Disruptive Attacks on Video Tactical Cognitive Radio Downlinks

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

***Abstract*—We consider video transmission over a mobile cognitive radio (CR) system operating in a hostile environment where an intelligent adversary tries to disrupt communications. We investigate the optimal strategy for spoofing, desynchronizing, and jamming a cluster-based CR network with a Gaussian noise signal over a slow Rayleigh fading channel. The adversary can limit access for secondary users (SUs) by either transmitting a spoofing signal in the sensing interval, or a desynchronizing signal in the code acquisition interval. By jamming the network during the transmission interval, the adversary can reduce the rate of successful transmission. We show how the adversary can optimally allocate its energy across subcarriers during sensing, code acquisition, and transmission intervals. We determine a worst-case optimal energy allocation for spoofing, desynchronizing, and jamming, which gives an upper bound to the received video distortion of SUs. We also propose cross-layer resource allocation algorithms and evaluate their performance under disruptive attacks.**

***Index Terms*—Cognitive radio, intelligent adversary, H.264/AVC, cross-layer optimization.**

I. Introduction

COGNITIVE radio (CR) [1], which allows dynamic spectrum access, has been widely investigated as a solution to the limited available spectrum and the inefficiency in spectrum usage. In CR systems, 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 that a licensed band is unused by PUs, 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 can transmit a spoofing signal during the sensing interval [2]. The SU might mistakenly conclude that the channel is occupied by a PU and not available for transmission. Such exploitations and their impact are discussed in [3]–[10].

Further, the adversary can disrupt communications using jamming techniques during the data transmission phase of the communication [11]. Direct sequence spread spectrum code division multiple access (DS-CDMA) offer resistance against jamming and is widely used in tactical communication networks. In DS-CDMA, the data is multiplied by a spreading sequence before transmission. At the receiver, the received signal is multiplied by the same sequence to retrieve the original data. Acquiring the correct phase of the sequence by the receiver (i.e. code acquisition), thus synchronizing itself with the transmitter, is critical for this process. Therefore, another way to attack is to transmit an interfering signal to degrade the performance of the code acquisition receiver. We call this a desynchronizing attack.

In this work, we analyze the impact of an intelligent adversary on a tactical, spread spectrum, CR system transmitting video in H.264/AVC format. 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 [12] to obtain spoofing performance under Nakagami-m fading. In [5] and [13], the optimal power allocation for spoofing and jamming was investigated under an AWGN channel, and Rayleigh fading, respectively. In [5], [13], a generic communication network was studied, and the adversary was optimized to minimize the network throughput. In this paper, we investigate H.264 video communication, and use the received video distortion as the performance metric. In [5], [13], channel sensing was done only at the cluster head. In this paper, we extend it to distributed sensing. In [5], [13], users were assigned equal numbers of subcarriers chosen at random. In the current paper we discuss several resource allocation methods and investigate performance for each of those algorithms. The main contributions of the current paper are: (i) Worst-case analysis of three modes of attack; spoofing, desynchronizing and jamming, (ii) Investigating video performance under hostile conditions, (iii) Evaluating various resource allocation algorithms and (iv) Proving the optimality of an attacking strategy based on a set of sufficient conditions. The set of sufficient conditions of the performance metrics (e.g. probability of false detection, probability of packet error) enables us to prove that the optimal attacking strategy of an adversary is to use equal-power, partial-band interference at low interference power, and as interference power increases, transition to equal-power, full-band interference, and then, while retaining full-band interference, transition multiple times from equal-power, to unequal-power, to equal-power, and so on. These transitions are due to the performance metric function transitioning between convex and concave regions.

In Section II, we present the system model, and derive performance metrics as functions of spoofing, desynchronizing or

Manuscript received August 27, 2015; revised December 3, 2015; accepted February 16, 2016. Date of publication February 26, 2016; date of current version April 13, 2016. This work was supported by the Army Research Office under Grant W911NF-14-1-0340. The associate editor coordinating the review of this paper and approving it for publication was H. Li.

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.2016.2535257

jamming power. Sections III, IV and V discuss the optimization of spoofing, desynchronizing and jamming, respectively. In Section VI, we discuss the optimal energy allocation among the different modes of attack. Section VII contains system simulations and Section VIII presents the conclusions. In Appendix I, we present the optimization approach.

II. System Model

We analyze four main subcomponents of the system; sensing, code acquisition, resource allocation and data transmission. In Subsection II-A, we present the sensing subsystem, and in Subsection II-B the code acquisition subsystem is discussed. In Subsection II-C, we describe the resource allocation algorithms. The transmission and receiver blocks are discussed in Subsection II-D. In Subsection II-E, the information available at the adversary is presented.

We investigate the impact of an adversary on the downlink of a cluster-based SU network. The cluster head (CH) serving SUs transmits video to the SUs over a multicarrier DS-CDMA (MC-DS-CDMA) system with N_T bands (or subcarriers). The N_T bands are shared among PUs and SUs. The system has periodic sensing intervals (T_0), each followed by a code acquisition interval (T_1) and a transmission interval (T_2). *Vacant bands* are ones unoccupied by PUs. *Busy bands* are bands that the SU network cannot use due to PU activity. All SUs perform spectrum sensing, and detect which bands are occupied during the sensing interval. This information is sent to CH and the bands detected as vacant by all SUs is the set of *allowed bands*. Then, CH broadcasts a known spreading sequence in all allowed bands during the code acquisition interval, which is used by the SUs for code acquisition and channel estimation. The estimated channel state information (CSI) and the rate-distortion curve of each SU are sent to CH via a secure feedback channel. This information is used by CH for channel allocation among SUs. The SUs then communicate during the transmission interval.

The adversary uses Gaussian noise signals when it spoofs, desynchronizes and jams, which undergo slow Rayleigh fading. The average gain of the channel from the adversary to user u_j in the i-th band is assumed to have the form $\bar{\alpha}_J^{(u_j)} = 10^{-\upsilon_{u_j}}\bar{\alpha}_J$, where $\upsilon_{u_j} \sim \mathcal{N}(0, \sigma_\upsilon^2)$. We assume all channels experience slow Rayleigh fading and are mutually independent. The distortion of the received video of user u_j is a function of the source rate (r_{u_j}) and the probability of packet error (e_{u_j}) during the transmission interval. Let $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ denote the average distortion of u_j. The function $f_D^{(u_j)}$ is dependent on the temporal and spatial correlation of the video. Let $B = \{1, 2, \ldots, N_T\}$ be the set of bands, and $B_{pu} \subseteq B$ be the set of bands occupied by PUs in a given transmission interval.

A. Sensing System Model

SUs use energy detectors for sensing [13, Fig. 2]. From [13], the energy detector output $Y_i^{(u_j)}(t) \sim \mathcal{N}\Big(T_0 W (\alpha_{J,i}^{(u_j)}\eta_{s,i} + N_0), T_0 W (\alpha_{J,i}^{(u_j)}\eta_{s,i} + N_0)^2\Big)$, where W is the bandwidth of one subcarrier, $\alpha_{J,i}^{(u_j)}$ is the gain of the channel from the adversary to u_j in the i-th band, $\frac{\eta_{s,i}}{2}$ is the power spectral density (PSD) of the spoofing signal in the i-th band, $\frac{N_0}{2}$ is the background noise PSD and $\alpha_{J,i}^{(u_j)}$ is exponentially distributed with mean $\bar{\alpha}_J^{(u_j)}$. This output is compared to the threshold $K\sqrt{T_0 W}$ by u_j to determine if the i-th band is vacant, and this information is communicated to CH. The threshold $K\sqrt{T_0 W}$ is selected to meet a predetermined target false alarm probability[1]. The i-th band is determined to be vacant if all SUs detect it as vacant. Therefore, a band will be falsely detected as occupied if $Y_i^{(u_j)}(t) > K\sqrt{T_0 W}$ for any $u_j \in U_{al}$, where U_{al} is the set of secondary users. The average probability of such a *false detection* is

$$\Pr\left(\bigcup_{u_j \in U_{al}} \left(Y_i^{(u_j)}(t) > K\sqrt{T_0 W}\right)\right) = 1 - \prod_{u_j \in U_{al}} \Pr\left(Y_i^{(u_j)}(t) < K\sqrt{T_0 W}\right) \tag{1}$$

Using [13, Eq. 5], we have $\Pr\Big(Y_i^{(u_j)}(t) < K\sqrt{T_0 W}\Big) = 1 - \frac{1}{\bar{\alpha}_J^{(u_j)}}\int_0^\infty Q\left(\frac{K}{\eta_{s,i}y + N_0} - \sqrt{T_0 W}\right)e^{\frac{-y}{\bar{\alpha}_J^{(u_j)}}}\,\mathrm{d}y$. Substituting this in (1), and using $\eta_{s,i} = \frac{P_{S,i}}{W}$, we can express the average probability of false detection in the i-th band ($p_{fd}(P_{S,i})$), where the spoofing signal power is $P_{S,i}$, as follows:

$$p_{fd}(P_{S,i}) = 1 - \prod_{u_j \in U_{al}}\left(1 - \frac{1}{\bar{\alpha}_J^{(u_j)}}\int_0^\infty Q\left(\frac{K}{\frac{P_{S,i}}{W}y + N_0} - \sqrt{T_0 W}\right)e^{-\frac{y}{\bar{\alpha}_J^{(u_j)}}}\,\mathrm{d}y\right) \tag{2}$$

B. Code Acquisition Block Analysis

Following the sensing interval, CH broadcasts a known sequence of chips in all allowed bands. SUs use this broadcasted sequence for coarse acquisition. For code acquisition, CH transmits the signal $x_i(t) = \left\{\sqrt{2E_c}\sum_{n=0}^{k_{acq}N_c^{acq}-1} c_n g(t - nT_c)\cos(\omega_c t)\right\}$ in the i-th band, where $\{c_n\}$ is the binary spreading sequence with chip duration T_c, $k_{acq}N_c^{acq}T_c$ is the code acquisition period, E_c is the chip energy, ω_c is the carrier frequency and $g(t)$ is a root raised cosine chip-wave shaping filter defined in [13, Eq.7]. The received signal at user u_j in the i-th band is

$$y(t) = \sqrt{2\alpha_{S,i}^{(u_j)}E_c}\sum_{n=0}^{k_{acq}N_c^{acq}-1} c_n g(t - t_d - nT_c) \times \cos\left(\omega_c(t - t_d) - \phi_{S,i}^{(u_j)}\right) + \sqrt{\alpha_{J,i}^{(u_j)}}\,n_{J,i}(t) + n_{w,i}(t) \tag{3}$$

where $\alpha_{S,i}^{(u_j)}$ and $\phi_{S,i}^{(u_j)}$ are the gain and phase components of the channel from CH to u_j in the i-th band. The gain of the

[1] A false alarm is detecting a vacant band as being occupied by a primary user, due to background noise.

