Title

Optimized Spoofing and Jamming a Cognitive Radio

Permalink

https://escholarship.org/uc/item/9nf8t892

Journal

IEEE Transactions on Communications, 62(8)

ISSN

0090-6778

Authors

Soysa, Madushanka
Cosman, Pamela C
Milstein, Laurence B

Publication Date

2014

DOI

10.1109/tcomm.2014.2331964

Peer reviewed

Optimized Spoofing and Jamming a Cognitive Radio

Madushanka Soysa, *Student Member, IEEE*, Pamela C. Cosman, *Fellow, IEEE*, and
Laurence B. Milstein, *Fellow, IEEE*

***Abstract*—We examine the performance of a cognitive radio system in a hostile environment where an intelligent adversary tries to disrupt communications by minimizing the system throughput. We investigate the optimal strategy for spoofing and jamming a cognitive radio network with a Gaussian noise signal over a Rayleigh fading channel. We analyze a cluster-based network of secondary users (SUs). The adversary may attack during the sensing interval to limit access for SUs by transmitting a spoofing signal. By jamming the network during the transmission interval, the adversary may reduce the rate of successful transmission. We present how the adversary can optimally allocate power across subcarriers during sensing and transmission intervals with knowledge of the system, using a simple optimization approach specific to this problem. We determine a worst-case optimal energy allocation for spoofing and jamming, which gives a lower bound to the overall information throughput of SUs under attack.**

***Index Terms*—Cognitive radio, intelligent adversary, partial-band jamming, 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], which allows dynamic spectrum access, 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 an unlicensed SU senses a licensed 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. An adversary intending to disrupt the communication in a CR network has two ways to attack. The first way is to exploit the inherent vulnerability of spectrum sensing, 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]. Further, the adversary can disrupt communications using jamming techniques during the data transmission phase [11]. Jamming in a cognitive radio network dynamically, using stochastic game models, was studied in [12], [13].

In this work, we analyze the impact of an intelligent adversary on a tactical, spread spectrum, CR system. In [3], the presence of such an intelligent adversary disrupting the sensing by spoofing with a noise signal 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 [5], the design of an adversary with optimal power allocation for spoofing and jamming under an AWGN channel was investigated. In this work, we extend the analysis to a Rayleigh fading channel, and include forward error correction (FEC) coding, which reduces the effectiveness of jamming. Assuming knowledge of the SU system at the adversary, we determine a worst-case optimal energy allocation for spoofing and jamming. We further propose an optimization method specific to this problem, to find the optimal power allocation over subcarriers to minimize throughput. This enables us to perform the optimization when a closed form expression for the objective function is not available. In [12] and [13], jamming attacks are analyzed as a dynamic game, where the users and the adversary use the probability of successful jamming as a predetermined parameter. In the jamming section of this work, we analyze the probability of successful jamming by the adversary, and optimize the adversary power allocation to maximize the average probability of successful jamming.

In Section II, we present the system model, and derive the performance metrics as functions of spoofing or jamming powers under fast and slow Rayleigh fading. Sections III and IV discuss the spoofing and jamming optimization, respectively, where we prove that the performance metric functions derived in Section II have the required properties that enable the optimization method in Appendix A to be used, in almost all cases. In Section V, we discuss the optimal energy allocation between spoofing and jamming. Section VI contains system simulation results and Section VII presents the conclusions.

II. System Model

We investigate the impact of an adversary on a cluster based SU network, as shown in Fig. 1. We denote the cluster head serving the SUs by CH_S, and A is the adversary. We consider the downlinks from the cluster head to the users of a multi-carrier direct sequence code division multiple access (MC-DS-CDMA) system with N_T bands (or subcarriers). The

Manuscript received May 30, 2013; revised March 20, 2014 and June 2, 2014; accepted June 10, 2014. Date of publication June 19, 2014; date of current version August 20, 2014. This work was supported in part by the Office of Naval Research under Grant N00014-11-1-0733, by the Army Research Office under Grant W9111NF-12-1-0510, and by the National Science Foundation under Grant CCF-1160832. The associate editor coordinating the review of this paper and approving it for publication was Y. J. Zhang.

The authors are with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA 92093-0407 USA (e-mail: msoysa@ucsd.edu; pcosman@ucsd.edu; lmilstein@ucsd.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2014.2331964

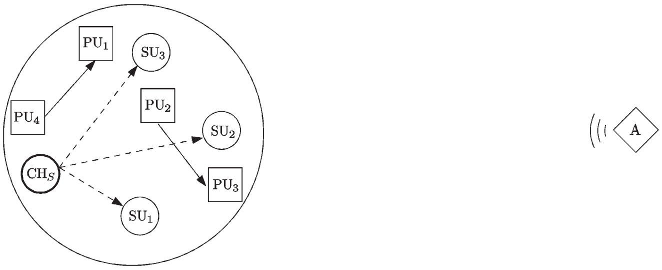


Fig. 1. The system network model.

N_T bands are shared among PUs and SUs. *Allowed bands* are ones unoccupied by PUs. The CH$_S$ periodically performs spectrum sensing, and uses a subset of allowed bands to transmit data to the SUs. *Busy bands* are bands that the SU network cannot use due to PU activity. An allowed band may appear busy due to background noise and spoofing. This is called a *false detection*. We ignore the effects of missed detections in this analysis, as the adversary cannot do anything to increase the probability of missed detections. The probability of missed detections can only decrease with spoofing, which will not disrupt the communications. The cluster head uses power control to maintain constant average link signal-to-noise ratio (SNR) for all SUs. We denote the length of the sensing interval by T_0 and the length of the data transmission interval by T_1.

Let $B = \{1, 2, \ldots, N_T\}$ be the set of bands, and $B_{su} \subseteq B$ be the subset of bands used by the SU network for communication in one transmission interval. The throughput (Γ) of the SU network during the data transmission interval is given by

$$\Gamma = \sum_{i \in B_{su}} \sum_{u=1}^{\Omega_i} L_P \left(1 - p_e^{(i,u)}\right) \log_2 M_{i,u} \tag{1}$$

where Ω_i is the number of SUs in the i-th band, L_P is the packet length in symbols, $p_e^{(i,u)}$ is the probability of packet error of the u-th user in the i-th band, and $\log_2 M_{i,u}$ is the number of bits per symbol in the alphabet used by the u-th user in the i-th band. The SUs use a single 4-QAM alphabet for fast fading, and may use either a single alphabet or adaptive modulation at slow fading. The adversary uses a Gaussian noise signal to attack by spoofing or jamming. Spoofing reduces $|B_{su}|$, and jamming increases $p_e^{(i,u)}$ in (1), thus reducing Γ.

In Section II-A, we discuss the portion of the system involved in sensing, and derive expressions for the probability of false detection. The transmission and receiver structures of SUs, i.e., the portion of the system involved in the transmission interval, are presented in Section II-B, with the derivation of the expressions for the packet error rate. The assumptions regarding the knowledge available for the adversary are detailed in Section II-C.

A. Sensing Subsystem

The CH$_S$ uses an energy detector for sensing (Fig. 2). Let W be the bandwidth of one subcarrier. 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 CHCH$_S$, $n_s(t)$ 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 $\eta_s/2$ in the band, $n_0(t)$ is Gaussian with PSD $N_0/2$ in the band, and $\alpha_J(t)$ is exponentially distributed with mean $\bar{\alpha}_J$. The integrand can be expressed as

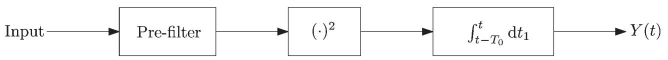


Fig. 2. Energy detector block diagram.

$$\sqrt{\alpha_J(t)} n_s(t) + n_0(t) = \left(\sqrt{\alpha_J(t)} n_{s,i}(t) + n_{0,i}(t)\right) \cos \omega_c t - \left(\sqrt{\alpha_J(t)} n_{s,q}(t) + n_{0,q}(t)\right) \sin \omega_c t$$

where ω_c is the subcarrier frequency, $n_{s,i}(t)$, $n_{s,q}(t)$ are Gaussian with PSD η_s in the frequency range $(-(W/2), W/2)$, and $n_{0,i}(t)$, $n_{0,q}(t)$ are Gaussian with PSD N_0 in the frequency range $(-(W/2), W/2)$.

From [14], we have

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

where $a_{i,k} = \sqrt{\alpha_J(t - T_0 + (k/W))} n_{s,i}(t - T_0 + (k/W)) + n_{0,i}(t - T_0 + (k/W))$ and $a_{q,k} = \sqrt{\alpha_J(t - T_0 + (k/W))} n_{s,q}(t - T_0 + (k/W)) + n_{0,q}(t - T_0 + (k/W))$.

1) Fast Fading: Under fast fading, 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 have $E[a_{i,k}^2] = \bar{\alpha}_J \eta_s W + N_0 W$, $E[a_{i,k}^4] = 6\bar{\alpha}_J^2 \eta_s^2 W^2 + 6\bar{\alpha}_J \eta_s N_0 W^2 + 3N_0^2 W^2$ and $\mathrm{Var}(a_{i,k}^2) = E[a_{i,k}^4] - E[a_{i,k}^2]^2 = 5\bar{\alpha}_J^2 \eta_s^2 W^2 + 4\bar{\alpha}_J \eta_s N_0 W^2 + 2N_0^2 W^2$. Following the same approach, we can show $E[a_{i,k}^2 + a_{q,k}^2] = 2(\bar{\alpha}_J \eta_s W + N_0 W)$ and $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2) = 2(5\bar{\alpha}_J^2 \eta_s^2 W^2 + 4\bar{\alpha}_J \eta_s N_0 W^2 + 2N_0^2 W^2)$. Since $\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2)$ is finite, we can use the Lindeberg-Lévy CLT to approximate $Y(t)$ in (2). Therefore, for large $T_0 W$, $Y(t) \sim \mathcal{N}(T_0 W(\bar{\alpha}_J \eta_s + N_0), T_0 W(5\bar{\alpha}_J^2 \eta_s^2 + 4\bar{\alpha}_J \eta_s N_0 + 2N_0^2)/2)$. A band is detected as occupied by PUs if the energy detector output is greater than the threshold $K\sqrt{T_0 W}$. 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,

$$p_{fd,f}(P_{S,i}) = \Pr\left(Y(t) > K\sqrt{T_0 W}\right) = Q\left(\frac{K\sqrt{T_0 W} - T_0 W\left(\bar{\alpha}_J (P_{S,i}/W) + N_0\right)}{\sqrt{T_0 W\left(5\bar{\alpha}_J^2 (P_{S,i}/W)^2 + 4\bar{\alpha}_J (P_{S,i}/W) N_0 + 2N_0^2\right)/2}}\right). \tag{3}$$

2) Slow Fading: Under slow fading, 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, $a_{i,k} = \sqrt{\alpha_J} n_{s,i}(t - T_0 + (k/W)) + n_{0,i}(t - T_0 + (k/W)) \sim \mathcal{N}(0, \alpha_J \eta_s W + \eta_0 W)$, and similarly, $a_{q,k} \sim \mathcal{N}(0, \alpha_J \eta_s W + \eta_0 W)$. Therefore, $E[a_{i,k}^2 + a_{q,k}^2 | \alpha_J] = 2(\alpha_J \eta_s W + \eta_0 W)$ and

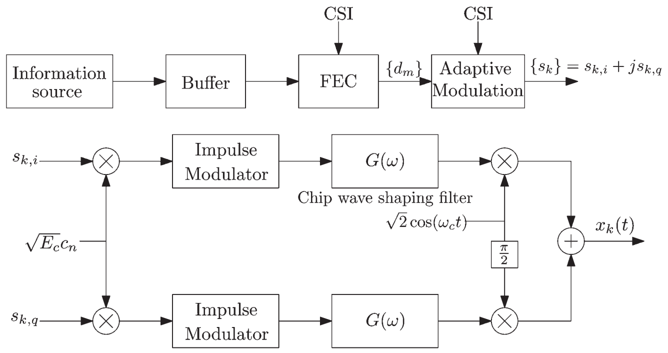


Fig. 3. Transmitter block diagram of a single subcarrier of MC-DS CDMA.

$\mathrm{Var}(a_{i,k}^2 + a_{q,k}^2|\alpha_J) = 4(\alpha_J\eta_s W + \eta_0 W)$. Using these results in (2), for large T_0W, we conclude, when conditioned on α_J, $Y(t) \sim \mathcal{N}(T_0W(\alpha_J\eta_s + \eta_0), T_0W(\alpha_J\eta_s + \eta_0)^2)$.

