [27], i.e.,

$$\vec{P}^* \succeq 0 \tag{29}$$

$$\mathbf{1}^T \vec{P}^* = P \tag{30}$$

$$\vec{\lambda}^* \succeq 0 \tag{31}$$

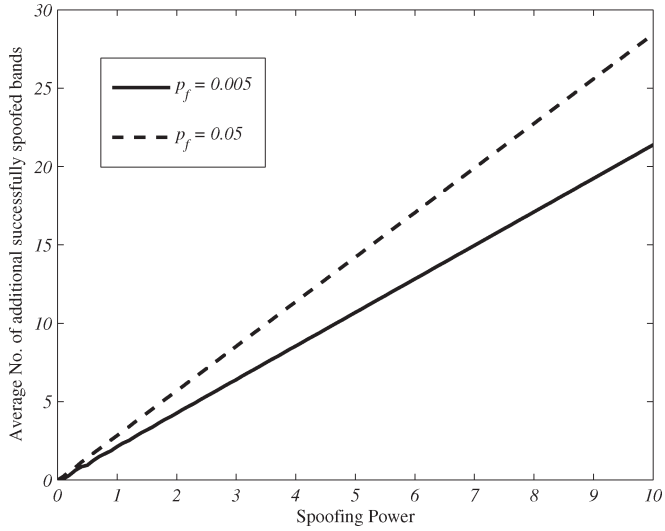


Fig. 8. Average number of additional false detections due to spoofing ΔN_J versus spoofing power ($\sigma_n^2 = 1, TW = 100, N = 1000$).

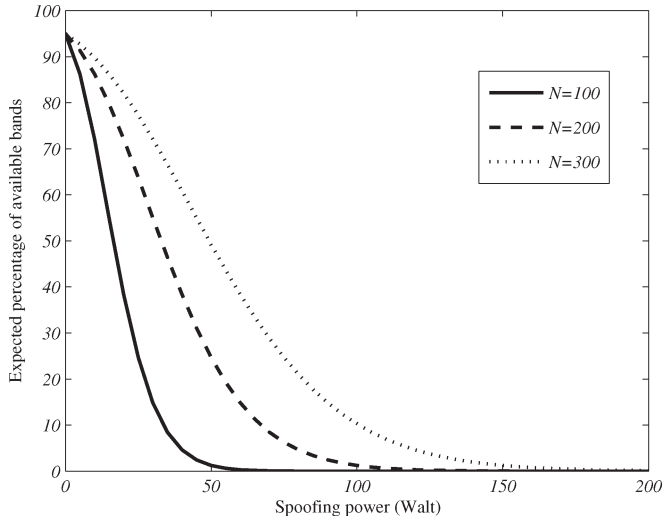


Fig. 9. Expected percentage of available bands versus spoofing power out of different numbers of allowable bands N with different spoofing powers P ($p_f = 0.05, \sigma_n^2 = 1, TW = 100$).

$$\lambda_k^* P_k^* = 0 \tag{32}$$

$$-\frac{a\beta^2 \exp\left(-\left(a/a\left(\beta^2 P_k^* + \sigma_n^2\right) + b\right)^2 \Big/ 2\right)}{\sqrt{2\pi}\left(\beta^2 P_k^* + \sigma_n^2\right)^2} - \lambda_k^* + v^* = 0. \tag{33}$$

The complementary slackness [27] in (32) indicates that the kth optimal Lagrange multiplier is zero unless the kth constraint $f_k(\vec{P})$ is active at the optimum. Based on the values of λ_k^*, we have the following two cases.

1) $\lambda_k^* > 0, P_k^* = 0$

From (33), we get

$$\lambda_k^* = v^* - \frac{a\beta^2}{\sqrt{2\pi}\sigma_n^4} \exp\left(-\frac{\left(a/\sigma_n^2 + b\right)^2}{2}\right). \tag{34}$$

Let $\phi_{0,N}$ denote the set such that $\phi_{0,N} = \{k | P_k^* = 0\}$, and let $N - n$ be the size of $\phi_{0,N}$. Since the right-hand side expression in (34) is independent of k, we must have λ_k^* constant for all $k \in \phi_{0,N}$.

