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...
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 \( u_j \) in the \( i \)-th band is assumed to have the form \( \alpha_{j,i}^{(u)} = 10^{-\nu_{u_j}} \bar{\alpha}_j \), where \( \nu_{u_j} \sim \mathcal{N}(0, \sigma^2_v) \). 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 \( f^{(u)}_{D}(r_{u_j}, e_{u_j}) \) denote the average distortion of \( u_j \). The function \( f^{(u)}_{D} \) 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 \( Y_i^{(u)}(t) \sim \mathcal{N}(T_0W (\alpha_{j,i}^{(u)} \eta_{s,i} + N_0), T_0W (\alpha_{j,i}^{(u)} \eta_{s,i} + N_0)^2) \), where \( W \) is the bandwidth of one subcarrier, \( \alpha_{j,i}^{(u)} \) is the gain of the channel from the adversary to \( u_j \) in the \( i \)-th band, \( \eta_{s,i} \) is the power spectral density (PSD) of the spoofing signal in the \( i \)-th band, \( N_0 \) is the background noise PSD and \( 1/\alpha_{j,i}^{(u)} \) is exponentially distributed with mean \( \alpha_{j,i}^{(u)} \). This output is compared to the threshold \( K\sqrt{T_0W} \) by \( u_j \) to determine if the i-th band is vacant, and this information is communicated to CH. The threshold \( K\sqrt{T_0W} \) is selected to meet a predetermined target false alarm probability. 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 \( Y_i^{(u)}(t) > K\sqrt{T_0W} \) 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

\[
\Pr \left( \bigcup_{u_j \in U_{al}} \left( Y_i^{(u)}(t) > K\sqrt{T_0W} \right) \right) = 1 - \prod_{u_j \in U_{al}} \Pr \left( Y_i^{(u)}(t) < K\sqrt{T_0W} \right)
\]

Using [13, Eq. 5], we have

\[
\Pr\left( Y_i^{(u)}(t) < K\sqrt{T_0W} \right) = 1 - \frac{1}{\alpha_{j,i}^{(u)}} \int_0^\infty Q \left( \frac{K}{\eta_{s,i} + N_0} - \sqrt{T_0W} \right) e^{-\frac{y}{\alpha_{j,i}^{(u)}}} dy.
\]

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:

\[
p_{fd}(P_{s,i}) = 1 - \frac{1}{\alpha_{j,i}^{(u)}} \int_0^\infty Q \left( \frac{K}{\frac{P_{s,i}}{W} + N_0} - \sqrt{T_0W} \right) e^{-\frac{y}{\alpha_{j,i}^{(u)}}} dy.
\]

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 \( x_i(t) = \sum_{n=0}^{N_{acq}-1} c_n g(t - nT_c) \cos(\omega_c t) \) in the \( i \)-th band, where \( c_n \) is the binary spreading sequence with chip duration \( T_c \), \( N_{acq} \) is code acquisition period, \( E_c \) is the chip energy, \( \omega_c \) 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

\[
y(t) = \sqrt{2\alpha_{j,i}^{(u)}} E_c \sum_{n=0}^{N_{acq}-1} c_n g(t - t_d - nT_c) \times \cos(\omega_c(t - t_d) - \phi_{S,j,i}^{(u)} + \sqrt{\frac{\alpha_{j,i}^{(u)}}{\eta_{s,i}}} n_{s,i}(t) + n_{w,i}(t))
\]

