2016 IEEE Conference on Communications and Network Security (CNS): The 2nd Workshop on Cognitive Radio and Electromagnetic Spectrum Security (CRESS)

Video Cognitive Radio Networks for Tactical Scenarios

Madushanka Soysa
OmniTier Storage Inc.
Rochester, Minnesota, USA 55901-2700
msoysa@ucsd.edu

Pamela C. Cosman and Laurence B. Milstein
Department of Electrical and Computer Engineering
University of California San Diego
La Jolla, California, USA 92093-0407
pcosman@ucsd.edu; lmilstein@ucsd.edu

Invited Paper

Abstract *– We examine the performance of uplink 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 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 to disrupt code acquisition by SUs or the cluster head. By jamming the network during the transmission interval, the adversary can reduce the rate of successful transmission. We also propose cross-layer resource allocation algorithms and evaluate their performance under disruptive attacks.*

I. INTRODUCTION

In this work, we analyze the impact of an intelligent adversary on the uplink of a tactical, spread spectrum, cognitive radio (CR) network. In [1], 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 [2] to obtain spoofing performance under Nakagami-*m* fading. In [3] and [4], the optimal power allocation for spoofing and jamming was investigated under an AWGN channel, and Rayleigh fading, respectively. In [5], this work was extended to analyze the optimal power allocation among spoofing, desynchronizing and jamming on the downlink. In this work, we extend the analysis to spoofing, desynchronizing and jamming attacks on the uplink. In [5], multiple access interference (MAI) was not an issue, because we used orthogonal spreading sequences on the downlink. In this work, we propose cross-layer resource allocation algorithms that account for MAI in the uplink.

This work was supported in part by the Army Research Office under Grant W911NF-14-1-0340.

II. SYSTEM MODEL

We assume a cluster-based architecture where the cluster head (CH) serves the secondary users (SUs) of the CR system. The SUs transmit video to the CH over a multi-carrier DS-CDMA (MC-DS-CDMA) system with N_T bands (or subcarriers), and we assume time-division duplex operation. The N_T bands are shared among primary users (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 primary users. *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. This information is sent to the CH at the end of the sensing interval (T_0). The CH uses the bands detected as vacant by all SUs as the set of *allowed bands*. Then, the CH broadcasts a known spreading sequence in all allowed bands during the first part of the code acquisition interval $(T_{1,d})$, which is used by the SUs for code acquisition and channel estimation. The SUs that performed code acquisition successfully transmit a pre-assigned sequence (different for each SU) in a subset of allowed bands, during the second part of the code acquisition interval $(T_{1,u})$. This is used by the CH to perform code acquisition. The estimated channel state information (CSI) and the rate-distortion curve of each SU is communicated to the CH following that. This information is used by the CH for channel allocation among the SUs. The SUs then communicate over a duration of T_2 in the allocated bands.

978-1-5090-3065-1/16/$31.00 ©2016 IEEE

The adversary uses Gaussian noise signals for spoofing, desynchronizing, and jamming. The average gain of the channel from the adversary to user u_j in the *i*-th band is assumed to have the form $\bar{\alpha}_J^{(u_j)} = 10^{-\upsilon_{uj}}\bar{\alpha}_J$, where $\upsilon_{uj} \sim \mathcal{N}(0, \sigma_\upsilon^2)$. 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_{uj}) and the probability of packet errors (e_{uj}) during a transmission interval. Let $f_D^{(u_j)}\left(r_{u_j}, e_{u_j}\right)$ 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 $B_{su} \subseteq B$ be the subset of bands used by the SU network for communication in one transmission interval.

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 $\sum_{\forall u_j} f_D^{(u_j)}\left(r_{u_j}, e_{u_j}\right)$.

The sensing model was described in [5], and the probability of code acquisition as a function of spoofing power $(P_{S,i})$ is [5, Eq.2]

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

where W is the subcarrier bandwidth, $\frac{N_o}{2}$ is the background noise power spectral density (PSD) and $K\sqrt{T_o W}$ is the threshold used in the energy detector.