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

$$\begin{aligned}\Pr&\left(Y(t) > K\sqrt{T_0W}|\eta_{S,i}\right)\\ &= \int_0^\infty \Pr\left(Y(t) > K\sqrt{T_0W}|\alpha_J = y, \eta_{S,i}\right) f_{\alpha_J}(y)\,\mathrm{d}y \quad (4)\end{aligned}$$

where $f_{\alpha_J}(y)$ is the probability density function of the channel gain α_J. Since the channel has Rayleigh fading, $f_{\alpha_J}(y) = (1/\bar{\alpha}_J)e^{-(y/\bar{\alpha}_J)}$. Substituting this in (4) yields

$$\begin{aligned}\Pr&(Y(t) > K\sqrt{T_0W}|\eta_{S,i})\\ &= \frac{1}{\bar{\alpha}_J}\int_0^\infty Q\left(\frac{K}{\eta_{S,i}y + \eta_0} - \sqrt{T_0W}\right)e^{-\frac{y}{\bar{\alpha}_J}}\,\mathrm{d}y. \quad (5)\end{aligned}$$

Note that $P_{S,i} = \eta_{S,i}W$. Hence, the probability of false detection in a band, as a function of the spoofing power allocated for that band under slow fading can be obtained substituting $\eta_{S,i} = P_{S,i}/W$ in (5), is given by

$$p_{fd,s}(P_{S,i}) = \frac{1}{\bar{\alpha}_J}\int_0^\infty Q\left(\frac{K}{\frac{P_{S,i}}{W}y + \eta_0} - \sqrt{T_0W}\right)e^{-\frac{y}{\bar{\alpha}_J}}\,\mathrm{d}y. \quad (6)$$

B. Transceiver Subsystem

The transmitter model is adapted from [5]. A block diagram of the transmitter for a single user is given in Fig. 3. Low density parity check (LDPC) codes are used for FEC. The output bit sequence of the FEC block of the u-th user is denoted by $d_m^{(u)}$. This binary sequence is mapped to a symbol sequence $s_k^{(u)}$ from an alphabet a_i, based on the predicted instantaneous CSI. Note that $s_k^{(l)}$ is generally complex valued, and normalized to have unit average energy, i.e., $E[|s_k|^2] = 1$. The $\{c_n^{(u)}\}$ are the chips of a pseudo-random spreading sequence, and there are N_c chips per symbol. The sequence $s_k^{(u)}c_n^{(u)}$ modulates an impulse train. After passing through both the chip-wave shaping filter $g(t)$ and modulator, the transmitted signal takes the form $x(t) = \Re\{\sum_{u=1}^{\Omega_u}\sqrt{2E_c^{(u)}}\sum_{n=-\infty}^{\infty}s_k^{(u)}c_n^{(u)}g(t - nT_c)e^{j\omega_c t + \phi_u}\}$, where $E_c^{(u)}$ is the energy per chip, T_c is the chip duration, Ω_u is the number of users sharing the band, ϕ_u is the carrier phase of the u-th user, $k = \lfloor n/N_c \rfloor$ and $g(t)$ is a root raised cosine chip-wave shaping filter, such that

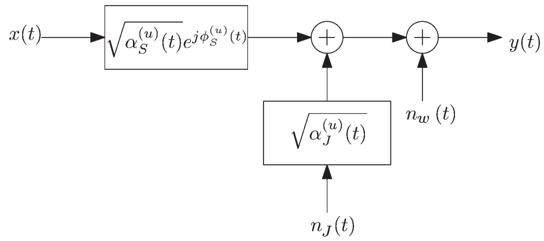

$x(t)$
$\sqrt{\alpha_S^{(u)}(t)}e^{j\phi_S^{(u)}(t)}$
$y(t)$
$\sqrt{\alpha_J^{(u)}(t)}$
$n_w(t)$
$n_J(t)$

Fig. 4. Channel response and jamming.

$$\begin{aligned}&G(\omega)G^*(\omega)\\ &= \begin{cases} T_c, & \text{if } |\omega| \le \frac{1-\beta}{2T_c}\\ \frac{T_c}{2}\left(1 + \cos\left(\frac{\pi T_c}{\beta}\left(|\omega| - \frac{1-\beta}{2T_c}\right)\right)\right), & \text{if } \frac{1-\beta}{2T_c} < |\omega| \le \frac{1+\beta}{2T_c}\\ 0, & \text{elsewhere}\end{cases} \quad (7)\end{aligned}$$

where $G(\omega)$ is the Fourier transform of $g(t)$ and β is the roll-off factor.

Fig. 4 shows the channel fading and jamming experienced by the l-th user in one subcarrier. The transmitted signal $x(t)$ is attenuated by Rayleigh fading, and corrupted by AWGN and jamming. The jamming signal undergoes Rayleigh fading, independent of the source-user channel.

The received signal of the u-th user $(y^{(u)}(t))$ is given by

$$\begin{aligned}y^{(u)}(t) = \Re\Bigg\{&\sqrt{2E_c^{(u)}\alpha_S^{(u)}(t)}e^{j\phi_S^{(u)}(t)}\sum_{u=1}^{\Omega_u}\sum_{n=-\infty}^{\infty}s_k^{(u)}c_n^{(u)}\\ &\times g(t - nT_c)e^{j\omega_c t + \phi_u} + n_w(t) + \sqrt{\alpha_J^{(u)}(t)}n_J(t)\Bigg\}\end{aligned}$$

where $\alpha_S^{(u)}(t)$ and $\phi_S^{(u)}(t)$ are the power gain and phase components of the response of the channel from the source to the u-th user. The power gain of the jammer to user channel is $\alpha_J^{(u)}(t)$. We assume the channel gains $\alpha_S^{(u)}(t)$ and $\alpha_J^{(u)}(t)$ are mutually independent. The background noise $n_w(t)$ is AWGN with a double-sided PSD $N_0/2$ and $\sqrt{\alpha_J^{(u)}(t)n_J(t)}$ is the received jamming signal. The receiver block diagram is given in Fig. 5. We assume the gains and phases of fading channels remain constant during a symbol detection. We denote the gain and phase components of the response of the channel from the source to the u-th user during k-th symbol detection by $\alpha_{S,k}^{(u)}$ and $\phi_{S,k}^{(u)}$, respectively. The gain of the jammer to user channel is denoted by $\alpha_{J,k}^{(u)}$. The complex output samples are given by

$$\begin{aligned}r_k^{(u)} &\triangleq r_{k,i}^{(u)} + r_{k,q}^{(u)}\\ &= \sqrt{E_S^{(u)}\alpha_{S,k}^{(u)}}s_k^{(u)} + \sqrt{\alpha_{J,k}^{(u)}}n_{J,k} + n_{w,k} + I_k \quad (8)\end{aligned}$$

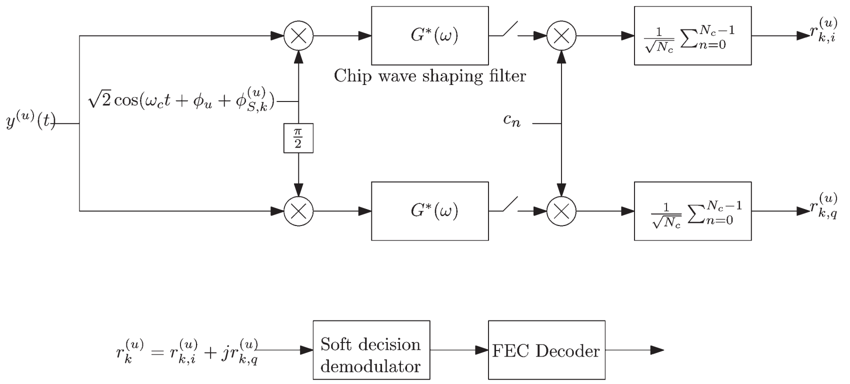

$y^{(u)}(t)$
$\sqrt{2}\cos(\omega_c t + \phi_u + \phi_{S,k}^{(u)})$
$\frac{\pi}{2}$
$G^*(\omega)$
Chip wave shaping filter
$G^*(\omega)$
c_n
$\frac{1}{\sqrt{N_c}}\sum_{n=0}^{N_c-1}$
$r_{k,i}^{(u)}$
$\frac{1}{\sqrt{N_c}}\sum_{n=0}^{N_c-1}$
$r_{k,q}^{(u)}$
$r_k^{(u)} = r_{k,i}^{(u)} + jr_{k,q}^{(u)}$
Soft decision demodulator
FEC Decoder

Fig. 5. u-th user receiver block diagram.

where $E_S^{(u)} = E_c^{(u)} N_c$, is the symbol energy, $n_{J,k}$ is the jamming signal, $n_{w,k}$ is the background noise and I_k is the interference from other users occupying the same band. Further, $n_{J,k} \sim \mathcal{CN}(0, \eta_J)$ and $n_{w,k} \sim \mathcal{CN}(0, N_0)$, where k is the time index and $\eta_J/2$ is the double sided PSD of the jamming signal. We assume the users in the downlink are synchronized at the transmitter, and hence the multiple access interference can be removed by using mutually orthogonal spreading codes (e.g., Walsh-Hadamard codes). The received instantaneous signal-to-interference-plus-noise ratio (SINR) at the k-th symbol detection can be written as

$$\gamma_k = \frac{E_S^{(u)} \alpha_{S,k}^{(u)}}{\eta_J \alpha_{J,k}^{(u)} + N_0} = \frac{\alpha_{S,k}^{(u)} \frac{E_S^{(u)}}{N_0}}{\alpha_{J,k}^{(u)} \frac{\eta_J}{N_0} + 1} = \frac{\frac{\alpha_{S,k}^{(u)}}{\bar{\alpha}_S^{(u)}} \bar{\gamma}_S}{\frac{\alpha_{J,k}^{(u)}}{\bar{\alpha}_J} \bar{\gamma}_J + 1} \quad (9)$$

where $\gamma_{S,k}^{(u)} \triangleq \alpha_{S,k}^{(u)}(E_S^{(u)}/N_0)$ and $\gamma_{J,k}^{(u)} \triangleq \alpha_{J,k}^{(u)}(\eta_J/N_0)$. $\bar{\gamma}_S = \mathrm{E}[\gamma_{S,k}] = ((\bar{\alpha}_S^{(u)} E_S^{(u)})/N_0)$ and $\bar{\gamma}_J = \bar{\alpha}_J \eta_J/N_0$, where $\bar{\alpha}_S^{(u)} = \mathrm{E}[\alpha_{S,k}^{(u)}]$ and $\bar{\alpha}_J = \mathrm{E}[\alpha_{J,k}^{(u)}]$. We define $\tilde{\alpha}_{S,k} \triangleq (\alpha_{S,k}^{(u)}/\bar{\alpha}_S^{(u)})$ and $\tilde{\alpha}_{J,k} \triangleq (\alpha_{J,k}^{(u)}/\bar{\alpha}_J)$ to simplify the analysis, so that

$$\gamma_k = \frac{\tilde{\alpha}_{S,k} \bar{\gamma}_S}{\tilde{\alpha}_{J,k} \bar{\gamma}_J + 1} \quad (10)$$

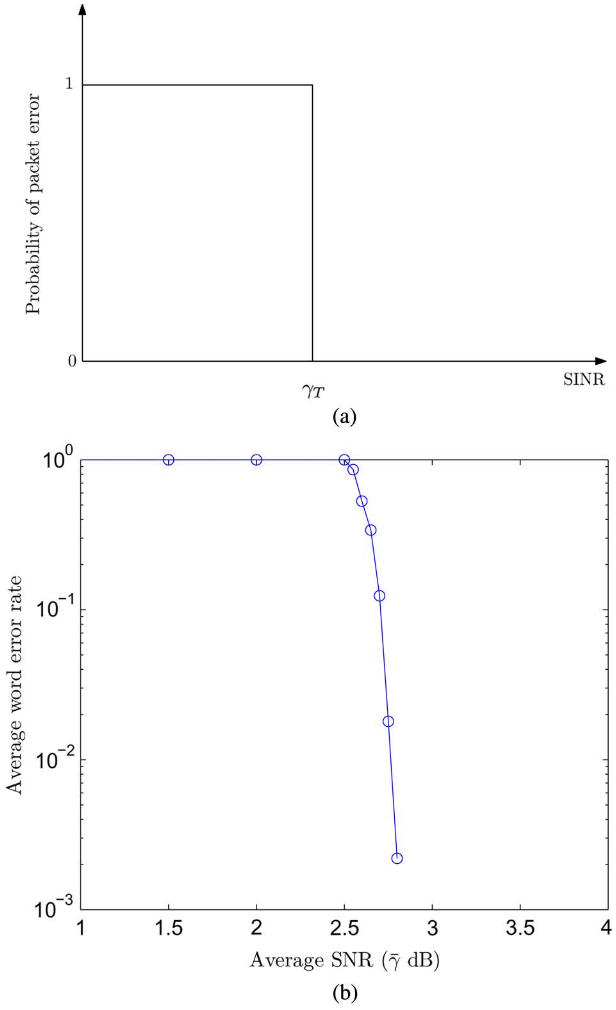
and $\tilde{\alpha}_{S,k}$, $\tilde{\alpha}_{J,k} \sim \mathrm{Exp}(1)$. Since $P_{J,i}$ is the jamming power allocated for the subcarrier, we know $P_{J,i} = \eta_J W$, so that

$$\bar{\gamma}_J = \frac{\bar{\alpha}_J P_{J,i}}{N_0 W}. \quad (11)$$

1) Fast Fading: Under fast fading, we assume the channel coherence time is significantly lower than the transmission duration of one codeword, T_1. The adversary models the probability of packet error as a step function of the received average SINR over a word, as shown in Fig. 6(a). Therefore,

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \tilde{\gamma} > \gamma_T \\ 1, & \text{if } \tilde{\gamma} \leq \gamma_T \end{cases} \quad (12)$$

where $\tilde{\gamma}$ is the SINR at the receiver averaged over the duration of the word, and γ_T is a threshold parameter dependent on the alphabet and the FEC used. Note that γ_T is determined through simulations, and in Fig. 6(b), the simulation results of the word error rate of the DVB-S2 rate 1/2 LDPC code with 4-QAM modulation under Rayleigh fading are presented.



