Spoofing or Jamming: Performance Analysis of a Tactical Cognitive Radio Adversary

Qihang Peng, Pamela C. Cosman, and Laurence B. Milstein

***Abstract*—The tradeoff between spoofing and jamming a cognitive radio network by an intelligent adversary is analyzed in this paper. Due to the vulnerabilities of spectrum sensing noted in recent studies, a cognitive radio can be attacked during the sensing interval by an adversary who puts spoofing signals in unused bands. Further, once secondary users access unused bands, the adversary can use traditional jamming to interfere with them during transmission. For an energy-constrained intelligent adversary, a two step procedure is formulated to distribute the energy between spoofing and jamming, such that the average sum throughput of the secondary users is minimized. That is, we optimally spoof in the sensing duration and then optimally jam in the transmission slot. In a cluster-based cognitive radio network, when the number of spectral vacancies required by secondary users increases, the optimal attack for the intelligent adversary will shift from jamming only, to a combination of spoofing and jamming, to spoofing only.**

***Index Terms*—Cognitive radio, intelligent adversary, partial-band noise spoofing, partial-band noise jamming.**

I. Introduction

COGNITIVE radio (CR) [1] has been widely studied as a promising solution to the contradiction between spectrum shortage and low spectrum utilization by allowing for dynamic access of unused bands through spectrum sensing. However, as one key component of cognitive radio, spectrum sensing exposes vulnerabilities [2] that an intelligent adversary, whose goal is to disrupt the system performance, can exploit. That is, it can launch spoofing signals in the sensing duration in the unused bands, so that secondary users are deceived into thinking that these bands are occupied by primary users and should be avoided. The feasibility of launching such sensing disruption is analyzed in [3]. By minimizing the available bandwidth to secondary users, an optimal design of such an intelligent adversary using a noise spoofing signal is presented in [4] and [5]. On the other hand, once a communication link is established for a secondary user after the sensing duration, that link can be degraded during data transmission by the intelligent adversary through traditional jamming techniques [6] (e.g., partial-band noise jamming [7]). Both attacks (spoofing and jamming) accomplish, in different manners, the degradation of the performance of a cognitive radio network: spoofing reduces the effective available bandwidth for information transmission, while jamming increases the symbol error rate of secondary users.

In this paper, we analyze the performance of a tactical, spread spectrum, cognitive radio system operating in the presence of an intelligent adversary whose objective is to minimize the throughput of the CR system. We assume that the adversary knows the basic characteristics of the system he is attacking, such as the waveform being used, the type of spreading, the receiver design, and the bandwidth of the waveform, but does not know the specifics, such as the received power levels and the spreading sequences [6]. Also, note that we are not assuming that either the spoofing or the jamming powers at the cognitive radios are known by the adversary. We are also not assuming that the adversary knows which method the cognitive radio user uses for sensing, or the number of spectral vacancies required by secondary users. The model and methodology used in this paper for performance analysis are consistent with the assumptions made over many decades regarding research on the intelligent jamming of spread spectrum communications systems [8]. The key difference in this paper is that we consider both spoofing and jamming the system, as will be discussed below.

The functional operation of the system is as follows: The physical layer is based around multicarrier, direct sequence code division multiple access (MC DS CDMA). All users, both primary and secondary, are nominally assigned a single subcarrier, but, depending on the intensity of the jamming that the primary users experience, the primary users have the option of requesting additional subcarriers. Because this system is designed for tactical use, the ground rules that we impose on it are different from those imposed on a civilian CR system. Specifically, a user is not primary because he pays a higher fee for his mobile service than does a secondary user. Rather, primary versus secondary status is due to normal military hierarchical ranks (e.g., a general would certainly be a primary user). Thus, in the context of how many subcarriers a primary might choose to use, the tradeoff that, say, the general would have to make is how much protection should be given to the (presumably fewer) primary user messages compared to how much additional throughput is needed from the secondary users, a decision that will vary with battlefield conditions. Thus, the number of subcarriers available for secondary users is a function of both the number of primary users and the number of subcarriers they demand at any instant of time.

The goal of the adversary is to spoof some fraction of the subcarriers that are available for secondary users so as

Manuscript received 1 December 2009; revised 26 May 2010. This research was partially supported by the Office of Naval Research under grant number N000140810081, and partially supported by the National Science Foundation under grant number CCF-0915727.

Q. Peng is with the School of Communications and Information Engineering, University of Electronic Science and Technology of China, Chengdu, China, 610054 (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, San Diego, CA 92093-0407 (emails: {pcosman, milstein}@ece.ucsd.edu).

Digital Object Identifier 10.1109/JSAC.2011.110420.

0733-8716/11/$25.00 © 2011 IEEE

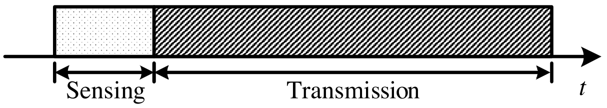


Fig. 1. Frame structure for cognitive radio with periodic spectrum sensing

to inhibit those users from transmitting in the spoofed bands, and also to jam those bands that the secondary users transmit over. Note that we are not going to discuss the problem of jamming primary users, because that problem has been studied for many years. That is, at any instant of time, whatever number of subcarriers are used by primary users, the adversary can choose to expend some fraction of his total power to jam the primary bands. That leaves some remaining fraction of his total power for attacking secondary users. For any given value of this remaining adversary power, this paper deals with the worst-case performance of the secondary users, which is measured by total throughput of all secondary users.

In order to emphasize the tradeoff between spoofing and jamming, we have made various idealizations to the system. We consider a cluster-based network, where communications are controlled by the cluster head. The cluster head performs the sensing function for the secondary users. Our analysis corresponds to the uplink from the mobile users to the cluster head, and we assume an intelligent adversary who has knowledge of the system timing (i.e., the timing of each sensing duration and the timing of each data transmission duration). We also assume that the adversary does not know, at the start of the sensing interval, how many subcarriers are required by the secondary users. However, we assume that the adversary does know this number during the data transmission interval, and indeed, knows which subcarriers are being used by secondary users. This could be accomplished, for example, by having the adversary continue sensing for some time in the data transmission interval. These assumptions clearly result in a worst-case scenario for system performance, and are not meant for system design. The link from any given mobile unit to the cluster head is subject to partial-band jamming of the secondary users' subcarriers, in addition to additive white Gaussian noise, and coherent detection is performed at the receiver. Based on this system set-up, exact expressions for the false detection probability and the packet error rate are presented. To reduce the complexity of the optimization, we propose a two-step strategy for the intelligent adversary: first optimally spoof in the sensing duration, and then optimally jam in the transmission duration. Numerical results indicate that there is a tradeoff between spoofing and jamming: a portion of the adversary's energy should be allocated to spoofing, and the remaining energy should be allocated to jamming.