Regarding code acquisition, consider the block diagram shown in Figure 1, where $\{c_n\}$ is the binary spreading sequence with chip duration T_c, $E_c^{(u_j)}$ is the energy per chip, ω_c is the carrier frequency, N_c^{acq} is the period of the spreading sequence, l_{acq} is the number of repetitions of the spreading sequence, and $g(t)$ is a root-raised cosine chip-wave shaping filter defined in [4, Eq.7]. The received signal at the CH is given by Eq. (1), which is shown at the bottom of the Conclusions section, where $U(i)$ is the set of users sharing the *i*-th band, and $\alpha_{S,i}^{(u_j)}$ and $\phi_{S,i}^{(u_j)}$ are the power gain and phase components of the response, respectively, of the channel from user u_j to CH in the *i*-th band. The gain of the jammer-to-CH channel is $\alpha_{J,i}^{(ch)}$. We assume the channel gains $\alpha_{S,i}^{(u_j)}$ and $\alpha_{J,i}^{(ch)}$ are mutually independent. The time delay of user u_j is denoted by $t_d^{u_j}$. The background noise $n_{w,i}(t)$ is AWGN with PSD $\frac{N_0}{2}$ and $\sqrt{\alpha_{J,i}^{(ch)}} n_{J,i}(t)$ is the received jamming signal. The chip energy $E_c^{(u_j)}$ is chosen so that $\alpha_{S,i}^{(u_j)} E_c^{(u_j)} = \tilde{E}_{c,Rx}$, where $\tilde{E}_{c,Rx}$ is the target received chip energy at the CH.

Let $p_{cqf,ul}(P_{ds,u,i})$ be the average probability of code acquisition failure by the CH, averaged over $\alpha_{J,i}^{(ch)}$, where $P_{ds,u,i}$ is the uplink desynchronizing power in the *i*-th band. Note that $\eta_{J,i} = \frac{P_{ds,u,i}}{W}$. It is shown in [6] that this probability can be lower bounded by

$$\int_0^\infty \frac{1}{2} \exp\left[-\frac{\mu^2}{2 l_{acq}\left(N_0 + \alpha_{J,i}^{(ch)} \frac{P_{ds,u,i}}{W} + \bar{E}_{c,Rx}\left(1 - \frac{\beta}{4}\right)(|U(i)| - 1)\right)}\right] \cdot \frac{1}{\bar{\propto}} \exp\left[\frac{\propto_{J,i}^{(ch)}}{\bar{\propto}_J^{(u_j)}}\right] d\propto_{J,i}^{(ch)}$$

where β is the excess bandwidth of the Nyquist filter.

We look at several user-subcarrier allocation methods which are presented in [6]. The first one is similar to simple multiuser diversity channel allocation, where each band is assigned to the user which can transmit with the least power in that band. We refer to it as MUD. Here, the user-subcarrier assignment which requires the least increase in total transmit power of all users, while not exceeding the power constraints, is selected first. Then the next user-subcarrier assignment which requires the least transmit power is made, and so on, until all users obtain the maximum required number of assignments $N_{sc,max}$, or until no further assignments can be made for users without $N_{sc,max}$ assignments due to the power constraints. In the second algorithm, named MXD, each user is initially assigned a single subcarrier, using the MUD algorithm. Then, a subset of users with the highest distortion under the current channel allocation is selected, and each user is allocated an additional subcarrier using the MUD algorithm. This process of assigning an additional subcarrier to the subset of users with highest distortion is done iteratively, until no further assignments can be made due to the power constraints. After the initial assignment from either of the above algorithms, a swapping algorithm can be used to check if changing

a channel assignment from one user to another will decrease the sum distortion of all users.

Consider now the video transmission mode. A block diagram of the transmitter of a single user and a single subcarrier is shown in Figure 2, and the corresponding receiver is shown in Fig. 3. Following the same approach as [5, Eq. 15], we can show that the expected number of packet errors of user u_j in the i-th band $N_{e,i}(P_{J,i})$, is given by Eq. (2), which is shown at the bottom of the Conclusions section, where N_p is the average number of packets of a single user, in a single band, per transmission interval, Υ_T is the threshold parameter that depends on the FEC from [5, Eq. 13], and $\bar{\alpha}_J^{(ch)}$ is the average gain of the adversary-to-CH channel.

