

Joint Jammer Mitigation and Data Detection for Smart, Distributed, and Multi-Antenna Jammers

Gian Marti and Christoph Studer

Department of Information Technology and Electrical Engineering, ETH Zurich, Switzerland

email: gimarti@ethz.ch and studer@ethz.ch

Abstract—Multi-antenna (MIMO) processing is a promising solution to the problem of jammer mitigation. Existing methods mitigate the jammer based on an estimate of its subspace (or receive statistics) acquired through a dedicated training phase. This strategy has two main drawbacks: (i) it reduces the communication rate since no data can be transmitted during the training phase and (ii) it can be evaded by smart or multi-antenna jammers that are quiet during the training phase or that dynamically change their subspace through time-varying beamforming. To address these drawbacks, we propose *joint jammer mitigation and data detection (JMD)*, a novel paradigm for MIMO jammer mitigation. The core idea is to estimate and remove the jammer interference subspace jointly with detecting the transmit data over multiple time slots. Doing so removes the need for a dedicated rate-reducing training period while enabling the mitigation of smart and dynamic multi-antenna jammers. We instantiate our paradigm with SANDMAN, a simple and practical algorithm for multi-user MIMO uplink JMD. Extensive simulations demonstrate the efficacy of JMD, and of SANDMAN in particular, for jammer mitigation.

I. INTRODUCTION

In a world that has become fundamentally reliant on wireless communications, averting the threat of jamming attacks has turned into a problem of critical importance [1]–[4]. An attractive solution is offered by multi-antenna (MIMO) processing, which enables the mitigation of jammers through spatial filtering [5]. Traditionally, a training period is used to estimate the jammer subspace, and the jammer’s interference is removed by projecting subsequent receive signals onto the orthogonal complement of that subspace [6]–[12]. This strategy has two major disadvantages: First, estimating the jammer subspace during a training period reduces the achievable data rate, since no data can be transmitted in the meantime. Second, estimating the jammer subspace during a training period is ineffective against smart jammers that transmit only at specific instances to evade estimation [13] or against jammers that change their subspace dynamically through time-varying multi-antenna transmit beamforming [14]. To overcome these limitations, we propose a novel paradigm for jammer mitigation through MIMO processing which we call *joint jammer mitigation and data detection (JMD)*.

The work of CS was supported in part by the U.S. National Science Foundation (NSF) under grants CNS-1717559 and ECCS-1824379. The work of GM and CS was supported in part by an ETH Research Grant.

The authors thank Sueda Taner for comments and suggestions.

A. State of the art

The fundamental challenge of jammer mitigation through spatial filtering is that it requires information about the jammer, such as the subspace spanned by the jammer’s channel [6]–[9] or the covariance matrix of the jammer’s interference [7], [15], [16]. Existing results often assume that the jammer transmits permanently (and with static signature). This would enable the receiver to estimate the required quantities during a dedicated training period in which the legitimate transmitters do not transmit [6], [7] or in which they transmit predetermined symbols that carry no information [8]–[12]. By relying on such a static jammer assumption, the receiver can filter the jammer in the subsequent communication period until the wireless channel changes and the process is started anew. A smart jammer, however, can circumvent such mitigation methods by deliberately violating their assumptions: It can pause jamming for the duration of the dedicated training period, so that the receiver learns nothing meaningful [13]. Or, if the jammer has multiple antennas, it can use beamforming to dynamically change its subspace (as well as the interference covariance matrix at the receiver), so that, after the training period, the receiver’s filter will no longer match the jammer’s transmit characteristics [14].¹ To mitigate smart jammers, methods have been suggested that attempt to fool the jammer into transmitting during the training period by distributing and randomizing the timing of the training period [6], [8]. However, such methods may not work against jammers that jam only intermittently at random time instants. Similarly, methods have been proposed to mitigate dynamic multi-antenna jammers by recurrently estimating their instantaneous subspace [14], but this may be effective only against jammers that change their subspace in a sufficiently slow manner. Furthermore, all training-period based mitigation methods are subject to an inherent trade-off between the time that they dedicate to the attempt of estimating the required jammer characteristics and the time that remains for payload data transmission.

In light of these considerations, there is a clear need for a more principled approach to MIMO-based jammer mitigation. We have recently proposed MAED [13], which, in hindsight, can be viewed as a special case of JMD. MAED unifies not only jammer mitigation and data detection, but also channel estimation—at the cost of high computational complexity.

¹Another hard-to-mitigate threat is posed by multiple single-antenna distributed jammers, which also cause high-rank interference [17], [18].

B. Contributions

We propose *joint jammer mitigation and data detection* (*JMD*), a novel paradigm for jammer mitigation. The core idea is to estimate and remove the subspace of the jammer interference *jointly* with detecting the data of an entire transmission frame (or coherence interval). *JMD* removes the need for a dedicated training period and enables higher data rates. Beyond that, considering an entire transmission period at once enables *JMD* to deal with smart jammers that try to evade mitigation (i) by jamming only at specific instances or (ii) by dynamically changing their subspace through multi-antenna beamforming.

As in [13], we exploit the fact that a jammer cannot leave its subspace within a coherence interval (this holds also for multi-antenna jammers with time-varying beamforming). Going beyond our work in [13], we show that this fact can be leveraged to mitigate contamination of the channel estimate even when the channel is estimated separately from jammer mitigation and data detection. This new insight opens the door to a wide range of efficient signal processing algorithms for jammer mitigation. We capitalize on it by proposing *SANDMAN* (short for SimultANeous Detection and MitigAtioN), an algorithm that offers all of the jammer mitigation capabilities of the *MAED* method from [13], but at reduced computational complexity. Furthermore, *SANDMAN* can mitigate distributed and multi-antenna jammers, while *MAED* only mitigates single-antenna jammers. This paper also goes beyond [13] by analyzing the rate improvements offered by the lack of a jammer estimation phase. Extensive simulations show the efficacy of *JMD*, and of *SANDMAN* in particular. An extended journal version with theoretical foundations, more detailed descriptions, and further empirical evaluation is in preparation.