where \( \alpha_{j,i}^{(u)} \) and \( \phi_{S,j,i}^{(u)} \) 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.
jammer-to-$u_j$ channel is $\alpha_{j,i}^{(u_j)}$. The channel gains $\alpha_{S,j}^{(u_j)}$ and $\alpha_{J,j}^{(u_j)}$ are exponential random variables (r.v.) with means $\alpha_{S}^{-1}$ and $\alpha_{J}^{-1}$, respectively. The background noise $n_{w,j}(t)$ is AWGN with a double-sided PSD $N_0/2$, and $\sqrt{\alpha_{J,j} n_{J,j}(t)}$ is the received jamming signal, where $n_{J,j}(t)$ is Gaussian with PSD $N_0/2$ 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 $\cos(\omega t + \phi_k)$ and $\sin(\omega t + \phi_k)$), and root-raised-cosine matched filters. The output sequences from the matched filters ($y_{l,a}$ and $y_{Q,a}$) are sampled at a frequency of $\frac{1}{T}$, and stored for processing in the next step. The matched filter output sequences are despreading using shifted versions of the $c_S$ sequence ($c_{n-k}$). For despreading, we use the samples with indices from $l_1$ to $l_1 + l_{acq} N_{acq} - 1$. 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 ($z_{k,l}$ 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 $|kT_e - t_d| < \frac{T}{2}$ [14]. For this, it is necessary to have a spreading that is orthogonal to its time-shifted versions. Let $k^\ast$ be the correct phase of the code. We can show that $z_{k^\ast}$ is an exponential r.v. with mean $l_{acq} \left( \frac{\alpha_{S}^2}{4} l_{acq} E_c N_{acq} c_{\alpha_S}^{-1} + \alpha_{J,j} n_{J,j} + N_0 \right)$. Here, $\zeta$ depends on $t_d$ mod $T_e$ and the pulse-shaping filter. From numerical evaluation of the autocorrelation of the root-raised cosine pulse, it can be shown that $\zeta \in [0.63, 1]$. We can also show that $z_k$ is an exponential r.v. with mean $l_{acq}(\alpha_{J,j} n_{J,j} + N_0)$, for $k \neq k^\ast$.

The probability of code acquisition, conditioned on $\alpha_{J,j}^{(u_j)}$, is $\Pr(z_k > z_k|\alpha_{J,j}^{(u_j)})$, $\forall k \neq k^\ast, k \in [0, 1, \ldots, N_{acq} - 1]$. Therefore, the probability of a code acquisition failure is given by

$$\Pr(z_k < x|\alpha_{J,j}^{(u_j)}) = \int_{0}^{\infty} \Pr(z_k < x|\alpha_{J,j}^{(u_j)}) f_{\alpha_{J,j}^{(u_j)}}(x) \, dx$$

where $f_{z_k|\alpha_{J,j}^{(u_j)}}(x)$ is the pdf of $z_k$ conditioned on $\alpha_{J,j}^{(u_j)}$.

Substituting these in (4), we obtain

$$\Pr \left( z_k < x|\alpha_{J,j}^{(u_j)} \right) = 1 - e^{-l_{acq}(\alpha_{J,j} n_{J,j} + N_0)} = \frac{1}{l_{acq}(\alpha_{J,j} n_{J,j} + N_0)}$$

The matched filter output sequences are despread using shifted versions of the $c_S$ sequence ($c_{n-k}$). For despreading, 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 $\cos(\omega t + \phi_k)$ and $\sin(\omega t + \phi_k)$), and root-raised-cosine matched filters. The output sequences from the matched filters ($y_{l,a}$ and $y_{Q,a}$) are sampled at a frequency of $\frac{1}{T}$, and stored for processing in the next step. The matched filter output sequences are despreading using shifted versions of the $c_S$ sequence ($c_{n-k}$). For despreading, we use the samples with indices from $l_1$ to $l_1 + l_{acq} N_{acq} - 1$. 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 ($z_{k,l}$ 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 $|kT_e - t_d| < \frac{T}{2}$ [14]. For this, it is necessary to have a spreading that is orthogonal to its time-shifted versions. Let $k^\ast$ be the correct phase of the code. We can show that $z_{k^\ast}$ is an exponential r.v. with mean $l_{acq} \left( \frac{\alpha_{S}^2}{4} l_{acq} E_c N_{acq} c_{\alpha_S}^{-1} + \alpha_{J,j} n_{J,j} + N_0 \right)$. Here, $\zeta$ depends on $t_d$ mod $T_e$ and the pulse-shaping filter. From numerical evaluation of the autocorrelation of the root-raised cosine pulse, it can be shown that $\zeta \in [0.63, 1]$. We can also show that $z_k$ is an exponential r.v. with mean $l_{acq}(\alpha_{J,j} n_{J,j} + N_0)$, for $k \neq k^\ast$.