(a)

(b)

Fig. 6. (a) Step function approximation for the probability of packet error r_e. (b) Average probability of word error of DVB-S2 LDPC code of rate 1/2 using 4-QAM vs. average SNR.

In fast fading, as the channel coherence time is significantly smaller than the duration of a codeword, we approximate the average SINR over a codeword with the ensemble average over the channel gains $\tilde{\alpha}_{S,k}$ and $\tilde{\alpha}_{J,k}$. The average SINR over a word in this case can be calculated as follows:

$$\tilde{\gamma}(\bar{\gamma}_{J,i}) = \int_0^\infty \int_0^\infty \frac{x\bar{\gamma}_S}{y\bar{\gamma}_{J,i}+1} e^{-x}e^{-y}\,\mathrm{d}x\,\mathrm{d}y \tag{13}$$

$$= -\frac{\bar{\gamma}_S e^{\frac{1}{\bar{\gamma}_{J,i}}}}{\bar{\gamma}_{J,i}} \mathrm{Ei}\left(-\frac{1}{\bar{\gamma}_{J,i}}\right) \quad [15,\ \text{Eq. } 4.2.6] \tag{14}$$

where $\mathrm{Ei}(x) = -\int_{-x}^{\infty}(e^{-t}/t)\,\mathrm{d}t$ is the exponential integral function [16, Eq. 5.1.2].

Lemma 1: $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is a monotonically decreasing function of $\bar{\gamma}_{J,i}$, and the range of $\tilde{\gamma}$ is $(0, \bar{\gamma}_S]$.

Proof in Appendix D.

From Lemma A1 in Appendix A, we know a unique $\bar{\gamma}_J^*$ exists $\forall\ \gamma_T \in (0, \bar{\gamma}_S]$, such that $\tilde{\gamma}(\bar{\gamma}_J^*) = \gamma_T$, and $\bar{\gamma}_{J,i} < \bar{\gamma}_J^* \Leftrightarrow \tilde{\gamma} > \gamma_T$. Using (11), we define $P_J^* \triangleq ((N_0 W \bar{\gamma}_J^*)/\bar{\alpha}_J)$. Since the jamming power in the band $P_{J,i} \propto \bar{\gamma}_{J,i}$, $P_{J,i} < P_J^* \Leftrightarrow \bar{\gamma}_{J,i} < \bar{\gamma}_J^* \Leftrightarrow \tilde{\gamma} > \gamma_T$. Using this result and (12), we can write the packet error rate as a function of jamming power under fast fading, $r_{e,f}(P_{J,i})$, as

$$r_{e,f}(P_{J,i}) = \begin{cases} 0, & \text{if } P_{J,i} < P_J^* \\ \log_2 M, & \text{if } P_{J,i} \geq P_J^* \end{cases} \tag{15}$$

where $\log_2 M$ is the number of bits per symbol.

2) Slow Fading: In slow fading, we assume the coherence time is larger than T_1. Therefore, the channel gains $\tilde{\alpha}_{S,k}$ and $\tilde{\alpha}_{J,k}$, and instantaneous SINR, γ_k, remain constant over a word. The adversary again models the probability of word error with a step function of the SINR.

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \gamma_k > \gamma_T \\ 1, & \text{if } \gamma_k \leq \gamma_T \end{cases} \tag{16}$$

where γ_k is the instantaneous SINR at the receiver, and γ_T is a threshold parameter dependent on the alphabet and the FEC used. Through simulations of word error rates of an ensemble of LDPC rate 1/2 codes of code length L_p, γ_T is estimated. Therefore, from (12), the probability of packet error in a band jammed with power $P_{J,i}$, as a function of $\bar{\gamma}_{J,i} = (\bar{\alpha}_J P_{J,i}/N_0 W)$ is given by

$$\Pr(\text{packet error}|\bar{\gamma}_{J,i}) = \Pr\left(\frac{\tilde{\alpha}_{S,i}\bar{\gamma}_S}{\tilde{\alpha}_{J,i}\bar{\gamma}_{J,i}+1} < \gamma_T\right)$$

$$= \int_0^\infty \int_0^{\frac{(y\bar{\gamma}_{J,i}+1)\gamma_T}{\bar{\gamma}_S}} f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y)\,\mathrm{d}x\,\mathrm{d}y$$

$$= \int_0^\infty \int_0^{\frac{(y\bar{\gamma}_{J,i}+1)\gamma_T}{\bar{\gamma}_S}} e^{-x}e^{-y}\,\mathrm{d}x\,\mathrm{d}y$$

$$= 1 - \frac{e^{\frac{-\gamma_T}{\bar{\gamma}_S}}}{\left(\frac{\bar{\gamma}_{J,i}\gamma_T}{\bar{\gamma}_S}+1\right)}. \tag{17}$$

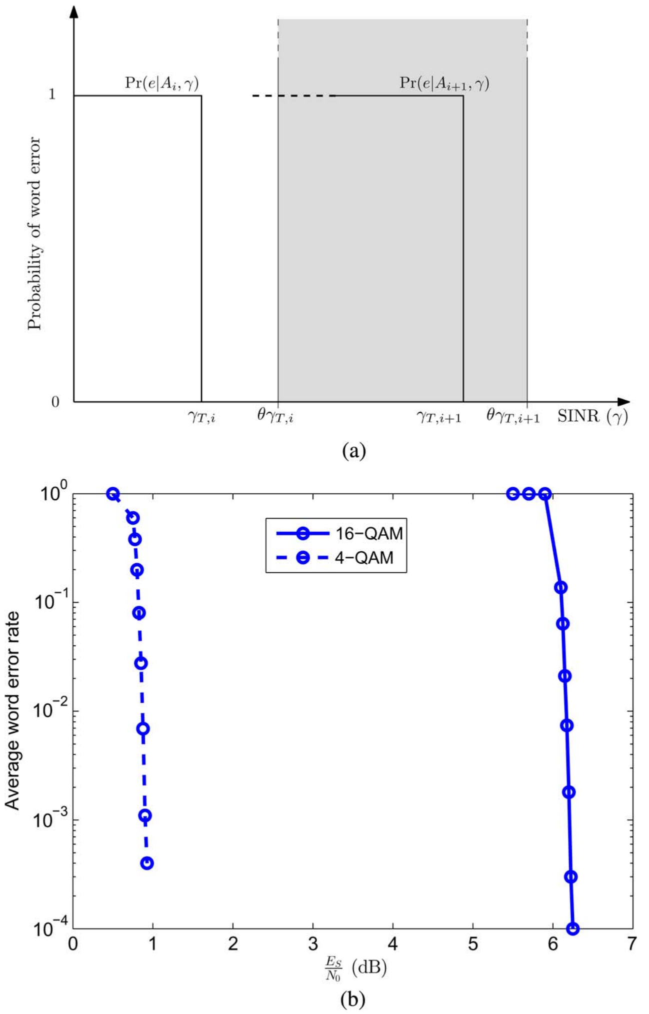


Fig. 7. (a) The probability of word error given an alphabet a_i ($\Pr(e|A_i)$). The shaded area represents the region of SNR in which the alphabet a_i is used. (b) Average word error rate of DVB-S2 LDPC code of rate 1/2 for alphabets 4-QAM and 16-QAM vs. SNR.

The packet error rate per user per band, $r_{e,s,1}(P_{J,i})$ under slow fading for a single alphabet size, as a function of the jamming power allocated to the band $P_{J,i}$ is given by

$$r_{e,s,1}(P_{J,i}) = \Pr\left(\text{packet error}\,\middle|\,\frac{\bar{\alpha}_J P_{J,i}}{N_0 W}\right)\log_2 M. \tag{18}$$

3) Slow Fading With Adaptive Modulation: If the SU network is experiencing slow fading due to low mobility, the system may use an adaptive modulation scheme to improve the system throughput. Here, we analyze the jamming optimization in an adaptive modulation system under slow fading. We assume the SU network has a choice of N_A alphabets, which is known to the adversary.

Let a_i denote the i-th alphabet and A_i denote the event that a_i is used for transmission. The probability of a received word being in error for a given alphabet a_i ($\Pr(e|A_i)$), is a step function of the instantaneous SINR (γ_k, Eq. (10)).

$$\Pr(e|A_i,\gamma_k) = \begin{cases} 0, & \text{if } \gamma_k > \gamma_{T,i} \\ 1, & \text{if } \gamma_k \leq \gamma_{T,i}. \end{cases} \tag{19}$$

As shown in Fig. 7(a), the alphabet (a_i) is used if the SNR $(\gamma_{S,k}) \in (\theta\gamma_{T,i}, \theta\gamma_{T,i+1})$. Fig. 7(b) shows the word error rate of the DVB-S2 rate 1/2 LDPC code for alphabets 4-QAM and 16-QAM in an AWGN channel. Consider the probability a word is received in error, when the alphabet a_i is selected $(\Pr(e \cap A_i))$. Since alphabet a_i is selected when $\tilde{\alpha}_{S,k} \in (\theta\gamma_{T,i}/\bar{\gamma}_S, \theta\gamma_{T,i+1}/\bar{\gamma}_S)$, we have

$$\Pr(A_i|\tilde{\alpha}_{S,k}) = \begin{cases} 1, & \text{if } \tilde{\alpha}_{S,k} \in \left(\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}, \frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}\right) \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

A word is received in error when $(\tilde{\alpha}_{S,k}\bar{\gamma}_S)/(\tilde{\alpha}_{J,k}\bar{\gamma}_J + 1) < \gamma_{T,i}$, so that

$$\begin{aligned}
&\Pr(e \cap A_i) \\
&= \int_0^\infty \int_0^\infty \Pr(e \cap A_i|\tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y) \\
&\quad \times f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y)\, \mathrm{d}x\, \mathrm{d}y \\
&= \int_0^{\frac{\theta-1}{\bar{\gamma}_J}} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \\
&\quad \times \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J + 1} < \gamma_{T,i}|\tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) \mathrm{d}x\, \mathrm{d}y \\
&\quad + \int_{\frac{\theta-1}{\bar{\gamma}_J}}^{\left(\frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \\
&\quad \times \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J + 1} < \gamma_{T,i}|\tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) \mathrm{d}x\, \mathrm{d}y \\
&\quad + \int_{\left(\frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)}^{\infty} \int_{\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S}}^{\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S}} f_{\tilde{\alpha}_{S,k}}(x) f_{\tilde{\alpha}_{J,k}}(y) \\
&\quad \times \Pr\left(\frac{x\bar{\gamma}_S}{y\bar{\gamma}_J + 1} < \gamma_{T,i}|\tilde{\alpha}_{S,k} = x, \tilde{\alpha}_{J,k} = y\right) \mathrm{d}x\, \mathrm{d}y \\
&= \frac{\bar{\gamma}_J\gamma_{T,i}}{\bar{\gamma}_J\gamma_{T,i} + \bar{\gamma}_S} \\
&\quad \times \left(e^{-\left(\frac{\theta\gamma_{T,i}}{\bar{\gamma}_S} + \frac{\theta-1}{\bar{\gamma}_J}\right)} - e^{-\left(\frac{\theta\gamma_{T,i+1}}{\bar{\gamma}_S} + \frac{\theta\gamma_{T,i+i}}{\gamma_{T,i}\bar{\gamma}_J} - \frac{1}{\bar{\gamma}_J}\right)}\right).
\end{aligned} \tag{21}$$

The average packet error rate per user per band, $r_{e,s,2}(P_{J,i})$ under slow fading with adaptive modulation, as a function of $P_{J,i}$ is given by

$$r_{e,s,2}(P_{J,i}) = \sum_{j=1}^{N_A} \Pr(e \cap A_j) \log_2 M_j \tag{22}$$

where $\log_2 M_i$ is the number of bits per symbol when using the alphabet a_i.

C. Adversary

The adversary uses Gaussian noise signals when it spoofs or jams. The objective of the adversary is to disrupt the communication, and we use the average throughput as the performance metric. We assume, in accordance with [3]–[5], that the adversary is aware of the basic characteristics of the system, including the receiver structure, type of spreading, bandwidth of the waveform, sensing and transmission times, background noise power spectral density (PSD), that all links undergo Rayleigh fading and whether it is slow or fast fading. We also assume that the links from the adversary to the SUs in the cluster have equal average gain in each band, which is known by the adversary.