The key theoretical basis for the results presented in this paper is a theorem that is proven in [5], and which is applicable to various scenarios involving either jamming or spoofing. If we consider jamming, the optimal strategy for the adversary is to use partial-band, equal power jamming at low values of JSR, then full-band, equal-power when JSR exceeds a particular threshold, and then, as JSR increases, transition (possibly multiple times) to full-band, unequal-power, then back to full-band, equal-power, and so on, until it ultimately saturates at full-band, equal-power jamming. In the above description, JSR corresponds to the ratio of jamming power to signal power per user, per stream. Also, a similar result holds for spoofing.

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 [1-5]. 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.

III. RESULTS

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 $N_T = 64, \bar{\alpha}_s = \bar{\alpha}_J = 1, \sigma_\nu = 0.01, \beta = 0.25, T_0 = 4T_s, T_{1,d} = T_{1,u} = 8T_s$ and $T_2 = 2048T_s$. The number of chips per symbol during a transmission interval (N_c) is 64, $N_c^{acq} = 64, l_{acq} = 4$ and $N_{acq,ul} = 2$. We use Gold codes as spreading sequences, a rate $\frac{1}{2}$ LDPC code with code-block-length 2048 bits, and QPSK modulation. The target received SNR is 7dB. Each user transmits the 'soccer' video sequence of 300 frames with 4CIF resolution (704 x 576) at 30 frames per second. The source video is compressed by the baseline profile of H.264/AVC reference software JM 11.0. The group of pictures (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 $\triangleq 10 \log_{10} \frac{255^2}{\mathbb{E}[MSE]}$.

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 a reference to which the performance of the optimized strategy is compared.

A. *Spoofing attacks*

In Fig. 4, we plot the average PSNR under equal-power spoofing (dashed curves) and optimized spoofing (solid curves). The optimal spoofing strategy, which we use here to evaluate the performance of the uplink resource algorithms under spoofing, was derived in [5].

The MXD algorithms perform better than MUD algorithms under the simulated parameters. While swapping improves the performance of MUD, MXD+swap does not have noticeable performance improvement over MXD. Optimized spoofing only reduces the performance of MXD algorithms by about 1 dB in the 2 – 6 dB JSR range. In contrast, the performance MUD algorithms worsens by about 5 db when the spoofing attack is optimized around 6 dB JSR. The average PSNR under MXD algorithms remains fairly constant up to about 6 dB JSR, and there is a steep drop in PSNR from 8-10 dB. We can conclude that the MXD algorithms are able to reduce the performance degradation due to false detections at low JSRs, when compared to MUD algorithms. The performance of the optimized spoofing attacks converges with equal power spoofing beyond 10 dB of JSR, since the optimal spoofing strategy becomes equal-power spoofing, as concluded from the optimization approach.

B. *Desynchronizing attacks*

In Figure 5, we have the average PSNR under equal-power desynchronizing attacks for both a lightly loaded system $(\Omega_{su} = 4$ and $\bar{N}_{pu} = 16)$ and a heavily loaded system $(\Omega_{su} = 8$ and $\bar{N}_{pu} = 32)$, where Ω_{su} is the number of SUs. The performances of the different resource allocation algorithms in the lightly loaded system are almost identical. In the heavily loaded system, the MXD algorithms perform significantly

better, with more than 10 dB higher average PSNR over MUD algorithms in the JSR < 30 dB region.