The probability of code acquisition, conditioned on $\alpha_{J,j}^{(u_j)}$, is $\Pr(z_k > z_k|\alpha_{J,j}^{(u_j)})$, $\forall k \neq k^\ast, k \in [0, 1, \ldots, N_{acq} - 1]$. Therefore, the probability of a code acquisition failure is given by

$$\Pr(z_k < x|\alpha_{J,j}^{(u_j)}) = \int_{0}^{\infty} \Pr(z_k < x|\alpha_{J,j}^{(u_j)}) f_{\alpha_{J,j}^{(u_j)}}(x) \, dx$$

where $f_{z_k|\alpha_{J,j}^{(u_j)}}(x)$ is the pdf of $z_k$ conditioned on $\alpha_{J,j}^{(u_j)}$.

Substituting these in (4), we obtain

$$\Pr \left( z_k < x|\alpha_{J,j}^{(u_j)} \right) = 1 - e^{-l_{acq}(\alpha_{J,j} n_{J,j} + N_0)} = \frac{1}{l_{acq}(\alpha_{J,j} n_{J,j} + N_0)}$$

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

$$p_{c,q}(P_{ds,i}) \geq \int_{0}^{\infty} \Pr \left( z_k < x|\alpha_{J,j}^{(u_j)} \right) f_{\alpha_{J,j}^{(u_j)}}(x) \, dx$$

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

\section{User Allocation Methods}

Let $B_d \subseteq B$ be the set of allowed bands in the current sensing interval, and let $\alpha$ be the $|B_d| \times |L_d|$ matrix, where $|L_d| = |\alpha|$. The channel gain of the $j$-th user in the $i$-th band. The maximum transmit power in a subcarrier is $P_{R_k}^{max}$, and $P_{Rx}$ is the target received power per stream. The number of spreading sequences available in each band is $N_{acq}$, and the maximum number of spreading sequences needed for user $j$ ($N_{acq} \cap \max[j]$) 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 $P_{ac}$
Fig. 2. MUD algorithm for user allocation.

1: procedure MUD_ALLOC
   \( (\alpha, U_{al}, B_{al}, C_{al}, P_{sc}, P_{Re}, P_{Tx,max}, N_{sc,max}, N_{ss}) \)
2: \( U'_{al} \leftarrow U_{al} \)
3: \( B_{al} \leftarrow B_{al} \)
4: while \( |U'_{al}| > 0 \) do \( \triangleright \) While set of users to be assigned a channel is non-empty
5: if \( \sum_{k \in U_{al}} C_{al}[i][k] \geq N_{ss} \) then
6: \( B_{al} \leftarrow B_{al} \setminus \{i\} \) \( \triangleright \) Remove band if all spreading sequences are assigned
7: end if
8: \( (i, j) \leftarrow \arg \max_{i \in U'_{al}, j \in B'_{al}} \{ \alpha[i][j] P_{sc}[i] + \frac{P_{Re}}{\alpha[i][j]} \leq P_{Tx,max} \} \) \( \triangleright \) Select best channel & user
9: \( C_{al}[i][j] \leftarrow C_{al}[i][j] + 1 \) \( \triangleright \) Update channel assignment matrix
10: \( P_{sc}[i] \leftarrow P_{sc}[i] + \frac{P_{Re}}{\alpha[i][j]} \) \( \triangleright \) Update transmit power in selected (i-th) band
11: if \( \sum_{k \in B_{al}} C_{al}[i][k] \geq N_{sc,max}[j] \) then
12: \( U'_{al} \leftarrow U'_{al} \setminus \{j\} \) \( \triangleright \) Remove user if max. no. of channel allocations is met
13: end if
14: \( U'_{al} \leftarrow \{j \in U'_{al} : \max_{i \in B'_{al}} \{ P_{sc}[i] + \frac{P_{Re}}{\alpha[i][j]} \} \leq P_{Tx,max} \} \) \( \triangleright \) Update set of users
15: end while
16: return \( (C_{al}, P_{sc}) \)
17: end procedure

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 \( \gamma_S \) 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 i-th symbol detection in the i-th band is

\[
\gamma_{i,k}^{(u_j)} = \frac{\gamma_S}{\alpha_{f,j,k}^{(u_j)}} \gamma_{f,j,k}^{(u_j)} + 1,
\]

where \( \alpha'_{f,j,k}^{(u_j)} \) is the gain of the adversary-to-\( u_j \) channel, \( \gamma_{f,j,k}^{(u_j)} = \frac{P_j}{\gamma_T} \) and \( P_j \) is the jamming power allocated for the i-th subcarrier.