We assume that the adversary has knowledge of the system false alarm probability, i.e., the probability of false detection caused only due to background noise with no spoofing. The adversary senses and detects the bands used for transmission before jamming, and hence knows $B_{su} \cup B_{pu}$, where $B_{pu} \subseteq \{1, 2, \ldots, N_T\}$ is the set of bands occupied by PUs. The average SNR of SUs maintained by the CH$_S$ through power control is assumed to be known by the adversary. We further assume that the adversary is aware of the type and rate of FEC, alphabet sizes and thresholds used. However, the adversary is not aware of instantaneous system parameters, such as the instantaneous CSI, the instantaneous numbers of secondary users in the i-th band (Ω_i), and which alphabet each user is using.

Because a practical adversary cannot have all the assumed knowledge, including the average channel gain, the work done here is a worst-case analysis, which gives a lower bound to the throughput with jamming and spoofing.

III. Spoofing Power Optimization

During the sensing interval, the adversary attacks the system by spoofing to reduce the bandwidth available to the SUs. Let $B_{al} \subseteq B$ be the set of allowed bands in the current sensing interval. The objective of the adversary when spoofing is to minimize the number of allowed bands accessible to SUs. 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 $p_{fd}^{(i)}$ is the probability of false detection of the i-th band, given that the i-th band is vacant.

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

$$\max \sum_{i=1}^{N_T} p_{fd}^{(i)}, \qquad \text{s.t.} \sum_{i=1}^{N_T} P_{S,i} \le P_S \tag{23}$$

where $P_{S,i}$ is the spoofing power allocated for the i-th band and P_S is the total spoofing power available.

A. Fast Fading

For fast fading, from (3), we have

$$p_{fd}^{(i)} = p_{fd,f}(P_{S,i}) \\ = Q\left(\frac{K\sqrt{T_0W} - T_0W\,(\bar{\alpha}_J(P_{S,i}/W) + N_0)}{\sqrt{T_0W(5\bar{\alpha}_J^2(P_{S,i}/W)^2 + 4\bar{\alpha}_J(P_{S,i}/W)N_0 + 2N_0^2)/2}}\right). \tag{24}$$

Therefore, the objective of the optimization in (23) is to maximize $\sum_{i=1}^{N_T} p_{fd,f}(P_{S,i})$, under the constraint $\sum_{i=1}^{N_T} P_{S,i} \le P_S$.

Proposition 1: $p_{fd,f}$ has properties **P0**, **P1**, and **P2** stated in Theorem 1 in Appendix A.

Proof in Appendix C.

Therefore, we can use Theorem 1 to solve this optimization problem.

B. Slow Fading

For slow fading, $p_{fd}^{(i)} = p_{fd,s}(P_{S,i})$, from (6).

Proposition 2: $\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})$ has properties **P0**, **P1**, and **P2** stated in Theorem 1.

Proof in Appendix C: Therefore, we can use Theorem 1 to solve this optimization problem.

IV. Jamming Power Optimization

In Section III, we analyzed the interference from the adversary during the sensing period, and discussed optimizing the adversary power allocation during the sensing period. In this section, we look at the interference from the adversary during the data transmission period, and the jamming power optimization of the adversary.

From (1), to minimize the throughput of the network by jamming, the adversary ideally aims to maximize $\sum_{i\in B_{su}} \sum_{u=1}^{\Omega_i} L_P p_e^{(i,u)} \log_2 M_{i,u}$. However, the adversary is not aware of instantaneous system parameters, such as the instantaneous CSI, the instantaneous number of secondary users in the i-th band (Ω_i), and which alphabet each user is using. Further, the adversary cannot differentiate between the bands occupied by PUs and SUs through observations during the transmission interval. Therefore, to minimize the average throughput without this information, the objective function to maximize is changed to be $\max \sum_{i\in B_{su}\cup B_{pu}} r_e(P_{J,i})$, under the constraint $\sum_{i\in B_{su}\cup B_{pu}} P_{J,i} \le P_J$, where P_J is the total power available for jamming, $P_{J,i}$ is the jamming power allocated for the i-th band, $r_e(P_{J,i})$ is the expected value of $p_e^{(i,u)} \log_2 M_{i,u}$ and the expectation is taken over the fading gains of the links from the CH$_S$ to the SUs, and the adversary to the SUs.

A. Fast Fading

Under fast fading, the objective is to maximize $\sum_{i\in B_{su}\cup B_{pu}} r_{e,f}(P_{J,i})$, under the constraint $\sum_{i\in B_{su}\cup B_{pu}} P_{J,i} \le P_J$. From (15), we have

$$r_{e,f}(P_{J,i}) = \begin{cases} 0, & \text{if } P_{J,i} < P_J^* \\ \log_2 M, & \text{if } P_{J,i} \ge P_J^*. \end{cases} \tag{25}$$

If the adversary has a total power P_J for jamming, to maximize $\sum_{i\in B_{su}\cup B_{pu}} r_{e,f}(P_{J,i})$, according to (25), the adversary aims to maximize the number of bands with $P_{J,i} \ge P_J^*$. Therefore, the optimal number of bands to jam is $n_J^* = \min(\lfloor P_J/P_J^* \rfloor, N_T)$.

Since the first and second derivatives of $r_{e,f}(P_{J,i})$ do not exist, we cannot use Theorem 1 here. Fortunately, we do not need Theorem 1, since the packet error rate as a function of jamming power $(r_{e,f}(P_{J,i}))$ is a step function, as shown in (25), so the optimal jamming strategy is trivial.

B. Slow Fading

Under slow fading with a single alphabet, the objective is to maximize $\sum_{i\in B_{su}\cup B_{pu}} r_{e,s,1}(P_{J,i})$, under the constraint $\sum_{i\in B_{su}\cup B_{pu}} P_{J,i} \le P_J$.

Proposition 3: $\Pr(\text{packet error}|\bar{\gamma}_{J,i})$ satisfies the conditions **P0**, **P0**, and **P0** of Theorem 1.

Proof:

1) **P0** is satisfied by definition.
2) $(\mathrm{d}/\mathrm{d}\bar{\gamma}_{J,i})\Pr(\text{packet error}|\bar{\gamma}_{J,i}) = (\mathrm{d}/\mathrm{d}\bar{\gamma}_{J,i})(1-(e^{-}(\gamma_T/\bar{\gamma}_S)/((\bar{\gamma}_{J,i}\gamma_T/\bar{\gamma}_S)+1) = ((\gamma_T/\bar{\gamma}_S)e^{-(\gamma_T/\bar{\gamma}_S})/((\bar{\gamma}_{J,i}\gamma_T/\bar{\gamma}_S)+1)^2) > 0$.
   $\therefore$ **P1** is satisfied.
3) $(\mathrm{d}^2/\mathrm{d}\bar{\gamma}_{J,i}^2)\Pr(\text{packet error}|\bar{\gamma}_{J,i}) = (\mathrm{d}/\mathrm{d}\bar{\gamma}_{J,i})((\gamma_T/\bar{\gamma}_S) e^{-(\gamma_T/\bar{\gamma}_S})/((\bar{\gamma}_{J,i}\gamma_T/\bar{\gamma}_S)+1)^2 = ((\gamma_T/\bar{\gamma}_S)e^{-(\gamma_T/\bar{\gamma}_S)}/((\bar{\gamma}_{J,i}\gamma_T/\bar{\gamma}_S)+1)^3(-2)(\gamma_T/\bar{\gamma}_S) < 0$.
   $\therefore$ **P2** is satisfied.

From (18), we have $r_{e,s,1}(P_{J,i}) = \Pr(\text{packet error}|(\bar{\alpha}_J P_{J,i}/N_0W))\log_2 M$. Since $\Pr(\text{packet error}|(\bar{\alpha}_J P_{J,i}/N_0W))$ satisfies **P0**, **P1**, and **P2**, $r_{e,s,1}(P_{J,i})$ also satisfies **P0**, **P1**, and **P2**. Therefore, we can use Theorem 1 to solve this optimization problem.

C. Slow Fading With Adaptive Modulation

Under slow fading with adaptive modulation, the objective is to maximize $\sum_{i\in B_{su}\cup B_{pu}} r_{e,s,2}(P_{J,i})$, under the constraint $\sum_{i\in B_{su}\cup B_{pu}} P_{J,i} \le P_J$.

Proposition 4: $r_{e,s,2}(P_{J,i})$ satisfies the conditions **P0**, **P0**, and **P0** of Theorem 1.

Proof:

1) By definition, we have $r_{e,s,2}(P_{J,i}) \le \sum_{i=1}^{N_A} \log_2 M_i$. Hence, **P0** is satisfied.
2) Define $t_i \overset{\Delta}{=} (\gamma_{T,i}/\bar{\gamma}_S)$. Note that $\theta > 1$ and $t_{i+1} > t_i > 0$ ($\because \gamma_{T,i} < \gamma_{T,i+1}$ by design). From (21),

$$r_{e,s,2}(P_{J,i}) = \sum_{i=1}^{N_A} h_i\left(\frac{\bar{\alpha}_J P_{J,i}}{N_0W}\right)$$

   where $h_i(x) \overset{\Delta}{=} (t_i x \log_2 M_i/1+t_i x)\ (e^{-(\theta t_i+(\theta-1/x))} - e^{-(\theta t_{i+1}+(t_{i+1}\theta/t_i)-1/x))})$. From Appendix E, Eq. (51), we show that $h_i'(x) \ge 0$. As a consequence, $(\mathrm{d}/\mathrm{d}P_{J,i})\, r_{e,s,2}(P_{J,i}) = (\bar{\alpha}_J/N_0W)\sum_{i=1}^{N_A} h_i'(\bar{\alpha}_J P_{J,i}/N_0W) \ge 0$. Therefore, **P1** is satisfied.

3) From Appendix E, Eq. (63), we see that $\sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^*$, and so

$$\frac{\mathrm{d}^2}{\mathrm{d}P_{J,i}^2} r_{e,s,2}(P_{J,i}) = \left(\frac{\bar{\alpha}_J}{N_0 W}\right)^2 \sum_{i=1}^{N_A} h_i''\left(\frac{\bar{\alpha}_J P_{J,i}}{N_0 W}\right) < 0 \Leftrightarrow \frac{\bar{\alpha}_J P_{J,i}}{N_0 W} > x^*. \quad (26)$$

Therefore, **P2** is satisfied.

Hence, we can use Theorem 1 to solve this optimization problem.

V. Joint Spoofing and Jamming Optimization

Suppose the adversary has an energy budget E for a single sensing-plus-transmission duration $T_0 + T_1$. It can be shown that the average throughput of the SUs is proportional to $\sum_{i=1}^{\min(\bar{N}_r, \bar{N}_a - N_{fd})}(\Gamma_1 - r_e(P_{J,i}))$, where Γ_1 is the average number of packets per user per band per transmission interval, $\bar{N}_r$ is the average number of bands required by SUs, $\bar{N}_a$ is the average number of allowed bands, and N_{fd} is the average number of false detections per sensing interval. The average number of bands occupied by PUs is $N_T - \bar{N}_a$. The objective of the adversary is to minimize $\sum_{i=1}^{\min(\bar{N}_r, \bar{N}_a - N_{fd})}(\Gamma_1 - r_e(P_{J,i}))$, under the constraint $T_0 P_S + T_1 P_J = E$. Let ξE be the amount of energy allocated for spoofing, where $\xi \in [0, 1]$. Therefore, $P_S = \xi E / T_0$ and $P_J = (1 - \xi)E/T_1$. The optimal energy allocation for spoofing (ξ^*) is given by

$$\xi^* = \underset{\xi \in [0,1]}{\arg\min}\; N_{su}(\xi)\Gamma_1 - \frac{N_{su}(\xi)}{N_{su}(\xi) + N_T - \bar{N}_a} \times F\left(r_e, \frac{(1-\xi)E}{T_1}, N_{su}(\xi) + N_T - \bar{N}_a\right) \quad (27)$$

where F is defined in Appendix A, Eq. (32) and $N_{su}(\xi) = \min(\bar{N}_r, \bar{N}_a - (\bar{N}_a / N_T) F(p_{fd}, \xi E/T_0, N_T))$.

The adversary can estimate $\bar{N}_r$ and $\bar{N}_a$ by detecting the average number of occupied bands in the T_0 and T_1 intervals, using an energy detector before it starts spoofing or jamming. From (28), in Appendix A, we know that the threshold x^* in $F(f, X_T, N)$ does not depend on X_T or N. Therefore, the thresholds in $F(r_e, (1-\xi)E/T_1, N_{su}(\xi) + N_T - \bar{N}_a)$ and $F(p_{fd}, \xi E/T_0, N_T)$ do not depend on ξ. Hence, (27) only involves direct evaluations of $r_e(P_{J,i})$ and $p_{fd}(P_{S,i})$. Therefore, the optimal fraction of energy allocation for spoofing, ξ^*, can be found from (27) using a single parameter search [17].