II. JOINT JAMMER MITIGATION AND DATA DETECTION

A. System model

We focus on mitigating jamming attacks in the (massive) MU-MIMO uplink, although our methods are easily translatable to other MIMO contexts. Consider a jamming attack such that the receive signal at the BS is given by

$$\mathbf{y}_k = \mathbf{H}\mathbf{s}_k + \mathbf{J}\mathbf{w}_k + \mathbf{n}_k. \quad (1)$$

Here, $\mathbf{y}_k \in \mathbb{C}^B$ is the BS receive vector at time k , $\mathbf{H} \in \mathbb{C}^{B \times U}$ is the UE channel matrix (we assume block fading with coherence time $K = D + U$), $\mathbf{s}_k \in \mathcal{S}^U$ contains the time- k transmit symbols of U single-antenna UEs with constellation \mathcal{S} , $\mathbf{J} \in \mathbb{C}^{B \times I}$ is the channel matrix of an I -antenna jammer,² $\mathbf{w}_k \in \mathbb{C}^I$ is the time- k jammer transmit vector, and $\mathbf{n}_k \sim \mathcal{CN}(\mathbf{0}, N_0 \mathbf{I}_B)$ is circularly-symmetric complex Gaussian noise with per-entry variance N_0 . In this paper, we consider \mathcal{S} to be QPSK (though larger constellations would also work) scaled to unit symbol power so that $\mathbb{E}[\mathbf{s}_k \mathbf{s}_k^H] = \mathbf{I}_U$. The jammer is a dynamic multi-antenna jammer, meaning that it can dynamically change its jamming activity. Specifically, the jammer can transmit

$$\mathbf{w}_k = \mathbf{A}_k \tilde{\mathbf{w}}_k, \quad (2)$$

²The model in (1) can also represent distributed single- or multi-antenna jammers with a total of I antennas. We consider this case in Sec. IV-D.

where, without loss of generality, the covariance of $\tilde{\mathbf{w}}_k \in \mathbb{C}^I$ is \mathbf{I}_I for all k , and $\mathbf{A}_k \in \mathbb{C}^{I \times I}$ is a beamforming matrix that can change arbitrarily over time, i.e., \mathbf{A}_k depends on k . In particular, \mathbf{A}_k can sometimes be the all-zero matrix (=no jamming), some of its rows can be zero (=the jammer uses only a subset of its antennas), or it can be rank-deficient in some other way.

B. Joint jammer mitigation and data detection

Existing methods typically null a jammer by projecting the receive signal onto the orthogonal complement of the jammer subspace through $\mathbf{P}\mathbf{y}_k$, where³ $\mathbf{P} = \mathbf{I}_B - \mathbf{J}\mathbf{J}^\dagger$ is the orthogonal projection onto $\text{col}(\mathbf{J})^\perp$, which has the property that $\mathbf{P}\mathbf{J} = \mathbf{0}$. After the projection, the data can be detected using the virtual channel matrix $\mathbf{H}_\mathbf{P} = \mathbf{P}\mathbf{H}$, since

$$\mathbf{P}\mathbf{y}_k = \mathbf{P}\mathbf{H}\mathbf{s}_k + \mathbf{P}\mathbf{J}\mathbf{A}_k \tilde{\mathbf{w}}_k + \mathbf{P}\mathbf{n}_k = \mathbf{P}\mathbf{H}\mathbf{s}_k + \mathbf{P}\mathbf{n}_k \quad (3)$$

$$\triangleq \mathbf{H}\mathbf{P}\mathbf{s}_k + \mathbf{n}_{\mathbf{P},k}. \quad (4)$$

Note that this works regardless of which vectors $\tilde{\mathbf{w}}_k$ and which matrices \mathbf{A}_k the jammer uses, since $\text{col}(\mathbf{J}) \supseteq \text{col}(\mathbf{J}\mathbf{A}_k)$ and so $\text{col}(\mathbf{J})^\perp \subseteq \text{col}(\mathbf{J}\mathbf{A}_k)^\perp$ for any \mathbf{A}_k . The problem, however, is how to reliably estimate \mathbf{J} —or $\text{col}(\mathbf{J})$ —when the jammer changes \mathbf{A}_k dynamically such that $\text{col}(\mathbf{J}\mathbf{A}_k)$ depends on k .

The central idea of *JMD* is to consider jammer subspace estimation, jammer mitigation, and data detection over an entire transmission frame (or coherence interval) simultaneously: The jammer subspace is identified with the subspace that is not explainable in terms of UE transmit signals, which are estimated iteratively while projecting the receive signals onto the orthogonal complement of the current estimate of the jammer subspace. Mathematically, this can be framed as solving

$$\min_{\tilde{\mathbf{S}}_D, \tilde{\mathbf{P}}} \|\tilde{\mathbf{P}}\mathbf{Y}_D - \tilde{\mathbf{P}}\mathbf{H}\tilde{\mathbf{S}}_D\|_F^2, \quad (5)$$

where $\mathbf{Y}_D = [\mathbf{y}_1, \dots, \mathbf{y}_D]$ is the data receive matrix over an entire coherence interval, $\tilde{\mathbf{S}}_D = [\tilde{\mathbf{s}}_1, \dots, \tilde{\mathbf{s}}_D] \in \mathcal{S}^{U \times D}$ is the data matrix estimate, and $\tilde{\mathbf{P}} = \mathbf{I}_B - \tilde{\mathbf{J}}\tilde{\mathbf{J}}^\dagger$ is the projection onto the orthogonal complement of the estimated jammer subspace $\text{col}(\tilde{\mathbf{J}})$, with $\tilde{\mathbf{J}} \in \mathbb{C}^{B \times I}$. The range over which we optimize $\tilde{\mathbf{P}}$ is the Grassmannian manifold $\mathcal{G}_{B-I}(\mathbb{C}^B)$, i.e., the set of orthogonal projections onto $(B-I)$ -dimensional subspaces of \mathbb{C}^B .