The channel gain \( \alpha'_{f,j,k}^{(u_j)} \) is exponentially distributed with average \( \bar{\alpha}^{(u_j)} \). 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]:

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

where \( \gamma_T \) 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 \( L_p \), \( \gamma_T \) is estimated.

Therefore, from (8), the probability of packet error is:

\[
Pr(\text{packet error}) = \Pr \left( \frac{\gamma_S}{\alpha_{f,j,k}^{(u_j)}} \gamma_{f,j,k}^{(u_j)} + 1 < \gamma_T \right)
= \frac{1}{\bar{\alpha}^{(u_j)}} \frac{1}{\gamma_T} \int_{\gamma_T}^{\infty} e^{-x} \frac{\gamma_S}{\bar{\alpha}^{(u_j)}} \gamma_{f,j,k}^{(u_j)} + 1 \ dx
= e^{\frac{\gamma_S}{\bar{\alpha}^{(u_j)}} \gamma_{f,j,k}^{(u_j)} + 1} \left( \frac{\gamma_T}{\gamma_T} - 1 \right)
\]

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

\[
N_{e,u_j,i}(P_{j,i}) = N_p Pr(\text{packet error}) = N_p e^{-\frac{N_p W}{\bar{\alpha}^{(u_j)} \gamma_{f,j,k}^{(u_j)} + 1}}
\]
SOYSA et al.: DISRUPTIVE ATTACKS ON VIDEO TACTICAL COGNITIVE RADIO DOWNLINKS

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

$$
\sum_{u_j} \mathbb{E} \left[ f^{(u_j)}(r_{u_j}, e_{u_j}) \right] = \sum_{u_j} \mathbb{E} \left[ \sum_{i \in B_{u_j}} r_{u_j,i} e_{u_j,i} \right].
$$

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 increased, 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 $B - B_{ps}$, the average number of bands detected as allowed by CH is $\sum_{i \in B - B_{ps}} (1 - p_{fd}(P_{S,i}))$, 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 $\sum_{i \in B - B_{ps}} p_{fd}(P_{S,i})$.

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 to 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

$$p_{fd}(P_{S,i}) = 1 - \left(1 - \frac{1}{\alpha J} \int_0^{\infty} Q \left( \frac{K}{p_{S,i} \alpha J y + N_0} - \sqrt{T_0 W} \right) e^{-\frac{K}{p_{S,i} \alpha J y + N_0}} dy \right)^{|u_{al}|}$$

(12)

where we use $\alpha_J$ as an approximation for $\alpha_{u_j}$. 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 $P_{S,i}$:

$$\frac{d}{dP_{S,i}} \left( p_{fd}(P_{S,i}) \right) = -|u_{al}| \left(1 - \frac{1}{\alpha J} \int_0^{\infty} Q \left( \frac{K}{p_{S,i} \alpha J y + N_0} - \sqrt{T_0 W} \right) e^{-\frac{K}{p_{S,i} \alpha J y + N_0}} dy \right)^{|u_{al}| - 1} \int_0^{\infty} \frac{dQ}{d \left( \frac{K}{p_{S,i} \alpha J y + N_0} - \sqrt{T_0 W} \right)} e^{-\frac{K}{p_{S,i} \alpha J y + N_0}} dy \times \frac{d}{dP_{S,i}} \left( \frac{K}{p_{S,i} \alpha J y + N_0} - \sqrt{T_0 W} \right) e^{-\frac{K}{p_{S,i} \alpha J y + N_0}} \left| u_{al} \right| > 0$$

(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 $J_D(u_j, e_{u_j})(1 - p_{cqf}(u_j)) + J_D(u_j) p_{cqf}(u_j) = J_D(u_j)(u_j, e_{u_j}) + J_D(u_j)(f_D(u_j), 0, 0) - J_D(u_j)(r_{u_j}, e_{u_j})$, where $p_{cqf}(u_j)$ is the probability of code acquisition failure of user $u_j$.