VI. Simulation Results

We consider a cluster-based SU system, sharing N_T DS-CDMA subcarriers with PUs. In the simulations, in each transmission and sensing interval, the PUs occupy $|B_{pu}| = \min(N_{pu}, N_T)$ bands at random, where N_{pu} is a Poisson random variable with mean parameter $\bar{N}_{pu}$. The number of SUs (Ω_{su}) in each transmission interval is modeled as a Poisson random variable with mean parameter $\bar{\Omega}_{su}$. The number of bands used by SUs in each transmission interval is $|B_{su}| = \min(\lceil \Omega_{su}/\Omega_M \rceil, |B - B_{pu}|)$, where Ω_M is the maximum number of SUs that can share a single band. We select $\bar{\alpha}_J = 1$, $\beta = 0.2$, $N_c = 256$, $\Omega_M = 8$, $T_0 = 128 T_s$ and $T_1 = 1024\ T_s$, where T_s is the symbol time. For FEC, we use rate 1/2 LDPC codes with block lengths varying from 1024 bits to 6144 bits. We assume the CH$_S$ uses power control to maintain $\bar{\gamma}_S = 10$ dB at each SU. We define the jamming-to-signal power ratio (JSR) as the ratio of adversary-power-to-signal-power per user. That is, the adversary power J is taken to be the sum of the jamming and the spoofing power available in all bands, and the signal power S is taken to be the transmission power available for a single SU. When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power spoofing or jamming across the total bandwidth. We use this equal power spoofing and jamming strategy as a reference, to which the performance of the optimized strategy is compared.

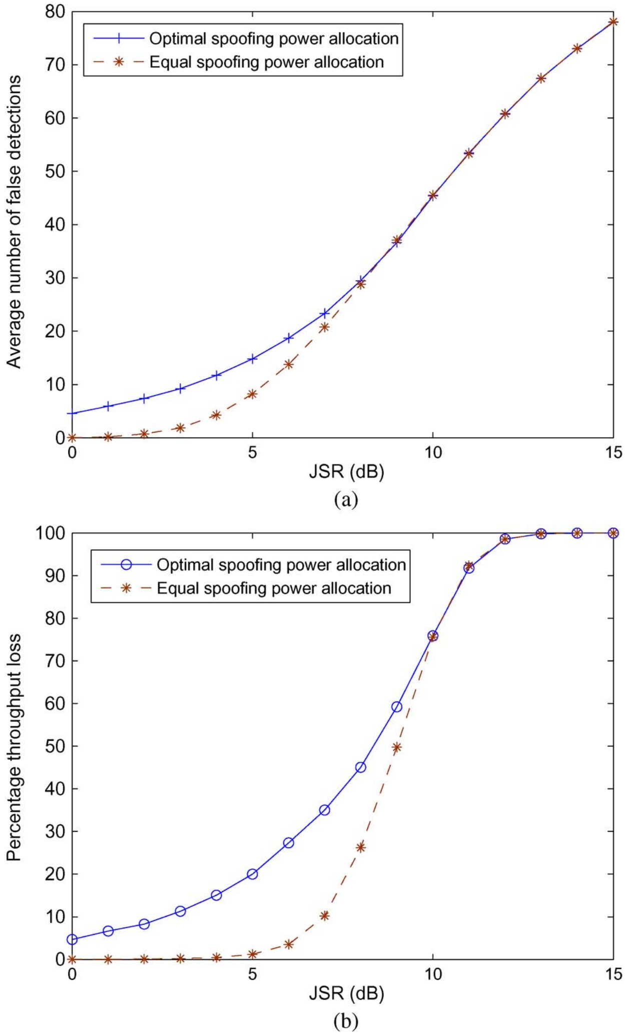


Fig. 8. $(p_{fd,f}(0) = 10^{-4}, N_c = 256, T_0 = 128\quad T_s, N_T = 100, \bar{\Omega}_{su}/\Omega_M = 50, \bar{N}_{pu} = 50)$: (a) Average number of false detections under slow fading (b) Percentage loss of throughput under fast fading.

A. *Spoofing*

Fig. 8(a) shows the average number of false detections per sensing interval versus the JSR under slow fading, when the

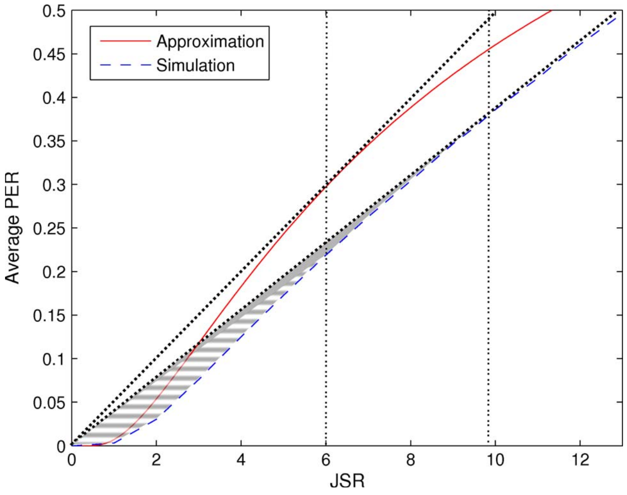


Fig. 9. Average packet error rate vs. JSR per band. ($N_c = 64, \bar{\gamma}_S = 12$ dB$, \theta = 2$ dB).

adversary employs the optimal jamming and spoofing strategy (solid curve). For comparison, the average number of false detections if the adversary spoofed all bands at equal power is also presented (dashed curve). The optimal spoofing power allocation increases the average number of false detections by more than 5 in JSR $\in$ (0,6) dB region, compared to equal spoofing power allocation across bands without optimization. As JSR 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 JSR. Fig. 8(a) shows the average throughput loss in the SU network due to spoofing, under fast fading. At a JSR of 7 dB, the optimal spoofing power allocation reduces the throughput by 35.1%, while the equal power allocation reduces the throughput only by 10.2%. For JSR >10 dB, the optimal spoofing strategy is equal power allocation across all bands.

B. Jamming

In the simulations of the slow fading system, we use the alphabets BPSK, 4-QAM, 16-QAM and 64-QAM for adaptive modulation. Fig. 9 shows the comparison of the average PER versus JSR per band, calculated using the step-function approximation and the simulations. We note that the values of the PER calculated using the approximation are notably different from the simulation results. The two vertical dotted lines show the threshold JSR, on which the decision for partial band jamming or full band jamming is made. We note that using the approximation, the adversary would decide to move to full band jamming at a lower JSR than the optimal value given by the simulations. The gray shaded region represents the reduction in the average PER, i.e., the performance loss of the adversary due to the use of the step function approximation when calculating the PER, to decide on the optimal jamming strategy. The horizontal-striped region represents the increase in the average BER using optimization based on the step function approximation, over jamming all bands at every JSR. Therefore, we note that, even though the average PER value given by the approximation is different from the simulations, the optimization based on the approximation yields results comparable to the optimal achievable with perfect information of the FEC performance by the adversary.

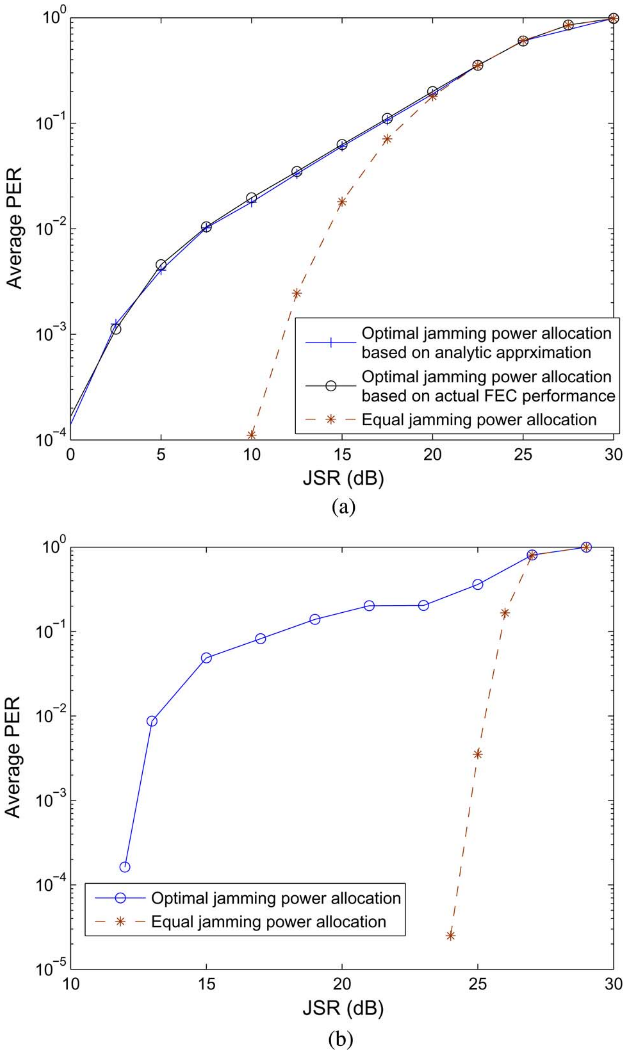
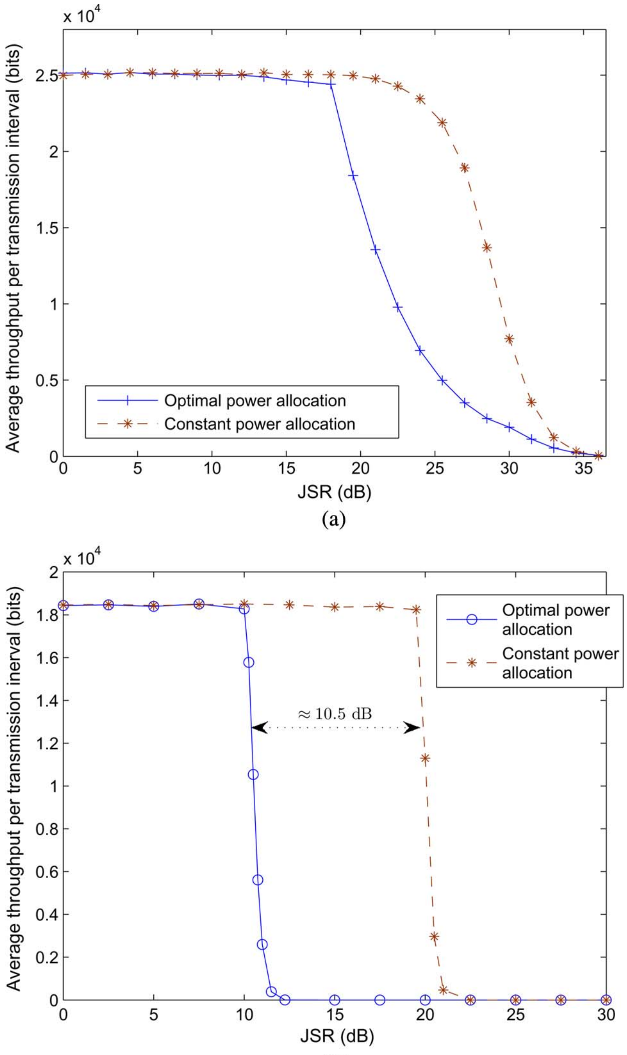


Fig. 10. Average packet error rate vs. JSR ($\bar{\gamma}_S = 12$ dB$, N_c = 64, \bar{\Omega}_{su}/\Omega_M = 10, \bar{N}_{pu} = 10, N_T = 20$): (a) under slow fading (b) under fast fading.

Fig. 10(a) shows the average PER versus JSR, with total power put into jamming by the adversary, under slow fading. We note that the optimal jamming power allocation based on the step function approximation performs very close to the optimal power allocation with perfect FEC information. The average PER of the system when all transmitting bands are jammed at equal power without any attempt at optimizing is also presented for comparison. The optimization significantly increases the average PER at low JSR. Fig. 10(b) shows the average PER due to jamming under fast fading. The optimal jamming power allocation achieves a 10^{-2} average PER at a JSR more than 10 dB below the JSR required for the same average PER with equal jamming power allocation.

C. Joint Optimization of Spoofing and Jamming

Fig. 11(a) shows the SU throughput-per-transmission interval versus JSR when the adversary jointly optimizes the jamming and spoofing power allocation under slow fading.



(a)

(b)

Fig. 11. Throughput vs. JSR ($T_0 = 128\ T_s, T_1 = 1024\ T_s, \bar{\Omega}_{su}/\Omega_M = 10$, $\bar{N}_{pu} = 10$, $N_T = 100$, $N_c = 256$): (a) under slow fading (b) under fast fading.

It is compared with the throughput if the adversary spoofed and jammed bands at equal power. Notice that for JSR in the vicinity of 25 dB, the use of the optimization technique by the adversary reduces the CR throughput by a factor of 4 to 5, relative to an adversary who divides power equally across all bands. At low JSR, below about 18 dB under simulated system parameters, spoofing is ineffective, as the system is lightly loaded. However, the optimized adversary is able to reduce the throughput slightly through increased packet error rate by jamming. Beyond 18 dB, the system throughput is significantly reduced, predominantly due to successful spoofing. Fig. 11(b) shows the SU throughput-per-transmission interval versus JSR under fast fading. We note that the optimal power allocation can significantly reduce the throughput of SUs at a JSR 10.5 dB lower than constant power allocation, under simulated system parameters.