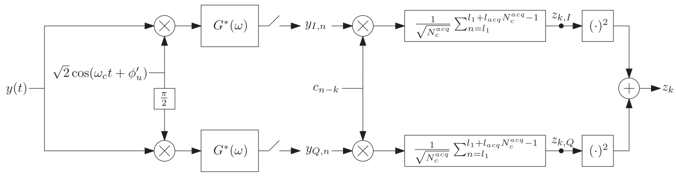


Fig. 1. Code acquisition block.

jammer-to-u_j channel is $\alpha_{J,i}^{(u_j)}$. The channel gains $\alpha_{S,i}^{(u_j)}$ and $\alpha_{J,i}^{(u_j)}$ are exponential random variables (r.v.) with means $\bar{\alpha}_S^{(u_j)}$ and $\bar{\alpha}_J^{(u_j)}$, respectively. The background noise $n_{w,i}(t)$ is AWGN with a double-sided PSD $\frac{N_0}{2}$, and $\sqrt{\alpha_{J,i}^{(u_j)}}\, n_{J,i}(t)$ is the received jamming signal, where $n_{J,i}(t)$ is Gaussian with PSD $\frac{\eta_{J,i}}{2}$ in the i-th band. The propagation delay is t_d.

We use the receiver block shown in Fig. 1 for code acquisition. The received signal $y(t)$ is sent through two down-converters (multiplied by $\cos(\omega_c t + \phi_u')$ and $\sin(\omega_c t + \phi_u')$), and root-raised-cosine matched filters. The output sequences from the matched filters ($y_{I,n}$ and $y_{Q,n}$) are sampled at a frequency of $\frac{1}{T_c}$, and stored for processing in the next step. The matched filter output sequences are despread using shifted versions of the c_n sequence (c_{n-k}). For despreading, we use the samples with indices from l_1 to $l_1 + l_{acq} N_c^{acq} - 1$. Here, we use $l_{acq} (\geq 1)$ repetitions of the spreading sequence in the summation to improve the probability of successful code acquisition, and we select l_1 and l_{acq}, such that the broadcast signal is present throughout the despreading interval. Because the SU knows T_0, an approximate estimate for the maximum distance to CH and an estimate for the maximum delay spread for the channel, the SU can pick l_1 and l_{acq} that satisfy the above constraint for a sufficiently large T_1. The despread samples ($z_{k,I}$ and $z_{k,Q}$) from the two signal paths are squared and summed to obtain the output sample z_k.

The output z_k has a signal component from CH, background noise component and desynchronizing signal component from the adversary. We make the simplifying assumption that the signal components are non-zero only when $|kT_c - t_d| < \frac{T_c}{2}$ [14]. For this, it is necessary to have a spreading sequence that is orthogonal to its time-shifted versions. Let k^* be the correct phase of the code. We can show that z_{k^*} is an exponential r.v. with mean $l_{acq}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)$. Here, ζ_d depends on t_d mod T_c and the pulse-shaping filter. From numerical evaluation of the autocorrelation of the root-raised cosine pulse, it can be shown that $\zeta_d \in [0.63, 1]$. We can also show that z_k is an exponential r.v. with mean $l_{acq}(\alpha_{J,i}^{(u_j)} \eta_{J,i} + N_0)$, for $k \neq k^*$.

The probability of code acquisition, conditioned on $\alpha_{J,i}^{(u_j)}$, is $\Pr(z_{k^*} > z_k|\alpha_{J,i}^{(u_j)}),\ \ \forall\, k \neq k^*, k \in \{0, 1, \ldots, N_c^{acq} - 1\}$. Therefore, the probability of a code acquisition failure is

$$\Pr\left(\bigcup_{k\in\{0,\ldots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(u_j)}\right) \geq \Pr\left(z_{k^*} < z_k|\alpha_{J,i}^{(u_j)}\right)$$
$$= \int_0^\infty \Pr\left(z_{k^*} < x|\alpha_{J,i}^{(u_j)}\right) f_{z_k|\alpha_{J,i}^{(u_j)}}(x)\, \mathrm{d}x \tag{4}$$

where $f_{z_k|\alpha_{J,i}^{(u_j)}}(x)$ is the pdf of z_k conditioned on $\alpha_{J,i}^{(u_j)}$, $f_{z_k|\alpha_{J,i}^{(u_j)}}(x) = \frac{1}{l_{acq}(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)} e^{\frac{-x}{l_{acq}(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)}}$, and $\Pr\left(z_{k^*} < x|\alpha_{J,i}^{(u_j)}\right) = 1 - e^{-\frac{x}{l_{acq}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)}}$. Substituting these in (4), we obtain

$$\Pr\left(\bigcup_{k\in\{0,\ldots,N_c^{acq}-1\}-k^*} z_{k^*} < z_k|\alpha_{J,i}^{(u_j)}\right)$$
$$\geq \int_0^\infty \left(1 - e^{\frac{-x}{l_{acq}(\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} + \alpha_J \eta_J + N_0)}}\right) \frac{e^{-\frac{x}{l_{acq}(\alpha_J\eta_J+N_0)}}}{l_{acq}(\alpha_J \eta_J + N_0)}\, \mathrm{d}x$$
$$= \frac{1}{\left(\frac{l_{acq}\zeta_d^2 E_c N_c^{acq} \bar{\alpha}_S^{(u_j)}}{(\alpha_{J,i}^{(u_j)}\eta_{J,i}+N_0)} + 2\right)} \tag{5}$$

Let $p_{cqf}(P_{ds,i})$ be the average probability of code acquisition failure, averaged over $\alpha_{J,i}^{(u_j)}$, where $P_{ds,i}$ is the desynchronizing power in the i-th band. Note that $\eta_{J,i} = \frac{P_{ds,i}}{W}$. Using (5),

$$p_{cqf}(P_{ds,i}) \geq \int_0^\infty \frac{1}{\left(\frac{\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)}}{\alpha_{J,i}^{(u_j)} \frac{P_{ds,i}}{W} + N_0} + 2\right)} \times \frac{e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}}}{\bar{\alpha}_J^{(u_j)}}\, \mathrm{d}\alpha_{J,i}^{(u_j)} \tag{6}$$

$$= \frac{1}{2}\left(1 + \frac{\zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} W}{2\bar{\alpha}_J^{(u_j)} P_{ds,i}} e^{\frac{2N_0 W + \zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} W}{2\bar{\alpha}_J^{(u_j)} P_{ds,i}}}\right.$$
$$\left. \times \mathrm{Ei}\left(-\frac{2N_0 W + \zeta_d^2 l_{acq} E_c N_c^{acq} \bar{\alpha}_S^{(u_j)} W}{2\bar{\alpha}_J^{(u_j)} P_{ds,i}}\right)\right) \tag{7}$$
$$\triangleq p_{cqf,lb}(P_{ds,i})$$

where $\mathrm{Ei}(\cdot)$ is the exponential integral function and $p_{cqf,lb}(P_{ds,i})$ is a lower bound to $p_{cqf}(P_{ds,i})$.

C. User Allocation Methods

Let $B_{al} \subseteq B$ be the set of allowed bands in the current sensing interval, and let α be the $|B_{al}| \times |U_{al}|$ matrix, where $\alpha[i][j]$ is the channel gain of the j-th user in the i-th band. The maximum transmit power in a subcarrier is $P_{Tx,max}$, and P_{Rx} is the target received power per stream. The number of spreading sequences available in each band is N_{ss}, and the maximum number of spreading sequences needed for user j ($N_{sc,\max}[j]$) is determined by the video properties, such as the temporal correlation among frames and the spatial correlation within the frames. Lower temporal and spatial correlations would increase the number of spreading sequences required to maintain the same video quality.