C. *Jamming attacks*

Figure 6 shows the performance of the system under jamming attacks. The solid curves correspond to worst-case jamming and the dashed curves represent equal-power jamming. From the dashed curves, we can see that the system is unaffected by equal-power jamming up to about 5 dB JSR. However, the reduction in PSNR in the solid curves in the -5 to 5 dB region shows that optimized jamming affects the system at a lower JSR compared to equal-power jamming. At JSR = 5 dB, the average PSNR for MXD algorithms is about 5 dB lower under optimized jamming than under equal power jamming. The performance difference between MXD and MUD+swap diminishes as JSR increases. At high JSR, the performance is less dependent on the source rate, which is a result of the resource allocation algorithm, and influenced more by the packet error rate, which affects all transmissions equally.

IV. CONCLUSIONS

In this paper, we extended the results of [5], which were appropriate for the downlink of a cluster-based, tactical, CR system, to the uplink of that system, where the key difference was the presence of MAI in the uplink scenario. We allowed an intelligent adversary to attack the system in three ways: spoofing in the sensing mode, jamming in the synchronization mode, and jamming in the video transmission mode. Using an optimization strategy that was derived in [5] for the downlink, and that also applies to the uplink, we found large gains in the adversary's ability to degrade the video transmissions compared to the degradation that the adversary could cause if full-band jamming/spoofing was employed.

REFERENCES

[1] 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.

[2] M. Soysa, P. Cosman, and L. Milstein, "Spoofing optimization over Nakagami-*m* fading channels of a cognitive radio adversary," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2013, Dec 2013, pp. 1190-1193.

[3] Q. Peng, P. Cosman, and L. Milstein, "Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary," *IEE J. Sel. Areas Commun*., vol. 29, no. 4, pp. 903-911, Apr. 2011.

[4] 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.

[5] M. Soysa, P. Cosman, and L. Milstein, "Disruptive attacks on video tactical cognitive radio downlink," *IEEE Trans. Commun*., vol. 64, no. 4, pp. 1411-1422, April 2016.

[6] Soysa, M. (2015). Video Transmission in Tactical Cognitive Radio Networks Under Distributive Attacks (Unpublished doctoral thesis). University of California San Diego.

$$y(t)=\sum_{u_j\in U(i)}\sqrt{2\alpha_{S,i}^{(u_j)}E_c^{(u_j)}}\sum_{n=0}^{\frac{T_{1,u}}{T_c}-1}c_n^{(u_j)}g(t-t_d^{(u_j)}-nT_c)\cos\left(\omega_c(t-t_d^{(u_j)})-\phi_{S,i}^{(u_j)}\right)+\sqrt{\alpha_{J,i}^{(ch)}}n_{J,i}(t)+n_{w,i}(t) \quad (1)$$

$$N_{e,i}(P_{J,i})=N_p e^{-\frac{\left(\tilde{E}_{c,Rx}\left(1-\frac{\beta}{4}\right)\sum_{u_l\in U(i)-\{u_j\}}\Omega_i^{(u_j)}+N_0\right)W}{\tilde{\alpha}_J^{(ch)}P_{J,i}}\left(\frac{\gamma_{S,ul}}{\gamma_T}-1\right)} \quad (2)$$