2) $\lambda_k^* = 0, P_k^* > 0$

From (33), we get

$$v^* = \frac{a\beta^2 \exp\left(-\left(a/\left(\beta^2 P_k^* + \sigma_n^2\right) + b\right)^2/2\right)}{\sqrt{2\pi}\left(\beta^2 P_k^* + \sigma_n^2\right)^2}. \tag{35}$$

Let $\phi_{\lambda,N}$ denote the set such that $\phi_{\lambda,N} = \{k | \lambda_k^* = 0\}$, and let n $(0 < n \leq N)$ be the size of $\phi_{\lambda,N}$. Since v^* is a scalar and independent of k, it is constant for all $k \in \phi_{\lambda,N}$. Therefore, $\{P_k^* = P/n, k \in \phi_{\lambda,N}\}$ is one solution for (35). However, since (35) is a nonlinear equation, it could have more than one set of points leading to the same v^*. To determine how many roots there are for the same v^*, let $v(P_k) = (a\beta^2/\sqrt{2\pi}(\beta^2 P_k + \sigma_n^2)^2)\exp(-(a/(\beta^2 P_k + \sigma_n^2) + b)^2/2)$. Then, the first derivative with respect to P_k is given by

$$\frac{dv(P_k)}{dP_k} = \left(\beta^2 P_k + \sigma_n^2\right)^{-5} \exp\left(-\frac{\left(a/\left(\beta^2 P_k + \sigma_n^2\right) + b\right)^2}{2}\right)$$

$$\cdot \frac{a\beta^4}{\sqrt{2\pi}}\left(a^2 + ab\left(\beta^2 P_k + \sigma_n^2\right) - 2\left(\beta^2 P_k + \sigma_n^2\right)^2\right). \tag{36}$$

The monotonicity of $v(P_k)$ is determined by the sign of $dv(P_k)/dP_k$, which, depends on the second-order polynomial component of (36), based on which, we can get the following results.

1) For $\beta^2 P + \sigma_n^2 \leq a(b + \sqrt{b^2 + 8})/4$ *or* $\sigma_n^2 \geq a(b + \sqrt{b^2 + 8})/4$*:*

- There is *one* and *only one* point satisfying (35). Therefore, for this case, all P_k should be identical for all $k \in \phi_{\lambda,k}$.

2) For $\sigma_n^2 < a(b + \sqrt{b^2 + 8})/4\beta^2 < \beta^2 P + \sigma_n^2$*:*

- There are *two* points $P_k^{(1)}, P_k^{(2)}$ satisfying (35), and

$$a^2 + ab\left(\beta^2 P_k^{(1)} + \sigma_n^2\right) - 2\left(\beta^2 P_k^{(1)} + \sigma_n^2\right)^2 < 0 \tag{37}$$

$$a^2 + ab\left(\beta^2 P_k^{(2)} + \sigma_n^2\right) - 2\left(\beta^2 P_k^{(2)} + \sigma_n^2\right)^2 > 0. \tag{38}$$

As stated earlier, the size of $\phi_{\lambda,N}$ is n. Thus, out of the n allowable bands, the spoofing power in each band could either be $P_k^{(1)}$ or $P_k^{(2)}$. That is

$$\tilde{f}_0(\vec{P}) = -\sum_{k=1}^{n} Q\left(\frac{a}{\beta^2 P_k + \sigma_n^2} + b\right) \tag{39}$$

where $P_k \in \{P_k^{(1)}, P_k^{(2)}\}$. To determine the optimum number of terms taking the value $P_k^{(1)}$, we resort to the sufficiency condition for a stationary point to be an extreme point [28] to

prove that all the n bands should be allocated identical $P_k^{(1)}$. The Hessian matrix of $\tilde{f}_0(P_k)$ is

$$\mathbf{H} = \begin{pmatrix} L_{11} & 0 & \cdots & 0 \\ 0 & L_{22} & \cdots & 0 \\ & \vdots & & \\ 0 & 0 & \cdots & L_{nn} \end{pmatrix} \tag{40}$$

where L_{kk} $(k = 1, 2, \ldots, n)$ is the second partial derivative of $\tilde{f}_0(P_k)$, which is expressed as

$$L_{kk} = \left(\beta^2 P_k + \sigma_n^2\right)^{-5} \exp\left(-\frac{\left(a\left(\beta^2 P_k + \sigma_n^2\right)^{-1} + b\right)^2}{2}\right)$$

$$\cdot \frac{a\beta^4}{\sqrt{2\pi}}\left(-a^2 - ab\left(\beta^2 P_k + \sigma_n^2\right) + 2\left(\beta^2 P_k + \sigma_n^2\right)^2\right). \tag{41}$$

