Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary

Madushanka Soysa, Pamela C. Cosman, and Laurence B. Milstein.
Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093-040
E-mail: msoysa@ucsd.edu, pcosman@ucsd.edu, lmilstein@ucsd.edu

***Abstract*—We examine the performance of a cognitive radio system in a hostile environment where an intelligent adversary tries to disrupt communications by spoofing. We analyze a cluster-based network of secondary users (SUs), where sensing is performed by the cluster head. The adversary may attack during the sensing interval to limit access for SUs by transmitting a Gaussian noise spoofing signal. We present how the adversary can optimally allocate power across subcarriers during the sensing interval over Nakagami-m fading channels, using an optimization approach specific to this problem. We determine a worst-case optimal spoofing power allocation, when the adversary has knowledge of the system, which gives a lower bound to the average number of accessible bands for SUs under attack.**

***Index Terms* - Cognitive radio, intelligent adversary, partial-band spoofing**

I. Introduction

Although the demand for wireless spectrum has been growing rapidly, a large portion of the assigned spectrum is used only sporadically. The limited available spectrum and the inefficiency in spectrum usage necessitate a new communication paradigm to exploit the existing wireless spectrum opportunistically. Cognitive radio (CR) [1] has been widely investigated as a solution. In CR systems, the users are defined as primary users (PUs) if they have priority of access over the spectrum, and secondary users (SUs) otherwise. Any time a SU senses a band is unused by the PU, it can dynamically access the band. Thus, spectrum sensing is a key concept for CR but it is also a vulnerable aspect. This can be exploited by transmitting a spoofing signal emulating a PU during the sensing interval [2]. Here the SU might mistakenly conclude that the channel is occupied by a PU and not available for transmission. In this way, an intelligent attacker reduces the bandwidth available for the SU. Such exploitations and their impact are discussed in [3]–[10].

In this work, we analyze the impact of an intelligent adversary on a tactical CR system. In [3], the presence of such an intelligent adversary in an additive white Gaussian noise (AWGN) channel was discussed. This work was extended in [4], to obtain spoofing performance bounds under Rayleigh fading, when the adversary is aware of instantaneous channel state information (CSI). In this work, we extend the analysis to spoofing over Nakagami-m fading channels, without instantaneous CSI at the adversary, and consider both fast and slow fading. We further propose an optimization method specific to this problem, to find the optimal spoofing power allocation.

In Section II, we present the system model, and Section III contains the optimization technique. Sections IV and V discuss the spoofing strategy for fast and slow fading, respectively. Section VI contains numerical results and Section VII presents the conclusions.

This work was supported in part by the Office of Naval Research under grant number N00014-11-1-0733, the Army Research Office under grant number W9111NF-12-1-0510, and the National Science Foundation under grant number CCF-0915727.

II. System model

We consider a multi-carrier system with N_T bands (or subcarriers) shared among PUs and SUs. *Allowed bands* are ones unoccupied by PUs. The cluster head, CH_S, periodically performs spectrum sensing, and detects the allowed bands. *Busy bands* are bands that the SU network cannot use due to PU activity. During the sensing interval, the adversary attacks the system transmitting a Gaussian noise signal. The channels from adversary to CH_S in each subcarrier are assumed to undergo i.i.d. Nakagami-m fading with $m \geq \frac{1}{2}$. An allowed band may appear busy due to background noise and spoofing. This is called a *false detection*. The objective of the adversary is to maximize the average number of false detections.

We assume, in accordance with [3]–[5], that the adversary is aware of the basic characteristics of the system, including the receiver structure, false alarm probability, sensing interval, background noise power spectral density (PSD), the probability distribution of fading gains and whether it is slow or fast fading. Because a practical adversary may not have all the assumed knowledge, the work done here is a worst-case analysis, which gives a lower bound to the number of accessible bands for SUs under attack.