Because $J_D(u_j)(r_{u_j}, e_{u_j}) < J_D(u_j)(0, 0)$, 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

$$p_{cqf}(u_j) = \prod_{i \in B_{ps}} p_{cqf}(P_{ds,i})$$

(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

$$\text{log} \left( p_{cqf}(u_j) \right) = \sum_{i \in B_{ps}} \text{log} \left( p_{cqf}(P_{ds,i}) \right)$$. As the adversary is not aware of $B_{al}$, we modify the objective function to $\sum_{i=1}^{N_T} \text{log} \left( p_{cqf}(P_{ds,i}) \right)$. 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 $\sum_{i=1}^{N_T} \text{log} \left( p_{cqf,lb}(P_{ds,i}) \right)$. Taking the derivative of $p_{cqf,lb}(P_{ds,i})$ from (6), with respect to $P_{ds,i}$, we get

$$\frac{d}{dP_{ds,i}} \left( p_{cqf,lb}(P_{ds,i}) \right) = \int_0^{\infty} \left( -\frac{2}{\sqrt{\alpha_{u_j}}} \frac{\alpha_{u_j}}{\alpha_{u_j}^2 + \alpha_{u_j}^2} \right) e^{-\frac{\alpha_{u_j}^2}{\alpha_{u_j}^2 + \alpha_{u_j}^2}} d\alpha_{u_j} > 0$$

(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

$$p_{cqf,lb}(P_{ds,i}) \leq \lim_{P_{ds,i} \rightarrow \infty} p_{cqf,lb}(P_{ds,i})$$

$$= \int_0^{\infty} 0 < 0$$

(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 $\frac{d^2}{dP_{ds,i}^2} \left( p_{cqf,lb}(P_{ds,i}) \right) < 0$. Because the log function is monotonically increasing, $\text{log} \left( p_{cqf,lb}(P_{ds,i}) \right)$ also has the properties P0 and P1. Therefore, we can use the proposed optimization approach to maximize $\sum_{i=1}^{N_T} \text{log} \left( p_{cqf,lb}(P_{ds,i}) \right)$. Because $p_{cqf,lb}(P_{ds,i}) \geq 0$ and $\frac{d^2}{dP_{ds,i}^2} \left( p_{cqf,lb}(P_{ds,i}) \right) < 0$, the second
derivative \( \frac{\partial^2}{\partial P_{u_j}^2} \left( \log \left( p_{c_{ij},l_b}(P_{d_{x,i}}) \right) \right) < 0 \). 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 \( \sum_{u_j} J_D(r_{u_j}, e_{u_j}) \), by increasing the probability of packet error \( e_{u_j} \). We know that \( J_D(r_{u_j}, e_{u_j}) \) 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 \( B_{ul} \cup B_{pu} \). To simplify the notation, we number the bands such that \( B_{ul} \cup B_{pu} = \{1, 2, \ldots, N_{Tx}\} \).

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 \( u_j \), \( N_{e,u_j} = \sum_{i \in B(u_j)} N_{e,u_j,i}(P_{J,j}) \). 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

\[
N_{e,u_j} = \sum_{i=1}^{N_{Tx}} \left\{ \frac{|B(u_j)|}{N_{Tx}} \sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,j}) \right\}. \tag{17}
\]

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

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

We can write the objective function to be maximized from (11) as \( \sum_{u_j} J_D \left( r_{u_j}, 0 \right) \left( \sum_{i=1}^{N_{Tx}} \frac{N_{e,u_j,i}(P_{J,j})}{N_{Tx}N_P} \right) \). 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 \( J_D \left( r_{u_j}, 0 \right) \), the adversary aims to maximize

\[
\sum_{i=1}^{N_{Tx}} N_{e,u_j,i}(P_{J,j}), \text{under the constraints} \sum_{i=1}^{N_{Tx}} P_{J,j} = P_T \text{ and } P_{J,j} \geq 0.
\]

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

\[
N_{e,i}(P_{J,j}) = N_{pe} \frac{N_{pe}^W}{\alpha_i^W} \left( \frac{2}{\gamma} - 1 \right) \tag{19}
\]

where we use \( \alpha_i \) as an approximation for \( \alpha_i^{(u_j)} \). We use the approach in Appendix I, as \( N_{e,i}(P_{J,j}) \) 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:

\[
f_D(r_{u_j}, e_{u_j}) = \begin{cases} f_D(r_{u_j}, 0), & \text{if } \gamma_{u_j} > \gamma_T \\ f_D(r_{u_j}, 1), & \text{if } \gamma_{u_j} \leq \gamma_T \end{cases}
\]