VII. Conclusion

In this paper, we analyze the optimal spoofing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization approach which enables simplified calculation of threshold JSRs, below which partial-band attacks are optimal. We derive the optimal jamming power allocation based on a simplified step-function approximation of the word error rate of LDPC codes. Through comparisons of the throughput with optimal spoofing and jamming power allocation with the throughput for equal power spoofing and jamming, we observe that the optimization has notable gains in the low and medium JSR regions.

We learn that it is generally optimal to attack with both spoofing and jamming, whereby the optimal energy allocation between the two methods of attack is dependent on system parameters and JSR. While successful spoofing has the most noticeable impact on SU throughput, we observe that when the system is not heavily loaded, spoofing is not effective at low JSR, and the optimal method of attack is jamming. An increase in the average number of subcarriers required by SUs, or a decrease in the sensing duration relative to the transmission duration, would lower the JSR, at which point the optimal strategy shifts from jamming to spoofing.

Appendix A
Optimization Approach

In this section we present the optimization approach we use in this work.

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 $x_i \ge 0$,

$$\sum_{i=1}^{N} f(x_i) \le \begin{cases} N f\left(\frac{X_T}{N}\right), & \text{if } \frac{X_T}{N} \ge x^* \\ (N-n^*)f(0)+n^* f\left(\frac{X_T}{n^*}\right), & \text{if } \frac{X_T}{N} < x^* \end{cases} \qquad (28)$$

where $n^* = X_T/x^*$ 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

$$\begin{aligned} S_x &= \underset{\sum_{i=1}^{N} x_i = X_T, x_i \ge 0}{\arg\max} \left(\sum_{i=1}^{N} f(x_i) \right) \\ &= \begin{cases} \Bigg\{ \underbrace{\frac{X_T}{N}, \ldots, \frac{X_T}{N}}_{N \text{ elements}} \Bigg\}, & \text{if } \frac{X_T}{N} \ge x^* \\ \Bigg\{ \underbrace{\frac{X_T}{n^*}, \ldots, \frac{X_T}{n^*}}_{n^* \text{ elements}}, \underbrace{0, \ldots, 0}_{(N-n^*)} \Bigg\}, & \text{if } \frac{X_T}{N} < x^*. \end{cases} \end{aligned} \qquad (29)$$

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

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. A false detection is mistakenly detecting a vacant band as being occupied by the PUs. In jamming, $f(x)$ is the packet error rate per user in a band, as a function of the jamming power allocated for that band. Geometrically, $g(x_t)$ is the difference between $f(0)$ and the y-intercept of the tangent to $f(x)$ at x_t.

Proof of Theorem 1:

Case 1: $(X_T/N) \geq x^*$: From Appendix B, (39), we know $f(x) \leq f(X_T/N) + (x - (X_T/N))f'(X_T/N)$.

$$\therefore \sum_{i=1}^{N} f\left(\frac{X_T}{N}\right) \leq \sum_{i=1}^{N}\left(f\left(\frac{X_T}{N}\right) + \left(x_i - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right)\right)$$
$$= Nf\left(\frac{X_T}{N}\right). \tag{30}$$

Case 2: $0 \leq (X_T/N) < x^*$: From Appendix B, Eq. (40), we have $f(x) \leq f(0) + (x_i/x^*)(f(x^*) - f(0))$.

$$\therefore \sum_{i=1}^{N} f(x_i) \leq \sum_{i=1}^{N}\left(f(0) + \frac{x_i}{x^*}\left(f(x^*) - f(0)\right)\right)$$
$$= (N - n^*)f(0) + n^* f(x^*) \tag{31}$$

where $n^* = X^T/x^*$. From (30) and (31),

$$\sum_{i=1}^{N} f(x_i) \leq F(f, X_T, N)$$
$$\triangleq \begin{cases} Nf\left(\frac{X_T}{N}\right), & \text{if } \bar{x} \geq x^* \\ (N - n^*)f(0) + n^* f(x^*), & \text{if } \bar{x} < x^*. \end{cases} \tag{32}$$

Lemma A1: $g(x) = 0$ has at most one solution in $x > 0$.

Proof of Lemma A1: Taking the derivative of $g(x) = f(x) - f(0) - xf'(x)$ with respect to x, we have $g'(x) = -xf''(x)$. From property **P2**, we know $f''(x) < 0\ \forall x > 0$ or $\exists x_0 > 0$ such that $f''(x) < 0$ for $x \in (x_0, \infty)$ and $f''(x) > 0$ for $x \in (0, x_0)$.

If $\forall x > 0\ f''(x) < 0$, then $g'(x) > 0$ and $g(x) > 0$ because $g(0) = 0$. Therefore, $g(x) = 0$ does not have any solutions in $x > 0$ and $x^* = 0$. If $f''(x) > 0$ for $0 < x < x_0$, then for $x \in (0, x_0)$, $g'(x) < 0$ and $g(x) < 0$. But, $\lim_{x\to\infty} g(x) = \lim_{x\to\infty}(f(x) - f(0) - xf'(x)) = \lim_{x\to\infty} f(x) - f(0) - 0 > 0$, because $f(x)$ is an increasing function (**P1**) and $\lim_{x\to\infty} xf'(x) = 0$ (see (34) below). Therefore, $g(x) = 0$ for some $x \in (x_0, \infty)$. Since $g'(x) > 0$ for $x \in (x_0, \infty)$, there is only one root.

Since we defined x^* is the largest root of $g(x) = 0$, from the above analysis we have

$$f''(x^*) < 0. \tag{33}$$

Proof $\lim_{x\to\infty} xf'(x) = 0$: We prove this by contradiction. Suppose $\lim_{x\to\infty} xf'(x) \neq 0$. Because $xf'(x) \geq 0$, we have $\lim_{x\to\infty} xf'(x) > 0$. Since $f'(x)$ is decreasing in $x > x_0$, we know $xf'(x)$ does not have oscillations and $\exists L > 0, x_L > x_0$, s.t. $xf'(x) > L\ \forall\ x > x_L$.

$$\Rightarrow f'(x) > \frac{L}{x} \quad \forall x > x_L$$
$$\Rightarrow \lim_{x_1\to\infty} \int_{x_L}^{x_1} f'(x)\mathrm{d}x > \lim_{x_1\to\infty} \int_{x_L}^{x_1} \frac{L}{x}\mathrm{d}x$$
$$\Rightarrow \lim_{x_1\to\infty}\left(f(x_1) - f(x_L)\right) > \lim_{x_1\to\infty} L\left(\ln(x_1) - \ln(x_L)\right)$$
$$\Rightarrow L < \frac{\lim_{x_1\to\infty}\left(f(x_1) - f(x_L)\right)}{\lim_{x_1\to\infty}\left(\ln(x_1) - \ln(x_L)\right)} = 0$$
$$(\because f(x) \text{ is finite, from property } \mathbf{P0})$$
$$\Rightarrow L < 0, \text{ but this is a contradiction.}$$

Therefore, we conclude that

$$\lim_{x\to\infty} xf'(x) = 0. \tag{34}$$

Appendix B
Proof of Upper Bounds to $f(x)$

Define $d_{x_0}(x) \triangleq f(x_0) + (x - x_0)f'(x_0) - f(x)$. Taking the derivative with respect to x, we obtain $d'_{x_0}(x) = f'(x_0) - f'(x)$ and

$$d''_{x_0}(x) = -f''(x). \tag{35}$$

From (33) and **P2**, we know $f''(x) < 0$ for $x \geq x^*$ and therefore, $d''_{x_0}(x) > 0$ for $x \geq x^*$.

Let $x_0 \geq x^*$. We have

$$d_{x_0}(x) \geq 0\ \forall x > x_0 \quad (\because\ d_{x_0}(x_0) = 0,\ d'_{x_0}(x_0) = 0). \tag{36}$$

Further, from (35) and **P2**, we know $d''_{x_0}(x) = 0$ has at most one root in $(0, x_0]$. Therefore, $d'_{x_0}(x)$ has at most one root in $(0, x_0)$ because $d'_{x_0}(x_0) = 0$. Since $d''_{x_0}(x_0) > 0$, $\lim_{x\to x_0^-} d'_{x_0}(x_0) = 0^-$. $\therefore$, $\exists x_1 \in [0, x_0)$ s.t. $d'_{x_0}(x) > 0\ \forall x \in (0, x_1)$ and $d'_{x_0}(x) < 0\ \ \forall x \in (x_1, x_0)$. From the definition of $d_{x0}(x)$, we have $d_{x_0}(0) = g(x_0)$ and from Appendix A, we know $g(x_0) > 0\ \forall x_0 \geq x^*$.

$$\therefore\ d_{x_0}(x) \geq 0\ \forall x \in [0, x_1]. \tag{37}$$

Further,

$$d_{x_0}(x) \geq 0\ \forall x \in (x_1, x_0] \tag{38}$$

because $d'_{x_0}(x) < 0\ \forall x \in (x_1, x_0), d_{x_0}(x_0) = 0$. From (36)–(38), we know when $x_0 \geq x^*$, $d_{x_0}(x) \geq 0\ \forall x \geq 0$. Therefore, when $X_T/N_0 \geq x^*$, $d_{X_T/N_0}(x) \geq 0$, and

$$f(x) \leq f\left(\frac{X_T}{N}\right) + \left(x - \frac{X_T}{N}\right) f'\left(\frac{X_T}{N}\right). \tag{39}$$

Further, since $d_{x^*}(x) \geq 0$, $f(x) \leq f(x^*) + (x - x^*)f'(x^*)$. From the definition of x^*, $g(x^*) = f(x^*) - f(0) - x^* f'(x^*) =$

0, and $f'(x^*) = (f(x^*) - f(0))/x^*$. Substituting this in (VII), we have

$$\begin{aligned} f(x) &\leq f(x^*) + (x - x^*)\frac{(f(x^*) - f(0))}{x^*} \\ &= f(0) + \frac{x}{x^*}\left(f(x^*) - f(0)\right) \end{aligned} \tag{40}$$

Appendix C
Proofs of Propositions 1 and 2

Proposition 1: $p_{fd,f}$ has properties **P0**, **P1**, and **P2** stated in Theorem 1.

Proof: Define

$$\begin{aligned} g_f(y) &\triangleq p_{fd,f}\left(\frac{WN_0 y}{\bar{\alpha}_J}\right) \\ &= Q\left(\frac{K\sqrt{2}/N_0 - \sqrt{2T_0W} - \sqrt{2T_0W}y}{\sqrt{(5y^2 + 4y + 2)}}\right) \\ &= Q\left(\frac{b - ay}{\sqrt{5y^2 + 4y + 2}}\right) \end{aligned} \tag{41}$$

where $b = (K\sqrt{2}/N_0) - \sqrt{2T_0W}$ 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 $g_f(y)$, we have

$$p_{fd,f}(P_{S,i}) = g\left(\frac{\bar{\alpha}_J P_{S,i}}{WN_0}\right) \tag{42}$$

and from (41),

$$\begin{aligned} g_f'(y) &= \frac{\mathrm{d}}{\mathrm{d}y}Q\left(\frac{b - ay}{\sqrt{5y^2 + 4y + 2}}\right) \\ &= \frac{((2a + 5b)y + 2a + 2b)}{(5y^2 + 4y + 2)^{\frac{3}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(5y^2+4y+2)}}. \end{aligned} \tag{43}$$

From (43), $g_f'(y) > 0 \; \forall y > 0$, because $a, b > 0$. From (42), $(\mathrm{d}/\mathrm{d}P_{S,i})p_{fd,f}(P_{S,i}) = (\bar{\alpha}_J/WN_0)g_f'(\bar{\alpha}_J P_{S,i}/WN_0) > 0 \; \forall P_{S,i} > 0$. Therefore, condition **P1** is satisfied.
3) From (43),

$$g_f''(y) = \frac{\mathrm{d}}{\mathrm{d}y}g_f'(y) = \frac{p(y)}{(5y^2+4y+2)^{\frac{7}{2}}\sqrt{2\pi}} e^{-\frac{(ay-b)^2}{2(5y^2+4y+2)}} \tag{44}$$

where $p(y) = c_4y^4 + c_3y^3 + c_2y^2 + c_1y + c_0$, $c_0 = -16a - 4b + 4a^2b + 8ab^2 + 4b^3$, $c_3 = -250a - 400b - a(2a + 5b)^2 < 0$, $c_4 = -50(2a + 5b) < 0$ and

$$\begin{aligned} c_1 &= -100a - 88b - 4a^3 + 24ab^2 + 20b^3 \\ &= 5c_0 - 20a - 68b - 4a^3 - 20a^2b - 16ab^2 \end{aligned} \tag{45}$$

$$\begin{aligned} c_2 &= -216a - 270b - 8a^3 - 24a^2b + 25b^3 \\ &= \frac{5}{4}c_1 - 91a - 160b - 3a^3 - 24a^2b - 30ab^2. \end{aligned} \tag{46}$$

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 $c_4, c_3 < 0$. From (45), we see that $c_0 \leq 0 \Rightarrow c_1 < 0$, and from (46), $c_1 \leq 0 \Rightarrow c_2 < 0$. Therefore, if $c_0 \leq 0$, all nonzero 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 ($\because c_0 > 0, c_1, c_2, c_3, c_4 \leq 0$). If otherwise, i.e., $c_1 > 0$, there will be only one sign change irrespective of the sign of $c_2 (\because c_0, c_1 > 0, c_3, c_4 < 0)$. 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 (44), we know $g_f''(y)$ has the same sign as $p(y)$. Therefore, we conclude that $g_f(y)$ satisfies the condition **P2**. From (42), $(\mathrm{d}^2 / \mathrm{d}P_{S,i}^2)p_{fd,f}(P_{S,i}) = (\bar{\alpha}_J^2 / W^2N_0^2)g_f''(\bar{\alpha}_J P_{S,i} / WN_0)$. Therefore, $p_{fd,f}(P_{S,i})$ satisfies the condition **P2**.