The CH_S uses an energy detector for sensing (Fig. 1). Let W be the bandwidth of one subcarrier, and T_0 be the duration of the sensing interval. The energy detector output, $Y(t)$, when there is no PU signal present, is given by $Y(t) = \int_{t-T_0}^{t} (\sqrt{\alpha_J(t_1)} n_s(t_1) + n_0(t_1))^2 \mathrm{d}t_1$, where $\alpha_J(t)$ is the gain of the channel from adversary to CH_S, $n_s(t)$ is the spoofing signal, and $n_0(t)$ is the noise after passing through the bandpass filter. The signal $n_s(t)$ is Gaussian with double sided PSD $\frac{\eta_s}{2}$ in the band, $n_0(t)$ is Gaussian with PSD $\frac{N_0}{2}$ in the band. The pdf of $\alpha_J(t)$, $f_{\alpha_J(t)}(x) = \frac{m^m x^{m-1} e^{-\frac{mx}{\Omega}}}{\Gamma(m)\Omega^m}$ with fading parameters m, Ω [11, Eq. 2.21]. From [12], we have

$$Y(t) = \frac{1}{2W} \sum_{k=1}^{T_0 W} (a_{i,k}^2 + a_{q,k}^2) \tag{1}$$

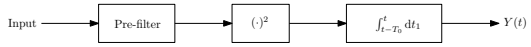


Fig. 1: Energy detector block diagram

where $a_{i,k} = \sqrt{\alpha_J\left(t-T_0+\frac{k}{W}\right)}n_{s,i}\left(t-T_0+\frac{k}{W}\right) + n_{0,i}\left(t-T_0+\frac{k}{W}\right)$, $a_{q,k} = \sqrt{\alpha_J\left(t-T_0+\frac{k}{W}\right)}n_{s,q}\left(t-T_0+\frac{k}{W}\right) + n_{0,q}\left(t-T_0+\frac{k}{W}\right)$, $n_{s,i}(t), n_{s,q}(t)$ are Gaussian with PSD η_s in the frequency range $(-\frac{W}{2}, \frac{W}{2})$, and $n_{0,i}(t), n_{0,q}(t)$ are Gaussian with PSD N_0 in the frequency range $(-\frac{W}{2}, \frac{W}{2})$. A band is detected as occupied by PUs if the energy detector output is greater than the threshold $K\sqrt{T_0W}$. Hence, the probability of false detection is equal to $\Pr(Y(t) > K\sqrt{T_0W})$.

Following the same approach as in [3, Eq. 1], we can show that the expected number of allowed bands accessible to SUs is $\sum_{i\in B_{al}}(1-p_{fd}^{(i)})$, where B_{al} is the set of allowed bands and $p_{fd}^{(i)}$ is the probability of false detection of the i-th band, given that the i-th band is allowed. At the start of the sensing interval the adversary does not know which bands are allowed for SUs. Therefore, from the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to maximize $\sum_{i=1}^{N_T} p_{fd}^{(i)}$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} = P_S$, where $P_{S,i}$ is the spoofing power allocated for the i-th band and P_S is the total spoofing power available.

III. Optimization approach

In this section we discuss the general optimization approach.

Theorem 1

Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be a function such that

P0: f is bounded above, i.e., $\exists M < \infty$, s.t. $f(x) \le M\ \forall x \in [0, \infty)$

P1: f is an increasing function, i.e., $f'(x) \ge 0$, where $f'(x)$ is the first derivative of $f(x)$,

P2: $f''(x) = 0$ has at most one root in $x > 0$, where $f''(x)$ is the second derivative of $f(x)$.

Also, define $g : \mathbb{R}^+ \to \mathbb{R}$, as $g(x) \triangleq f(x) - f(0) - xf'(x)$. Then, if $\sum_{i=1}^{N} x_i \le X_T$ and $x_i \ge 0$,

$$\sum_{i=1}^{N} f(x_i) \le \begin{cases} Nf\left(\frac{X_T}{N}\right), & \text{if } \frac{X_T}{N} \ge x^* \\ (N-n^*)\,f(0) + n^* f\left(\frac{X_T}{n^*}\right), & \text{if } \frac{X_T}{N} < x^* \end{cases} \quad (2)$$

where $n^* = \frac{X_T}{x^*}$ and x^* is the largest root of $g(x) = 0$. Also, the set of arguments, S_x, that correspond to the equality when n^* is an integer, is given by