The objective function to maximize is

\[
\sum_{u_j} \mathbb{E} \left[ f_D(r_{u_j}, e_{u_j}) \right] = \sum_{i=1}^{N_{Tx}} \sum_{u_j \in U(i)} \left( f_D(r_{u_j}, 0) \right. \left. + f_D(r_{u_j}, 1) e^{-\alpha_i^{(u_j)} \gamma_{u_j}} \right) \tag{20}
\]

The expected video distortion for \( u_j \) is

\[
\mathbb{E} \left[ f_D(r_{u_j}, e_{u_j}) \right] = f_D(r_{u_j}, 0) \frac{N_{pe}}{N_{Tx}N_P} \tag{21}
\]

The terms \( f_D(r_{u_j}, 0) \) and \( f_D(r_{u_j}, 1) \) 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 these terms, but do affect error rate. Hence, the objective to maximize is

\[
\sum_{i=1}^{N_{Tx}} \sum_{u_j \in U(i)} f_D(r_{u_j}, 0) e^{-\alpha_i^{(u_j)} \gamma_{u_j}} \left( \frac{2}{\gamma} - 1 \right)
\]

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

\[
\sum_{i=1}^{N_{Tx}} \sum_{u_j \in U(i)} f_D(r_{u_j}, 0) e^{-\alpha_i^{(u_j)} \gamma_{u_j}} \left( \frac{2}{\gamma} - 1 \right)
\]

Now, since only \( e^{-\alpha_i^{(u_j)} \gamma_{u_j}} \left( \frac{2}{\gamma} - 1 \right) \) can be changed by jamming, the function reduces to maximizing

\[
\sum_{i=1}^{N_{Tx}} e^{-\frac{\alpha_i^{(u_j)} \gamma_{u_j}}{\left( \frac{2}{\gamma} - 1 \right)}} \tag{22}
\]

where \( \alpha_i \) approximates \( \alpha_i^{(u_j)} \). 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 $\theta_{sp}$ be the fraction of energy allocated for spoofing and let $\theta_{ds}$ 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 $\sum_{u_j} J^{(u_j)}(r_{u_j}, e_{u_j})$. In the separate optimizations of spoofing, desynchronizing, and jamming attacks, we were able to derive objective functions to replace $f^{(u_j)}(r_{u_j}, e_{u_j})$, using the knowledge that $f^{(u_j)}(r_{u_j}, e_{u_j})$ 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 $f^{(u_j)}$ to optimize energy allocation among the attacking methods. Because $f^{(u_j)}$ depends on the video properties and encoding parameters that are not known by the adversary, we are not able to calculate $f^{(u_j)}$ at the adversary. Therefore, we use throughput as an alternative target for this section.

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

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

where $\tilde{p}_{cqf} \left( \theta_{ds}, \tilde{B}_{su}(\theta_{sp}) \right)$ is the probability of code acquisition failure, $\tilde{N}_e \left( \theta_{jm}, \tilde{B}_{su}(\theta_{sp}), [B_{pu}] \right)$ 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

$$\tilde{B}_{su}(\theta_{sp}) \triangleq \min_{\theta_{su}} \sum_{i=1}^{N_{su}} p_{i} \left\{ \frac{E\left( |B_{ad}| \right)}{N_{T}} \right\}$$

$$= \left( \frac{N_{T} - |B_{pu}|}{N_{T}} \right) \left( N_{T} - F \left( p_{jd}, \frac{\theta_{sp}E_{ad}}{T_0} , N_{T} \right) \right) \tag{23}$$

where $F$ is defined in (26), and that

$$\tilde{N}_e \left( \theta_{jm}, \tilde{B}_{su}(\theta_{sp}), [B_{pu}] \right) \triangleq \max \left\{ \sum_{i=1}^{\tilde{B}_{su}(\theta_{sp})} \right\} \sum_{i=1}^{B_{pu}} E \left[ \sum_{i=1}^{N_{r,i}} \right]$$

$$= \tilde{B}_{su}(\theta_{sp}) F \left( \frac{\theta_{jm}E_{ad}}{T_2}, \tilde{B}_{su}(\theta_{sp}) + |B_{pu}| \right) \tag{24}$$