In practice, however, the UE channel matrix \mathbf{H} is *a priori* unknown and has to be estimated with pilots. In the presence of jamming, the obtained estimate can be contaminated. Thankfully, however, the contamination of the pilot receive signal will be restricted to the subspace $\text{col}(\mathbf{J})$. In [13], it was thus proposed to jointly solve the problems of channel estimation, jammer subspace estimation and mitigation, and data detection by solving an optimization problem which depends on $\tilde{\mathbf{S}}_D$, $\tilde{\mathbf{P}}$, and $\tilde{\mathbf{H}}_{\tilde{\mathbf{P}}}$. This approach is highly effective, but unfortunately, even approximately solving the proposed optimization problem is computationally demanding. For instance, the algorithm proposed in [13] requires the inversion of a $U \times U$ matrix for gradient calculation in every iteration.

As it turns out, and this is a key insight of our paper, it is not necessary to estimate \mathbf{H} jointly with the jammer subspace and

³In this paper, \dagger denotes the pseudo-inverse, $\text{col}(\mathbf{M})$ is the column space of \mathbf{M} , and \perp denotes the orthogonal complement.

the data symbols: One can also estimate the channel separately, leading to algorithms with significantly lower complexity. Consider least square (LS) channel estimation with unitary pilots $\mathbf{S}_T \in \mathbb{C}^{U \times \bar{U}}$ and receive matrix \mathbf{Y}_T :

$$\mathbf{Y}_T = \mathbf{H}\mathbf{S}_T + \mathbf{J}\mathbf{W} + \mathbf{N} \quad (6)$$

$$\hat{\mathbf{H}} = \mathbf{Y}_T \mathbf{S}_T^H = \mathbf{H} + \mathbf{J}\mathbf{W}\mathbf{S}_T^H + \mathbf{N}\mathbf{S}_T^H. \quad (7)$$

Note how after despreading, the jammer contamination of the channel estimate is still restricted to $\text{col}(\mathbf{J})$.⁴ If we therefore simply plug this estimate $\hat{\mathbf{H}}$ into (5) as follows

$$\min_{\tilde{\mathbf{S}}_D, \tilde{\mathbf{P}}} \|\tilde{\mathbf{P}}\mathbf{Y}_D - \tilde{\mathbf{P}}\hat{\mathbf{H}}\tilde{\mathbf{S}}_D\|_F^2, \quad (8)$$

then the “true” projection $\mathbf{P} = \mathbf{I}_B - \mathbf{J}\mathbf{J}^\dagger$ also removes the jammer contamination of the channel estimate. This means that we can leverage the concept of joint jammer subspace estimation, jammer mitigation, and data detection, without having to also jointly estimate \mathbf{H} , and without having to worry about jammer contamination of the channel estimate. In summary, the JMD paradigm can be formulated as follows:

Joint Jammer Mitigation and Data Detection (JMD)

Given the received data matrix $\mathbf{Y}_D \in \mathbb{C}^{B \times D}$ of an entire coherence interval and a linear channel estimate $\hat{\mathbf{H}} = f(\mathbf{Y}_D)$ from that same coherence interval, solve

$$\min_{\substack{\tilde{\mathbf{S}}_D \in \mathcal{S}^{U \times D}, \\ \tilde{\mathbf{P}} \in \mathcal{G}_{B-I}(\mathbb{C}^B)}} \|\tilde{\mathbf{P}}(\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}_D)\|_F^2. \quad (9)$$

III. THE SANDMAN ALGORITHM

Solving (9) exactly is difficult, so we solve it approximately. A key difficulty is that, due to the discreteness of \mathcal{S} , the problem in (9) is NP-hard even when fixing $\tilde{\mathbf{P}}$ and solving only for $\tilde{\mathbf{S}}_D$ [19]. We thus relax the constraint set \mathcal{S} to its convex hull $\mathcal{C} \triangleq \text{conv}(\mathcal{S})$. To promote symbol estimates at, or near, the corner points of \mathcal{C} (i.e., the constellation points \mathcal{S}), we add a concave regularizer $-\|\tilde{\mathbf{S}}_D\|_F^2$ weighted by $\alpha > 0$ to the objective [20]. We colloquially refer to the resulting constraint and regularizer as a *box prior*. The modified problem is thus

$$\min_{\substack{\tilde{\mathbf{S}}_D \in \mathcal{C}^{U \times D}, \\ \tilde{\mathbf{P}} \in \mathcal{G}_{B-I}(\mathbb{C}^B)}} \|\tilde{\mathbf{P}}(\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}_D)\|_F^2 - \alpha\|\tilde{\mathbf{S}}_D\|_F^2. \quad (10)$$

This problem is still non-convex, mainly due to the non-convex constraint set $\mathcal{G}_{B-I}(\mathbb{C}^B)$ of $\tilde{\mathbf{P}}$. However, we have the following theorem, the proof of which is omitted due to lack of space.