The remainder of this paper is organized as follows: Section II outlines the system model, and a general optimization formulation for the joint spoofing and jamming of a cognitive radio network is presented. Section III describes the cognitive radio network that is considered in the paper, and proposes the two-step attacking strategy. Section IV presents the numerical results, and Section V presents our conclusions.

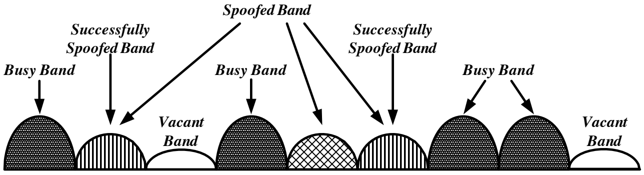


Fig. 2. Spectral band elaboration: Busy bands are ones used by primary users. All others are allowable bands.

II. System Model

The cognitive radio system considered in this paper employs periodic spectrum sensing. The frame structure [12] is illustrated in Fig. 1, which consists of a sensing slot and a data transmission slot in each frame. Let T_0 be the duration of the sensing slot, and T_1 be the duration of the transmission slot. The ratio of transmission-to-sensing duration, α, is defined as $\alpha = T_1/T_0$.

A. Spoofing in the Sensing Slot

As illustrated in Fig. 2, spectral bands not currently used by primary users are termed *allowable bands*. Those allowable bands in which the adversary chooses to emit spoofing signals are termed *spoofed bands*. The allowable bands that are not spoofed are called *vacant bands*.

The adversary will either sense or spoof during each of the CR system's sensing intervals. We assume that the duration of a typical primary user's message will span many sensing/data frames, so that the adversary's strategy is to sense every, say, nth frame, where n is a parameter to be chosen. For example, if the adversary senses during frame i, he will not sense again until frame $i+n$. During the $n-1$ frames between frames i and $i+n$, the adversary will spoof some fraction of those bands which he determined to be not busy when he sensed during frame i. In this paper, we are concerned with the system performance, given that the adversary has made a choice on which bands to spoof. The choice of the specific value of n to use is beyond the scope of the paper.

The probability that a vacant band is sensed to be busy by a secondary user due to the presence of thermal noise is called the *false alarm* probability. The probability that an allowable band is sensed to be busy due to both noise and spoofing is termed the *false detection* probability [5]. The average number of false detections, N_J, is shown in [5] to equal the sum of the false detection probabilities of all allowable bands. Assume that during a given sensing interval, there are N allowable bands. False detections reduce the average number of available bands (i.e., $N - N_J$) for a secondary user. Note that the false detection probability includes false detections due to both spoofing and thermal noise, which reduces to the false alarm probability when the spoofing signal is absent. If all allowable bands are spoofed, and the spoofing power in each band is large enough, the false detection probabilities will approach unity, i.e., N_J approaches N.

B. Jamming in the Data Transmission Slot

After spectrum sensing, some allowable bands are falsely determined to be busy, while the others are identified as vacant. Secondary users can then access these vacant bands for information transmission. In this slot, the intelligent adversary can use jamming techniques to attack secondary users.

The throughput of the secondary users is considered here. Let $\Gamma_k^{(j)}$ denote the throughput of the jth secondary user in the kth band, given by [13]

$$\Gamma_k^{(j)} = \left(1 - PER_k^{(j)}\right)\left(z log_2 M\right) \tag{1}$$

where z is the total number of modulated symbols in one packet, $log_2 M$ is the number of bits in one symbol, and $PER_k^{(j)}$ is the probability of packet error of the jth user in the kth band.

C. Joint Spoofing and Jamming by the Intelligent Adversary

To induce the worst effect on the secondary, a joint strategy for spoofing and jamming a cognitive radio system by an intelligent adversary is presented in the following. Let Ω_k denote the number of secondary users in the kth band. The sum throughput in the kth band, Γ_k, is expressed as

$$\Gamma_k = \sum_{j=1}^{\Omega_k} \Gamma_k^{(j)} \tag{2}$$

where $\Gamma_k^{(j)}$ is defined in (1). The maximum number of secondary users that can coexist with each other in the same frequency band is denoted $\Omega^{(0)}$. At the start of any data transmission slot, the total number of spectral vacancies for secondary users is $N_a\Omega^{(0)}$, where N_a is an integer random variable in the range $[0,N]$, representing the number of bands sensed to be vacant by the cluster head. Also, the number of spectral vacancies required by secondary users is denoted by N_R. It is a system parameter for evaluating the performance of the CR network, and can be any positive integer.

Let $N_a = i$ be the number of bands sensed to be vacant by the cluster head at some particular instant of time. The number of spectral vacancies accessed by secondary users, n_S, is jointly determined by both $N_a = i$ and N_R. That is,

$$n_S = \min\{i\Omega^{(0)}, N_R\} \tag{3}$$

The conditional average sum throughput of the secondary users, Γ_i^{sum}, conditioned on $N_a = i$, and parameterized by N_R, is given by

$$\Gamma_i^{sum} = \sum_{k=1}^{i} \Gamma_k \tag{4}$$

Then the average sum throughput of the secondary users, Γ^{sum}, parameterized by N_R, is given by

$$\Gamma^{sum} = \sum_{i=1}^{N} p_{N,i}\Gamma_i^{sum} \tag{5}$$

where $p_{N,i}$ is the probability that i out of N bands are sensed to be vacant by the cluster head.

The expression for the average sum throughput, Γ^{sum}, is a function of two parameters: one is $p_{N,i}$, which is the result of spoofing in the sensing slot; the other one is $PER_k^{(j)}$, which is the result of jamming in the transmission slot. Therefore, the strategy for joint spoofing and jamming by an intelligent adversary with an energy constraint is given by

$$\begin{aligned} \min \quad & \Gamma^{sum} \\ s.t. \quad & T_0 \sum_{k=1}^{N} P_{D,k} + \alpha T_0 \sum_{k=1}^{N} P_{J,k} = E \end{aligned} \tag{6}$$

where E is the energy budget of the intelligent adversary, and $P_{D,k}$ and $P_{J,k}$ are the spoofing power and the jamming power transmitted in the kth allowable band, respectively.