One user allocation method is simple multi-user diversity, where each band is assigned to the user with the best channel gain in that band. The algorithm is given in Fig. 2. We use P_{sc}

procedure MUD_ALLOC $(\alpha, U_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, N_{sc,\max}, N_{ss})$
  $U'_{al} \leftarrow U_{al}$
  $B'_{al} \leftarrow B_{al}$
  while $|U'_{al}| > 0$ **do** ▷ While set of users to be assigned a channel is non-empty
    if $\sum_{k \in U_{al}} C_{al}[i][k] \geq N_{ss}$ **then**
      $B'_{al} \leftarrow B'_{al} - \{i\}$ ▷ Remove band if all spreading sequences are assigned
    end if
    $(i, j) \leftarrow \underset{j \in U'_{al}, i \in B'_{al}}{\arg\max} \left\{ \alpha[i][j] \middle| P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} \leq P_{Tx,\max} \right\}$ ▷ Select best channel & user
    $C_{al}[i][j] \leftarrow C_{al}[i][j] + 1$ ▷ Update channel assignment matrix
    $P_{sc}[i] \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]}$ ▷ Update transmit power in selected (i-th) band
    if $\sum_{k \in B_{al}} C_{al}[k][j] \geq N_{sc,\max}[j]$ **then**
      $U'_{al} \leftarrow U'_{al} - \{j\}$ ▷ Remove user if max. no. of channel allocations is met
    end if
    $U'_{al} \leftarrow \left\{ j \middle| \max_{i \in B_{al}} \left(P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} \right) \leq P_{Tx,\max},\ j \in U'_{al} \right\}$ ▷ Update set of users
  end while
  return $\{C_{al}, P_{sc}\}$
end procedure

Fig. 2. MUD algorithm for user allocation.

procedure MX_ALLOC $(\alpha, U_{al}, B_{al}, P_{Rx}, P_{Tx,\max}, N_{ss}, \vartheta)$
  $U''_{al} \leftarrow U_{al}$
  $C_{al} \leftarrow \mathbf{0}_{|U_{al}| \times |B|}$
  $P_{sc} \leftarrow \mathbf{0}_{|B| \times 1}$
  while $|U''_{al}| > 0$ **do**
    $\{C_{al}, P_{sc}\} \leftarrow$ MUD_ALLOC $(\alpha, U''_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, 1, N_{ss})$
    Calculate D_{su}; the video distortion of users with current channel allocation C_{al}.
    $U'_{al} \leftarrow \left\{ j \middle| \max_{i \in B_{al}} \left(P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} \right) \leq P_{Tx,\max}, j \in U_{al} \right\}$
    Select $U''_{al} \subseteq U'_{al}$; up to $\vartheta |U_{al}|$ users with largest video distortion (D_{su})
  end while
  return C_{al}
end procedure

Fig. 3. Algorithm 'MXD' for user allocation.

to keep track of the transmit power in each subcarrier, and C_{al}, a $|B| \times |U_{al}|$ matrix, to keep track of the user-subcarrier assignment. A second algorithm, named MXD, iteratively assigns additional subcarriers to the set of users with the maximum distortion, and is given in Fig. 3. After the initial assignment from either of the above algorithms, the swapping algorithm in Fig. 4 can be used to check if changing a channel assignment from one user to another will decrease the sum distortion of all users.

D. Transmission System Model

The transmitter and receiver models are adapted from [13]. Low density parity check (LDPC) codes are used for FEC. We assume the users in the downlink are synchronized at the transmitter, and hence the interference can be removed by using mutually orthogonal spreading codes (e.g., Walsh-Hadamard codes). We consider a slow fading environment, where the channel remains constant over one transmission interval. We assume the transmitter has perfect CSI at the beginning of the transmission interval. The transmitter selects the average symbol energy (E_s) so that the received SNR is maintained at a constant γ_S for all users. If the required transmit power exceeds a predetermined threshold, we do not transmit to that user in that channel, in accordance with the resource allocation algorithms discussed in Subsection II-C.

Following the approach in Section II-B in [13], we can show that the received instantaneous SINR of user u_j at the k-th symbol detection in the i-th band is $\gamma_{i,k}^{(u_j)} = \frac{\gamma_S}{\alpha_{J,i,k}^{(u_j)} \bar{\gamma}_{J,i} + 1}$, where $\alpha_{J,i,k}^{(u_j)}$ is the gain of the adversary-to-u_j channel, $\bar{\gamma}_{J,i} = \frac{P_{J,i}}{N_0 W}$ and $P_{J,i}$ is the jamming power allocated for the i-th subcarrier. The channel gain $\alpha_{J,i,k}^{(u_j)}$ is exponentially distributed with average $\bar{\alpha}_J^{(u_j)}$. To obtain an approximation for the packet error rate, the adversary models the probability of word error with a step function of the SINR [13]:

$$\Pr(\text{packet error}) = \begin{cases} 0, & \text{if } \gamma_{i,k}^{(u_j)} > \gamma_T \\ 1, & \text{if } \gamma_{i,k}^{(u_j)} \leq \gamma_T \end{cases} \tag{8}$$

where $\gamma_{i,k}^{(u_j)}$ is the instantaneous SINR at the receiver, and γ_T is a threshold dependent on the alphabet and FEC used. We consider a system using a single alphabet size and LDPC coding rate. Through simulations of word error rates of an ensemble of LDPC rate $\frac{1}{2}$ codes of code length L_p, γ_T is estimated. Therefore, from (8), the probability of packet error is

$$\begin{aligned} \Pr(\text{packet error}) &= \Pr\left(\frac{\gamma_S}{\alpha_{J,i,k}^{(u_j)} \bar{\gamma}_{J,i} + 1} < \gamma_T \right) \\ &= \frac{1}{\bar{\alpha}_J^{(u_j)}} \int_{\frac{1}{\bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1 \right)}^{\infty} e^{-\frac{x}{\bar{\alpha}_J^{(u_j)}}} \, dx \\ &= e^{-\frac{1}{\bar{\alpha}_J^{(u_j)} \bar{\gamma}_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1 \right)} \end{aligned} \tag{9}$$

The expected number of packet errors of user u_j in the i-th band $N_{e,u_j,i}(P_{J,i})$, is

$$N_{e,u_j,i}(P_{J,i}) = N_p \Pr(\text{packet error}) = N_p e^{-\frac{N_0 W}{\bar{\alpha}_J^{(u_j)} P_{J,i}} \left(\frac{\gamma_S}{\gamma_T} - 1 \right)} \tag{10}$$

procedure SWAP_ALLOC $(\alpha, U_{al}, B_{al}, C_{al}, P_{sc}, P_{Rx}, P_{Tx,\max}, \max\_it)$
  $iter \leftarrow 0$
  while $iter < \max\_it$ **do**
    Calculate $D_{su}^{(0)}[j]$; video distortion of j with current channel allocation, $\forall j \in U_{al}$.
    Calculate $D_{su}^{(1)}[j]$; Distortion of j with one additional channel allocation, $\forall j \in U_{al}$.
    for $i \in B_{al}$ **do**
      for $j \in U_{al}$ **do**
        $p_{sc} \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i][j]} - P_{Tx,max}$
        for $k \in U_{al} - \{j\}$ **do**
          $c_{sc,l} \leftarrow \left\lceil \frac{p_{sc}\alpha[i][k]}{P_{Rx}} \right\rceil$
          if $c_{sc,l} \leq C_{al}[i][k]$ **then**
            $c_{sc}[k] \leftarrow \sum_{i \in B_{al}} C_{al}[i][k] - c_{sc,l}$
            Calculate $D_{su}^{(-1)}[k]$; distortion of k with $c_{sc}[k]$ channel allocations.
            $\Delta D_{su}[i][k][j] \leftarrow (D_{su}^{(1)}[j] + D_{su}^{(-1)}[k]) - (D_{su}^{(0)}[j] + D_{su}^{(0)}[k])$
          else
            $\Delta D_{su}[i][k][j] \leftarrow 0$
          end if
        end for
      end for
    end for
    if $\min \Delta D_{su}[i][j][k] < 0$ **then**
      $(i', j', k') \leftarrow \underset{j,k \in U_{al}; i \in B_{al}}{\arg\max} \Delta D_{su}[i][k][j]$
      $C_{al}[i'][j'] \leftarrow C_{al}[i'][j'] + 1$
      $C_{al}[i'][k'] \leftarrow C_{al}[i'][k'] - \left\lceil \left(\frac{P_{sc}[i]}{P_{Rx}} + \frac{1}{\alpha[i'][j']} - \frac{P_{Tx,max}}{P_{Rx}} \right) \alpha[i'][k'] \right\rceil$
      $P_{sc}[i] \leftarrow P_{sc}[i] + \frac{P_{Rx}}{\alpha[i'][j']} - \left\lceil \left(\frac{P_{sc}[i]}{P_{Rx}} + \frac{1}{\alpha[i'][j']} - \frac{P_{Tx,max}}{P_{Rx}} \right) \alpha[i'][k'] \right\rceil \frac{P_{Rx}}{\alpha[i'][k']}$
    else
      return C_{al}
    end if
    $iter \leftarrow iter + 1$
  end while
  return C_{al}
end procedure

Fig. 4. Algorithm to swap subcarriers between users to decrease sum distortion.

where N_p is the number of packets of a single user in a single band per transmission interval.

E. 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 distortion (or mean square error (MSE)) of the received video as the performance metric. The objective of the adversary is to maximize $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$.

In this work we assume that the system design parameters and statistical averages of system parameters are known by the adversary, but that knowledge of instantaneous system parameters is not available for the adversary, in accordance with previous work [3]–[5], [13]. Because a practical adversary does not have all the assumed knowledge, the work done here is a worst-case analysis, which gives an upper bound to the distortion with jamming and spoofing.

1) System Design Parameters: We assume that the adversary is aware of the bandwidth of the waveform, sensing, code acquisition and transmission times, receiver structure and system false alarm probability i.e., the probability of false detection caused only due to background noise with no spoofing. The SNR of SUs, which is maintained constant by the CH through power control, is also 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.

2) Statistical Averages of System Parameters: We assume that the adversary knows the PSD of the background noise, and that all links undergo Rayleigh fading. We assume that the adversary can estimate $\bar{\alpha}_J$ using a path loss model and the physical distance to the SU cluster, even though the adversary does not know the actual average gain on the channels to individual SUs. We also assume that the adversary knows the average number of SUs and the average number of bands occupied by PUs.