Proposition 2: $p_{fd,s}(P_{S,i})$ has properties **P0**, **P1**, and **P2** stated in Theorem 1.

Proof: Consider $\Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i})$.

1) Condition **P0** is obviously satisfied from (5).
2) We have, $(\mathrm{d}/\mathrm{d}\eta_{S,i}) \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) = (K/\bar{\alpha}_J \sqrt{2\pi}) \int_0^\infty (y/(y\eta_{S,i} + N_0)^2) e^{-(1/2)((K/(y\eta_{S,i}+N_0)) - \sqrt{T_0W})^2} e^{-(y/\bar{\alpha}_J)}\mathrm{d}y > 0$. Therefore, condition **P1** is satisfied.
3)

$$\begin{aligned} &\frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0W}|\eta_{S,i}) \\ &= \frac{K}{\bar{\alpha}_J\sqrt{2\pi}} \int\limits_0^\infty e^{-\frac{y}{\bar{\alpha}_J}} e^{-\frac{1}{2}\left(\frac{K}{y\eta_{S,i}+N_0} - \sqrt{T_0W}\right)^2} \\ &\quad \times \frac{y^2\left\{K(K - (y\eta_{S,i} + N_0)\sqrt{T_0W}) - \frac{2}{(y\eta_{S,i}+N_0)^2}\right\}}{(y\eta_{S,i} + N_0)^5}\,\mathrm{d}y \\ &= \frac{K}{\bar{\alpha}_J\sqrt{2\pi}} \int\limits_0^\infty e^{-\frac{y}{\bar{\alpha}_J\eta_{S,i}}} e^{-\frac{1}{2}\left(\frac{K}{y+N_0} - \sqrt{T_0W}\right)^2} y^2 \\ &\quad \times \frac{(K^2 - K\sqrt{T_0W}(y + N_0) - \frac{2}{(y+N_0)^2})}{\eta_{S,i}^3(y + N_0)^5}\mathrm{d}y = \frac{I(\eta_{S,i})}{\eta_{S,i}^3} \end{aligned} \tag{47}$$

where $I(\eta_{S,i}) \triangleq \int_0^\infty \iota(y)e^{-(y/\bar{\alpha}_J\eta_{S,i})}\mathrm{d}y$ and $\iota(y) \triangleq (Ky^2(K^2 - K\sqrt{T_0W}(y+N_0) - 2(y+N_0)^2)/\bar{\alpha}_J\sqrt{2\pi}(y+N_0)^5)e^{-(1/2)(K/(y+N_0)-\sqrt{T_0W})^2}$. 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, $\iota(y) > 0 \Leftrightarrow K^2 - K\sqrt{T_0W}(y + N_0) - 2(y + N_0)^2 > 0 \Leftrightarrow y + N_0 \in (-(K(\sqrt{T_0W+8} + \sqrt{T_0W})/4),\; K(\sqrt{T_0W+8} - \sqrt{T_0W})/4)$. Define $y_0 \triangleq \max((K(\sqrt{T_0W+8} - \sqrt{T_0W})/$

$4)-N_0,0)$. From the definition of y_0, $y>y_0 \Rightarrow \iota(y)<0$ and $0<y<y_0 \Rightarrow \iota(y)>0$. Also,

$$\begin{aligned}
I'(\eta_{S,i}) &\triangleq \frac{\mathrm{d}}{\mathrm{d}\eta_{S,i}} I(\eta_{S,i}) = \frac{1}{\bar{\alpha}_J \eta_{S,i}^2} \int_0^\infty y\iota(y) e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}} \,\mathrm{d}y \\
&< \frac{1}{\bar{\alpha}_J \eta_{S,i}^2} \left(\int_0^{y_0} y_0 \iota(y) e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}} \,\mathrm{d}y + \int_{y_0}^\infty y_0 \iota(y) e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}} \,\mathrm{d}y \right) \\
&= \frac{y_0}{\bar{\alpha}_J \eta_{S,i}^2} \int_0^\infty \iota(y) e^{-\frac{y}{\eta_{S,i}\bar{\alpha}_J}} \,\mathrm{d}y \\
I'(\eta_{S,i}) &< \frac{y_0 I(\eta_{S,i})}{\bar{\alpha}_J \eta_{S,i}^2}. \qquad (48)
\end{aligned}$$

From (48), 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 (47), $(\mathrm{d}^2/\mathrm{d}\eta_{S,i}^2)\Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i}) \leq 0 \Leftrightarrow I(\eta_{S,i}) \leq 0$.

$$\begin{aligned}
&\therefore \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i})(\tilde{\eta}_{S,i}) \leq 0 \\
&\Rightarrow I(\tilde{\eta}_{S,i}) \leq 0 \Rightarrow I(\eta_{S,i}) < 0 \;\forall\; \eta_{S,i} > \tilde{\eta}_{S,i} \\
&\Rightarrow \frac{\mathrm{d}^2}{\mathrm{d}\eta_{S,i}^2} \Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i}) < 0 \;\forall\; \eta_{S,i} > \tilde{\eta}_{S,i}.
\end{aligned}$$

Therefore, $\Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i})$ satisfies condition **P2**.

Note that $p_{fd,s}(P_{S,i}) = \Pr(Y(t) > K\sqrt{T_0 W}|P_{S,i}/W) = \Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i})$. Since $\Pr(Y(t) > K\sqrt{T_0 W}|\eta_{S,i})$ satisfies the conditions **P0**, **P1**, and **P2**, $p_{fd,s}(P_{S,i})$ also satisfies the conditions **P0**, **P1**, and **P2**.

Appendix D
Proof of Lemma 1

Lemma 1: $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is a monotonically decreasing function of $\bar{\gamma}_{J,i}$, and the range of $\tilde{\gamma}$ is $(0, \bar{\gamma}_S]$.

Proof: From (13), we can see $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is monotonically decreasing in $\bar{\gamma}_{J,i}$. From (13), we further have $\tilde{\gamma}(0) = \int_0^\infty \int_0^\infty (x\bar{\gamma}_S/(y.0+1)) e^{-x} e^{-y} \,\mathrm{d}x \,\mathrm{d}y = \bar{\gamma}_S$. and from (14), we have

$$\begin{aligned}
\lim_{\bar{\gamma}_{J,i}\to\infty} \tilde{\gamma}(\bar{\gamma}_{J,i}) &= \lim_{\bar{\gamma}_{J,i}\to\infty} -\frac{\bar{\gamma}_S e^{\frac{1}{\bar{\gamma}_{J,i}}}}{\bar{\gamma}_{J,i}} \mathrm{Ei}\left(-\frac{1}{\bar{\gamma}_{J,i}}\right) \\
&\propto \lim_{\bar{\gamma}_{J,i}\to\infty} \lim - \frac{1}{\bar{\gamma}_{J,i}} \log\left(\frac{-1}{\bar{\gamma}_{J,i}}\right) = 0. \qquad (49)
\end{aligned}$$

Note that $\lim_{x\to 0}\mathrm{Ei}(x) \propto \log x$ [16]. Hence, we have shown $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is a monotonically decreasing function in $\mathbb{R}^+$, and the range of $\tilde{\gamma}(\bar{\gamma}_{J,i})$ is $(0, \bar{\gamma}_S]$.

Appendix E
Derivations Supporting the Analysis in Section V-D

Proof $h_i'(x) \geq 0$*:*

$$\begin{aligned}
h_i'(x) = \frac{t_i e^{-t_i} \log_2 M_i}{(1+t_i x)^2} &\left\{ \left((t_i\theta - t_i)\left(1 + \frac{1}{t_i x}\right) + 1 \right) \right. \\
&\times e^{-\left((t_i\theta - t_i)\left(1+\frac{1}{t_i x}\right)\right)} - e^{-\left((t_{i+1}\theta - t_i)\left(1+\frac{1}{t_i x}\right)\right)} \\
&\left. \times \left((t_{i+1}\theta - t_i)\left(1 + \frac{1}{t_i x}\right) + 1 \right) \right\}. \qquad (50)
\end{aligned}$$

Define $q_t(x) \triangleq (t_i\theta - t_i)(1 + (1/t_i x))$ and $q_v(x) \triangleq (t_{i+1}\theta - t_i)(1 + (1/t_i x))$. Note $q_v(x) > q_t(x) > 0$.

$$\begin{aligned}
h_i'(x) &= \frac{t_i e^{-(t_i + q_v(x))}(q_t(x)+1)\log_2 M_i}{(1+t_i x)^2} \\
&\quad \times \left(e^{(q_v(x) - q_t(x))} - \left(1 + \frac{q_v(x) - q_t(x)}{q_t(x)+1}\right)\right) \\
&> \frac{t_i e^{-(t_i + q_v(x))}(q_t(x)+1)\log_2 M_i}{(1+t_i x)^2} \\
&\quad \times \left(e^{(q_v(x) - q_t(x))} - (1 + (q_v(x) - q_t(x)))\right) \geq 0. \qquad (51)
\end{aligned}$$

Proof $\exists x^* \geq 0$ *s.t.* $\sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^*$*:*

$$\begin{aligned}
&h_i''(x) \\
&= \left(\frac{e^{-t_i}\log_2 M_i}{x^2(1+t_i x)^3} \right) \\
&\quad \times \left\{ ((t_i\theta - t_i)(1 + t_i x) q_t(x) \right. \\
&\qquad -2t_i^2 x^2 (q_t(x)+1)) e^{-q_t(x)} \\
&\quad - ((t_{i+1}\theta - t_i)(1 + t_i x) q_v(x) \\
&\qquad \left. -2t_i^2 x^2 (q_v(x)+1)) e^{-q_v(x)} \right\} \qquad (52)
\end{aligned}$$

$$\begin{aligned}
&\frac{t_i x^3 e^{t_i} h_i''(x)}{\log_2 M_i} \\
&= \left((t_i\theta - t_i)^2 e^{-q_t(x)} - (t_{i+1}\theta - t_i)^2 e^{-q_v(x)} \right) \\
&\quad - \frac{2t_i^3 x^3}{(1+t_i x)^3} \left\{ \left(\frac{q_t^2(x)}{2} + q_t(x) + 1 \right) e^{-q_t(x)} \right. \\
&\qquad \left. - \left(\frac{q_v^2(x)}{2} + q_v(x) + 1 \right) e^{-q_v(x)} \right\}. \qquad (53)
\end{aligned}$$

