Resilient-By-Design Framework for MIMO-OFDM Communications under Smart Jamming

Vlad C. Andrei*, Aladin Djuhera*, Xinyang Li*, Ullrich J. Mönich*, Holger Boche*and Walid Saad†

*Chair of Theoretical Information Technology, Technical University of Munich, Munich, Germany
†Electrical and Computer Engineering Department, Virginia Tech, Arlington, USA,
Emails: {vlad.andrei, aladin.djuhera, xinyang.li, moenich, boche}@tum.de, walids@vt.edu

Abstract—Native jamming mitigation is essential for addressing security and resilience in future 6G wireless networks. In this paper a resilient-by-design framework for effective anti-jamming in MIMO-OFDM wireless communications is introduced. A novel approach that integrates information from wireless sensing services to develop anti-jamming strategies, which do not rely on any prior information or assumptions on the adversary's concrete setup, is explored. To this end, a method that replaces conventional approaches to noise covariance estimation in anti-jamming with a surrogate covariance model is proposed, which instead incorporates sensing information on the jamming signal's directions-of-arrival (DoAs) to provide an effective approximation of the true jamming strategy. The study further focuses on integrating this novel, sensing-assisted approach into the joint optimization of beamforming, user scheduling and power allocation for a multi-user MIMO-OFDM uplink setting. Despite the NP-hard nature of this optimization problem, it can be effectively solved using an iterative water-filling approach. In order to assess the effectiveness of the proposed sensing-assisted jamming mitigation, the corresponding worst-case jamming strategy is investigated, which aims to minimize the total user sum-rate. Experimental simulations eventually affirm the robustness of our approach against both worst-case and barrage jamming, demonstrating its potential to address a wide range of jamming scenarios. Since such an integration of sensing-assisted information is directly implemented on the physical layer, resilience is incorporated preemptively by-design.

Index Terms—6G, Worst-Case Jamming, Multiple-Input-Multiple-Output (MIMO), Resilience-by-Design, Resource Allocation, User Scheduling

I. INTRODUCTION

The advent of 6G networks is set to advance wireless communications with the introduction of novel applications such as immersive extended reality, distributed learning and ultra-precise localization services [1]. In order to guarantee security and ensure user trust, such services will inevitably demand more stringent and increasingly challenging requirements regarding resilience and trustworthiness of the wireless system design [2]. A critical aspect of ensuring this trust

is the implementation of robust protection schemes against adversarial jammers, who may seek to severely disrupt these services. In particular, resilient-by-design systems [3] will be needed, i.e. systems, which preemptively provide protection against denial-of-service (DoS) attacks, as well as inherently detect, remediate and recover from those. Furthermore, with the continuous fusion of data and services in 6G, wireless sensing services may offer an additional wealth of valuable information. This motivates the study of whether such sensing information can be harnessed to augment existing jamming mitigation schemes [4].

Prior works in the context of anti-jamming, while substantial, have traditionally either only studied mitigation techniques for OFDM and multi-user MIMO systems separately, as in [5]–[7], or imposed strong assumptions on the adversary's knowledge and setup. For example, recent work in [8] and [9] only consider single- or few-antenna jammers with common secrets being exchanged between legitimate parties. This essentially excludes worst-case jammers, i.e. the most disruptive kind with comprehensive system knowledge, as studied in [10]–[13]. Thus, we move away from such strong and potentially unrealistic assumptions towards intelligent and reconfigurable worst-case jammers with arbitrary antenna configurations and develop a universally applicable anti-jamming methodology on the basis of sensing-assisted information on the jamming signal DoAs. Additionally, we extend our studies by further considering optimal scheduling and resource allocation, filling the gap in the literature regarding the integration of anti-jamming strategies with the complexities of joint beamforming, scheduling, and resource allocation in multi-user MIMO-OFDM channels [6].