Theorem 1. *When $\tilde{\mathbf{P}}$ is fixed and $\alpha \leq \lambda_{\min}((\tilde{\mathbf{P}}\hat{\mathbf{H}})^H\tilde{\mathbf{P}}\hat{\mathbf{H}})$, then the objective in (10) is convex in $\tilde{\mathbf{S}}_D$. Vice versa, when $\tilde{\mathbf{S}}_D$ is fixed, then the objective in (10) is minimized with respect to $\tilde{\mathbf{P}}$ by $\mathbf{I}_B - \mathbf{U}_I \mathbf{U}_I^H$, where $\mathbf{U}_I \in \mathbb{C}^{B \times I}$ consists of the I dominant left-singular vectors of $\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}_D$.*

This theorem suggests to use an alternating minimization strategy, as solving (10) for either $\tilde{\mathbf{S}}_D$ or $\tilde{\mathbf{P}}$ is straightforward while the other quantity is fixed.

⁴This would also be the case for other linear channel estimates $\hat{\mathbf{H}} = f(\mathbf{Y}_D)$, such as the LMMSE channel estimate.

1) *Solving for $\tilde{\mathbf{S}}_D$:* To solve the problem in (10) for $\tilde{\mathbf{S}}_D$, we use forward-backward splitting (FBS) [21]. FBS is a method for iteratively solving convex optimization problems of the form

$$\min_{\tilde{\mathbf{s}}} f(\tilde{\mathbf{s}}) + g(\tilde{\mathbf{s}}), \quad (11)$$

where f is convex and differentiable, and g is convex but need not be differentiable, smooth, or bounded. FBS solves the problem in (11) by iteratively computing

$$\tilde{\mathbf{s}}^{(t+1)} = \text{prox}_g(\tilde{\mathbf{s}}^{(t)} - \tau^{(t)} \nabla f(\tilde{\mathbf{s}}^{(t)}); \tau^{(t)}), \quad (12)$$

where $\tau^{(t)}$ is the stepsize at iteration t , ∇f is the gradient of f , and prox_g is the proximal operator of g , defined as [22]

$$\text{prox}_g(\tilde{\mathbf{s}}; \tau) = \arg \min_{\tilde{\mathbf{x}}} \tau g(\tilde{\mathbf{x}}) + \frac{1}{2} \|\tilde{\mathbf{s}} - \tilde{\mathbf{x}}\|_2^2. \quad (13)$$

FBS solves convex problems exactly (for a sufficient number of iterations with suitable stepsizes $\tau^{(t)}$), but it is also effective for approximately solving non-convex problems [21]. To solve the problem in (10), we define the functions f and g as

$$f(\tilde{\mathbf{S}}_D) = \|\tilde{\mathbf{P}}(\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}_D)\|_F^2, \quad (14)$$

$$g(\tilde{\mathbf{S}}_D) = -\alpha\|\tilde{\mathbf{S}}_D\|_F^2 + \chi_{\mathcal{C}}(\tilde{\mathbf{S}}_D), \quad (15)$$

where $\chi_{\mathcal{C}}$ acts entrywise on $\tilde{\mathbf{S}}_D$ as the indicator function of \mathcal{C} ,

$$\chi_{\mathcal{C}}(\tilde{s}) = \begin{cases} 0 & : \tilde{s} \in \mathcal{C} \\ \infty & : \tilde{s} \notin \mathcal{C}. \end{cases} \quad (16)$$

The gradient of f in $\tilde{\mathbf{S}}_D$ is given as

$$\nabla f(\tilde{\mathbf{S}}) = -2\hat{\mathbf{H}}^H\tilde{\mathbf{P}}(\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}). \quad (17)$$

The proximal operator of g acts entrywise on $\tilde{\mathbf{S}}_D$ and is given as $\text{prox}_g(\tilde{s}; \tau) = \text{clip}(\tilde{s}/(1 - \tau\alpha); \sqrt{1/2})$ when $\alpha\tau < 1$ (where $\text{clip}(z; a)$ clips the real and imaginary part of $z \in \mathbb{C}$ to the interval $[-a, a]$), and otherwise as $\arg \min_{\tilde{x} \in \{\pm \sqrt{\frac{1}{2}} \pm i\sqrt{\frac{1}{2}}\}} |\tilde{s} - \tilde{x}|^2$.

2) *Solving for $\tilde{\mathbf{P}}$:* According to Thm. 1, we can solve for $\tilde{\mathbf{P}}$ (for fixed $\tilde{\mathbf{S}}_D$) by calculating the I dominant left-singular vectors \mathbf{U}_I of $\mathbf{Y}_D - \hat{\mathbf{H}}\tilde{\mathbf{S}}_D$. Instead of performing an exact but computationally expensive singular value decomposition of this matrix, we approximate \mathbf{U}_I with the power method from [23], where we perform a single power iteration per dimension.

The SANDMAN algorithm alternates between descent steps in $\tilde{\mathbf{S}}_D$ and approximate computations of $\tilde{\mathbf{P}}$ for a total number of t_{\max} iterations. We choose $\alpha = 2.5$, and the stepsizes $\tau^{(t)}$ are selected using the Barzilai-Borwein criterion detailed in [24]. SANDMAN is summarized in Alg. 1 and has a complexity of $O(t_{\max}UDB)$, i.e., its complexity is linear in U , D , and B .