$$S_x = \underset{\sum_{i=1}^{N} x_i = X_T,\ x_i \ge 0}{\arg\max} \left(\sum_{i=1}^{N} f(x_i)\right) = \begin{cases} \underbrace{\left\{\frac{X_T}{N}, \ldots, \frac{X_T}{N}\right\}}_{N \text{ elements}}, & \text{if } \frac{X_T}{N} \ge x^* \\ \underbrace{\left\{\frac{X_T}{n^*}, \ldots, \frac{X_T}{n^*}\right.}_{n^* \text{ elements}}, \underbrace{\left.0, \ldots, 0\right\}}_{(N-n^*)}, & \text{if } \frac{X_T}{N} < x^* \end{cases} \quad (3)$$

When $\frac{X_T}{x^*}$ is not an integer, we use the approximation $n^* = \underset{n=\left\{\left\lfloor \frac{X_T}{x^*}\right\rfloor, \left\lceil \frac{X_T}{x^*}\right\rceil\right\}}{\arg\max} (N-n)\,f(0) + nf\left(\frac{X_T}{n}\right)$, to arrive at a suboptimal set S_x.

The proof of Theorem 1 is given in [13]. In optimizing power allocation for spoofing, $f(x)$ is the probability of false detection in one band as a function of the spoofing power allocated for that band.

IV. Fast fading

Here we assume the channel coherence time is much smaller than the sensing duration T_0, and the channel varies significantly during the sensing interval so that the channel samples in time are mutually independent. We can show that $E[a_{i,k}^2 + a_{q,k}^2] = 2(\Omega\eta_s W + N_0 W)$, and $\text{Var}(a_{i,k}^2 + a_{q,k}^2) = 2(\tilde{m}\Omega^2\eta_s^2 W^2 + 4\Omega\eta_s N_0 W^2 + 2N_0^2 W^2)$, where $\tilde{m} = \frac{2m+3}{m}$. Since $\text{Var}(a_{i,k}^2 + a_{q,k}^2)$ is finite, we can use the Lindeberg-Lévy CLT to approximate $Y(t)$ in (1). Therefore, for large T_0W, $Y(t) \sim \mathcal{N}(T_0W(\Omega\eta_s + N_0), T_0W(\tilde{m}\Omega^2\eta_s^2 + 4\Omega\eta_s N_0 + 2N_0^2)/2)$. Let $p_{fd,f}(P_{S,i})$ be the probability of false detection under fast fading, as a function of the spoofing power in that band $P_{S,i}$. Then,

$$p_{fd,f}(P_{S,i}) = \Pr(Y(t) > K\sqrt{T_0W}) = Q\left(\frac{K\sqrt{T_0W} - T_0W\left(\Omega\left(\frac{P_{S,i}}{W}\right) + N_0\right)}{\sqrt{\frac{T_0W}{2}\left(\tilde{m}\Omega^2\left(\frac{P_{S,i}}{W}\right)^2 + 4\Omega\left(\frac{P_{S,i}}{W}\right)N_0 + 2N_0^2\right)}}\right) \quad (4)$$

Define

$$g(y) \triangleq p_{fd,f}\left(\frac{WN_0 y}{\Omega}\right) = Q\left(\frac{b - ay}{\sqrt{\tilde{m}y^2 + 4y + 2}}\right) \quad (5)$$

where $b = \frac{K\sqrt{2}}{N_0} - \sqrt{2T_0W}$ and $a = \sqrt{2T_0W}$. As long as the detector threshold is selected so that the false alarm probability (false detection without spoofing) is less than 0.5, then $p_{fd,f}(0) < 0.5 \Leftrightarrow g(0) < 0.5 \Leftrightarrow b > 0$. We now show that the conditions of Theorem 1 are satisfied.

1) From the definition of $p_{fd,f}(P_{S,i})$, condition **P0** is obviously satisfied by $p_{fd,f}(P_{S,i})$.