According to the sufficiency condition, the matrix $\mathbf{H}$ needs to be positive definite to make $f_0(\mathbf{P})$ a relative minimum. Therefore, only $P_k^{(1)}$ achieves a relative minimum. For this case, all the P_k should be identical for all $k \in \phi_{\lambda,k}$.

Based on the aforementioned analysis, we conclude that, for all $k \in \phi_{\lambda,k}$, P_k should be identical, that is

$$P_k = P/n, \qquad k \in \phi_{\lambda,k}. \tag{42}$$

In summary, the optimal spoofing power allocation is given by

$$\begin{cases} P_k^* = P/n, & k \in \phi_{\lambda,k} \\ P_k^* = 0, & \text{otherwise.} \end{cases} \tag{43}$$

APPENDIX B
ANALYSIS OF THE LOCATION OF x^*

Since $f'(x)$ (as in (13)) is a nonlinear expression, it is very difficult to obtain the analytical expression for x^* so that $f'(x^*) = 0$. However, the following observations can be made.

Remark: $f'(x)$ starts with a positive value at $x = 0$ and approaches 0 as x approaches infinity.

Proof:

$$f'(x)\big|_{x=0} = Q(b) - p_f = Q(b) - Q\left(a/\sigma_n^2 + b\right). \tag{44}$$

Since $a/\sigma_n^2 + b > b$ and $Q(\cdot)$ is a monotonically decreasing function

$$f'(x)|_{x=0} > 0 \tag{45}$$

$$\lim_{x\to\infty} f'(x) = Q\left(a/\sigma_n^2 + b\right) - p_f = 0. \tag{46}$$

■

We need to analyze how $f'(x)$ changes as x increases in the range $(0, +\infty)$ to locate x^*; therefore, we use the second derivative of $f(x)$, which is given by

$$f''(x) = -\left(\left(2 - a_0^2 - a_0 b\right)x^2 + (4 - a_0 b)\beta^2 kx + 2\beta^4 k^2\right) \times \frac{a_0 k^2 \beta^4}{\sqrt{2\pi}(\beta^2 k + x)^5} \exp\left(-\frac{u^2(x)}{2}\right) \tag{47}$$

where $a_0 = a/\sigma_n^2$, $k = P/\sigma_n^2$, and $u(x) = (a_0 x/(\beta^2 k + x)) + b$. It is seen from (47) that the sign of $f''(x)$ is determined by the polynomial

$$f_0(x) = \left(2 - a_0^2 - a_0 b\right)x^2 + (4 - a_0 b)\beta^2 kx + 2\beta^4 k^2 \tag{48}$$

since $a_0 > 0$, $k > 0$, and $\exp(-u^2(x)/2) > 0$. This is a second-order polynomial function of x. The roots x_1 and x_2 of the equation $f_0(x) = 0$ are

$$x_1 = \frac{(a_0 b - 4)k - a_0 k\sqrt{b^2 + 8}}{2\left(2 - a_0^2 - a_0 b\right)}\beta^2 \tag{49}$$

$$x_2 = \frac{(a_0 b - 4)k + a_0 k\sqrt{b^2 + 8}}{2\left(2 - a_0^2 - a_0 b\right)}\beta^2. \tag{50}$$

Depending on the sign of the coefficient of x^2 in (48), $f_0(x)$ could be either convex or concave. Note that there are three separate cases.

1) $(2 - a_0^2 - a_0 b) < 0$, i.e., $(TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2 < K$

In this case, the roots in (49) and (50) are $x_1 > 0$ and $x_2 < 0$. This directly leads to the results that $f''(x) < 0$ for $0 \le x < x_1$ and $f''(x) \ge 0$ for $x \ge x_1$. Combining the results in (45) and (46), in this regime, $f'(x)$ first decreases from a positive value to a negative one and then continuously increases, approaching 0, as x approaches positive infinity. Thus, there is one and only one point $x = x^*$ $(0 < x^* < x_1)$ satisfying $f'(x^*) = 0$. Furthermore, since $f''(x) < 0$ for $0 < x^* < x_1$, $x = x^*$ is the maximum point of $f(x)$.