IV. EVALUATION

A. Simulation setup

We evaluate SANDMAN through simulations. We simulate a MU-MIMO system with $B = 32$ BS antennas and $U = 16$ single-antenna UEs at a carrier frequency of 2 GHz using the 3GPP 38.901 urban macrocellular (UMa) channel model [25]. The channel vectors are generated with QuaDRiGa [26]. The

Algorithm 1 SANDMAN

```

1: function SANDMAN( $\mathbf{Y}_D, \mathbf{Y}_T, \mathbf{S}_T, I, t_{\max}$ )
2:    $\hat{\mathbf{H}} = \mathbf{Y}_T \mathbf{S}_T^H$  // LS channel estimate
3:    $\tilde{\mathbf{S}}^{(0)} = \mathbf{0}_{U \times D}$ 
4:   for  $t = 0$  to  $t_{\max} - 1$  do
5:      $\tilde{\mathbf{E}}^{(t)} = [\mathbf{Y}_T, \mathbf{Y}_D] - \hat{\mathbf{H}}[\mathbf{S}_T, \tilde{\mathbf{S}}^{(t)}]$ 
6:      $\tilde{\mathbf{J}}^{(t)} = \text{APPROXSVDF}(\tilde{\mathbf{E}}^{(t)}, I)$  // cf. [23]
7:      $\tilde{\mathbf{P}}^{(t)} = \mathbf{I}_B - \tilde{\mathbf{J}}^{(t)}(\tilde{\mathbf{J}}^{(t)})^\dagger$ 
8:      $\nabla f(\tilde{\mathbf{S}}^{(t)}) = -2 \hat{\mathbf{H}}^H \tilde{\mathbf{P}}^{(t)} (\mathbf{Y}_D - \hat{\mathbf{H}} \tilde{\mathbf{S}}^{(t)})$ 
9:      $\tilde{\mathbf{S}}^{(t+1)} = \text{prox}_g(\tilde{\mathbf{S}}^{(t)} - \tau^{(t)} \nabla f(\tilde{\mathbf{S}}^{(t)}); \tau^{(t)})$ 
10:   end for
11:   output:  $\tilde{\mathbf{S}}^{(t_{\max})}$ 
12: end function

```

BS antennas are arranged as a uniform linear array (ULA) and spaced at half wavelength. The UEs are uniformly distributed at distances between 10 m and 250 m in a 120° angular sector in front of the BS, and with a minimum angular separation of 1° between any two UEs. All antennas are omnidirectional. We assume ±3 dB per-UE power control. Furthermore, we assume a coherence time of $K = 100$ channel uses. The specific jammer model varies between the different experiments. In general, we consider $J \geq 1$ jammers placed randomly in the same area as the UEs, with a minimum angular separation of 1° between any two jammers as well as between any jammer and any UE. Every jammer is equipped with $I/J \geq 1$ antennas arranged as a ULA with half-wavelength spacing that is frontally facing in the direction of the BS.

We consider QPSK transmission. The pilots are selected as rows of a $U \times U$ Hadamard matrix (normalized to unit symbol energy). We define the average signal-to-noise ratio (SNR) as

$$SNR \triangleq \frac{\mathbb{E}_S[\|\mathbf{H}\mathbf{S}\|_F^2]}{\mathbb{E}_N[\|\mathbf{N}\|_F^2]}. \quad (18)$$

Furthermore, we characterize the strength of the jammer interference relative to the strength of the average UE via

$$\rho \triangleq \frac{\|\mathbf{J}\mathbf{W}\|_F^2}{\frac{1}{U} \mathbb{E}_S[\|\mathbf{H}\mathbf{S}\|_F^2]}, \quad (19)$$

where we deterministically scale $\mathbf{J}\mathbf{W}$ to a pre-specified ρ . As performance metrics, we consider uncoded bit error rate (BER) and a metric that we call the modulation error ratio (MER) between the data symbols \mathbf{S}_D and their estimate $\hat{\mathbf{S}}_D$,

$$MER \triangleq \mathbb{E}[\|\hat{\mathbf{S}}_D - \mathbf{S}_D\|_F] / \mathbb{E}[\|\mathbf{S}_D\|_F]. \quad (20)$$

We use the MER as a surrogate for error vector magnitude (EVM), which the 3GPP 5G NR technical specification requires to be below 17.5% [27, Tbl. 6.5.2.2-1] for QPSK transmission.

B. Higher data rates against simple jammers

The first advantage of joint jammer mitigation and data detection is increased achievable rates, because no channel uses need to be reserved for estimating the jammer's subspace.

Jammer Model: The rate advantage afforded by the absence of a jammer estimation phase is shown on the following model:

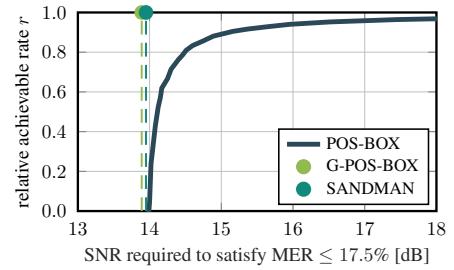


Fig. 1. Trade-off between the relative achievable rate r and the smallest SNR for which the different receivers satisfy the criterion $\text{MER} \leq 17.5\%$ when mitigating a single-antenna barrage jammer ①.

① **Strong single-antenna barrage jammer:** In this model, a single jammer with a single antenna transmits i.i.d. circularly-symmetric complex Gaussian noise over the entire coherence interval, with a relative receive strength that exceeds the receive strength of the average UE by $\rho = 30$ dB.

Baselines: The following receivers are used as baselines:

G-POS-BOX: This receiver serves as a performance upper bound. It works analogous to SANDMAN but is furnished with ground-truth knowledge of the jammer channel \mathbf{J} , and fixes $\tilde{\mathbf{P}}^{(t)}$ in line 7 of Alg. 1 to the optimal projector $\mathbf{P} = \mathbf{I}_B - \mathbf{J}\mathbf{J}^\dagger$.