2) From the definition of $g(y)$, we have

$$p_{fd,f}(P_{S,i}) = g\left(\frac{\Omega P_{S,i}}{WN_0}\right) \quad (6)$$

and from (5),

$$g'(y) = \frac{\mathrm{d}g(y)}{\mathrm{d}y} = \frac{(2a + \tilde{m}b)y + 2a + 2b}{(\tilde{m}y^2 + 4y + 2)^{\frac{3}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(\tilde{m}y^2+4y+2)}} \quad (7)$$

From (7), $g'(y) > 0\ \forall y > 0$, because $a, b > 0$. From (6), $\frac{\mathrm{d}}{\mathrm{d}P_{S,i}} p_{fd,f}(P_{S,i}) = \frac{\Omega}{WN_0} g'\left(\frac{\Omega P_{S,i}}{WN_0}\right) > 0\ \forall P_{S,i} > 0$. Therefore, condition **P1** is satisfied.

3) From (7),

$$g''(y) = \frac{\mathrm{d}}{\mathrm{d}y} g'(y) = \frac{p(y)}{(\tilde{m}y^2 + 4y + 2)^{\frac{7}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(\tilde{m}y^2+4y+2)}} \quad (8)$$

where $p(y) = c_4y^4 + c_3y^3 + c_2y^2 + c_1y + c_0$, $c_0 = -16a - 4(6-\tilde{m})b + 4a^2b + 8ab^2 + 4b^3$, $c_3 = -2\tilde{m}(10+3\tilde{m})a - 16\tilde{m}^2b - a(2a+\tilde{m}b)^2 < 0$, $c_4 = -2\tilde{m}^2(2a+\tilde{m}b) < 0$,

$$c_1 = \tilde{m}c_0 - 4(10-\tilde{m})a - 4((\tilde{m}-2)^2+8)b - 4a^3 - 4\tilde{m}a^2b - 4(\tilde{m}-1)ab^2, \text{ and} \quad (9)$$

$$c_2 = \frac{\tilde{m}}{4}c_1 - (16+3\tilde{m}(10-\tilde{m}))a - 32\tilde{m}b - (8-\tilde{m})a^3 - 4(\tilde{m}+1)a^2b - \tilde{m}(\tilde{m}+1)ab^2. \quad (10)$$

According to Descartes' rule of signs, the number of real positive roots of the polynomial $p(y) = 0$ equals the number of sign changes between nonzero c_is (ordered from c_4 to c_0), or is less than the number of sign changes by a multiple of 2. Note that $c_4, c_3 < 0$ and $\tilde{m} \in (2, 8]$ because $m \geq \frac{1}{2}$. From (9), we see that $c_0 \leq 0 \Rightarrow c_1 < 0$, and from (10), $c_1 \leq 0 \Rightarrow c_2 < 0$. Therefore, if $c_0 \leq 0$, all non-zero coefficients are negative and there are no sign changes, i.e., there are no positive roots.

Let us consider the case $c_0 > 0$. If $c_1 \leq 0$, then $c_2 < 0$, and there is only one sign change in the coefficients. If otherwise, i.e., $c_1 > 0$, there will be only one sign change irrespective of the sign of c_2. Therefore, we can see that the number of sign changes between coefficients is either 0 or 1. Hence, there will be at most one positive root for $p(y) = 0$. Further, since $c_4 < 0$, $\lim_{y\to\infty} p(y) \to -\infty$. We conclude that $p(y) < 0\ \forall y > 0$ or $\exists y_0 > 0$, s.t. $q(y) < 0\ \forall y > y_0$ and $p(y) \geq 0\ \forall y \leq y_0$. From (8), we know $g''(y)$ has the same sign as $p(y)$. Therefore, we conclude that $g(y)$ satisfies the condition **P2**. From (6), $\frac{\mathrm{d}^2}{\mathrm{d}P_{S,i}^2} p_{fd,f}(P_{S,i}) = \frac{\Omega^2}{W^2N_0^2} g''\left(\frac{\Omega P_{S,i}}{WN_0}\right)$. Therefore, $p_{fd,f}(P_{S,i})$ satisfies the condition **P2**.