3) Instantaneous System Parameters: We do not assume the adversary knows which channels are occupied by PUs at the start of the sensing interval, which channels each user is assigned to, or other instantaneous values of time-varying system parameters (e.g., channel gains).

III. Spoofing Power Optimization

During the sensing interval, the adversary attacks the system by spoofing to reduce the transmission rate available to SUs by reducing the bandwidth available to them. The adversary aims to maximize the following objective function:

$$\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j}) = \sum_{\forall u_j} f_D^{(u_j)} \left(\sum_{i \in B(u_j)} r_{u_j,i}, e_{u_j} \right). \quad (11)$$

where $B(u_j)$ is the set of bands allocated for u_j, and $r_{u_j,i}$ is the data rate of u_j in the i-th band.

The average distortion decreases monotonically with the source rate (r_{u_j}) and increases monotonically with the probability of packet error (e_{u_j}). Therefore, there are two ways to increase distortion by spoofing; by making the SUs decrease the source rate or increase the error rates.

Increasing distortion by decreasing the source rate: Successful spoofing can directly decrease the source rate by limiting SU access to vacant channels. To maximize the objective function in (11) by reducing the source rate, the adversary needs to minimize $\sum_{i \in B(u_j)} r_{u_j,i}$. Note that $B(u_j)$ and $r_{u_j,i}$ depend on the resource allocation algorithms, channel gains, video properties and the set of bands detected as vacant (B_{al}). Out of these parameters, the adversary can only influence B_{al}. Therefore, we use minimizing $|B_{al}|$ as the objective of the adversary.

Increasing distortion by increasing the probability of packet error: The probability of packet error e_{u_j} is not directly affected by spoofing, but is increased by jamming. But the effectiveness of jamming increases when the number of transmitting bands is decreased, so minimizing $|B_{al}|$ will also increase e_{u_j}, thus increasing the distortion.

Therefore, maximizing the distortion in (11) through spoofing is equivalent to minimizing $|B_{al}|$. Conditioned on $B - B_{pu}$, the average number of bands detected as allowed by CH is $\sum_{i \in B - B_{pu}} (1 - p_{fd}(P_{S,i}))$, where $p_{fd}(P_{S,i})$ is the probability of false detection of the i-th band as a function of the spoofing power ($P_{S,i}$) in the i-th band, given that the i-th band is vacant [3]. Hence, the objective of the adversary is maximizing $\sum_{i \in B - B_{pu}} p_{fd}(P_{S,i})$.

At the start of the sensing interval, the adversary does not know which bands are vacant. From the adversary's perspective, every band has an equal probability of being vacant. Hence, the objective of the adversary is to maximize $\sum_{i=1}^{N_T} p_{fd}(P_{S,i})$, 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. This N_T variable optimization can be reduced to two dimensions, using the behavior of $p_{fd}(P_{S,i})$. We use the theorem in Appendix I Subsection A, to simplify this optimization problem, using the properties **P0** (bounded above) and **P1** (non decreasing and twice differentiable). The adversary's estimate of $p_{fd}(P_{S,i})$ can be obtained from (2) as

$$p_{fd}(P_{S,i}) = 1 - \left(1 - \frac{1}{\bar{\alpha}_J} \int_0^{\infty} Q\left(\frac{K}{\frac{P_{S,i}}{W} y + N_0} - \sqrt{T_0 W}\right) \times e^{-\frac{y}{\bar{\alpha}_J}} \mathrm{d}y\right)^{|U_{al}|} \tag{12}$$

where we use $\bar{\alpha}_J$ as an approximation for $\bar{\alpha}_J^{(u_j)}$. Because $p_{fd}(P_{S,i})$ is a probability, we know that $p_{fd}(P_{S,i}) \leq 1$, and hence bounded above. Therefore, condition **P0** is satisfied. Taking the derivative with respect to $P_{S,i}$:

$$\frac{\mathrm{d}}{\mathrm{d}P_{S,i}} \left(p_{fd}(P_{S,i})\right) = -|U_{al}| \left(1 - \frac{1}{\bar{\alpha}_J} \int_0^{\infty} Q\left(\frac{K}{\frac{P_{S,i}}{W} y + N_0} - \sqrt{T_0 W}\right) e^{\frac{-y}{\bar{\alpha}_J}} \mathrm{d}y\right)^{|U_{al}|-1} \left(\frac{-1}{\bar{\alpha}_J} \int_0^{\infty} \frac{\mathrm{d}Q\left(\frac{K}{\frac{P_{S,i}}{W} y + N_0} - \sqrt{T_0 W}\right)}{\mathrm{d}\left(\frac{K}{\frac{P_{S,i}}{W} y + N_0} - \sqrt{T_0 W}\right)} \times \frac{\mathrm{d}}{\mathrm{d}P_{S,i}} \left(\frac{K}{\frac{P_{S,i}}{W} y + N_0} - \sqrt{T_0 W}\right) e^{-\frac{y}{\bar{\alpha}_J}} \mathrm{d}y\right) > 0 \tag{13}$$

From this, we see that $p_{fd}(P_{S,i})$ has the property **P1**. So, we use Appendix I to maximize $\sum_{i=1}^{N_T} p_{fd}(P_{S,i})$.

IV. Desynchronizing Power Optimization

After the sensing interval, CH determines which bands are allowed for SUs, and broadcasts a spreading sequence for code acquisition during the T_1 interval. The adversary can transmit an interference signal to disrupt the code acquisition process. If the code acquisition fails for an SU, that SU will not be able to estimate the channel gains and will not be assigned subcarriers. Therefore, the video distortion of user u_j is $f_D^{(u_j)}(r_{u_j}, e_{u_j})(1 - p_{cqf}^{(u_j)}) + f_D^{(u_j)}(0,0) p_{cqf}^{(u_j)} = f_D^{(u_j)}(r_{u_j}, e_{u_j}) + p_{cqf}^{(u_j)}(f_D^{(u_j)}(0,0) - f_D^{(u_j)}(r_{u_j}, e_{u_j}))$, where $p_{cqf}^{(u_j)}$ is the probability of code acquisition failure of user u_j. Because $f_D^{(u_j)}(r_{u_j}, e_{u_j}) < f_D^{(u_j)}(0,0)$, in order to maximize the distortion of user u_j through desynchronizing attacks, the adversary must maximize $p_{cqf}^{(u_j)}$.

Each SU tries to acquire the code in all the allowed bands on which the CH is broadcasting. The acquisition in each band is followed by code tracking, and we assume that all incorrect phases will be rejected in the tracking mode. Hence, if the correct code phase is acquired in any band, the SU achieves code acquisition. Therefore, the probability of code acquisition failure is

$$p_{cqf}^{(u_j)} = \prod_{i \in B_{al}} p_{cqf}(P_{ds,i}) \tag{14}$$

where $p_{cqf}(P_{ds,i})$ is the probability of code acquisition failure as a function of desynchronizing power. The adversary aims to maximize $p_{cqf}^{(u_j)}$, which is equivalent to maximizing $\log\left(p_{cqf}^{(u_j)}\right) = \sum_{i \in B_{al}} \log\left(p_{cqf}(P_{ds,i})\right)$. As the adversary is not aware of B_{al}, we modify the objective function to $\sum_{i=1}^{N_T} \log\left(p_{cqf}(P_{ds,i})\right)$. We use the lower bound $p_{cqf,lb}(P_{ds,i})$ derived in (7) in place of $p_{cqf}(P_{ds,i})$, and the objective function to maximize is $\sum_{i=1}^{N_T} \log\left(p_{cqf,lb}(P_{ds,i})\right)$. Taking the derivative of $p_{cqf,lb}(P_{ds,i})$ from (6), with respect to $P_{ds,i}$, we get

$$\frac{\mathrm{d}}{\mathrm{d}P_{ds,i}} \left(p_{cqf,lb}(P_{ds,i})\right) = \int_0^{\infty} \frac{\zeta_d^2 l_{acq} E_c N_c \bar{\alpha}_S^{(u_j)} \alpha_{J,i}^{(u_j)} e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}}}{\left(\zeta_d^2 l_{acq} E_c N_c \bar{\alpha}_S^{(u_j)} + 2(\alpha_{J,i}^{(u_j)} \frac{P_{ds,i}}{W} + N_0)\right)^2 W \bar{\alpha}_J^{(u_j)}} \mathrm{d}\alpha_{J,i}^{(u_j)} > 0 \tag{15}$$

This shows that $p_{cqf,lb}(P_{ds,i})$ is monotonically increasing with $P_{ds,i}$, and property **P1** is satisfied. Therefore, we also know that

$$p_{cqf,lb}(P_{ds,i}) \leq \lim_{P_{ds,i} \to \infty} p_{cqf,lb}(P_{ds,i}) = \int_0^{\infty} \frac{1}{2} \times \frac{1}{\bar{\alpha}_J^{(u_j)}} e^{-\frac{\alpha_{J,i}^{(u_j)}}{\bar{\alpha}_J^{(u_j)}}} \mathrm{d}\alpha_{J,i}^{(u_j)} = \frac{1}{2} \tag{16}$$

This shows that the function is bounded above and has the property **P0**. Further, taking the derivative of (15) with respect to $P_{ds,i}$, we can also show that $\frac{\mathrm{d}^2}{\mathrm{d}P_{ds,i}^2} \left(p_{cqf,lb}(P_{ds,i})\right) < 0$. Because the log function is monotonically increasing, $\log\left(p_{cqf,lb}(P_{ds,i})\right)$ also has the properties **P0** and **P1**. Therefore, we can use the proposed optimization approach to maximize $\sum_{i=1}^{N_T} \log\left(p_{cqf,lb}(P_{ds,i})\right)$. Because $p_{cqf,lb}(P_{ds,i}) \geq 0$ and $\frac{\mathrm{d}^2}{\mathrm{d}P_{ds,i}^2} \left(p_{cqf,lb}(P_{ds,i})\right) < 0$, the second derivative $\frac{d^2}{dP_{ds,i}^2}\left(\log\left(p_{cqf,lb}(P_{ds,i})\right)\right) < 0$. Therefore, from (26), the optimal power allocation is equal power allocation at all desynchronizing power values.