where $\theta_{jm}$ 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

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

Using (22), we find the optimal energy allocation ratios $(\theta_{sp}, \theta_{ds}) = \arg \min \Gamma(\theta_{sp}, \theta_{ds})$ 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 $\lfloor B_{pu} \rfloor = \min(N_B, pu, N_T)$ bands at random, where $N_B$ is a Poisson r.v. with mean parameter $\lambda_{pu}$. We select $\lambda_{s} = \lambda_{j} = 1$, $T_0 = 4T_1$, $T_2 = 16T_1$, and $T_2 = 2048T_1$, where $T_1$ is the symbol time. The number of chips per symbol during the transmission interval ($N_{c}$) is 64, $N_{av} = 256$, 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 $(\gamma_{s})$ 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 $(704 \times 576)$ 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) $\triangleq 10 \log_{10} \left( \frac{MSE}{\text{MAX}} \right)$.

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.
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 $\gamma_S$ 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. 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

![Fig. 5. Average PSNR under spoofing attacks ($N_T = 64$, $\Omega_{iu} = 4$, $\bar{N}_{pu} = 16$).](image1.png)

![Fig. 6. Average PSNR vs JSR ($N_T = 64$, $\Omega_{iu} = 4$, $\bar{N}_{pu} = 16$): (a) under desynchronizing (b) under jamming.](image2.png)

![Fig. 7. Optimal energy allocation among the methods of attack: (a) Heavily loaded system ($N_T = 128$, $\Omega_{iu} = 4$, $\bar{N}_{pu} = 64$). (b) Lightly loaded system ($N_T = 256$, $\Omega_{iu} = 4$, $\bar{N}_{pu} = 32$).](image3.png)
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 the result of the resource allocation algorithm, and depends more on JSR, the performance depends less on source rate, which is a result of the MXD algorithm. The robustness against jamming is improved if the LDPC code rate is lowered while maintaining JSR 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 $N_T = 256$, $N_{pu} = 32$, 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 cause 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. $f(x) \leq M \forall x \in [0, \infty)$.

**P1:** $f'(x) \geq 0$ and $f'(x)$ is differentiable over $x \in [0, \infty)$, where $f'(x)$ is the first derivative.

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

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

**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. $f(x) \leq M \forall x \in [0, \infty)$.

**P1:** $f'(x) \geq 0$ and $f'(x)$ is differentiable over $x \in [0, \infty)$, where $f'(x)$ is the first derivative.

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

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

where $j \in \{1, 2, \ldots, N_r\}$, and $x_j$s and $y_j$s are defined in the discussion below.

Definition of $x_0$ : Let

$$g_0(x) \triangleq \min_{i \geq 0} \left( f(0) + \frac{(f(x) - f(0))t}{x} - f(t) \right) \quad x > 0$$

$$g_0(x) \triangleq \min_{i \geq 0} \left( f(0) + f'(0)t - f(t) \right) \quad x = 0$$

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

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

$$l_y(t) \triangleq f(y) + (t - y)f'(y), \quad (28)$$

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

$$g(y) \triangleq \min_{i > y} (l_y(t) - f(t)) \quad (29)$$

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

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

and

$$x_j \triangleq \max \{ t | l_y(t) - f(t) = 0 \} \quad (31)$$

where $j = 1, 2, \ldots, N_r$, and $N_r$ is the number of all pairs $(y_j, x_j)$. We can obtain $x_j$s and $y_j$s 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 $|y_j|g(y) = 0, y > x_{N_r}|$ 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 I: $\frac{X_T}{N} \leq x_0$

Since $X_T > 0$, and $\frac{X_T}{N} \leq x_0$, we have $x_0 > 0$. Therefore, from the definition of $x_0$, we have $g_0(x_0) = 0$. From (27), $\min_{t \geq 0} f(0) + \frac{(f(x_0) - f(0))t}{x_0} - f(t) = 0$. Therefore, $\forall t \geq 0, f(0) + \frac{(f(x_0) - f(0))t}{x_0} - f(t) \geq 0$. Hence,
In Eq. (43) in Subsection C, we show that

\[ N \sum_{i=0}^{N} f(\bar{x}_i) \leq N \sum_{i=0}^{N} \left[ f(0) + \frac{f(x_0) - f(0)}{x_0} \bar{x}_i \right] \]

\[ \leq N f(0) + \frac{f(x_0) - f(0)}{x_0} X_T \]

\[ = \left( N - \frac{X_T}{x_0} \right) f(0) + \frac{X_T}{x_0} f(x_0) \]