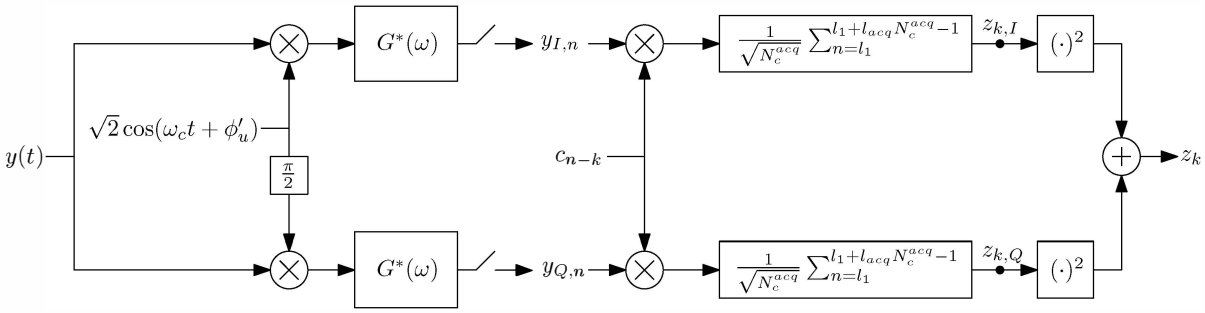

Fig. 1: Code acquisition block

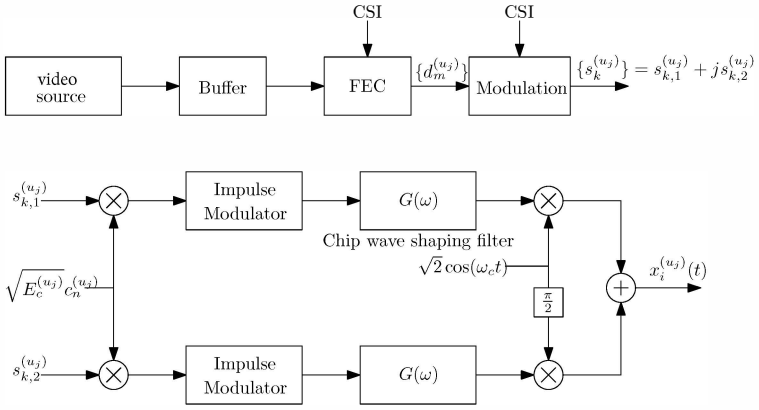

Fig. 2: Transmitter block diagram for user u_j in the i-th band

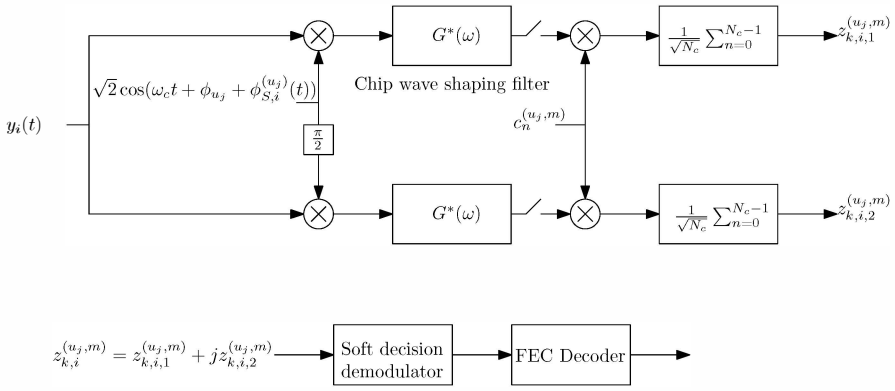

Fig. 3: Receiver block diagram for decoding the signal from user u_j in the i-th band