Substituting $y = 1 + (1/t_i x)$, we can rewrite (53) as follows:

$$\begin{aligned}
g_i(y) &\triangleq \frac{t_i x^3 e^{t_i} h_i''(x)}{\log_2 M_i} \\
&= k_{t_i}^2 e^{-k_{t_i} y} - k_{v_i}^2 e^{-k_{v_i} y} - \frac{2}{y^3} \left[\left(\frac{k_{t_i}^2 y^2}{2} + k_{t_i} y + 1 \right) \right. \\
&\quad \left. \times e^{-k_{t_i} y} - \left(\frac{k_{v_i}^2 y^2}{2} + k_{v_i} y + 1 \right) e^{-k_{v_i} y} \right] \qquad (54)
\end{aligned}$$

where $k_{t_i} = t_i\theta - t_i$, $k_{v_i} = t_{i+1}\theta - t_i$ and $y = 1 + (1/t_i x) \in (1, \infty)$. We have $k_{v_i} - k_{t_i} = (t_{i+1} - t_i)\theta > 0$. Further $k_{t_i} = t_i(\theta - 1) > 0$. Therefore, we have $k_{v_i} > k_{t_i} > 0$. Further, $g_i'(y) = -k_{t_i}^3 e^{-k_{t_i} y} + k_{v_i}^3 e^{-k_{v_i} y} + (6/y^4)[((k_{t_i}^3 y^3/6) + (k_{t_i}^2 y^2/2) + k_{t_i} y + 1)e^{-k_{t_i} y} - ((k_{v_i}^3 y^3/6) + (k_{v_i}^2 y^2/2) + k_{v_i} y + 1)e^{-k_{v_i} y}]$. We have

$$\begin{aligned}
&g_i'(y) + k_{t_i} g_i(y) \\
&\quad = k_{v_i}^2 \left(k_{v_i} - k_{t_i}\right) e^{k_{v_i} y} \\
&\qquad + \frac{1}{y^4}\Bigg\{ \left[k_{t_i}^2 y^2 + 4k_{t_i} y + 6\right] e^{-k_{t_i} y} \\
&\qquad\qquad - \left(6 + 4k_{t_i} y + k_{t_i}^2 y^2\right) e^{-k_{v_i} y} \\
&\qquad\qquad \times \Bigg[1 + \left(k_{v_i} - k_{t_i}\right) y + \frac{\left(3 + 2k_{t_i} y\right)\left(k_{v_i} - k_{t_i}\right)^2 y^2}{\left(6 + 4k_{t_i} y + k_{t_i}^2 y^2\right)} \\
&\qquad\qquad\quad + \frac{\left(k_{v_i} - k_{t_i}\right)^3 y^3}{\left(6 + 4k_{t_i} y + k_{t_i}^2 y^2\right)}\Bigg]\Bigg\} \\
&> k_{v_i}^2 \left(k_{v_i} - k_{t_i}\right) e^{k_{v_i} y} + \frac{(6 + 4k_{t_i} y + k_{t_i}^2 y^2) e^{-k_{v_i} y}}{y^4} \\
&\quad \times \Bigg\{ e^{\left(k_{v_i} - k_{t_i}\right) y} - \Bigg(1 + \left(k_{v_i} - k_{t_i}\right) y + \frac{\left(k_{v_i} - k_{t_i}\right)^2 y^2}{2} \\
&\qquad\qquad + \frac{\left(k_{v_i} - k_{t_i}\right)^3 y^3}{6}\Bigg)\Bigg\} \\
&> 0 \qquad (55)
\end{aligned}$$

because $k_{v_i} > k_{t_i} > 0$ and $y > 1$. Further,

$$\begin{aligned}
g_i(1) &= -2\left[\left(k_{t_i} + 1\right) e^{-k_{t_i}} - \left(k_{v_i} + 1\right) e^{-k_{v_i}}\right] \\
&= -2\left(k_{t_i} + 1\right) e^{-k_{v_i}} \left(e^{\left(k_{v_i} - k_{t_i}\right)} - \left(1 + \frac{k_{v_i} - k_{t_i}}{1 + k_{t_i}}\right)\right) \\
&< -2\left(k_{t_i} + 1\right) e^{-k_{v_i}} \left(e^{\left(k_{v_i} - k_{t_i}\right)} - \left(1 + \left(k_{v_i} - k_{t_i}\right)\right)\right) \\
&< 0 \qquad (56)
\end{aligned}$$

because $k_{v_i} > k_{t_i} > 0$, and

$$\begin{aligned}
\lim_{y\to\infty} g_i(y) &= \lim_{y\to\infty} k_{t_i}^2 e^{-k_{t_i} y} - k_{v_i}^2 e^{-k_{v_i} y} - \frac{2}{y^3} \\
&\quad \times \left[\left(\frac{k_{t_i}^2 y^2}{2} + k_{t_i} y + 1\right) e^{-k_{t_i} y} - \left(\frac{k_{v_i}^2 y^2}{2} + k_{v_i} y + 1\right) e^{-k_{v_i} y}\right] \\
&= \lim_{y\to\infty} k_{t_i}^2 e^{-k_{t_i} y} - k_{v_i}^2 e^{-k_{v_i} y} \\
&= 0^+ \qquad (57)
\end{aligned}$$

because $k_{t_i}^2 e^{-k_{t_i} y} - k_{v_i}^2 e^{-k_{v_i} y} > 0 \Leftrightarrow y > (2\ln(k_{v_i}/k_{t_i})/(k_{v_i} - k_{t_i}))$ from (64).

We need to show that $\sum_{i=1}^{N_A} h_i''(x)$ has only one zero for $x \in (0, \infty)$, and goes from positive to negative with increasing x. From (54),

$$\begin{aligned}
\sum_{i=1}^{N_A} h_i''(x) < 0 &\Leftrightarrow \sum_{i=1}^{N_A} \frac{\log_2 M_i g_i\left(1 + \frac{1}{t_i x}\right)}{t_i x^3 e^{t_i}} < 0 \\
&\Leftrightarrow \sum_{i=1}^{N_A} \frac{g_i(y_i) \log_2 M_i}{t_i e^{t_i}} < 0 \qquad (58)
\end{aligned}$$

where $y_i = 1 + (1/t_i x)$. Define

$$G(y_1) \triangleq \sum_{i=1}^{N_A} \frac{g_i(y_i) \log_2 M_i}{t_i e^{t_i}} \qquad (59)$$

where $y_i = 1 + (1/t_i x) = (t_1/t_i) y_1 + 1 - (t_1/t_i)$. Therefore, we have $(\mathrm{d}/\mathrm{d}y_1) y_i = t_1/t_i$ and $k_{t_i} = (\theta - 1) t_i = (t_i/t_1) k_{t_1}$.

$$\begin{aligned}
G'(y_1) &= \frac{\mathrm{d}}{\mathrm{d}y_1} \sum_{i=1}^{N_A} \frac{g_i(y_i) \log_2 M_i}{t_i e^{t_i}} \\
&= \sum_{i=1}^{N_A} \frac{g_i'(y_i) \log_2 M_i}{t_i e^{t_i}} \frac{\mathrm{d}y_i}{\mathrm{d}y_1} \\
&= \sum_{i=1}^{N_A} \frac{g_i'(y_i) \log_2 M_i}{t_i e^{t_i}} \left(\frac{t_1}{t_i}\right) \\
&> \sum_{i=1}^{N_A} \frac{-k_{t_i} g_i(y_i) \log_2 M_i}{t_i e^{t_i}} \left(\frac{t_1}{t_i}\right) \\
&= -k_{t_1} \sum_{i=1}^{N_A} \frac{g_i(y_i) \log_2 M_i}{t_i e^{t_i}} \\
&= -k_{t_i} G(y_1). \qquad (60)
\end{aligned}$$

Further, because $y_1 = 1 \Rightarrow y_i = 1$ and $g_i(1) < 0$ from (56), we have

$$G(1) = \sum_{i=1}^{N_A} \frac{g_i(1) \log_2 M_i}{t_i e^{t_i}} < 0 \qquad (61)$$

and because $y_1 \to \infty \Rightarrow y_i \to \infty$ and $\lim_{y_i\to\infty} g_i(y_i) = 0^+$ from (57), we have

$$\begin{aligned}
\lim_{y_1\to\infty} G(y_1) &= \lim_{y_1\to\infty} \sum_{i=1}^{N_A} \frac{g_i(y_i) \log_2 M_i}{t_i e^{t_i}} \\
&= \sum_{i=1}^{N_A} \frac{\lim_{y_i\to\infty} g_i(y_i) \log_2 M_i}{t_i e^{t_i}} = 0^+. \qquad (62)
\end{aligned}$$

From (61) and (62), we know $G(y_1) = 0$ has at least one finite solution in $y_1 \in (1, \infty)$. From (60) we know at a root of $G(y_1) = 0$, $G'(y_1) > 0$, i.e., at the roots the function is increasing, and therefore, must go from negative to positive. Hence, there can be only one solution for $G(y_1) = 0$. Define y_1^*, s.t. $G(y_1^*) = 0$. From (61) it follows that, $G(y_1) < 0 \Leftrightarrow y_1 < y_1^*$. Define $x^* \triangleq 1/t_1(y_1^* - 1)$. Therefore, $y_1 < y_1^* \Leftrightarrow x > x^*$ and $G(y_1) < 0 \Leftrightarrow \sum_{i=1}^{N_A} h_i''(x) < 0$ from (58).

$$\therefore \sum_{i=1}^{N_A} h_i''(x) < 0 \Leftrightarrow x > x^*. \qquad (63)$$

Proof $\exists y^* > 0$ *s.t.* $k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y} < 0 \Leftrightarrow y < y^*$*:* Define $Q_n^{(i)} : \Re^+ \to \Re$, $Q_n^{(i)}(y) \triangleq k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y}$, where $0 < k_{t_i} < k_{v_i}$ are constants. Note that $Q_n^{(i)}(0) = k_{t_i}^n - k_{v_i}^n < 0$, because $k_{t_i} < k_{v_i}$. Further, $Q_n^{(i)}(y) = 0 \Leftrightarrow k_{t_i}^n e^{-k_{t_i} y} - k_{v_i}^n e^{-k_{v_i} y} = 0 \Leftrightarrow e^{(k_{v_i} - k_{t_i}) y} = (k_{v_i}^n / k_{t_i}^n) \Leftrightarrow y =$

$n\ln(k_{v_i}/k_{t_i})/k_{v_i}-k_{t_i}$, i.e., $Q_n^{(i)}(y)=0$ has exactly one solution at $y=n\ln(k_{v_i}/k_{t_i})/k_{v_i}-k_{t_i}\in(0,\infty)$. Therefore,

$$Q_n^{(i)}(y)<0\Leftrightarrow y<\frac{n\ln\left(\frac{k_{v_i}}{k_{t_i}}\right)}{k_{v_i}-k_{t_i}}. \qquad (64)$$

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 *Proc. Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, 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] Q. Peng, P. Cosman, and L. Milstein, "Analysis and simulation of sensing deception in fading cognitive radio networks," in *Proc. Int. Conf. Wireless Commun. Netw. Mobile Comput.*, Sep. 2010, pp. 1–4.

[5] Q. Peng, P. Cosman, and L. Milstein, "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 *Proc. IEEE Symp. New Frontiers Dyn. Spectr. Access Netw.*, 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] H. Li and Z. Han, "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 *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, Aug. 2012, pp. 371–376.

[11] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I. Rockville, MD, USA: Computer Science, 1985.

[12] B. Wang, Y. Wu, K. Liu, and T. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[13] W. Conley and A. Miller, "Cognitive jamming game for dynamically countering ad hoc cognitive radio networks," in *Proc. IEEE MILCOM Conf.*, Nov. 2013, pp. 1176–1182.

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

[15] A. Erdelyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi, *Tables of Integral Transforms*, vol. 1. New York, NY, USA: McGraw-Hill, 1954, ser. Bateman Manuscript Project, California Institute of Technology.

[16] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions*. New York, NY, USA: Dover, 1970.

[17] L. Rastrigin, "The convergence of the random search method in the extremal control of a many parameter system," *Autom. Remote Control*, vol. 24, no. 11, pp. 1337–1342, 1963.

Madushanka Soysa (S'09) received the B.Sc. degree in engineering (with first-class honor) from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009 and the M.Sc. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2011. He is currently working toward the Ph.D. degree in electrical and computer engineering with the University of California at San Diego, La Jolla, CA, USA.

From 2009 to 2011, he was with the University of Alberta, working on cooperative communication systems with channel outdates. In 2013, he was with the University of Oulu, Oulu, Finland, working on filter bank multicarrier systems. His research interests include cooperative communications, cognitive radio networks, and image and video processing. He received a best paper award at the IEEE ICC 2012.

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

During 1993–1995, she was an NSF Postdoctoral Fellow with Stanford University and a Visiting Professor with the University of Minnesota, Minneapolis, MN, USA. In 1995, she joined the Faculty of the Department of Electrical and Computer Engineering at the University of California at San Diego, La Jolla, CA, where she is currently a Professor and Associate Dean for Students of the Jacobs School of Engineering. From 2006 to 2008, she was the Director of the Center for Wireless Communications. Her research interests include image and video compression and processing and wireless communications.

Dr. Cosman's awards include the ECE Departmental Graduate Teaching Award, a Career Award from the National Science Foundation, a Powell Faculty Fellowship, the Globecom 2008 Best Paper Award, and the HISB 2012 Best Poster 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 has been a member of the Technical Program Committee or the Organizing Committee for numerous conferences, including ICIP 2008–2011, QOMEX 2010–2012, ICME 2011–2013, VCIP 2010, PacketVideo 2007–2013, WPMC 2006, ICISP 2003, ACIVS 2002–2012, ICC 2012, Asilomar Conference on Signals, Systems and Computers 2003, and EUSIPCO 1998. 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, 2010–2013) 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, USA, 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, CA, USA, where he is a Distinguished Professor and the Ericsson Professor of Wireless Communications Access Techniques. He is a former Department Chairman and works in the area of digital communication theory with special emphasis on spread-spectrum communication systems. He has been also a consultant to both government and industry in the areas of radar and communications.

Dr. Milstein was an Associate Editor of Communication Theory for the IEEE TRANSACTIONS ON COMMUNICATIONS, an Associate Editor of Book Reviews for the IEEE TRANSACTIONS ON INFORMATION THEORY, an Associate Technical Editor of the *IEEE Communications Magazine*, and the Editor-in-Chief of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He has been a member of the Board of Governors of both the IEEE Communications Society and the IEEE Information Theory Society and was the Vice President for Technical Affairs in 1990 and 1991 of the IEEE Communications Society. He is a former Chair of the IEEE Fellows Selection Committee and was 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 Communications Society Armstrong Technical Achievement Award, and various prize paper awards. He was also the recipient of the IEEE Communications Theory Technical Committee (CTTC) Service Award in 2009 and the CTTC Achievement Award in 2012.