V. Slow fading

Here we assume the channel coherence time is larger than the sensing duration T_0. Therefore, the channel gain remains constant during the sensing interval and we denote it by α_J. When conditioned on α_J, $a_{i,k} = \sqrt{\alpha_J} n_{s,i}\left(t - T_0 + \frac{k}{W}\right) + n_{0,i}\left(t - T_0 + \frac{k}{W}\right) \sim \mathcal{N}(0, \alpha_J\eta_s W + N_0 W)$, and similarly, $a_{q,k} \sim \mathcal{N}(0, \alpha_J\eta_s W + N_0 W)$. Therefore, $E[a_{i,k}^2 + a_{q,k}^2|\alpha_J] = 2(\alpha_J\eta_s W + N_0 W)$ and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2|\alpha_J) = 4(\alpha_J\eta_s W + N_0 W)$. Using these results in (1), for large T_0W, we conclude, when conditioned on α_J, $Y(t) \sim \mathcal{N}(T_0W(\alpha_J\eta_s + N_0), T_0W(\alpha_J\eta_s + N_0)^2)$.

The average probability of false detection under slow fading, when the spoofing signal PSD is $\eta_{S,i}$, is given by

$$\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) = \int_0^\infty \Pr(Y(t) > K\sqrt{T_0W}|\alpha_J = y, \eta_{S,i}) f_{\alpha_J}(y)\mathrm{d}y \quad (11)$$

where $f_{\alpha_J}(y) = \frac{m^m y^{m-1}}{\Gamma(m)\Omega^m} e^{-\frac{my}{\Omega}}$ is the probability density function of the channel gain α_J. Substituting this in (11) yields

$$\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) = \frac{m^m}{\Gamma(m)\Omega^m} \int_0^\infty Q\left(\frac{K}{\eta_{S,i}y + N_0} - \sqrt{T_0W}\right) y^{m-1} e^{-\frac{my}{\Omega}} \mathrm{d}y \quad (12)$$

As for the fast fading case, we now show that the three conditions of Theorem 1 are satisfied.

1) Condition **P0** is obviously satisfied from (12).

2) We have

$$\frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) = \frac{m^m K}{\Gamma(m)\Omega^m\sqrt{2\pi}} \times \int_0^\infty \frac{y^m}{(y\eta_{S,i} + N_0)^2} e^{-\frac{1}{2}\left(\frac{K}{y\eta_{S,i}+N_0} - \sqrt{T_0W}\right)^2} e^{-\frac{my}{\Omega}}\ \mathrm{d}y > 0$$

Therefore, condition **P1** is satisfied.

3) We can show that

$$\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) = \frac{m^m K}{\Gamma(m)\Omega\sqrt{2\pi}} \int_0^\infty e^{-\frac{my}{\Omega\eta_{S,i}}} e^{-\frac{1}{2}\left(\frac{K}{y+N_0} - \sqrt{T_0W}\right)^2} y^{m+1} \times \frac{K^2 - K\sqrt{T_0W}(y+N_0) - 2(y+N_0)^2}{\eta_{S,i}^{m+2}(y+N_0)^5} \mathrm{d}y = \frac{I(\eta_{S,i})}{\eta_{S,i}^{m+2}} \quad (13)$$

where $I(\eta_{S,i}) \triangleq \int_0^\infty \iota(y) e^{-\frac{my}{\Omega\eta_{S,i}}}\ \mathrm{d}y$ and $\iota(y) \triangleq \frac{m^m K y^{m+1}(K^2 - K\sqrt{T_0W}(y+N_0) - 2(y+N_0)^2)}{\Gamma(m)\Omega\sqrt{2\pi}(y+N_0)^5} e^{-\frac{1}{2}\left(\frac{K}{y+N_0} - \sqrt{T_0W}\right)^2}$. Note that the sign of $\iota(y)$ depends only on the sign of the quadratic polynomial $K^2 - K\sqrt{T_0W}(y+N_0) - 2(y+N_0)^2$. Further, $\iota(y) > 0 \Leftrightarrow K^2 - K\sqrt{T_0W}(y+N_0) - 2(y+N_0)^2 > 0 \Leftrightarrow y + N_0 \in \left(-\frac{K(\sqrt{T_0W+8} + \sqrt{T_0W})}{4}, \frac{K(\sqrt{T_0W+8} - \sqrt{T_0W})}{4}\right)$. Define $y_0 \triangleq \max\left(\frac{K(\sqrt{T_0W+8} - \sqrt{T_0W})}{4} - N_0, 0\right)$. From the definition of y_0, $y > y_0 \Rightarrow \iota(y) < 0$ and $0 < y < y_0 \Rightarrow \iota(y) > 0$. Also,