V. Jamming Power Optimization

The objective of the adversary is to maximize $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$, by increasing the probability of packet error e_{u_j}. We know that $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ is an increasing function of e_{u_j}, when r_{u_j} remains constant. Let $B(u_j)$ be the set of subcarriers allocated for user u_j. We assume that the adversary senses and detects the bands used for transmission before jamming, and hence knows $B_{al} \cup B_{pu}$. To simplify the notation, we number the bands such that $B_{al} \cup B_{pu} = \{1, 2, \ldots, N_{Tx}\}$.

A. Lightly Loaded System

In a lightly loaded system, each SU will generally be assigned many subcarriers; i.e. $|B(u_j)| \gg 1$. During one transmission interval, the expected number of packet errors of u_j, $N_{e,u_j} = \sum_{i\in B(u_j)} N_{e,u_j,i}(P_{J,i})$. However, without knowledge of $B(u_j)$, the adversary assumes that each band has an equal probability $\frac{|B(u_j)|}{N_{Tx}}$ of being assigned to u_j. Under this assumption, the expected number of packet errors of u_j during T_1, estimated by the adversary, is

$$N_{e,u_j} = \sum_{i=1}^{N_{Tx}} \left\{\begin{array}{l}\text{Probability band}\\ i \text{ is assigned to}\\ u_j\end{array}\right\} \times \left\{\begin{array}{l}\text{Expected number of}\\ \text{packet errors of } u_j \text{ in}\\ i\text{-th band if assigned}\end{array}\right\}$$
$$= \sum_{i=1}^{N_{Tx}} \frac{|B(u_j)|}{N_{Tx}} N_{e,u_j,i}(P_{J,i}) \tag{17}$$

Using the result in (17), we can calculate the probability of packet error e_{u_j} as follows:

$$e_{u_j} = \frac{\text{Expected number of packet errors}}{\text{Total transmitted packets}} = \frac{\sum_{i=1}^{N_{Tx}} \left(\frac{|B(u_j)|}{N_{Tx}}\right) N_{e,u_j,i}(P_{J,i})}{|B_{u_j}| N_p} = \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx} N_p} \tag{18}$$

We can write the objective function to be maximized from (11) as $\sum_{\forall u_j} f_D^{(u_j)}\left(r_{u_j}, \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx}N_p}\right)$. For any given source rate r_{u_j}, the distortion of a received video increases with the packet error rate. Further, r_{u_j} is affected only by spoofing power, and is unaffected by jamming. Therefore, to maximize $f_D\left(r_{u_j}, \frac{\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})}{N_{Tx}N_p}\right)$, the adversary aims to maximize $\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,i})$, under the constraints $\sum_{i=1}^{N_{Tx}} P_{J,i} = P_T$ and $P_{J,i} \geq 0$.

Using (10), we can write the approximation of the expected number of packet errors calculated by the adversary, $N_{e,i}(P_{J,i})$ as follows:

$$N_{e,i}(P_{J,i}) = N_p e^{-\frac{N_0 W}{\bar{\alpha}_J P_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \tag{19}$$

where we use $\bar{\alpha}_J$ as an approximation for $\bar{\alpha}_J^{(u_j)}$. We use the approach in Appendix I, as $N_{e,i}(P_{J,i})$ satisfies properties **P0** and **P1**.

B. Heavily Loaded System

In this scenario, we assume that, due to heavy PU activity, SUs are often assigned only a single subcarrier; i.e. $|B(u_j)| = 1$. Suppose user u_j is assigned only the i-th band. Using (8), we write the video distortion as: $f_D^{(u_j)}(r_{u_j}, e_{u_j}) = \begin{cases} f_D^{(u_j)}(r_{u_j}, 0), & \text{if} \gamma_{i,k}^{(u_j)} > \gamma_T \\ f_D^{(u_j)}(r_{u_j}, 1), & \text{if} \gamma_{i,k}^{(u_j)} \leq \gamma_T \end{cases}$.

The expected video distortion for u_j is

$$\begin{aligned}
&\mathbb{E}\left[f_D^{(u_j)}(r_{u_j}, e_{u_j})\right] \\
&= f_D^{(u_j)}(r_{u_j}, 0)\Pr(\gamma_{i,k}^{(u_j)} > \gamma_T) + f_D^{(u_j)}(r_{u_j}, 1)\Pr(\gamma_{i,k}^{(u_j)} \leq \gamma_T) \\
&= f_D^{(u_j)}(r_{u_j}, 0) + \left(f_D^{(u_j)}(r_{u_j}, 1) - f_D^{(u_j)}(r_{u_j}, 0)\right)\Pr(\gamma_{i,k}^{(u_j)} \leq \gamma_T) \\
&\approx f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1)\Pr(\gamma_{i,k}^{(u_j)} \leq \gamma_T) \\
&= f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}
\end{aligned} \tag{20}$$

Let $U(i)$ be the set of users in the i-th band. The objective function to maximize is

$$\sum_{\forall u_j} \mathbb{E}\left[f_D^{(u_j)}(r_{u_j}, e_{u_j})\right] = \sum_{i=1}^{N_{Tx}} \sum_{\forall u_j \in U(i)} \left(f_D^{(u_j)}(r_{u_j}, 0) + f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)} \right) \tag{21}$$

The terms $f_D^{(u_j)}(r_{u_j}, 1)$ and $f_D^{(u_j)}(r_{u_j}, 0)$ depend on the properties of the video of user u_j and the source rate r_{u_j}. Different jamming power allocations do not affect those terms, but do affect error rate. Hence, the objective to maximize is $\sum_{i=1}^{N_{Tx}} \sum_{\forall u_j \in U(i)} f_D^{(u_j)}(r_{u_j}, 1) e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}$.

The adversary does not know the instantaneous channel assignment, and assumes each user has a probability $\frac{1}{N_{Tx}}$ of being assigned the i-th band. Hence, taking the expectation over all channel assignments, the function to maximize can be rearranged as $\sum_{\forall u_j} \frac{f_D^{(u_j)}(r_{u_j}, 1)}{N_{Tx}} \sum_{i=1}^{N_{Tx}} e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}$. Now, since only $e^{-\frac{1}{\bar{\alpha}_J^{(u_j)}\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}$ can be changed by jamming, the function reduces to maximizing $\sum_{i=1}^{N_{Tx}} e^{-\frac{1}{\bar{\alpha}_J\bar{\gamma}_{J,i}}\left(\frac{\gamma_S}{\gamma_T}-1\right)}$, where $\bar{\alpha}_J$ approximates $\bar{\alpha}_J^{(u_j)}$. Since the function satisfies the properties **P0** and **P1**, we use Appendix I to optimally allocate jamming power.

VI. Energy Optimization Among Modes of Attack

Let E_{ad} be the total energy available for the adversary during a $T_0 + T_1 + T_2$ interval. Let θ_{sp} be the fraction of energy allocated for spoofing and let θ_{ds} be the fraction of energy allocated for desynchronizing attacks. We have $E_{sp} = \theta_{sp} E_{ad}$, $E_{ds} = \theta_{ds} E_{ad}$, and $E_{jm} = (1 - \theta_{sp} - \theta_{ds}) E_{ad}$.

The objective of the adversary is to find $(\theta_{sp}, \theta_{ds})$ that maximizes $\sum_{\forall u_j} f_D^{(u_j)}(r_{u_j}, e_{u_j})$. In the separate optimizations of spoofing, desynchronizing, and jamming attacks, we were able to derive objective functions to replace $f_D^{(u_j)}\left(r_{u_j}, e_{u_j}\right)$, using the knowledge that $f_D^{(u_j)}(r_{u_j}, e_{u_j})$ is a monotonically decreasing function of r_{u_j}, and a monotonically increasing function of e_{u_j}, when the other parameters are kept constant. But we now need knowledge of $f_D^{(u_j)}$ to optimize energy allocation among the attacking methods. Because $f_D^{(u_j)}$ depends on the video properties and encoding parameters that are not known by the adversary, we are not able to calculate $f_D^{(u_j)}$ at the adversary. Therefore, we use throughput as an alternative target for this section.