In the following sections, a sensing-assisted anti-jamming framework is developed solely on the basis of available DoA information at the legitimate transceivers, whereno limitations are imposed onto the jammer. To this end, first the wireless system model for multi-user MIMO-OFDM channels is introduced. Second, jamming resilience is incorporated into the system by means of an optimization objective, which maximizes the user sum-rate at the legitimate parties. In this problem, any explicit knowledge about the jamming strategy is replaced by a surrogate expression, which is dependent on the jamming signal DoAs only. The optimization problem is then solved using an iterative water-filling approach [14]. In order to

verify the effectiveness of the solution, the worst-case jamming strategy is developed with full system knowledge at the adversary and the anti-jamming framework is benchmarked against it, yielding substantially better performance. This introduces a novel, sensing-assisted approach to anti-jamming, which is robust even against the worst-case of adversarial jamming.

II. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a MIMO-OFDM uplink scenario involving Q legitimate users (UEs), one legitimate base station (BS), and one jammer. In every slot, each user $q \in \mathcal{Q} = \{1, \ldots, Q\}$ is allocated a resource set $\mathcal{R}_q = \mathcal{N}_q \times \mathcal{K}_q$ consisting of a subcarrier set $\mathcal{N}_q$ and a symbol set $\mathcal{K}_q$, which satisfy $\cup_{q=1}^Q \mathcal{N}_q \subseteq \mathcal{N} = \{1, \ldots, N\}$ and $\cup_{q=1}^Q \mathcal{K}_q \subseteq \mathcal{K} = \{1, \ldots, K\}$, where N and K denote the total number of subcarriers and OFDM symbols available. Each user q subsequently maps his zero-mean, unit-variance Gaussian data symbol s_{qnk} onto the resource element (RE) and transmits the signal $\boldsymbol{x}_{qnk} = \alpha_{qnk} \sqrt{p_{qnk}} \boldsymbol{w}_{qnk} s_{qnk}$ through his N_{T_q} antennas. Here $\boldsymbol{w}_{qnk}$, p_{qnk} denote the beamforming vector and the power allocation, while $\alpha_{qnk} \in \{0, 1\}$ indicates whether data is scheduled at subcarrier n and OFDM symbol k. Without loss of generality we assume $N_{T_q} = N_T, \forall q \in \mathcal{Q}$.

The legitimate transmit signals propagate through the channels $\boldsymbol{H}_{qnk}$ before arriving at the BS, which is equipped with N_R receive antennas. The received signal is further corrupted by additive white noise $\boldsymbol{\eta}_{nk} \sim \mathcal{N}\left(\boldsymbol{0}, \sigma^2 \mathbf{I}\right)$ and the worst-case jamming signal $\boldsymbol{u}_{nk} \sim \mathcal{N}\left(\boldsymbol{0}, \boldsymbol{C}_{\boldsymbol{u}_{nk}}\right) \in \mathbb{C}$, which propagates through a separate jamming channel $\boldsymbol{G}_{nk}$. More formally,

$$\boldsymbol{z}_{nk} = \boldsymbol{G}_{nk} \boldsymbol{u}_{nk} + \boldsymbol{\eta}_{nk}, \tag{1}$$

$$\boldsymbol{y}_{nk} = \sum_{q \in \mathcal{Q}} \boldsymbol{H}_{qnk} \boldsymbol{x}_{qnk} + \boldsymbol{z}_{nk} \in \mathbb{C}^{N_R}. \tag{2}$$