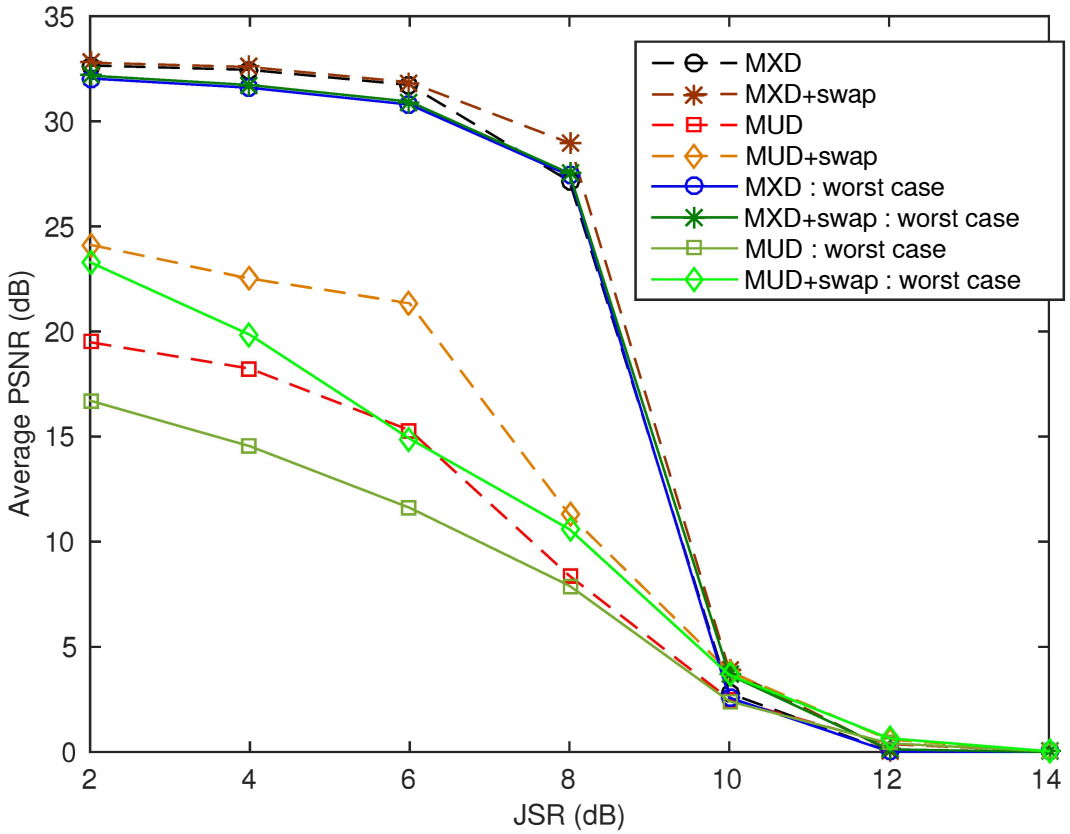

Fig. 4: Average PSNR under spoofing attacks on the uplink $\left(N_T = 64, \Omega_{su} = 8, \bar{N}_{pu} = 16\right)$