POS-BOX: This receiver uses a protocol in which, at the beginning of every coherence interval, the UEs do not transmit for L channel uses (at cost of a reduced $D = K - U - L$). The receive matrix $\mathbf{Y}_J \in \mathbb{C}^{B \times L}$ from this period is used to estimate the jammer subspace as the strongest I left singular vectors of \mathbf{Y}_J . The jammer is then mitigated by projecting subsequent receive signals onto the orthogonal complement of the estimated subspace, and by performing LS channel estimation and FBS-based data detection with a box prior (analogous to SANDMAN) in that projected space.

All algorithms run for $t_{\max} = 30$ iterations.

Results: Fig. 1 depicts the results. To assess the rate advantage afforded by the absence of a jammer estimation phase, we consider the tradeoff between the SNR threshold for which a receiver satisfies the criterion $\text{MER} \leq 17.5\%$ and the ratio

$$r = \frac{K - U - L}{K - U} \quad (21)$$

that is the number of samples $K - U - L$ available per coherence interval for data transmission, normalized by the maximum number of samples $K - U$ available when using orthogonal pilots and no jammer estimation phase. Clearly, r translates directly to achievable data rate (in bits/s). Both SANDMAN and G-POS-BOX do not have a jammer estimation phase ($L = 0$) and hence have $r = 1$. In contrast, the performance of POS-BOX improves as L is increased to obtain a better estimate of the jammer subspace, at the expense of r . The results show that SANDMAN, which utilizes the receive data of the entire coherence interval to estimate the jammer subspace, achieves virtually the same performance as G-POS-BOX, with the required SNR differing only by about 0.1 dB. POS-BOX, in contrast, can use only a subset of the receive samples to estimate

the jammer subspace, and so performs much worse even when sacrificing a large part of the coherence time for jammer estimation. To approach the performance of SANDMAN up to 0.5 dB, G-POS-BOX has to accept a 20% rate reduction. G-POS-BOX does not even outperform SANDMAN when using virtually the *entire* coherence interval for jammer estimation (at the expense of a vanishing rate r). This shows that SANDMAN can leverage the same receive data *twice*—for jammer estimation *and* for data detection—without impairing performance.

C. Mitigating smart single-antenna jammers

In this experiment, we analyze SANDMAN’s ability to mitigate smart jammers that would suspending jamming during a potential training phase, and that target only specific parts (such as the pilot phase or the data phase) of the transmission.

Jammer Model: Besides a strong barrage jammer (1), we consider the following types of smart (time-variant) jammers:

(2) **Strong single-antenna data jammer:** A single-antenna jammer that does not jam the pilot phase but transmits i.i.d. complex Gaussian noise during the data phase with $\rho = 30$ dB.

(3) **Strong single-antenna pilot jammer:** A single-antenna jammer that does not jam the data phase but transmits i.i.d. complex Gaussian noise during the pilot phase with $\rho = 30$ dB.

Baselines: Besides G-POS-BOX (cf. Sec. IV-B), the following baselines are considered:⁵

LMSE: This receiver does not mitigate the jammer and so provides a lower bound on performance. It performs LS channel estimation and (jammer-oblivious) LMSE data detection.

MAED 2.0: This is an extension of MAED [13] for single-*and* multi-antenna jammers. In contrast to SANDMAN, it uses joint channel estimation and data detection (JED), which leads to better performance at increased computational cost [28].⁶

G-POS-JED: A performance upper bound for MAED 2.0. It works analogous to MAED 2.0 (using JED) but uses ground-truth knowledge of \mathbf{J} for the optimal projector $\mathbf{P} = \mathbf{I}_B - \mathbf{J}\mathbf{J}^\dagger$.

All iterative algorithms run for $t_{\max} = 30$ iterations.

Results: Fig. 2 depicts the results. As expected, the non-mitigating LMSE receiver always has by far the worst performance, though it does not suffer equally under all jammers. G-POS-BOX and the G-POS-JED use ground-truth knowledge to null the jammer perfectly in all cases, so that their performance does not depend on the jammer transmit signal. Consequently, their BER curves are identical for all types of single-antenna jammers (1 - 3), with G-POS-JED slightly outperforming G-POS-BOX due to the advantage of JED over separate channel estimation and data detection. The results show that SANDMAN and MAED 2.0 both achieve virtually the same performance as their respective performance upper bounds (which rely on ground-truth jammer knowledge) for all simulated jammer types. This implies that SANDMAN and MAED 2.0 are able to estimate the jammer subspace essentially perfectly, regardless of when the jammer is active.

⁵Training-period based mitigation methods are incapable of mitigating smart jammers, see [13], which is why our comparison omits POS-BOX.

⁶A full description of MAED 2.0 will be provided in an extended journal version of this paper which is in preparation.

D. Mitigating distributed jammers and multi-antenna jammers

Jammer Model: We consider both distributed and multi-antenna jammers. The difference is that distributed jammers cannot form beams while multi-antenna jammers can use dynamic beamforming to change their subspace but are colocated.

(4) **Distributed barrage jammers:** We consider four distributed single-antenna jammers that transmit (independent of each other) i.i.d. Gaussian noise with $\rho = 30$ dB (each jammer transmits at 24 dB more receive power than the average UE).

(5) **Jump-varying beamforming jammer:** We consider a single four-antenna jammer that, at every instant k , transmits only on a random subset of between one and three of its antennas. This is achieved by selecting only a random subset of the rows of its beamforming matrix \mathbf{A}_k (see (2)) to be nonzero (nonzero rows have i.i.d. Gaussian entries), and by switching to a completely new matrix \mathbf{A}_k at random instances $k_1, \dots, k_M, M = 5$. The jamming vectors $\tilde{\mathbf{w}}_k$ have distribution $\{\tilde{\mathbf{w}}_k\} \stackrel{\text{i.i.d.}}{\sim} \mathcal{CN}(\mathbf{0}, \mathbf{I}_I)$.