Finally, the BS forms estimates $\hat{s}_{qnk} = \boldsymbol{v}_{qnk}^{\mathsf{H}} \boldsymbol{y}_{nk}$ of the data symbols on each RE by applying the linear equalizer $\boldsymbol{v}_{qnk}^{\mathsf{H}} \in \mathbb{C}^{1 \times N_R}$. Both $\boldsymbol{H}_{qnk}$ and $\boldsymbol{G}_{nk}$ are modeled as beamspace channels, that is

$$\boldsymbol{H}_{qnk} = \sum_{l=1}^{L_{H_q}} b_{H_q, lnk} \boldsymbol{a}_{N_R}(\boldsymbol{\theta}_{q,l}) \boldsymbol{a}_{N_{T_q}}^{\mathsf{H}}(\boldsymbol{\psi}_{q,l}), \tag{3}$$

$$\boldsymbol{G}_{nk} = \sum_{l=1}^{L_G} b_{G, lnk}(\boldsymbol{\theta}_{G,l}) \boldsymbol{a}_{N_J}^{\mathsf{H}}(\boldsymbol{\psi}_{G,l}). \tag{4}$$

Here, L_{H_q}, L_G indicate the number of resolvable paths, $\boldsymbol{a}_{\cdot}(\boldsymbol{\theta})$ the steering vectors, and $\boldsymbol{\theta}_{\cdot,l}$, $\boldsymbol{\psi}_{\cdot,l}$, $\alpha_{\cdot,l}$ the azimuth and elevation directions-of-arrival, directions-of-departure, respectively. The terms $b_{H_q, lnk}$ and $b_{G, lnk}$ include the contribution of the path gains, propagation delays and Doppler shift of each multipath component l.

We assume the legitimate parties have perfect knowledge of their link parameters, i.e. $\{\alpha_{qnk}, p_{qnk}, \boldsymbol{w}_{qnk}, \boldsymbol{v}_{qnk}, \boldsymbol{H}_{qnk}, \sigma^2\}$ for all $q \in \mathcal{Q}$ and $(n, k) \in \mathcal{R}_q$, and of the jamming signal DoAs $\boldsymbol{\theta}_G = \{\theta_{G,l}\}_{l=1}^{L_G}$, which might be estimated by the BS and fed

back to the UEs using bistatic sensing services in 6G [1]. For the receiver we consider the *user-sum-rate* metric, defined as

$$R^B = \sum_{\substack{(n,k) \in \mathcal{R} \\ q \in \mathcal{Q}}} \alpha_{qnk} I\left(\hat{s}_{qnk}; s_{qnk}\right) \tag{5}$$

$$= \sum_{\substack{(n,k) \in \mathcal{R} \\ q \in \mathcal{Q}}} \log\left(1 + \frac{|\boldsymbol{v}_{qnk}^{\mathsf{H}} \boldsymbol{H}_{qnk} \boldsymbol{b}_{qnk}|^2}{\boldsymbol{v}_{qnk}^{\mathsf{H}} \boldsymbol{X}_{qnk} \boldsymbol{v}_{qnk}}\right) \tag{6}$$

where $I(\boldsymbol{x}; \boldsymbol{y})$ is the mutual information between two random variables and we defined the interference-plus-noise covariance matrix

$$\boldsymbol{C}_{\boldsymbol{z}_{nk}} = \boldsymbol{G}_{nk} \boldsymbol{C}_{\boldsymbol{u}_{nk}}^{\mathsf{H}} \boldsymbol{G}_{nk} + \sigma^2 \boldsymbol{I}_{N_R} \tag{7}$$

$$\boldsymbol{X}_{qnk} = \sum_{q' \neq q} \boldsymbol{H}_{q'nk} \boldsymbol{b}_{q'nk} \boldsymbol{b}_{q'nk}^{\mathsf{H}} \boldsymbol{H}_{q'nk}^{\mathsf{H}} + \boldsymbol{C}_{\boldsymbol{z}_{nk}}, \tag{8}$$

with $\boldsymbol{b}_{qnk} = \sqrt{p_{qnk}} \alpha_{qnk} \boldsymbol{w}_{qnk}$. The unnormalized optimal equalizers can be then found in closed form as

$$\boldsymbol{v}_{qnk}^B = \boldsymbol{X}_{qnk}^{-1} \boldsymbol{H}_{qnk} \boldsymbol{b}_{qnk} \tag{9}$$