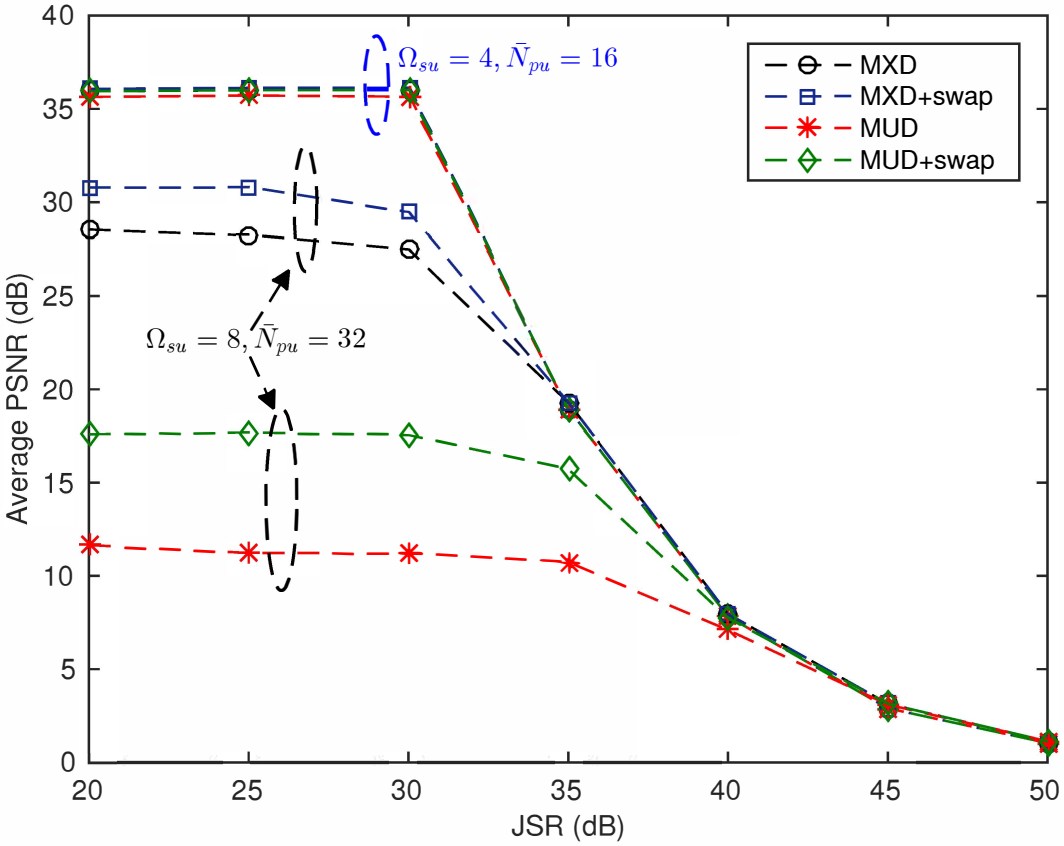

Fig. 5: Average PSNR under desynchronizing attacks on the uplink ($N_T = 64$)

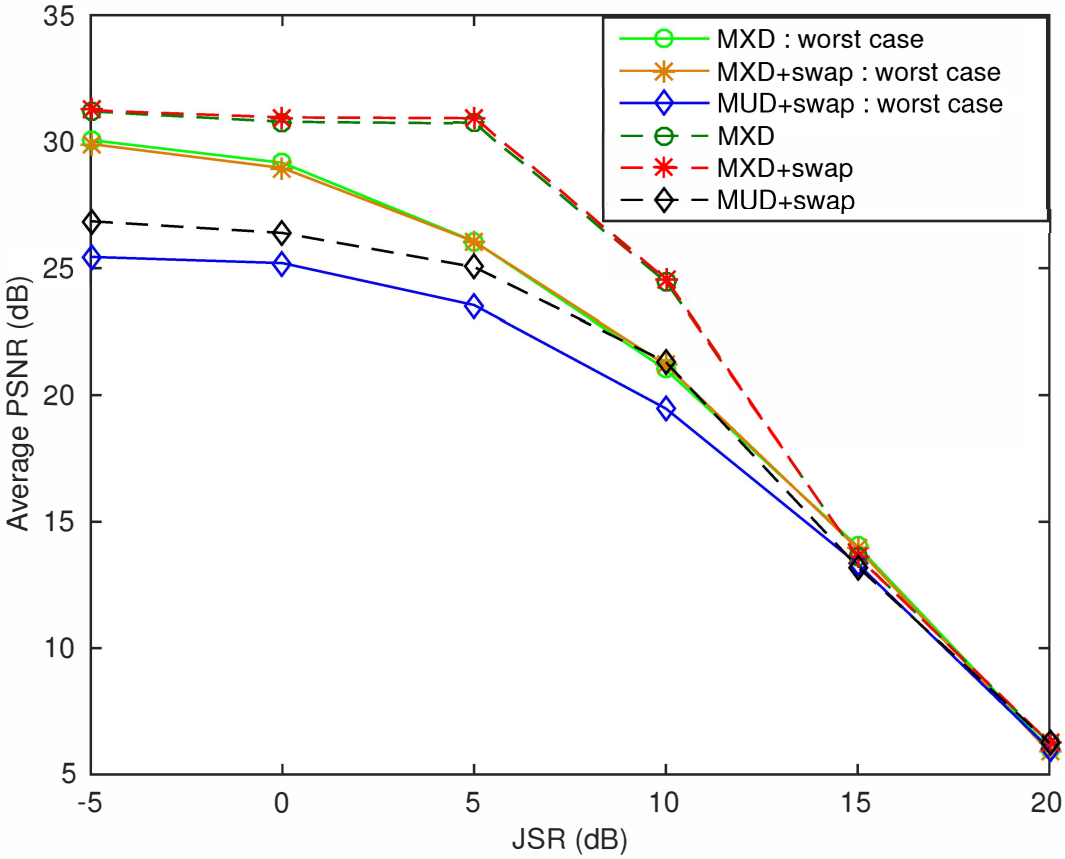

Fig. 6: Average PSNR under jamming attacks $\left(N_T = 64, \Omega_{su} = 8, \bar{N}_{pu} = 16, \rho_{fac} = 100\right)$