(6) **Continuously-varying beamforming jammer:** This (single) jammer also has four antennas. Only the leftmost column $\mathbf{a}_{k,1}$ of its beamforming matrix \mathbf{A}_k (see (2)) is nonzero. For randomly selected instances $k_1, \dots, k_M, M = 5$, with $k_m < k_{m+1}$, the vector $\mathbf{a}_{k,1}$ is fixed to randomly and independently drawn vectors $\{\mathbf{a}^{(m)}\}_{m=1}^M$. For $k_m < k < k_{m+1}$, $\mathbf{a}_{k,1}$ interpolates smoothly between $\mathbf{a}^{(m)}$ and $\mathbf{a}^{(m+1)}$. The jamming vectors $\tilde{\mathbf{w}}_k$ have distribution $\{\tilde{\mathbf{w}}_k\} \stackrel{\text{i.i.d.}}{\sim} \mathcal{CN}(\mathbf{0}, \mathbf{I}_I)$.

Baselines: We consider the same baselines as in Sec. IV-C. All iterative algorithms run for $t_{\max} = 50$ iterations.

Results: Fig. 3 depicts the results. The LMSE receiver has again by far the worst performance with double-digit BER percentages. Because they have to null four dimensions, G-POS-JED and G-POS-BOX perform slightly worse than in Sec. IV-C (where they only have to project away one dimension), but they again null all jammers perfectly. In case of the distributed barrage jammers (4), SANDMAN and MAED 2.0 perform again very close to their respective performance bounds, meaning that they mitigate the jammers almost perfectly. SANDMAN and MAED 2.0 are also able to successfully mitigate the dynamic multi-antenna jammers (5, 6): They achieve BERs significantly below 1% at high SNR, even if the BER eventually levels off a bit above 0.1%. But the jammers (5) and (6) are incredibly difficult to mitigate, since the jamming subspace is changed repeatedly, with some subspaces potentially being used only for extremely brief amounts of time.

V. CONCLUSIONS

We have proposed joint jammer mitigation and data detection (JMD), a novel paradigm for mitigating jammers in MIMO systems that does not use a dedicated jammer training period. As a result, JMD is able to mitigate smart jammers regardless of (i) when they are active and (ii) how they vary their multi-antenna transmit beamforming. We then have proposed SANDMAN, an efficient JMD-type algorithm for jammer mitigation in the MU-MIMO uplink. Simulation results for a variety of different jammers types have demonstrated the utility of the JMD paradigm, and of SANDMAN in particular.

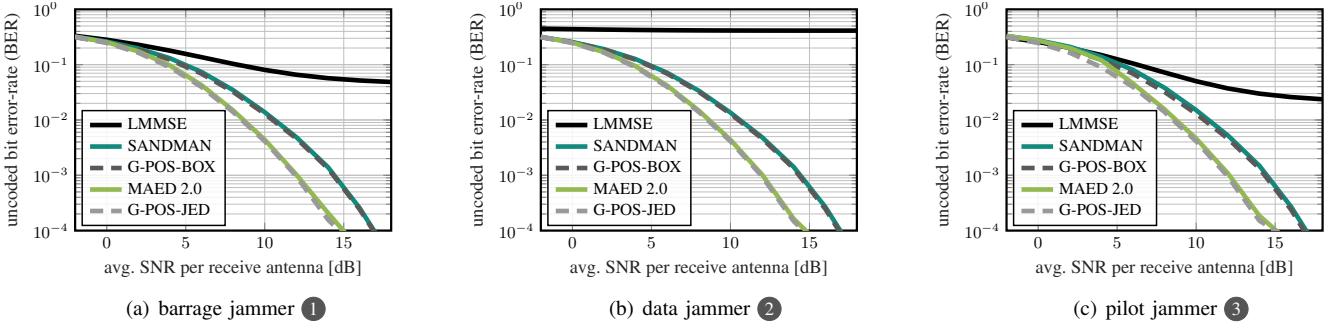


Fig. 2. Uncoded bit error-rate (BER) vs. SNR performance of different receivers when mitigating different kinds of smart single-antenna jammers.

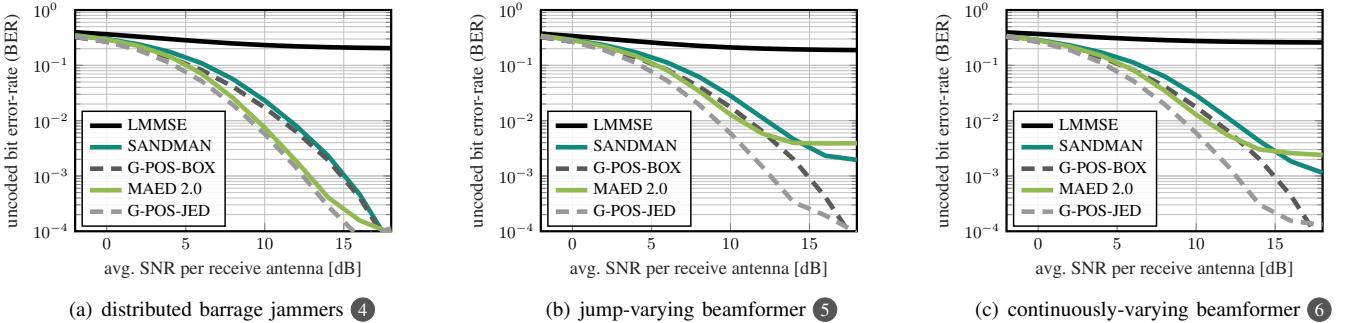


Fig. 3. Uncoded bit error-rate (BER) vs. SNR performance of different receivers when mitigating distributed jammers or dynamic multi-antenna jammers.