Note that when N_R spectral vacancies are required by secondary users, and n_a subcarriers are available, the N_R data packets are assumed to occupy the n_a subcarriers as evenly as possible. So for example, if 10 spectral vacancies are required and 3 subcarriers are available, the subcarriers are filled with 4, 3, and 3 data packets. Since the jammer is, in general, a partial-band jammer, and may hit fewer than the total number of subcarriers occupied, it would make a difference in the throughput if the more heavily occupied subcarriers were hit (e.g., 4 instead of 3). In Section IV, we present numerical results for the worst-case allocation of jammed subcarriers.

III. Joint Spoofing and Jamming a Cognitive Radio Network

In this section, to address the joint spoofing and jamming design, a cluster-based cognitive radio system is assumed. As analyzed in Section II, once $p_{N,i}$ and $PER_k^{(j)}$ are established, the exact expression for the average sum throughput in (6) can be obtained. In the following, we derive $p_{N,i}$ in terms of the false detection probability in the sensing slot, and $PER_k^{(j)}$ in the data transmission slot.

A. $p_{N,i}$ under Spoofing in Sensing Slot

In the sensing slot, spectrum sensing is carried out to find unused bands. A number of sensing methods have been proposed [14][15]. For example, a matched filter is optimal, but it requires prior knowledge of the primary system. Energy detection is suboptimal, but it is simple to implement. Furthermore, if the secondary only knows the local noise power, then energy detection is optimal [16]. In this paper, we assume the primary signaling is unknown at the secondary users' receivers, and hence energy detection is adopted for spectrum sensing by the secondary system. The false detection probability in the kth allowable band, p_k, can be approximately expressed as a function of spoofing power in that band, given by [17][4][5]

$$p_k\left(P_{D,k}\right) \simeq Q\left(\frac{a}{\tilde{P}_{D,k} + \sigma_n^2} + b\right) \tag{7}$$

where σ_n^2 is the thermal noise power, and $\tilde{P}_{D,k}$ is the received spoofing power in the kth band. The parameters a and b are given by $a = K/2\sqrt{T_0 W}$, and $b = -\sqrt{T_0 W}$, where K is the threshold used by the secondary for sensing, W is the bandwidth of one allowable band, and $T_0 W$ corresponds to the integration-time-bandwidth product at the energy detection receiver. As discussed in the Introduction, we assume that the cluster head performs the spectrum sensing. Therefore, the probability that i out of N bands are sensed to be vacant by the cognitive radio network, $p_{N,i}$, is given by

$$\begin{aligned} p_{N,1} &= (1-p_1)\prod_{k\neq 1} p_k + \cdots + (1-p_N)\prod_{k\neq N} p_k && (8)\\ p_{N,2} &= (1-p_1)(1-p_2)\prod_{k\neq 1,2} p_k + \cdots + (1-p_1)\cdot \\ &\quad (1-p_N)\prod_{k\neq 1,N} p_k + (1-p_2)(1-p_3)\cdot \\ &\quad \prod_{k\neq 2,3} p_k + \cdots + (1-p_2)(1-p_N)\prod_{k\neq 2,N} p_k \\ &\quad \vdots \\ &\quad +(1-p_{N-1})(1-p_N)\prod_{k\neq N-1,N} p_k && (9)\\ p_{N,N} &= \prod_{k=1}^{N}(1-p_k) && (10) \end{aligned}$$

B. Probability of Packet Error under Jamming in Transmission Slot

The cognitive radios in the tactical communications network utilize multicarrier DS-CDMA for transmission, which allows multiple secondary users to simultaneously occupy the same frequency band, i.e., $\Omega^{(0)} > 1$. The transmitter for the jth user is shown in Fig. 3, where $d_m^{(j)}$ is a random binary sequence representing data, and $c_n^{(j)}$ is a pseudo-random signature sequence. We assume that there are N_c chips per symbol, and that each user has a different signature sequence. The sequence $d_m^{(j)} c_n^{(j)}$ modulates an impulse train, where the energy per chip is E_c. After passing through a chip wave-shaping filter, the signal out of the filter modulates the carrier and is transmitted. Therefore, the transmitted signal, $S_j(t)$, is given by

$$S_j(t) = \sqrt{2E_c}\sum_{n=-\infty}^{\infty} d_m^{(j)} c_n^{(j)} h(t-nT_c)\, cos\,(w_j t + \theta_j) \qquad (11)$$

where E_c is the energy per chip, $m = \lfloor n/N_c \rfloor$, $h(t)$ is the impulse response of the chip wave-shaping filter, and θ_j is a random carrier phase uniformly distributed over $[0, 2\pi]$.

The transmitted signal is corrupted by AWGN and the jamming signal of the intelligent adversary. A Gaussian noise jammer is considered in this paper, and is assumed to be independent of the background additive Gaussian noise. The spectrum of the jamming signal in each band is rectangular, and has a bandwidth equal to the width of that band. The block diagram for the receiver of a secondary user is presented in Fig. 4, where we assume the chip wave-shaping filter satisfies the Nyquist criterion to guarantee that the DS waveforms do not overlap in adjacent bands. Furthermore, $X(f) = H(f)H^*(f)$ is a raised-cosine filter such that

$$X(f) = \begin{cases} T_c & \left(|f| \leq \frac{1-\beta}{2T_c}\right) \\ \dfrac{T_c}{2}\left\{1 + cos\left[\dfrac{\pi T_c}{\beta}\left(|f| - \dfrac{1-\beta}{2T_c}\right)\right]\right\} & \left(\frac{1-\beta}{2T_c} \leq |f| \leq \frac{1+\beta}{2T_c}\right) \\ 0 & \text{elsewhere} \end{cases} \qquad (12)$$

where β is a measure of the excess bandwidth of the cognitive radio system. Therefore, the received signal is given by