2) $(2 - a_0^2 - a_0 b) > 0$, i.e., $(TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2 > K$

In this case, both roots x_1 and x_2 are negative. This indicates that for any $x \ge 0$, $f_0(x) > 0$. According to (47), $f''(x) < 0$. Combining (45) and (46), $f'(x)$ monotonically decreases from a positive value to zero, as x increases from 0 to infinity. In other words, $f'(x) > 0$ for any $x \ge 0$. This shows that the objective function $f(x)$ in (12) continuously increases as x increases for any $x \ge 0$. That is, $f'(x)$ approaches 0 as x approaches positive infinity, and x^* is positive infinity for this scenario.

3) $(2 - a_0^2 - a_0 b) = 0$, i.e., $(TW + \sqrt{(TW)^2 + 8TW})\sigma_n^2 = K$

In this case, $f(x)$ reduces to a linear function, expressed as $f_0(x) = (4 - a_0 b)\beta^2 kx + 2\beta^4 k^2$. The slope of $f_0(x)$ is $(4 - a_0 b)\beta^2 k > 0$, and $f_0(x)|_{x=0} = 2\beta^4 k^2 > 0$. It is then straightforward that $f'(x) > 0$ for any $x \ge 0$. Therefore, the same conclusion as in case 2 is made for this scenario: $f(x)$ continuously increases as x increases, for any $x \ge 0$.

ACKNOWLEDGMENT

The authors would like to thank an anonymous reviewer for valuable comments on simplifying some of the derivations.

REFERENCES

[1] Federal Communications Commission, "Spectrum Policy Task Force," Rep. ET Docket no. 02-135, Nov. 2002.

[2] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proc. 38th Asilomar Conf. Signals, Syst. Comput.*, 2004, vol. 1, pp. 772–776.

[3] Fed. Commun. Comm., ET Docket No. 03-322, Notice of Proposed Rule Making and Order, Dec. 2003.

[4] J. Mitola, III and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[5] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

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

[7] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.

[8] S. Shellhammer and R. Tandra, "An evaluation of DTV pilot power detection," in *IEEE 802.22-06/0188r0*, Sep. 2006.

[9] W. A. Gardner, "Signal interception: A unifying theoretical framework for feature detection," *IEEE Trans. Commun.*, vol. 36, no. 8, pp. 897–906, Aug. 1988.

[10] H. S. Chen and W. Gao, "Text on cyclostationary feature detector—For informative annex on sensing techniques," *IEEE 802.22 Meeting Documents*, Jul. 2007.

[11] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2006, vol. 4, pp. 1658–1663.

[12] J. Ma and Y. G. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2007, pp. 3139–3143.

[13] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 28–40, Feb. 2008.

[14] R. L. Chen, J. M. Park, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

[15] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," in *Proc. IEEE Int. Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, Aug. 2007, pp. 456–464.

[16] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges, and design trade-offs," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 32–39, Apr. 2008.

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

[18] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. IEEE 3rd Int. Conf. Cognitive Radio Oriented Wireless Netw. Commun.*, May 2008, pp. 1–8.

[19] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE Int. Conf. Commun.*, May 2008, pp. 3406–3410.

[20] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis, and G. F. Marias, "Cognitive spectrum and its security issues," in *Proc. IEEE 2nd Int. Conf. Next Generation Mobile Appl., Services Technol.*, Sep. 2008, pp. 565–570.

[21] N. R. Prasad, "Secure cognitive networks," in *Proc. 1st Eur. Wireless Technol. Conf.*, Oct. 2008, pp. 107–110.

[22] S. Anand, Z. Lin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proc. IEEE 3rd Symp. New Frontiers Dyn. Spectrum Access Netw.*, Oct. 2008, pp. 1–6.

[23] R. L. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Proc. IEEE 1st Workshop Netw. Technol. Softw. Defined Radio Netw.*, Sep. 2006, pp. 110–119.

[24] R. L. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[25] R. L. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1876–1884.