The transmit parameters are chosen such that they maximize the *sum-rate* R^A:

$$R^A = \sum_{(n,k) \in \mathcal{R}} I\left(\boldsymbol{y}_{nk}; \{s_{qnk}\}_{q \in \mathcal{Q}}\right) \tag{10}$$

$$= \sum_{(n,k) \in \mathcal{R}} \log\left(1 + \sum_{q \in \mathcal{Q}} \alpha_{qnk} p_{qnk} \gamma_{qnk}^A(\boldsymbol{C}_{\boldsymbol{z}_{nk}})\right) \tag{11}$$

where $\gamma_{qnk}^A(\boldsymbol{B}) = \boldsymbol{w}_{qnk}^{\mathsf{H}} \boldsymbol{H}_{qnk}^{\mathsf{H}} \boldsymbol{B}^{-1} \boldsymbol{H}_{qnk} \boldsymbol{w}_{qnk}$ for $\boldsymbol{B} \in \mathbb{C}^{N_R \times N_R}$ is the signal-to-interference-noise ratio (SINR). Thus, we can now pose the following joint beamforming, scheduling and power allocation problem as

$$\max_{\substack{\alpha_{qnk}, p_{qnk}, \boldsymbol{w}_{qnk} \\ (n,k) \in \mathcal{R}_q, q \in \mathcal{Q}}} R^A \quad \text{s.t.} \tag{P1}$$

$$\alpha_{qnk} \in \{0, 1\} \tag{C1}$$

$$\alpha_{qnk} p_{qnk} \geq 0 \tag{C2}$$

$$\sum_{(n,k) \in \mathcal{R}_q} \alpha_{qnk} \leq B_q \tag{C3}$$

$$\sum_{(n,k) \in \mathcal{R}_q} \alpha_{qnk} p_{qnk} \leq P_q \tag{C4}$$

$$\|\boldsymbol{w}_{qnk}\|_2^2 \leq 1, \tag{C5}$$

where $B_q = |\mathcal{R}_q|$ is the maximum number of resource blocks which can be allocated to user q and P_q the power constraints. Note that the optimization problem (P1) together with the constraints (C1) to (C5) is a non-linear, non-convex, mixed-integer problem which is generally NP-hard due to the binary variables α_{qnk}. Furthermore, the metrics R^A and R^B depend on the noise covariances $\boldsymbol{C}_{\boldsymbol{z}_{nk}}$ which contain the jamming strategy and channel and are thus not known at the legitimate parties.

In our resilience framework, we assume the jammer has access to all system and physical parameters of all links and

employs more transmit power and antennas than any legitimate party $q \in \mathcal{Q}$, i.e. $P_J \gg P_q$ and $N_J > N_{T_q}, N_R$. The attacker thus seeks to find a jamming strategy for each RE $\boldsymbol{C}_{\boldsymbol{u}_{nk}} \in N_J$ which minimizes the sum rate R^A. This is in contrast to prior works [8], [9], which do not consider this worst-case scenario. More formally,

$$\min_{\substack{\boldsymbol{C}_{\boldsymbol{u}_{nk}} \in \mathbb{C}^{N_J \times N_J} \\ (n,k) \in \mathcal{R}}} R^A \quad \text{s.t.} \tag{P2}$$

$$\boldsymbol{C}_{\boldsymbol{u}_{nk}} = \boldsymbol{C}_{\boldsymbol{u}_{nk}}^{\mathsf{H}}, \quad \boldsymbol{C}_{\boldsymbol{u}_{nk}} \succeq \boldsymbol{0} \tag{J1}$$

$$\sum_{(n,k) \in \mathcal{R}} \left(\operatorname{tr} \left(\boldsymbol{C}_{\boldsymbol{u}_{nk}} \right) \leq P_J, \tag{J2}$$

where $\succeq$ denotes the Löwner partial order. The optimization problem above is a semidefinite program (SDP), which is a convex problem [15]. Thus, a globally optimal solution can be found in polynomial time using interior-point or first-order methods. Both methods traditionally have the disadvantage that they do not scale well for high-dimensional SDPs like this one with a complexity of $O(N_J^4 N^2 K^2)$ or higher [15]. Consequently, in Sections III-A and III-B, we will focus on answering following questions:

1) How can the legitimate parties compute the filters in Equation (9) and solve the problem (P1) efficiently in the absence of the true covariance matrix $\boldsymbol{C}_{\boldsymbol{z}_{nk}}$ using the sensing information $\boldsymbol{\theta}_G$?

2) How can we find a scalable and efficient approximate solution to the worst-case jamming problem (P2)?

III. PROPOSED APPROACH

A. Resilient-by-Design Transceivers

In addition to the NP-hardness of (P1), the rate expression R^A depend on the noise covariance matrix $\boldsymbol{C}_{\boldsymbol{z}_{nk}}$. Since the latter contains the jamming strategy, which is not known in the considered setup, a surrogate expression $\widetilde{\boldsymbol{C}}_{\boldsymbol{z}_{nk}}$ needs to be found, which effectively approximates the true covariance $\boldsymbol{C}_{\boldsymbol{z}_{nk}}$. To this end, it was shown in [16] that such a surrogate covariance can be constructed using available information on the jamming signal DoAs, such that

$$\widetilde{\boldsymbol{C}}_{\boldsymbol{z}_{nk}} = \eta \boldsymbol{A}(\boldsymbol{\theta}_G) \boldsymbol{A}(\boldsymbol{\theta}_G)^H + \sigma^2 \boldsymbol{I}_{N_R} \succeq \boldsymbol{C}_{\boldsymbol{z}_{nk}}, \tag{12}$$

with the array manifold evaluated at the known DoAs, i.e.

$$\boldsymbol{A}(\boldsymbol{\theta}_G) = \begin{bmatrix} \boldsymbol{a}_{N_R}(\boldsymbol{\theta}_{G,1}) & \cdots & \boldsymbol{a}_{N_R}(\boldsymbol{\theta}_{G,L_G}) \end{bmatrix} \tag{13}$$

It is then straightforward to show that by inserting Eq. (12) into (P1) and (9), we maximize a lower bound on R^A and R^B respectively. Now, instead of treating η as unknown, we consider it a hyperparameter that controls the resilience level of our system. Since η indicates the influence of the jamming signals, we conjecture that by choosing it much larger than the noise variance σ^2, we obtain approximately the same performance as if the true channel and jammer setup are known. For the theoretical justification, we refer again to [16], and in Section IV we will numerically demonstrate that this is the case for most scenarios considered. This approach is resilient by design since in the jammer-free case the parties adapt their system parameters with $\eta = 0$ and if any illegitimate party is detected, η is changed to a higher value. Thus the optimal receive filters in (9) can be computed and problem (P1) can be solved using the surrogate covariance in (12).

We now turn our attention to (P1) and propose an iterative water-filling [14] inspired algorithm for joint scheduling, power allocation, and beamforming shown in Algorithm 1. Our main motivation for this is the fact that the original algorithm achieves capacity, as well as its excellent convergence properties. To our knowledge, there are no works extending this algorithm to account for scheduling. In our case, each

---

Algorithm 1 Joint Iterative Scheduling, Beamforming, and Power Allocation

---

Input: Channels $\boldsymbol{G}_{qnk}$, surrogate covariances $\widetilde{\boldsymbol{C}}_{\boldsymbol{z}_{nk}}$, power constraints P_q, maximum number of REs B_q
Output: Wireless system design variables α_{qnk}, p_{qnk}, $\boldsymbol{w}_{qnk}$