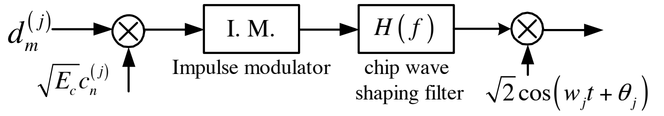


Fig. 3. Transmitter of the jth secondary user in the data transmission slot

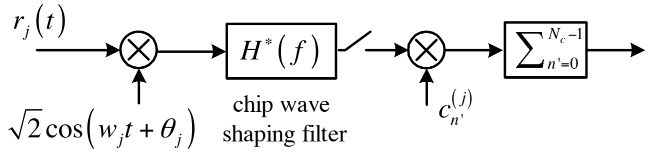


Fig. 4. Receiver of the jth secondary user in the data transmission slot

$$\begin{aligned} r_k^{(j)}(t) &= \sum_{j=1}^{\Omega_k}\{\sqrt{2E_c}\sum_{n=-\infty}^{\infty} d_m^{(j)} c_n^{(j)} h(t-nT_c)\cdot && (13)\\ &\quad cos(w_j t + \theta_j)\} + n_w(t) + n_J(t) \end{aligned}$$

where $n_w(t)$ is AWGN with a double-sided power spectral density of $\eta_0/2$, and $n_J(t)$ is the received jamming signal with a double-sided power spectral density of $\eta_J/2$ in each jammed band. Note that $P_{J,k}$ in Eq. (6) is related to η_J by $\xi^2 P_{J,k} = \eta_J \Delta W$, where ΔW and ξ denote the bandwidth of an allowable band, and the path loss factor between the adversary and the secondary user's receiver, respectively. Using the techniques in [11] and [18], the symbol error rate for the jth user with BPSK modulation in the kth band is approximately given by

$$SER_k^{(j)} \simeq Q\left(\sqrt{\frac{2N_c E_c}{(\Omega_k - 1)(1-\beta/4)E_c + \eta_J + \eta_0}}\right) \qquad (14)$$

Furthermore, the transmission scheme for the cognitive radio network in this paper is such that a single symbol error causes the loss of the whole packet. Thus, the packet error for the jth user in the kth band is given by

$$PER_k^{(j)} = 1 - \left(1 - SER_k^{(j)}\right)^z \qquad (15)$$

Substituting (15) into (1), the expression for the throughput of the jth user in the kth band is obtained. Therefore, the average sum throughput for the cognitive radio system can be found by combining (1), (2), (5), (14) and (15).

C. Joint Spoofing and Jamming: A Two-Step Strategy

To reduce the computational complexity of the joint optimization, we subdivide the problem as follows.

Assign a portion ρ $(0 \leq \rho \leq 1)$ of the adversary's energy to spoofing:

1) Optimally spoof in the sensing slot: for the allocated amount of energy, an optimal partial-band noise spoofing strategy, from [4][5], is carried out.

2) Optimally jam in the data transmission slot: the remaining energy is used for jamming, which corresponds to a fraction $1-\rho$ of the total energy. A partial-band noise jammer is adopted, and the optimal number of bands to jam, denoted N_J^*, is computed through minimizing the sum throughput of the secondary users in any particular time slot.

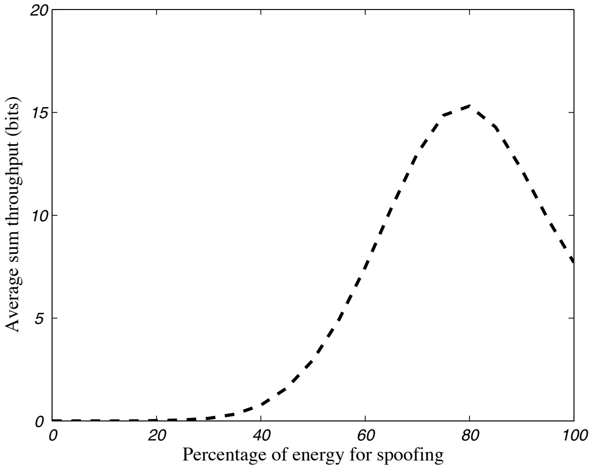


Fig. 5. Average sum throughput versus the percentage of energy for spoofing ($N=20$, $TW=25$, $p_f=10^{-4}$, $J/S=21dB$, and $N_R=1$)

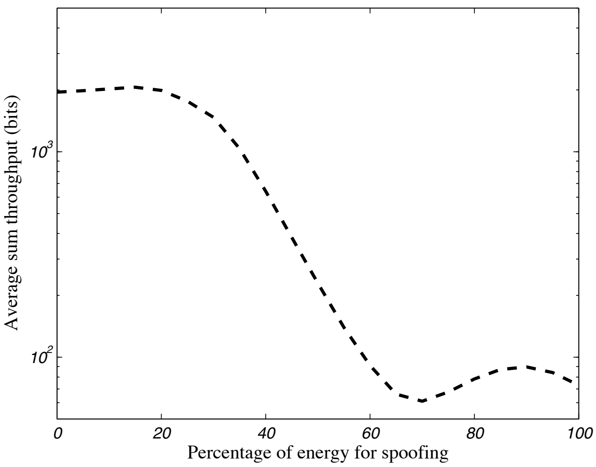


Fig. 6. Average sum throughput versus the percentage of energy for spoofing ($N=20$, $TW=25$, $p_f=10^{-4}$, $J/S=21dB$, and $N_R=10$)

By minimizing the average sum throughput in (6) over all possible values of ρ, the attacking strategy for the intelligent adversary is then established.

IV. Numerical Results

In this section, numerical results are provided for the above cognitive radio network where the transmission-to-sensing duration ratio, α, is set to 10 [12], and the number of symbols in one packet, z equals 256. The thermal noise power in one allowable band at the energy detection receiver, σ_n^2 (as in (7)), is normalized to unity. It is assumed that we have perfect power control at the cluster head, i.e., the average received energy of each secondary user is identical, and E_b/η_0 is set to 10dB. The maximum number of users that can coexist with each other in the same band, $\Omega^{(0)}$, is set to 10, such that even when $\Omega^{(0)}$ users are operating in the same band, the symbol error rate is between 10^{-4} and 10^{-3}. Here we define J/S to be the jamming-to-signal power ratio, where J is the jamming power when all the adversary's energy is put into jamming, i.e., $J=E/\alpha T_0$, and S is the signal power at a secondary user.

A. Joint Spoofing and Jamming

In Fig. 5, the average sum throughput, Γ^{sum}, is plotted versus the percentage of energy for spoofing, for the case when there are 20 allowable bands (a total of $N\Omega^{(0)}=200$ spectral vacancies), and only a small fraction of them are required by the cognitive radio system, e.g., $N_R=1$. It is seen that the minimum of Γ^{sum} is achieved when all the energy is allocated to jamming. That is, the optimal strategy for the intelligent adversary in this case is to jam only.