The minimum throughput (worst case throughput) under spoofing, jamming and desyncrhonizing attacks, $\Gamma(\theta_{sp}, \theta_{ds})$, as a function of θ_{sp} and θ_{ds}, can be written as

$$\Gamma(\theta_{sp},\theta_{ds}) = L_p\Big(N_p \tilde{B}_{su}(\theta_{sp}) - \tilde{N}_{er}\Big(1-\theta_{sp}-\theta_{ds}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\Big)\Big)\Big(1 - \tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right)\Big) \tag{22}$$

where $\tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right)$ is the probability of code acquisition failure, $\tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right)$ is the expected number of packet errors under optimized jamming, and $\tilde{B}_{su}(\theta_{sp})$ is the expected number of allowed bands under optimized spoofing. Note that

$$\tilde{B}_{su}(\theta_{sp}) \triangleq \min_{\sum_{i=1}^{N_T} P_{s,i} \le \frac{\theta_{sp} E_{ad}}{T_0}} E\left[|B_{al}|\right] = \frac{(N_T - \overline{|B_{pu}|})}{N_T}\left(N_T - F\left(p_{fd}, \frac{\theta_{sp} E_{ad}}{T_0}, N_T\right)\right) \tag{23}$$

where F is defined in (26), and that

$$\tilde{N}_{er}\left(\theta_{jm}, \tilde{B}_{su}(\theta_{sp}), \overline{|B_{pu}|}\right) \triangleq \max_{\sum_{i=1}^{\tilde{B}_{su}(\theta_{sp})+\overline{|B_{pu}|}} P_{J,i} \le \frac{\theta_{jm} E_{ad}}{T_2}} E\left[\sum_{i \in B_{al}} N_{e,i}^{(u_j)}\right] = \frac{\tilde{B}_{su}(\theta_{sp})}{\tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}} F\left(N_{e,i}, \frac{\theta_{jm} E_{ad}}{T_2}, \tilde{B}_{su}(\theta_{sp}) + \overline{|B_{pu}|}\right) \tag{24}$$

where θ_{jm} is the fraction of energy allocated for jamming. Substituting the desynchronizing power $P_{ds,i} = \frac{\theta_{ds} E_{ad}}{T_1 N_T}$ in (14), we have

$$\tilde{p}_{cqf}\left(\theta_{ds}, \tilde{B}_{su}(\theta_{sp})\right) = \prod_{i=1}^{\tilde{B}_{su}(\theta_{sp})} p_{cqf,lb}^{(u_j)}\left(\frac{\theta_{ds} E_{ad}}{T_1 N_T}\right). \tag{25}$$

Using (22), we find the optimal energy allocation ratios $\left(\theta_{sp}^*, \theta_{ds}^*\right) = \arg\min_{\theta_{sp},\theta_{ds} \in [0,1]} \Gamma(\theta_{sp}, \theta_{ds})$ numerically, from a grid search.

VII. Simulation Results

We consider a cluster-based SU system, sharing N_T DS-CDMA subcarriers with PUs. In the simulations, in each sensing, acquisition, and transmission interval, the PUs occupy $|B_{pu}| = \min(N_{B,pu}, N_T)$ bands at random, where $N_{B,pu}$ is a Poisson r.v. with mean parameter $\bar{N}_{pu}$. We select $\bar{\alpha}_S = \bar{\alpha}_J = 1$, $T_0 = 4T_s$, $T_1 = 16T_s$ and $T_2 = 2048T_s$, where T_s is the symbol time. The number of chips per symbol during the transmission interval (N_c) is 64, $N_c^{acq} = 256$ and $l_{acq} = 4$. We use Walsh-Hadamard codes as spreading sequences, a rate $\frac{1}{2}$ LDPC code with code-block-length 2048 bits, and QPSK modulation. The target probability of false alarm is 0.001 and the target received SNR maintained (γ_S) is 5 dB. We define the jamming-to-signal power ratio (JSR) as the ratio of average received adversary power to received signal power per user per stream.

Each user transmits the 'soccer' video sequence with 4CIF resolution (704×576) at 30 frames per second. The source video is compressed by the baseline profile of H.264/AVC reference software JM 11.0 [15]. The GOP structure is IPP with 15 frames per GOP. Each user starts at a random frame of the video, and the resource allocation decision is done at the start of each GOP. The video performance is evaluated using peak signal-to-noise ratio (PSNR) $\triangleq 10 \log_{10} \frac{255^2}{\mathbb{E}[\mathrm{MSE}]}$.

In Sections III, IV and V, we derived the objective functions that the adversary must attempt to maximize in order to optimally disrupt the communication through spoofing, desynchronizing and jamming, respectively. We use the analysis to find the optimal power allocations, and then use those optimal allocation in the simulation to get the PSNR performance. When there is no knowledge of the system other than its operating frequency range, the adversary can perform equal power attacks across the total bandwidth. We use this equal power spoofing and jamming strategy as our baseline. For desynchronizing attacks, the optimal strategy is an equal-power attack, as shown in Section IV.

1) Spoofing Attacks: Fig. 5 shows the video PSNR, averaged over users, against JSR, for the resource allocation algorithms of Subsection II-C. We plot average PSNR under equal-power spoofing (dashed curves) and optimized worst case spoofing (solid curves).

The MUD algorithm, which only uses physical-layer information for channel allocation, has the worst performance, as it fails to account for the differences in the video properties. MUD+swap has notable gains over MUD, as the swapping enables more subcarriers to be assigned to users with higher motion video. The MXD algorithms perform the best under the simulated parameters.

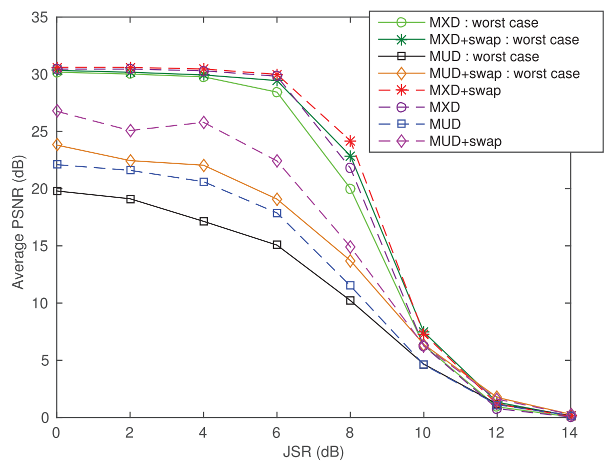
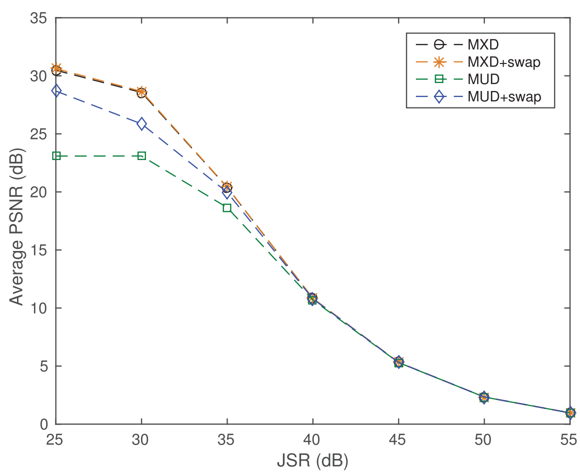
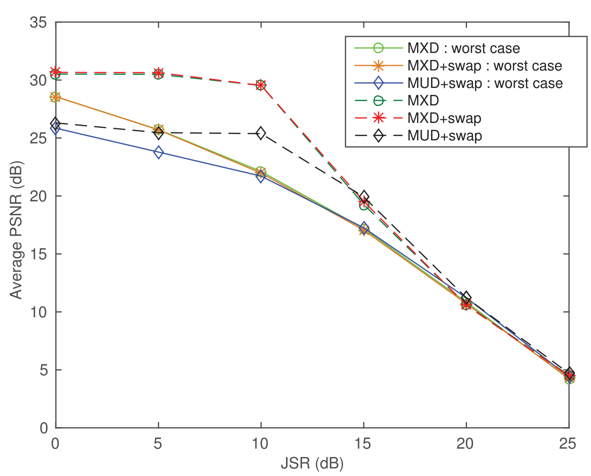


Fig. 5. Average PSNR under spoofing attacks ($N_T = 64$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 16$).

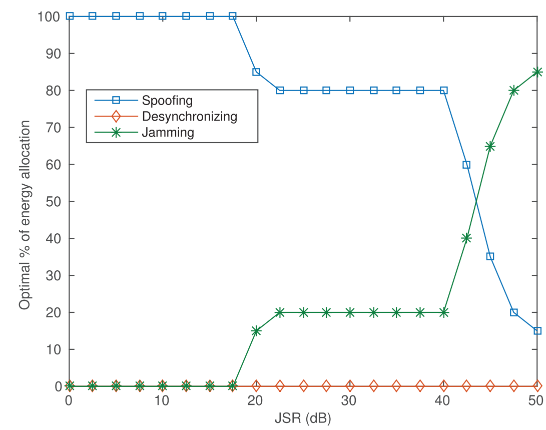


(a)

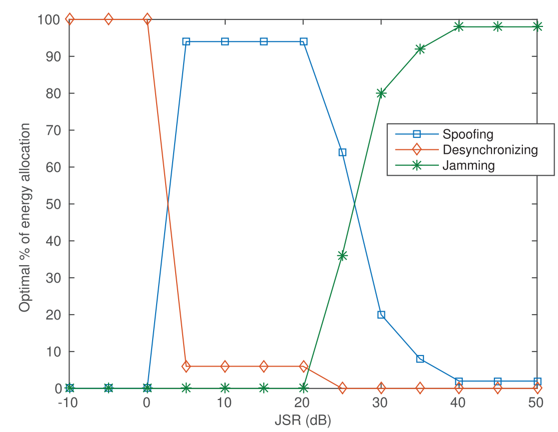


(b)

Fig. 6. Average PSNR vs JSR ($N_T = 64$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 16$): (a) under desynchronizing (b) under jamming.



(a)



(b)

Fig. 7. Optimal energy allocation among the methods of attack: (a) Heavily loaded system ($N_T = 128$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 64$). (b) Lightly loaded system ($N_T = 256$, $\Omega_{su} = 4$, $\bar{N}_{pu} = 32$).

Switching from equal power spoofing to optimized spoofing reduces the average PSNR by 3-4 dB in the MUD algorithms when operating in the 0-6 dB JSR range. However, the MXD based algorithms are not notably affected by optimized spoofing in the same JSR range. It appears that MXD algorithms are more robust against a small bandwidth loss than are MUD algorithms. In MXD, as subcarriers are allocated to the users with maximum distortion first, a subcarrier loss means rate loss for a lower distortion user. But, in MUD, subcarrier loss could hit a high distortion user. Thus, optimizing spoofing at low JSR has a higher impact on MUD. Further simulations with lower rate LDPC codes showed that the PSNR performance under spoofing remains approximately similar, if γ_S is lowered accordingly with the LDPC rate.