1: Initialize the interference-plus-noise covariance matrix to $\boldsymbol{X}_{qnk} = \widetilde{\boldsymbol{C}}_{\boldsymbol{z}_{nk}}$
2: Initialize the design variables α_{qnk}^0, p_{qnk}^0, $\boldsymbol{w}_{qnk}^0$ using the single user update in procedure in steps (6)-(11)
3: **while** not converged **do**
4:     **for** $q = 1$ to Q **do**
5:         Update $\boldsymbol{X}_{qnk}$ using Equation (8)
6:         Compute *maximum eigenvalues* $\{\lambda_{qnk}\}_{(n,k) \in \mathcal{R}_q}$ of $\{\boldsymbol{H}_{qnk}^H \boldsymbol{X}_{qnk}^{-1} \boldsymbol{H}_{qnk}\}_{(n,k) \in \mathcal{R}_q}$ and corresponding eigenvectors $\{\boldsymbol{t}_{qnk}\}_{(n,k) \in \mathcal{R}_q}$
7:         Determine indices $\mathcal{I}_q$ of the largest B_q eigenvalues
8:         Set $\alpha_{qnk} = 1$ for all $(n,k) \in \mathcal{I}_q$ and 0 else
9:         Compute $p_{qnk} = (\mu - \lambda_{qnk}^{-1})^+$ with μ chosen such that $\sum_{\mathcal{I}_q} p_{qnk} \leq P_q$
10:         Set $\boldsymbol{w}_{qnk} = \boldsymbol{t}_{qnk}$ for $(n,k) \in \mathcal{I}_q$
11:     **end for**
12: **end while**

---

user computes the matrices $\boldsymbol{X}_{qnk}$ and updates its variables according to

$$\max_{\substack{\alpha_{qnk}, p_{qnk}, \boldsymbol{w}_{qnk} \\ (n,k) \in \mathcal{R}_q}} \sum_{(n,k) \in \mathcal{R}} \alpha_{qnk} \log \left(1 + p_{qnk} \gamma_{qnk}^A(\boldsymbol{X}_{qnk}) \right)$$
$$\text{s.t. (C1) to (C5)} \tag{14}$$

using lines 6 to 11 in Algorithm 1 until convergence, with $\gamma_{qnk}^A(\boldsymbol{X}_{qnk})$ as in Sec. III-A. In order to see why the proposed method will offer good performance, first note that the sum rate is maximized if we maximize the sum rate of all resource elements individually. Secondly, as already stated, the iterative water-filling algorithm [14] in its' original formulation converges quickly to the sum capacity of the MIMO MAC, and thirdly it can be easily shown that the proposed single-user updates given by lines 6 to 11 in Algorithm 1 find the globally optimal solution to the problem in (14). Note that the complexity of this algorithm is dominated by the computation of the maximum eigenvalue and eigenvector. This can be solved

by a power iteration algorithm which scales quadratically in the number of variables. Thus the total complexity scales as $O(N_{\text{iter}}QN_T^2NK)$ in both time and memory, but note that the innermost loop can be paralellized over the subcarriers and OFDM symbols. Finally, a preliminary experimental convergence analysis shows that the proposed algorithm reaches convergence after very few iterations. Due to lack of space, we defer it to future work.

B. Worst-Case Jamming Strategy

In order to benchmark the proposed sensing-assisted resilience framework even against the most disruptive kind of adversarial jammers, we now address the question of finding a computationally efficient approximate solution to the problem (P2). To this end, a two-step approximation procedure is proposed in Algorithm 2, consisting of a prior user selection stage and a closed form computation of the jamming convariances, which is derived in the following.