When the number of spectral vacancies required by secondary users, N_R, increases from 1 to 10, the average sum throughput versus the percentage of energy for spoofing is shown in Fig. 6. It is now seen that, when the adversary puts roughly 70 percent of its energy in spoofing, the average sum throughput of secondary users is minimized. That is, the remaining 30 percent of energy should be allocated to jamming. Therefore, for the intelligent adversary, the attack in this case is a combination of partial-band noise spoofing and partial-band noise jamming.

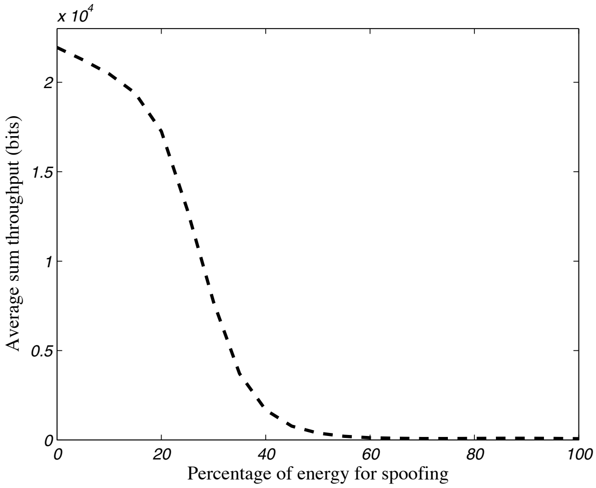


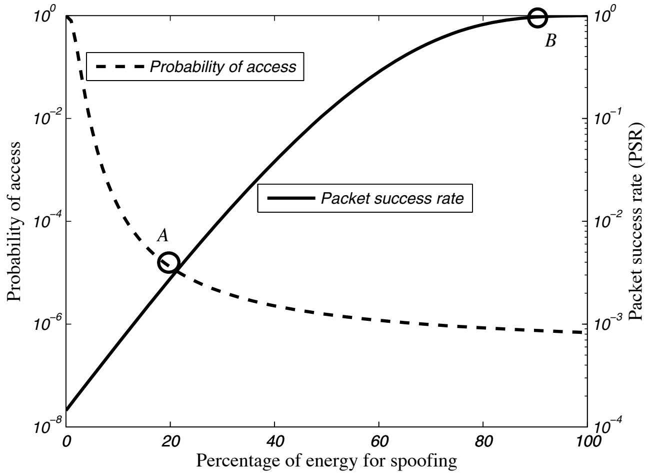
Fig. 7. Average sum throughput versus the percentage of energy for spoofing ($N=20$, $TW=25$, $p_f=10^{-4}$, $J/S=21dB$, and $N_R=100$)

When we further increase N_R to be a large fraction of the total spectral vacancies, e.g., $N_R=100$, the average sum throughput of secondary users is plotted in Fig. 7. It is seen that Γ^{sum} monotonically decreases when the spoofing energy increases. Therefore, the minimum of Γ^{sum} occurs when all the energy is allocated to spoofing, i.e., zero energy is put in jamming.

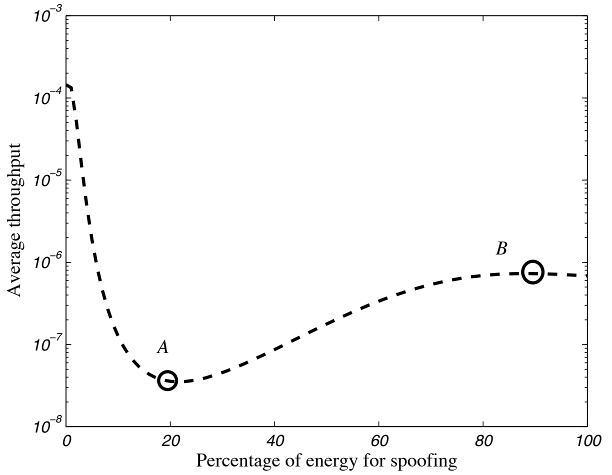
Note that the average sum throughput in Fig. 6 decreases and then increases and then decreases again. In the following, we explain this behavior by taking a simple example, whereby only one allowable band and one secondary user are involved. In this case, the average throughput reduces to the following form:

$$\tilde{\Gamma}=(1-p_k)(1-PER)z\log_2 M \tag{16}$$

where p_k is the false detection probability due to spoofing in the kth band, as given in (7). PER is the packet error rate, and



(a)



(b)

Fig. 8. Average throughput and its components versus the percentage of energy for spoofing for single-band and single-user ($J/S = 19.8dB$, $\sigma_n^2 = 1$, $TW = 25$, and $p_f = 10^{-4}$): (a) probability of access/packet success rate (b) average throughput.

is given in (14) and (15), where the number of users in the kth band $\Omega_k = 1$. Ignoring the constant $z \log_2 M$, we consider the average throughput as $\Gamma = (1 - p_k)(1 - PER)$. It is seen that Γ is the product of two terms: $(1 - p_k)$ due to spoofing, and $(1 - PER)$ due to jamming. In the following, we show how $(1 - p_k)$ (referred to as the *probability of access*), $(1 - PER)$ (referred to as the *packet success rate* (PSR)), and Γ vary with the percentage of energy for spoofing, with a given energy budget of the adversary.

The probability of access and the packet success rate versus the percentage of energy for spoofing are shown in Fig. 8(a), where the energy budget of the adversary corresponds to $J/S = 19.8dB$. It can be seen that as the spoofing energy increases, the probability of access first decreases sharply until roughly Point A, and then slows down as the spoofing energy further increases. Meanwhile, the PSR first increases sharply as the spoofing energy increases (i.e., jamming energy decreases) up to roughly Point B, and then starts to saturate. Note that when the percentage of energy for spoofing is to the left of Point A, the probability of access decreases more sharply than the increase in the packet success rate. So the trend of the average throughput in this region is dominated by the probability of access. This is consistent with the curve in Fig. 8(b), where Γ decreases as the spoofing energy increases until Point A, and its minimum is achieved. In the region from Point A to Point B, the probability of access starts to saturate while the PSR still increases sharply. So it is seen in Fig. 8(b) that Γ starts to increase up to Point B. At this point, the PSR flattens out such that its slight increase cannot compensate for the decrease in the probability of access as the spoofing energy further increases. As a consequence, the average throughput decreases again.