2) Desynchronizing Attacks: Fig. 6(a) shows the performance under desynchronizing attacks. There is a steep reduction in PSNR in the JSR range 30-45 dB, due to successful desynchronizing.

3) Jamming Attacks: Fig. 6(b) shows the performance of the system under jamming. Solid curves correspond to optimized jamming and dashed curves represent equal power jamming. The system is unaffected by equal power jamming up to about 10 dB JSR. However, the reduction in PSNR in the solid curves in the 0 to 10 dB region shows that optimized jamming affects the system at a lower JSR compared to equal power jamming. At JSR = 10dB, the average PSNR under MXD algorithms is about 7 dB lower under optimized jamming than under equal power jamming. The difference between

MXD and MUD+swap diminishes as JSR increases. At high JSR, the performance depends less on source rate, which is a result of the resource allocation algorithm, and depends more on packet error rate, which affects all transmissions equally. Further simulations with lower rate LDPC codes showed that the PSNR performance under jamming remains comparable, if γ_S is lowered accordingly with the LDPC code rate. The robustness against jamming is improved if the LDPC code rate is lowered while maintaining γ_S constant, at the cost of decreased source rate.

4) Optimal Energy Allocation Among Attacking Methods: In Fig. 7(a), we plot the optimal percentage of energy allocation among the three methods of attack. The spoofing-only attack is optimal at low JSR. As we use a strong FEC code, at low JSR, jamming attacks have a low probability of success. As seen in Fig. 6(a), successful desynchronizing attacks require JSR to be beyond 30 dB. Therefore, at low JSR, spoofing only is optimal.

As JSR increases, the optimal energy allocation involves both spoofing and jamming. At high JSR, limiting the available bandwidth by spoofing, and attacking the resulting smaller number of available subcarriers by jamming, appears to be the best strategy. Even at high JSR, desynchronizing is not used, because the other two methods of attack are more effective.

In Fig. 7(a), we plot the optimal energy allocation for a lightly loaded system with $N_T = 256$, $\bar{N}_{pu} = 32$ and $\Omega_{su} = 4$. For this system, at low JSR, the optimal strategy is desynchronizing. If the system is lightly loaded, the small reduction of bandwidth due to spoofing at low JSR is unlikely to cause a notable performance degradation. Additionally, the probability of jamming success at low JSR is low. As the JSR increases, spoofing becomes more effective, and as the JSR increases beyond 20 dB, optimal energy allocation includes jamming.

VIII. Conclusion

In this paper, we analyze the optimal spoofing, desynchronizing and jamming power allocations across subcarriers, in a Rayleigh fading channel, with an optimization approach which enables a simplified calculation of the threshold JSRs that determine the optimal power allocation. We note that at low JSRs, optimizing spoofing and jamming gives the adversary a notable advantage. We evaluated the performance of two types of resource allocation algorithms, and observed that the MXD algorithm offers superior performance. We learned that spoofing has the most noticeable impact on the received video distortion at low and medium JSR, with the exception of lightly loaded systems at low JSR, for which desynchronizing attacks causes the most increase in video distortion. Jamming is effective at high JSR.

Appendix I
Optimization Approach

A. Theorem

Let $f : \mathbb{R}^+ \cup \{0\} \to \mathbb{R}^+ \cup \{0\}$ 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: $f'(x) \ge 0$ and $f'(x)$ is differentiable over $x \in [0, \infty)$, where $f'(x)$ is the first derivative.

Then, if $0 \le \sum_{i=1}^{N} \tilde{x}_i \le X_T$, $\tilde{x}_i \ge 0$ and $X_T > 0$,

$$\sum_{i=1}^{N} f(\tilde{x}_i) \le F(f, X_T, N)$$

$$\triangleq \begin{cases} \left(N - \frac{X_T}{x_0}\right) f(0) + \frac{X_T}{x_0} f(x_0), & \text{if } \frac{X_T}{N} \le x_0 \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{j-1} < \frac{X_T}{N} < y_j, \\ \frac{X_T - Ny_j}{x_j - y_j} f(x_j) + \frac{Nx_j - X_T}{x_j - y_j} f(y_j), & \text{if } y_j \le \frac{X_T}{N} \le x_j, \\ Nf\left(\frac{X_T}{N}\right), & \text{if } x_{N_r} < \frac{X_T}{N} nd \end{cases} \tag{26}$$

where $j \in \{1, 2, \ldots, N_r\}$, and x_js and y_js are defined in the discussion below.

Definition of x_0 : Let

$$g_0(x) \triangleq \begin{cases} \min\limits_{t \ge 0} \left(f(0) + \frac{(f(x) - f(0))t}{x} - f(t) \right) & x > 0 \\ \min\limits_{t \ge 0} \left(f(0) + f'(0)t - f(t) \right) & x = 0 \end{cases} \tag{27}$$

Then x_0 is the largest root of $g_0(x) = 0$.

Definition of y_js, and x_js for $j = 1, 2, \ldots, N_r$: Define the function $l_y(t)$ as follows:

$$l_y(t) \triangleq f(y) + (t - y) f'(y), \tag{28}$$

where $y \in [0, \infty)$ and $t \in [0, \infty)$. Also, define the function $g : \mathbb{R}^+ \cup \{0\} \to \mathbb{R}$ as follows:

$$g(y) \triangleq \min_{t > y} \left(l_y(t) - f(t) \right) \tag{29}$$

where $y \in [0, \infty)$ (according to the function domain) and $t \in (0, \infty)$. Then

$$y_j \triangleq \min\{y | g(y) = 0, y > x_{j-1}\} \tag{30}$$

and

$$x_j \triangleq \max\{t | l_{y_j}(t) - f(t) = 0\} \tag{31}$$

where $j = 1, 2, \ldots, N_r$, and N_r is the number of all pairs (y_j, x_j). We can obtain x_js and y_js from the algorithm shown in Fig. 8. Here we calculate (y_j, x_j) pairs iteratively, for $j = 1, 2, \ldots, N_r$. First we calculate x_0 from (27). Then, we use x_0 in (30) to calculate y_1. We use this y_1 to find x_1, using (31). Now we can use x_1 to calculate y_2, and so on. Note that $x_{j-1} < y_j < x_j$. When we iteratively attempt finding the (y_j, x_j)s, we will stop after (y_{N_r}, x_{N_r}), when $\{y | g(y) = 0, y > x_{N_r}\}$ does not yield any solutions. When $N_r = 0$, (26) reduces to [13, Eq. 28].

B. Proof

We consider the different ranges of $\frac{X_T}{N}$ separately in 4 cases in the proof below.

1) Case 1: $\frac{X_T}{N} \le x_0$

Since $X_T > 0$, and $\frac{X_T}{N} \le x_0$, we have $x_0 > 0$. Therefore, from the definition of x_0, we have $g_0(x_0) = 0$. From (27), $\min\limits_{t \ge 0} \left(f(0) + \frac{(f(x_0) - f(0))t}{x_0} - f(t) \right) = 0$. Therefore, $\forall\, t \ge 0$, $f(0) + \frac{f(x_0) - f(0)}{x_0} t - f(t) \ge 0$. Hence,

```
1: procedure OPTPARAM (f, f', g, x_0)
2:     j ← 0
3:     while {y|g(y) = 0, y > x_j} ≠ {} do
4:         j ← j + 1
5:         y_j ← min{y|g(y) = 0, y > x_{j-1}}
6:         x_j ← max{t|f(y_j) + (t − y_j)f'(y_j) − f(t) = 0}
7:     end while
8:     N_r ← j
9:     return {y_j|j = 1, 2, ..., N_r}, {x_j|j = 0, 1, ..., N_r}, N_r
10: end procedure
```

Fig. 8. Algorithm to obtain x_js and y_js.

$$\begin{aligned}\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N}\left[f(0)+\frac{f(x_0)-f(0)}{x_0}\tilde{x}_i\right]\\ &\leq Nf(0)+\frac{f(x_0)-f(0)}{x_0}X_T\\ &=\left(N-\frac{X_T}{x_0}\right)f(0)+\frac{X_T}{x_0}f(x_0)\end{aligned}\tag{32}$$

2) Case 2: $x_{j-1} < \frac{X_T}{N} < y_j,\ j = 1, 2, \ldots, N_r$

In Eq. (43) in Subsection C, we show that $l_{\frac{X_T}{N}}(t) \geq f(t),\ \forall\, t \geq 0$. Thus,

$$\begin{aligned}\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N} l_{\frac{X_T}{N}}(\tilde{x}_i)\\ &=\sum_{i=0}^{N}\left[f\left(\frac{X_T}{N}\right)+\left(\tilde{x}_i-\frac{X_T}{N}\right)f'\left(\frac{X_T}{N}\right)\right]\\ &\leq Nf\left(\frac{X_T}{N}\right)\end{aligned}\tag{33}$$

3) Case 3: $y_j \leq \frac{X_T}{N} \leq x_j$.