Algorithm 2 Approximate Worst-Case Jamming Strategy

Input: Legitimate channel $\boldsymbol{H}_{qnk}$, jamming channel $\boldsymbol{G}_{nk}$, jamming power budget P_J

Output: Worst-case jamming covariance matrix $\boldsymbol{C}_{\boldsymbol{u}_{nk}}$

1: For each user $q \in \mathcal{Q}$, compute the alignment matrix
$\boldsymbol{R}_{qnk} = \boldsymbol{G}_{nk}^{\dagger}\boldsymbol{H}_{qnk}\boldsymbol{H}_{qnk}^{H}\boldsymbol{G}_{nk}^{\dagger,H}$
2: Determine the strongest user
$q^* = \arg\max_{q \in \mathcal{Q}} \lambda_{\max}(\boldsymbol{R}_{qnk})$
3: For the strongest user alignment $\boldsymbol{R}_{q^*nk}$, compute the eigenvectors $\boldsymbol{U}_{q^*nk}$ and eigenvalues $\{\lambda_{q^*nk,d}\}_{d=1}^{N_J}$
4: Compute the jamming power allocation weighting
$h_{nk} = p_{q*nk}\sum_{d=1}^{N_J} \lambda_{q*nk,d}$
5: Compute the jamming power scaling factors
$g_{nk} = \left(P_J\sqrt{h_{nk}}\right)\left(\left(\sum_{nk}\sqrt{h_{nk}}\right)\right)$
6: Compute the jamming power allocation matrix
$\boldsymbol{\Lambda}_{\boldsymbol{u}_{nk}} = \text{diag}\left\{\dfrac{g_{nk}\lambda_{q^*nk,d}}{\sum_{d=1}^{N_J}\lambda_{q^*nk,d}}\right\}_{d=1}^{N_J}$
7: Compute the jamming covariance matrix
$\boldsymbol{C}_{\boldsymbol{u}_{nk}} = \boldsymbol{U}_{q^*nk}\boldsymbol{\Lambda}_{\boldsymbol{u}_{nk}}\boldsymbol{U}_{q^*nk}^{H}$

The corresponding user selection stage is motivated by the importance of the strongest users in terms of SINR γ_{qnk}^A for each RE. Using standard linear algebra arguments and Jensen's inequality one can show that

$$R^A \leq |\mathcal{R}_J|\log\left(\left(+\frac{Q}{|\mathcal{R}_J|}\sum_{(n,k)\in\mathcal{R}_J}\gamma_{\max}\left(\boldsymbol{C}_{\boldsymbol{z}_{nk}}\right)\right)\right) \quad (15)$$

where $\gamma_{\max}\left(\boldsymbol{C}_{\boldsymbol{z}_{nk}}\right) = \max_{q\in\mathcal{Q}}p_{qnk}\lambda_{\max}\left(\boldsymbol{H}_{qnk}^{H}\boldsymbol{C}_{\boldsymbol{z}_{nk}}^{-1}\boldsymbol{H}_{qnk}\right)$ and $\mathcal{R}_J$ is the set of scheduled REs. Accordingly, disrupting the latter for each RE implies a deterioration of the total sum-rate. Furthermore, as the worst-case jammer is assumed to be in the jammer-dominant regime, it follows from $P_J \gg \sigma^2$ that

$$\boldsymbol{C}_{\boldsymbol{z}_{nk}} = \boldsymbol{G}_{nk}\boldsymbol{C}_{\boldsymbol{u}_{nk}}^{H}\boldsymbol{G}_{nk} + \sigma^2\boldsymbol{I}_{N_R} \approx \boldsymbol{G}_{nk}\boldsymbol{C}_{\boldsymbol{u}_{nk}}^{H}\boldsymbol{G}_{nk}. \quad (16)$$