$$I'(\eta_{S,i}) \triangleq \frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}} I(\eta_{S,i}) = \frac{m}{\Omega\eta_{S,i}^2} \int_0^\infty y\iota(y) e^{-\frac{my}{\Omega\eta_{S,i}}} \mathrm{d}y < \frac{m}{\Omega\eta_{S,i}^2} \left(\int_0^{y_0} y_0\iota(y) e^{-\frac{my}{\Omega\eta_{S,i}}} \mathrm{d}y + \int_{y_0}^\infty y_0\iota(y) e^{-\frac{my}{\Omega\eta_{S,i}}} \mathrm{d}y\right) = \frac{my_0}{\Omega\eta_{S,i}^2} \int_0^\infty \iota(y) e^{-\frac{my}{\Omega\eta_{S,i}}} \mathrm{d}y = \frac{my_0 I(\eta_{S,i})}{\Omega\eta_{S,i}^2} \quad (14)$$

From (14), we have $I(\eta_{S,i}) \leq 0 \Rightarrow I'(\tilde{\eta}_{S,i}) < 0$. Therefore, if $\exists \tilde{\eta}_{S,i} \geq 0$ s.t. $I(\tilde{\eta}_{S,i}) \leq 0$, then $I(\eta_{S,i}) < 0\ \forall\ \eta_{S,i} > \tilde{\eta}_{S,i}$. Further, from (13), $\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) \leq 0 \Leftrightarrow I(\eta_{S,i}) \leq 0$.

$$\therefore \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})(\tilde{\eta}_{S,i}) \leq 0$$
$$\Rightarrow I(\tilde{\eta}_{S,i}) \leq 0 \Rightarrow I(\eta_{S,i}) < 0\ \forall\ \eta_{S,i} > \tilde{\eta}_{S,i}$$
$$\Rightarrow \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) < 0\ \forall\ \eta_{S,i} > \tilde{\eta}_{S,i}.$$

Therefore, $\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})$ satisfies condition **P2**.

Since $P_{S,i} = \eta_{S,i}W$, the probability of false detection in a band, as a function of the spoofing power allocated for that band under slow fading, is given by $p_{fd,s}(P_{S,i}) = \Pr\left(Y(t) > K\sqrt{T_0W}|\frac{P_{S,i}}{W}\right)$. Since $\Pr\left(Y(t) > K\sqrt{T_0W}|\eta_{S,i}\right)$ satisfies the conditions **P0**, **P1** and **P2**, $p_{fd,s}(P_{S,i})$ also satisfies **P0**, **P1** and **P2**.

VI. Results

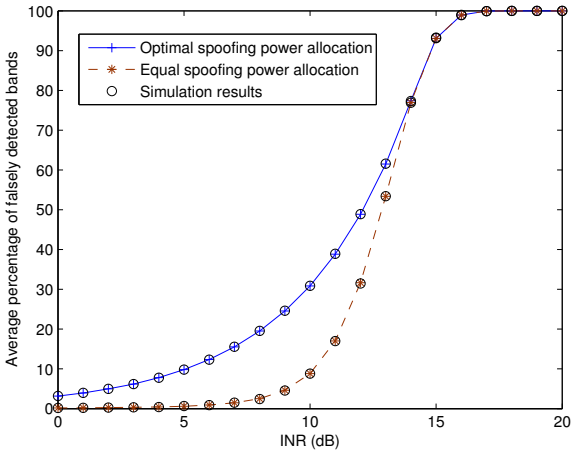
We consider a multi-carrier system with $N_T = 100$ bands, $m = 4$, $\Omega = 1$, $T_0W = 256$, and the false alarm probability $p_{fd,f}(0) = 0.001$. We derive the optimal spoofing power allocation using (3). The average number of falsely detected bands as a percentage of the number of allowed bands under the optimal spoofing power allocation is evaluated using (4) and (11), and verified through Monte Carlo simulations. The performance under equal power allocation without optimization is also presented for comparison. We define the interference-to-noise power ratio (INR) as the ratio of adversary-spoofing-power to background-noise-power-per-band.