[26] Q. H. Peng, P. C. Cosman, and L. B. Milstein, "Worst-case sensing deception in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2009, to be published.

[27] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[28] S. S. Rao, *Optimization: Theory and Applications,* 2nd ed. Hoboken, NJ: Wiley, 1983.

[29] H. Hancock, *Theory of Maxima and Minima*. New York: Dover, 1960.

Qihang Peng received the B.S. and M.S. degrees (both with honors) in June 2004 and March 2007, respectively, from the University of Electronic Science and Technology of China, Chengdu, China, where she is currently working toward the Ph.D. degree with the School of Communications and Information Engineering.

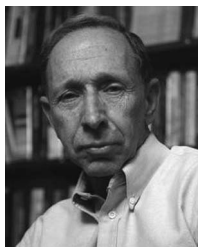
She is also currently a Visiting Scholar with the Department of Electronic and Computer Engineering, University of California, San Diego, La Jolla.

Ms. Peng has been serving as a member of the Technical Program Committee of the IEEE INFOCOM 2010 Workshop on Cognitive Wireless Communications and Networking.

Pamela C. Cosman (S'88–M'93–SM'00–F'08) received the B.S. degree (with honor) in electrical engineering from the California Institute of Technology, Pasadena, in 1987 and the M.S. and Ph.D. degrees in electrical engineering from Stanford University, Stanford, CA, in 1989 and 1993, respectively.

She was a National Science Foundation Postdoctoral Fellow with Stanford University and a Visiting Professor with the University of Minnesota, Minneapolis, during 1993–1995. In 1995, she joined the faculty of the Department of Electrical and Computer Engineering (ECE), University of California, San Diego, La Jolla, where she is currently a Professor. She was the Director of the Center for Wireless Communications from 2006 to 2008. Her research interests are in the areas of image and video compression and processing and wireless communications.

Dr. Cosman is a member of Tau Beta Pi and Sigma Xi. She is the recipient of the ECE Departmental Graduate Teaching Award, a Career Award from the National Science Foundation, a Powell Faculty Fellowship, and a Globecom 2008 Best Paper Award. She was a Guest Editor of the June 2000 Special Issue of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS on "Error-resilient image and video coding" and was the Technical Program Chair of the 1998 Information Theory Workshop in San Diego. She was an Associate Editor of the IEEE COMMUNICATIONS LETTERS (1998–2001) and the IEEE SIGNAL PROCESSING LETTERS (2001–2005). She was the Editor-in-Chief (2006–2009) and a Senior Editor (2003–2005 and 2010–present) of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS.



Laurence B. Milstein (S'66–M'68–SM'77–F'85) received the B.E.E. degree from the City College of New York in 1964 and the M.S. and Ph.D. degrees in electrical engineering from the Polytechnic Institute of Brooklyn, Brooklyn, NY, in 1966 and 1968, respectively.

From 1968 to 1974, he was with the Space and Communications Group of Hughes Aircraft Company, Culver City, CA. From 1974 to 1976, he was a member of the Department of Electrical and Systems Engineering, Rensselaer Polytechnic Institute, Troy, NY. Since 1976, he has been with the Department of Electrical and Computer Engineering, University of California, San Diego (UCSD), La Jolla, where he is the Ericsson Professor of Wireless Communications and the former Department Chairman, working in the area of digital communication theory with special emphasis on spread-spectrum communication systems. He has also been a consultant to both the government and industry in the areas of radar and communications.

Dr. Milstein is a recipient of the 1998 Military Communications Conference (MILCOM) Long-Term Technical Achievement Award, an Academic Senate 1999 UCSD Distinguished Teaching Award, an IEEE Third Millennium Medal in 2000, the 2000 IEEE Communication Society Armstrong Technical Achievement Award, and the 2002 MILCOM Fred Ellersick Award. He was an Associate Editor for Communication Theory for the IEEE TRANSACTIONS ON COMMUNICATIONS, an Associate Editor for Book Reviews for the IEEE TRANSACTIONS ON INFORMATION THEORY, an Associate Technical Editor for *IEEE Communications Magazine*, and the Editor-in-Chief of the IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS. He was the Vice President for Technical Affairs of the IEEE Communications Society in 1990 and 1991 and is a former Chair of the IEEE Fellow Selection Committee.