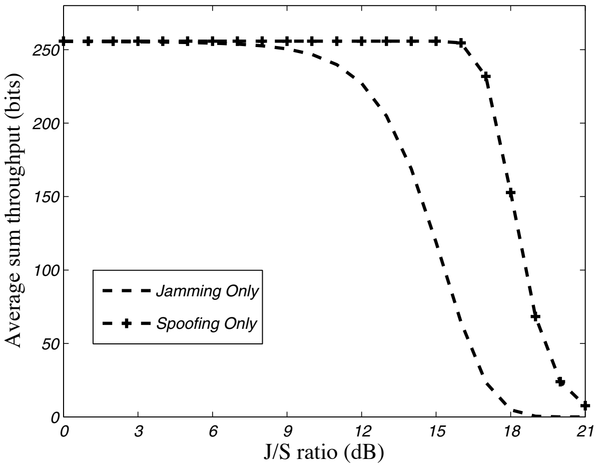


Fig. 9. Average sum throughput versus J/S ratio ($N = 20$, $TW = 25$, $p_f = 10^{-4}$, and $N_R = 1$)

Note that there are also cases where the average throughput monotonically decreases as the percentage of energy for spoofing increases, for example, when the energy budget is set corresponding to $J/S = 12.8dB$. This is because, under this scenario, the decrease in the probability of access is always more significant than the increase in the packet success rate as the spoofing energy increases. In other words, spoofing is always more effective than jamming in this case (see, for example, Fig. 7).

In order to understand the results in Fig. 5 to Fig. 7 more clearly, in the following, we present numerical results for two cases: 1) Spoofing only: the adversary only optimally spoofs in the sensing duration; 2) Jamming only: the adversary only optimally jams in the transmission slot. In Fig. 9, Γ^{sum} versus the J/S ratio (in dB) for both spoofing only and jamming only are plotted, where the parameters are the same as in Fig. 5. Note that in scenarios of spoofing only, the adversary power J represents the spoofing power, not the jamming power. It is seen that, for the same J/S ratio, the average sum throughput of secondary users under jamming is smaller than that under spoofing. In this case, jamming is more effective than spoofing. This explains why the jamming only strategy is the best attack for the adversary in the scenario depicted in Fig. 5.

For the same parameters as those in Fig. 6, the average sum throughput versus J/S for spoofing only and jamming only is given in Fig. 10. The spoofing and jamming capabilities are

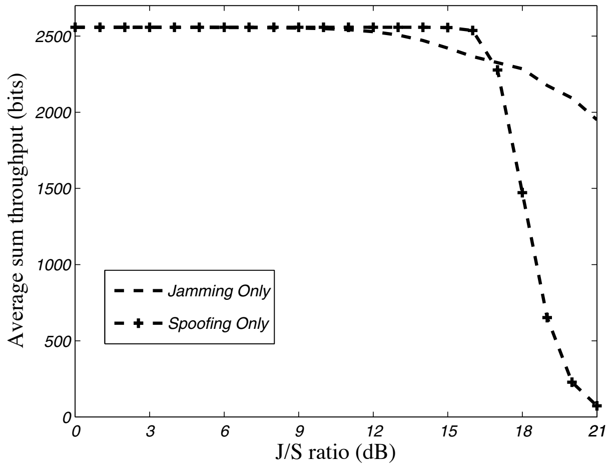


Fig. 10. Average sum throughput versus J/S ratio ($N = 20$, $TW = 25$, $p_f = 10^{-4}$, and $N_R = 10$)

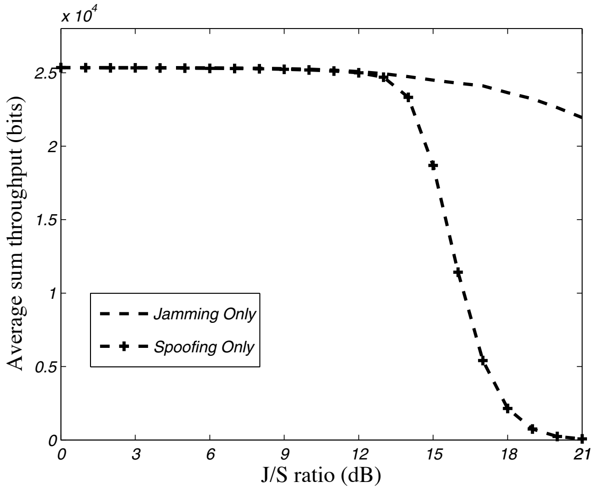


Fig. 11. Average sum throughput versus J/S ratio ($N = 20$, $TW = 25$, $p_f = 10^{-4}$, and $N_R = 100$)

comparable with each other. This is consistent with the result for joint spoofing and jamming in Fig. 6, where there is a tradeoff between spoofing and jamming, such that the average sum throughput is minimized. In Fig. 11, the average sum throughput under spoofing only and jamming only is plotted for the same parameters as those in Fig. 7. For the same Γ^{sum}, the jamming-only strategy requires a higher J/S, i.e., a larger amount of energy. Therefore, spoofing is more effective than jamming. This is in accordance with the result illustrated in Fig. 7, which indicates that the optimal attack of the adversary in this scenario is to spoof only.

The results in Figures 5 to 11 are intuitively reasonable. When there is only one spectral vacancy required by secondary users, then the adversary is better off not spoofing at all. After the secondary user has selected its one spectral vacancy, the adversary can jam it. Pouring energy into spoofing a large number of bands would have been wasteful, because the overwhelming majority of those allowable bands were not, in any case, going to be accessed by any secondaries, in this lightly loaded scenario. At the opposite extreme, there is the case where a large number of secondary users is going to heavily load the system, so that in the absence of the adversary, every allowable band would be used with multiple users coexisting. In this case, spoofing bands is more efficient than jamming because any band that is successfully spoofed would almost surely have had secondaries using it in the absence of spoofing, and those users will now have to coexist on a smaller number of bands. In between these extremes of jamming-only and spoofing-only strategies lies a region where both techniques should be deployed in tandem by the adversary. As stated before, we assume that the adversary knows which spectral vacancies are used by the secondaries. So this paragraph should not be taken as a design procedure for the adversary, but rather is an explanation of the performance as seen in Figures 5 to 11.

In order to get a more in-depth understanding of the spoofing capability and jamming capability, in the following we analyze, individually, how they vary with different system parameters.