(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,

\[ \sum_{i=0}^{N} f(\bar{x}_i) \leq \sum_{i=0}^{N} l_{\frac{x_T}{N}}(\bar{x}_i) \]

\[ = \sum_{i=0}^{N} \left[ f\left( \frac{X_T}{N} \right) + \left( \bar{x}_i - \frac{X_T}{N} \right) f'\left( \frac{X_T}{N} \right) \right] \]

\[ \leq N f\left( \frac{X_T}{N} \right) \]

(33)

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

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

\[ \sum_{i=1}^{N} f(\bar{x}_i) \leq \sum_{i=1}^{N} l_{\frac{x_T}{N}}(\bar{x}_i) = \sum_{i=1}^{N} f(y_j) + (\bar{x}_i - y_j) f'(y_j) \]

\[ \leq N f(y_j) + (X_T - N y_j) f'(y_j) \]

\[ = N x_j - X_T \]

\[ \frac{x_j - y_j}{x_j - y_j} f(y_j) + \frac{X_T - N y_j}{x_j - y_j} f(x_j) \]

(34)

4) Case 4: \( x_N < \frac{X_T}{N} \)

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 \( x_N < \frac{X_T}{N} \). Thus,

\[ \sum_{i=0}^{N} f(\bar{x}_i) \leq \sum_{i=0}^{N} l_{\frac{x_T}{N}}(\bar{x}_i) \]

\[ = \sum_{i=0}^{N} \left[ f\left( \frac{X_T}{N} \right) + \left( \bar{x}_i - \frac{X_T}{N} \right) f'\left( \frac{X_T}{N} \right) \right] \]

\[ \leq N f\left( \frac{X_T}{N} \right) \]

(35)

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

A detailed proof is available [16].

C. Proof that \( l_{\lambda_j}(x) \) and \( l_{\lambda_j}(x) \) 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, \( g(\bar{x}) \geq 0 \), ... from (29)

\[ l_{\bar{x}}(t) \geq f(t), \forall t \geq 0, \leq \bar{x} \]

(36)

For \( x_{j-1} \leq t \leq \bar{x} \): Define \( d_1(t) = l_{\bar{x}}(t) - f(t) = f(\bar{x}) + (t - \bar{x}) f'(\bar{x}) - f(t) \). 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, \( d_1(t) \geq 0 \) \( \forall t \geq 0 \), so that

\[ l_{\bar{x}}(t) \geq f(t), \forall t \leq \bar{x} \]

(37)

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

\[ d_2'(t) = f'(\bar{x}) - f'(t) \leq 0 \]

(38)

Substituting \( t = x_{j-1} \), we have

\[ d_2(x_{j-1}) = l_{\bar{x}}(x_{j-1}) - l_{x_{j-1}}(x_{j-1}) = l_{x_{j-1}}(x_{j-1}) - f(x_{j-1}) \geq 0 \]

(39)

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

\[ l_{\bar{x}}(t) \geq l_{x_{j-1}}(t) \forall t \leq x_{j-1} \]

(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

\[ l_{x_0}(t) - f(t) = f(x_0) + \frac{f(x_0) - f(0)}{x_0} \]

\[ \geq f(0) + \frac{f(x_0) - f(0)}{x_0} t - f(t) \geq 0, \forall t \geq 0 \]

Assume \( l_{x_{j-1}}(t) \geq f(t), \forall t \geq 0 \). From (40), \( l_{\bar{x}}(t) \geq l_{x_{j-1}}(t) \geq f(t), \forall t \leq x_{j-1} \).

\[ l_{\bar{x}}(t) \geq f(t), \forall t \leq x_{j-1} \]

(41)

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

\[ l_{\bar{x}}(t) \geq f(t), \forall t \geq 0, \text{ for } x_{j-1} < \bar{x} \leq y_j \]

(42)

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

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

(43)
REFERENCES