Note that by definition in (31), we have $l_{y_j}(x_j) - f(x_j) = f(y_j) + (x_j - y_j)f'(y_j) - f(x_j) = 0$ and $f'(y_j) = \frac{f(x_j)-f(y_j)}{x_j-y_j}$. In Eq. (43) in Subsection C, we show that $\forall\, t \geq 0$, $l_{y_j}(t) \geq f(t)$. Hence,

$$\begin{aligned}\sum_{i=1}^{N} f(\tilde{x}_i) &\leq \sum_{i=1}^{N} l_{y_j}(\tilde{x}_i)=\sum_{i=1}^{N} f(y_j)+(\tilde{x}_i-y_j)f'(y_j)\\ &\leq Nf(y_j)+\left(X_T-Ny_j\right)f'(y_j)\\ &=\frac{Nx_j-X_T}{x_j-y_j}f(y_j)+\frac{X_T-Ny_j}{x_j-y_j}f(x_j)\end{aligned}\tag{34}$$

4) Case 4: $x_{N_r} < \frac{X_T}{N}$

Following an approach similar to Eq. (43) in Subsection C, we can show that $l_{\frac{X_T}{N}}(t) \geq f(t),\ \forall\, t \geq 0$, for $x_{N_r} < \frac{X_T}{N}$. Thus,

$$\begin{aligned}\sum_{i=0}^{N} f(\tilde{x}_i) &\leq \sum_{i=0}^{N} l_{\frac{X_T}{N}}(\tilde{x}_i)\\ &=\sum_{i=0}^{N}\left[f\left(\frac{X_T}{N}\right)+\left(\tilde{x}_i-\frac{X_T}{N}\right)f'\left(\frac{X_T}{N}\right)\right]\\ &\leq Nf\left(\frac{X_T}{N}\right)\end{aligned}\tag{35}$$

From (32), (33), (34) and (35), we have (26).

A detailed proof is available [16].

C. *Proof that $l_{y_j}(x)$ and $l_{x_j}(x)$ are upper bounds to $f(x)$*

Select $\bar{x}$ such that $x_{j-1} < \bar{x} \leq y_j$. We know $g(x_{j-1}) > 0$ and by definition of y_j in (30), $y_j \geq \bar{x}$ is the smallest root of $g(y) = 0$ greater than x_{j-1}. Hence, $g(\bar{x}) \geq 0$. $\therefore$ from (29)

$$l_{\bar{x}}(t) \geq f(t),\ \forall\, t > \bar{x},\ \text{and} \tag{36}$$

For $x_{j-1} \leq t \leq \bar{x}$: Define $d_1(t) \triangleq l_{\bar{x}}(t) - f(t) = f(\bar{x}) + (t-\bar{x})\, f'(\bar{x}) - f(t)$. It can be shown that $f''(t) \leq 0$ for $t \in [x_{j-1}, \bar{x}]$, and it follows that $d_1'(t) = f'(\bar{x}) - f'(t) \leq 0$. Further, $d_1(\bar{x}) = f(\bar{x}) + (\bar{x}-\bar{x})\, f'(\bar{x}) - f(\bar{x}) = 0$. Therefore, $d_1(t) \geq 0\ \forall x_{j-1} \leq t \leq \bar{x}$, and

$$l_{\bar{x}}(t) \geq f(t),\ \forall\, x_{j-1} \leq t \leq \bar{x}. \tag{37}$$

For $t \leq x_{j-1}$: Define $d_2(t) \triangleq l_{\bar{x}}(t) - l_{x_{j-1}}(t) = f(\bar{x}) + (t-\bar{x})f'(\bar{x}) - \left(f\left(x_{j-1}\right) + \left(t - x_{j-1}\right)f'\left(x_{j-1}\right)\right)$. Then

$$d_2'(t) = f'(\bar{x}) - f'(x_{j-1}) \leq 0 \tag{38}$$

Substituting $t = x_{j-1}$, we have

$$d_2(x_{j-1}) = l_{\bar{x}}(x_{j-1}) - l_{x_{j-1}}(x_{j-1}) = l_{\bar{x}}(x_{j-1}) - f(x_{j-1}) \geq 0 \tag{39}$$

From (38) and (39), $d_2(t) \geq 0\ \forall\, t \leq x_{j-1}$. Therefore,

$$l_{\bar{x}}(t) \geq l_{x_{j-1}}(t)\ \forall\, t \leq x_{j-1} \tag{40}$$

Proof that: $l_{x_0}(t) \geq f(t)$:

From the definition of x_0, we have $f(0) + \frac{f(x_0)-f(0)}{x_0}t - f(t) \geq 0,\ \forall t \geq 0$, so that

$$\begin{aligned}l_{x_0}(t) - f(t) &= f(x_0) + \frac{f(x_0)-f(0)}{x_0}(t-x_0) - f(t)\\ &= f(0) + \frac{f(x_0)-f(0)}{x_0}t - f(t) \geq 0, \forall t \geq 0\end{aligned}$$

Assume $l_{x_{j-1}}(t) \geq f(t),\ \forall t \geq 0$.

From (40), $l_{\bar{x}}(t) \geq l_{x_{j-1}}(t) \geq f(t),\ \forall t \leq x_{j-1}$.

$$l_{\bar{x}}(t) \geq f(t),\ \forall t \leq x_{j-1}. \tag{41}$$

From (36), (37) and (41),

$$l_{\bar{x}}(t) \geq f(t), \forall t \geq 0,\ \text{for}\ x_{j-1} < \bar{x} \leq y_j. \tag{42}$$

Because $l_{y_j}(t) \equiv l_{x_j}(t)$, if $l_{y_j}(t) \geq f(t), \forall t \geq 0$, then $l_{x_j}(t) \geq f(t), \forall t \geq 0$. Therefore, we have shown that $l_{x_j}(t) \geq f(t), \forall t \geq 0$, for $j = 0, 1, \ldots, N_r - 1$, using induction. From (42),

$$l_{\bar{x}}(t) \geq f(t), \forall\, t \geq 0, \text{for}\ x_{j-1} \leq \bar{x} \leq y_j,\ j = 1, 2, \ldots, N_r. \tag{43}$$

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. Cognit. 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 Front. 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*. Rockville, MD, USA: Computer Science Press, 1985, vol. I.

[12] M. Soysa, P. Cosman, and L. Milstein, "Spoofing optimization over Nakagami-m fading channels of a cognitive radio adversary," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2013, pp. 1190–1193.

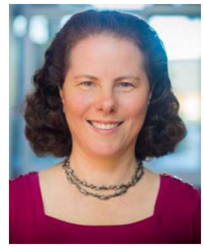
[13] M. Soysa, P. Cosman, and L. Milstein, "Optimized spoofing and jamming a cognitive radio," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 2681–2695, Aug. 2014.

[14] H. Kwon, I. Song, S. Y. Kim, and S. Yoon, "Noncoherent constant false-alarm rate schemes with receive diversity for code acquisition under homogeneous and nonhomogeneous fading circumstances," *IEEE Trans. Veh. Technol.*, vol. 56, no. 4, pp. 2108–2120, Jul. 2007.

[15] H. Schwarz, D. Marpe, and T. Wiegand, "Overview of the scalable video coding extension of the H.264/AVC standard," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 9, pp. 1103–1120, Sep. 2007.

[16] M. Soysa, P. Cosman, and L. Milstein. (2015, Nov.). *Detailed Presentation of the Optimization Approach* [Online]. Available: http://acsweb.ucsd.edu/~msoysa/opt_proof_151104.pdf.

Madushanka Soysa (S'09) received the B.Sc. degree in engineering (with first-class Hons.) from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Sc. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada, in 2011, and the Ph.D. degree in electrical engineering from the University of California, San Diego, La Jolla, CA, USA, in 2015. From 2009 to 2011, he was working on cooperative communication systems with channel outdates at University of Alberta. In 2013, he was with University of Oulu, Oulu, Finland, working on filterbank multicarrier systems. His research interests include cooperative communications, cognitive radio networks, and image and video processing. He was the recipient of the Best Paper Award in IEEE ICC 2012.



Pamela C. Cosman (S'88–M'93–SM'00–F'08) received the B.S. degree (with Hons.) in electrical engineering from the California Institute of Technology, Pasadena, CA, USA, in 1987, and the Ph.D. degree in electrical engineering from Stanford University, Stanford, CA, USA, in 1993. She was an NSF Postdoctoral Fellow with Stanford University and a Visiting Professor at the University of Minnesota, Minneapolis, MN, USA, from 1993 to 1995. In 1995, she joined as a Faculty of the Department of Electrical and Computer Engineering, University of California, San Diego, La Jolla, CA, USA, where she is currently a Professor as well as Associate Dean for Students of the Jacobs School of Engineering. She was the Director of the Center for Wireless Communications from 2006 to 2008. Her research interests include image and video compression and processing, and wireless communications. Dr. Cosman 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, EUSIPCO 1998. She was an Associate Editor of the IEEE COMMUNICATIONS LETTERS (1998–2001), and an Associate Editor of the IEEE SIGNAL PROCESSING LETTERS (2001–2005). She was the Editor-in-Chief (2006–2009) as well as a Senior Editor (2003–2005, 2010–2013) of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. She is a member of Tau Beta Pi and Sigma Xi. She was the recipient of the ECE Departmental Graduate Teaching Award, the Career Award from the National Science Foundation, the Powell Faculty Fellowship, GLOBECOM 2008 Best Paper Award, and the HISB 2012 Best Poster Award.

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, USA, in 1966 and 1968, respectively. From 1968 to 1974, he was with the Space and Communications Group, 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, USA. 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 also been a consultant to both government and industry in the areas of radar and communications. Dr. Milstein was an Associate Editor for Communication Theory for the IEEE TRANSACTIONS ON COMMUNICATIONS, an Associate Editor for Book Reviews for the IEEE TRANSACTIONS ON INFORMATION THEORY, an Associate Technical Editor for the *IEEE Communications Magazine*, and the Editor-in-Chief of the IEEE 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 of the IEEE Communications Society, in 1990 and 1991. He was also a former Chair of the IEEE Fellows Selection Committee. He was the 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.