It is shown in [4] and [5] that the spoofing capability increases when TW increases. In the following, we analyze how the spoofing and jamming capabilities vary with the total number of allowable bands, N, and with the number of spectral vacancies required by secondary users, N_R.

To construct a fair comparison, we define a metric to evaluate the effectiveness of the attack as the *percentage of throughput degradation*, given by

$$\zeta = \left(1 - \frac{\Gamma^{sum}}{\Gamma^{(0)}}\right) \times 100 \tag{17}$$

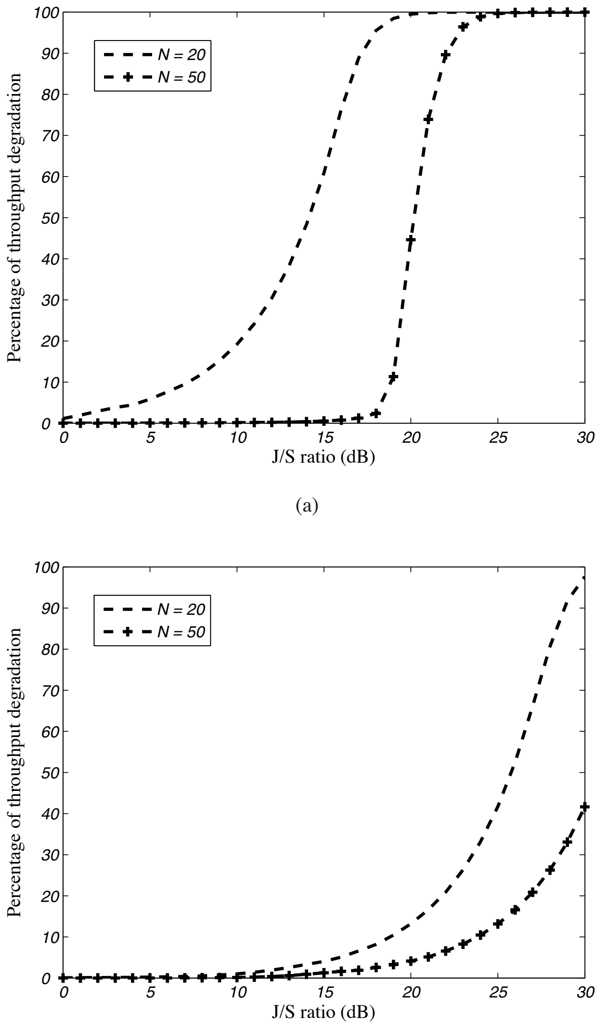
where Γ^{sum} is the average sum throughput under the attack by the intelligent adversary, and $\Gamma^{(0)}$is the average sum throughput of secondary users when the adversary is absent. From (17) we can see that a larger value of ζ indicates a more effective attack by the intelligent adversary.

The percentage of throughput degradation versus the J/S ratio for spoofing only is plotted in Fig. 12(a), for different values of N. For the same amount of the adversary's energy, the percentage of throughput degradation when $N = 20$ is larger than that for $N = 50$. This indicates that an increase in the total number of allowable bands will decrease the spoofing capability. Similar observations can be obtained from Fig. 12(b), for the jamming-only attack, namely, that an increase in N will also lower the capability of jamming.

For a given number of allowable bands, e.g., $N = 50$, the percentage of throughput degradation versus J/S is plotted in Fig. 13, parameterized by different values of N_R. In Fig. 13(a), when N_R increases, the percentage of throughput degradation increases. That is, increases in N_R boost the capability of spoofing. On the flip side, as seen in Fig. 13(b), the percentage of throughput degradation decreases as N_R increases, and hence the jamming capability is decreased. Therefore, we can reach the following conclusions:

1) Spoofing capability increases when: *a*) N decreases; *b*) N_R increases; *c*) TW increases.

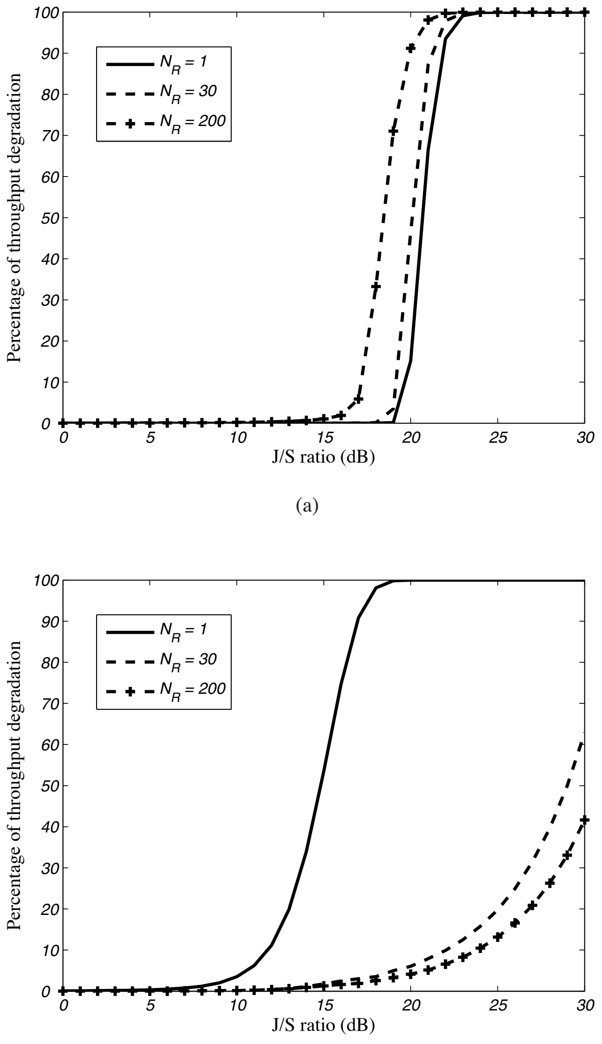
2) Jamming capability increases when: *a*) N decreases; *b*) N_R decreases.



(a)

(b)

Fig. 12. Percentage of throughput degradation versus J/S ratio, parameterized by the total number of allowable bands, N ($TW = 25$, $p_f = 10^{-4}$, and $N_R = 200$): (a) spoofing only (b) jamming only.



(a)

(b)

Fig. 13. Percentage of throughput degradation versus J/S ratio, parameterized by N_R ($N = 50$, $TW = 50$, $p_f = 10^{-4}$): (a) spoofing only (b) jamming only.