Figure 2(a) shows the average percentage of falsely detected bands per sensing interval versus the INR under fast fading. The optimal spoofing power allocation increases the average percentage of false detections by more than 11 in INR $\in [6, 12]$ dB region, compared to equal spoofing power allocation across bands without optimization. As INR is further increased, the optimal spoofing power allocation strategy shifts from partial band spoofing to full band spoofing, and hence the curves overlap at high INR.

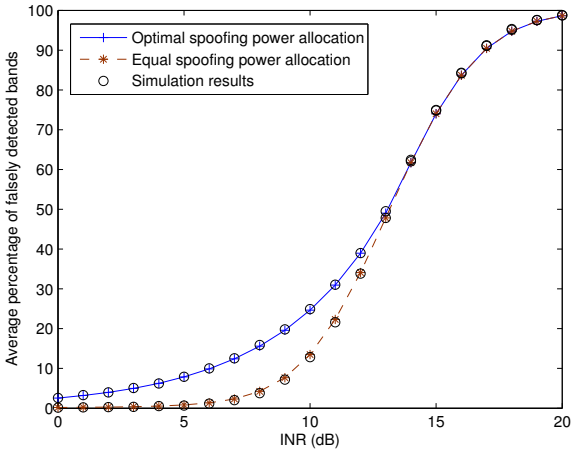
Figure 2(b) shows the average percentage of false detections due to spoofing, under slow fading. At an INR of 8 dB, the optimal spoofing power allocation causes 15.88% false detections on average, while the equal power allocation produces only 3.77%. For INR > 14dB, the optimal spoofing strategy is equal power allocation across all bands, as can be seen from figure 2(b).

VII. Conclusion

In this paper, we analyze the optimal spoofing power allocations across subcarriers, in a Nakagami-m fading channel, with an optimization approach which enables simplified calculation of threshold adversary power, below which partial-band attacks are optimal. Through comparisons of the average number of false detections with optimal spoofing power allocation with that for equal power spoofing, we observe that the optimization has notable gains in the low and medium INR regions.



(a)



(b)

Fig. 2: Average number of false detections ($p_{fd,f}(0) = 0.001$, $T_0W = 256$, $N_T = 100$, $m = 4$, $\Omega = 1$): (a) under fast fading (b) under slow fading.

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 analysis and assessment," in *International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Aug. 2007, pp. 456 –464.

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

[4] ——, "Analysis and simulation of sensing deception in fading cognitive radio networks," in *International Conference on Wireless Communications Networking and Mobile Computing*, Sep. 2010, pp. 1 –4.

[5] ——, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 903 –911, Apr. 2011.

[6] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008, pp. 1 –6.

[7] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part I: Known channel statistics," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3566 – 3577, Nov. 2010.

[8] ——, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274 –283, Jan. 2011.

[9] Z. Jin, S. Anand, and K. Subbalakshmi, "Impact of primary user emulation attacks on dynamic spectrum access networks," *IEEE Trans. Commun.*, vol. 60, no. 9, pp. 2635 –2643, Sep. 2012.

[10] C. Zhang, R. Yu, and Y. Zhang, "Performance analysis of primary user emulation attack in cognitive radio networks," in *International Wireless Communications and Mobile Computing Conference*, Aug. 2012, pp. 371 –376.

[11] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*, ser. Wiley series in telecommunications and signal processing. Hoboken, N.J. Wiley-Interscience, 2005.

[12] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, April.

[13] M. Soysa, P. Cosman, and L. Milstein, "Spoofing and jamming optimization over Rayleigh fading channels of a cognitive radio adversary," *submitted to IEEE Trans. Commun.*