REFERENCES

- [1] J. Kosinski *et al.*, “Top Gun: Maverick,” Paramount Pictures, 2022.
- [2] 5G Threat Model Working Panel, “Potential threat vectors to 5G infrastructure,” *CISA, NSA, and DNI*.
- [3] T. Harrison, K. Johnson, M. Young, N. Wood, and A. Goessler, “Space threat assessment 2022,” *Center Strategic Int. Studies (CSIS)*, Apr. 2022.
- [4] “Satellite-navigation systems such as GPS are at risk of jamming,” *The Economist*, May 2021. [Online]. Available: <https://www.economist.com/science-and-technology/2021/05/06/satellite-navigation-systems-such-as-gps-are-at-risk-of-jamming>
- [5] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 767–809, Mar. 2022.
- [6] W. Shen, P. Ning, X. He, H. Dai, and Y. Liu, “MCR decoding: A MIMO approach for defending against wireless jamming attacks,” in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Oct. 2014, pp. 133–138.
- [7] G. Marti, O. Castañeda, and C. Studer, “Jammer mitigation via beam-slicing for low-resolution mmWave massive MU-MIMO,” *IEEE Open J. Circuits Syst.*, vol. 2, pp. 820–832, Dec. 2021.
- [8] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, “Jamming resilient communication using MIMO interference cancellation,” *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1486–1499, Jul. 2016.
- [9] T. T. Do, E. Björnsson, E. G. Larsson, and S. M. Razavizadeh, “Jamming-resistant receivers for the massive MIMO uplink,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.
- [10] H. Akhlaghpasand, E. Björnsson, and S. M. Razavizadeh, “Jamming suppression in massive MIMO systems,” *IEEE Trans. Circuits Syst. II*, vol. 68, no. 1, pp. 182–186, Jan. 2020.
- [11] T. T. Nguyen and K.-K. Nguyen, “Anti-jamming in cell free mMIMO systems,” in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, Dec. 2021, pp. 1–6.
- [12] Y. Léost, M. Abdi, R. Richter, and M. Jeschke, “Interference rejection combining in LTE networks,” *Bell Labs Tech. J.*, vol. 17, no. 1, pp. 25–50, Jun. 2012.
- [13] G. Marti, T. Kölle, and C. Studer, “Mitigating smart jammers in multi-user MIMO,” *arXiv preprint arXiv:2208.01453*.
- [14] L. M. Hoang, J. A. Zhang, D. N. Nguyen, X. Huang, A. Kekirigoda, and K.-P. Hui, “Suppression of multiple spatially correlated jammers,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10489–10500, Sep. 2021.
- [15] H. Zeng, C. Cao, H. Li, and Q. Yan, “Enabling jamming-resistant communications in wireless MIMO networks,” in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Oct. 2017, pp. 1–9.
- [16] G. Marti, O. Castañeda, S. Jacobsson, G. Durisi, T. Goldstein, and C. Studer, “Hybrid jammer mitigation for all-digital mmWave massive MU-MIMO,” in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Nov. 2021, pp. 93–99.
- [17] Z. Gülgün, E. Björnsson, and E. G. Larsson, “Is massive MIMO robust against distributed jammers?” *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 457–469, Jan. 2021.
- [18] J. Vinogradova, E. Björnsson, and E. G. Larsson, “Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory,” in *Proc. IEEE Int. Workshop Signal Process. Advances Wireless Commun. (SPAWC)*, Jul. 2016.
- [19] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric algorithms and combinatorial optimization*. Springer, 2012.
- [20] S. Shah, A. K. Yadav, C. D. Castillo, D. W. Jacobs, C. Studer, and T. Goldstein, “Biconvex relaxation for semidefinite programming in computer vision,” in *Eur. Conf. Comput. Vision*, Sep. 2016, pp. 717–735.
- [21] T. Goldstein, C. Studer, and R. G. Baraniuk, “A field guide to forward-backward splitting with a FASTA implementation,” Feb. 2016. [Online]. Available: <https://arxiv.org/abs/1411.3406>
- [22] N. Parikh and S. Boyd, “Proximal algorithms,” *Found. Trends Optim.*, vol. 1, no. 3, pp. 127–239, Jan. 2014.
- [23] E. Liberty, “Algorithms in Data Mining, Lecture 7: Singular Value Decomposition,” Lecture Notes, Tel Aviv University, Fall 2013.
- [24] B. Zhou, L. Gao, and Y.-H. Dai, “Gradient methods with adaptive step-sizes,” *Comp. Optimization Applicat.*, vol. 35, no. 1, pp. 69–86, Mar. 2006.
- [25] 3GPP, “3GPP TR 38.901,” Mar. 2022, version 17.0.0.
- [26] S. Jaeckel, L. Raschkowski, K. Börner, and L. Thiele, “QuaDRiGa: A 3-D multi-cell channel model with time evolution for enabling virtual field trials,” *IEEE Trans. Antennas Propag.*, vol. 62, no. 6, pp. 3242–3256, Jun. 2014.
- [27] 3GPP, “5G; NR; base station (BS) radio transmission and reception,” Mar. 2021, TS 38.104 version 17.1.0 Rel. 17.
- [28] H. Vikalo, B. Hassibi, and P. Stoica, “Efficient joint maximum-likelihood channel estimation and signal detection,” *IEEE Trans. Wireless Commun.*, vol. 5, no. 7, pp. 1838–1845, Jul. 2006.