Note that the increase in N_R will increase spoofing capability while decreasing the jamming capability. This is consistent with the results from Fig. 5 to Fig. 7, where the optimal attack shifts from jamming only to spoofing only when N_R increases.

Now we increase TW in Fig. 6 from 25 to 50 and keep the other parameters unchanged. The average sum throughput of the secondary users versus the percentage of energy for spoofing is plotted in Fig. 14. It is seen that the optimal attack is to spoof only instead of a combination of spoofing and jamming illustrated in Fig. 6. This is because the increase in TW boosts the capability of spoofing. As discussed in [4] and [5], an increase in TW leads to an increase in the number of received signal samples for accumulation, and thus the energy detector can more accurately determine whether the received signal power is above or below the threshold.

V. Conclusion

In this paper, we analyzed two attacks on a cognitive radio network: spoofing and jamming. For an intelligent adversary with an energy constraint, a joint optimization problem considering both spoofing and jamming is formulated by minimizing the average sum throughput of the secondary users. Numerical results show that the optimal attack for an intelligent adversary is a combination of spoofing and jamming. Furthermore, we have numerically analyzed how the spoofing and jamming capabilities vary with different system parameters. Specifically, in our cognitive radio system, as either the number of spectral vacancies required by secondary users increases, or the value of TW at the energy detector of the secondary increases, the optimal attack for the intelligent adversary transitions from jamming to spoofing.

References

[1] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," *IEEE J. Sel. Areas Commun.*, 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

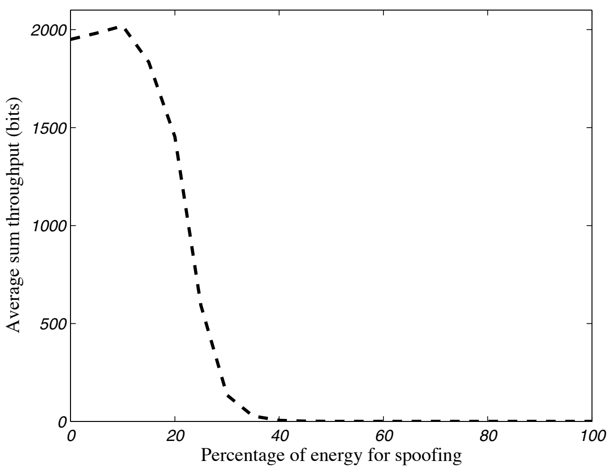


Fig. 14. Average sum throughput versus percentage of energy for spoofing ($N = 20$, $TW = 50$, $p_f = 10^{-4}$, $J/S = 21dB$, and $N_R = 10$)

analysis and assessment," *IEEE International Conf. on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 456-464, Aug. 2007.

[3] S. Anand, Z. Lin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *IEEE 3rd Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008.

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

[5] Q. H. Peng, P. C. Cosman, and L. B. Milstein, "Optimal sensing disruption for a cognitive radio adversary", *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1801-1810, May 2010.

[6] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I, Computer Science Press, 1985.

[7] C. Lo, E. Masry, and L. B. Milstein, "Design and analysis of a fast frequency-hopped DBPSK communication system, Part II. Error performance in AWGN plus partial-band noise jamming," *IEEE Trans. Commun.*, vol. 41, no. 11, pp. 1723-1735, Nov. 1993.

[8] D. J. Torrieri, *Principles of Secure Communication Systems*, Artech House Inc., 1985.

[9] S. Kondo and L. B. Milstein, "Performance of multicarrier DS CDMA systems," *IEEE Trans. Commun.*, vol. 44, no. 2, pp. 238-246, Feb. 1996.

[10] A. Attar, M. R. Nakhai, and A. H. Aghvami, "Cognitive radio transmission based on Direct Sequence MC-CDMA," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1157-1162, Apr. 2008.

[11] Q. Qu, L. B. Milstein, and D. R. Vaman, "Cognitive radio based multiuser resource allocation in mobile ad hoc networks using multi-carrier CDMA modulation," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 70-82, Jan. 2008.

[12] Y. C. Liang, Y. H. Zheng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[13] S. S. Tan, M. J. Rim, P. C. Cosman, and L. B. Milstein, "Adaptive Modulation for OFDM-based Multiple Description Progressive Image Transmission," *IEEE Globecom*, 2008.

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

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

[16] 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.

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

[18] W. Xu and L. B. Milstein, "Performance of multicarrier DS CDMA systems in the presence of correlated fading," *Proc. VTC*, vol. 3, pp. 2050-2054, 1997.

Qihang Peng received the B.S. and the M.S. degrees (both with honors) from the School of Communications and Information Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, China, in June 2004 and March 2007, respectively. She is currently working toward the Ph.D. degree from UESTC. She was a visiting scholar in the Department of Electrical and Computer Engineering, University of California at San Diego, USA. She has been serving as a member of the TPC of the IEEE INFOCOM 2010 Workshop on Cognitive Wireless Communications and Networking.

Pamela C. Cosman (S'88-M'93-SM'00-F'08) obtained her B.S. with Honor in Electrical Engineering from the California Institute of Technology in 1987, and her M.S. and Ph.D. in Electrical Engineering from Stanford University in 1989 and 1993, respectively. She was an NSF postdoctoral fellow at Stanford University and a Visiting Professor at the University of Minnesota during 1993-1995. In 1995, she joined the faculty of the department of Electrical and Computer Engineering at the University of California, San Diego, 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 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 an associate editor of the IEEE Signal Processing Letters (2001-2005). She was the Editor-in-Chief (2006-2009) as well as a Senior Editor (2003-2005, 2010-present) of the IEEE Journal on Selected Areas in Communications. She is a member of Tau Beta Pi and Sigma Xi.

Laurence B. Milstein (S'66-M'68-SM'77-F'85) received the B.E.E degree from the City College of New York, New York, NY, 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, and 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 at San Diego, La Jolla, where he is the Ericsson Professor of Wireless Communications and 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 government and industry in the areas of radar and communications.

Dr. Milstein 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 the IEEE Communications Magazine, and the Editor-in-Chief of the IEEE J. Sel. Areas Commun.. He was the Vice President for Technical Affairs in 1990 and 1991 of the IEEE Communications Society, and is a former Chair of the IEEE Fellow Selection Committee. He is a recipient of the 1998 Military Communications Conference 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.