We now introduce the alignment matrix

$$\boldsymbol{R}_{qnk} = \boldsymbol{G}_{nk}^{\dagger}\boldsymbol{H}_{qnk}\boldsymbol{H}_{qnk}^{H}\boldsymbol{G}_{nk}^{\dagger,H}, \quad (17)$$

where $(\cdot)^{\dagger}$ denotes the Moore-Penrose pseudoinverse, to quantify impact of jamming on the corresponding REs. Using the analysis in [10, Proposition 1] we have that

$$\lambda_{\max}\left(\boldsymbol{H}_{qnk}^{H}\boldsymbol{C}_{\boldsymbol{z}_{nk}}^{-1}\boldsymbol{H}_{qnk}\right) \approx \lambda_{\max}\left(\boldsymbol{R}_{qnk}\boldsymbol{C}_{\boldsymbol{u}_{nk}}^{-1}\right) \quad (18)$$

with $\lambda_{\max}(\boldsymbol{A})$ the largest eigenvalue of the matrix $\boldsymbol{A}$. Accordingly, the jammer will choose the strongest user q^* as

$$q^* = \arg\max_{q \in \mathcal{Q}} p_{qnk}\lambda_{\max}(\boldsymbol{R}_{qnk}). \quad (19)$$

With this user selection stage, the original optimization problem in (P2) can be recast as

$$\min_{\boldsymbol{C}_{\boldsymbol{u}_{nk}}} \quad \lambda_{\max}\left(\boldsymbol{R}_{q^*nk}\boldsymbol{C}_{\boldsymbol{u}_{nk}}^{-1}\right) \quad \text{s.t.} \quad \text{(J1)} \quad \text{(P3)}$$

$$g_{nk} \geq 0 \quad \text{(K1)}$$

$$\text{tr}(\boldsymbol{C}_{\boldsymbol{u}_{nk}}) \leq g_{nk}, \quad \text{(K2)}$$

where the constraint (K1) refers to the non-negativeness of the power scaling factors g_{nk} and (K2) incorporates these into a power allocation constraint for each resource element. Due to the previous user selection stage, user q^* and its resource elements (n,k) are iteratively fixed. A corresponding closed-form solution to the alternative problem statement in (P3) has been derived in [10, Proposition 2] as

$$\boldsymbol{C}_{\boldsymbol{u}_{nk}} = \boldsymbol{U}_{q^*nk}\boldsymbol{\Lambda}_{\boldsymbol{u}_{nk}}\boldsymbol{U}_{q^*nk}^{H}. \quad (20)$$

In this expression, $\boldsymbol{U}_{q^*nk}$ denotes the eigenvector matrix of the alignment $\boldsymbol{R}_{q^*nk}$ and $\boldsymbol{\Lambda}_{\boldsymbol{u}_{nk}}$ denotes the jamming power allocation matrix with $\lambda_{q^*nk,d}$ being the d-th eigenvalue of $\boldsymbol{R}_{q^*nk}$, i.e.

$$\boldsymbol{\Lambda}_{\boldsymbol{u}_{nk}} = \text{diag}\left\{\frac{g_{nk}\lambda_{q^*nk,d}}{\sum_{d=1}^{N_J}\lambda_{q^*nk,d}}\right\}_{d=1}^{N_J} \quad (21)$$

The remaining power scaling factors g_{nk} are determined by solving the convex subproblem

$$\min_{\substack{g_{nk} \\ (n,k)\in\mathcal{R}_J}} \sum_{(n,k)\in\mathcal{R}_J}\frac{h_{nk}}{g_{nk}} \quad \text{s.t.} \quad \text{(K1)} \quad \text{(P4)}$$

$$\sum_{(n,k)\in\mathcal{R}_J} g_{nk} \leq P_J, \quad \text{(L1)}$$

with the jamming power allocation $h_{nk} = p_{q^*nk}\sum_{d=1}^{N_J}\lambda_{q^*nk,d}$. This can be analytically solved using Lagrange multipliers with the solution being given in lines 4 and 5 of Algorithm 2. Note that the complexity of this algorithm is dominated by the eigenvalue decomposition, which scales as $O(N_J^3)$ per RE.

Taking into account these factors, the problem originally presented in (P3), which is convex but scales as $O(N_J^4N^2K^2)$, has been converted into an approximate problem which scales as $O(N_J^3NK)$. This latter is addressed through a sequence of closed-form solutions, following an initial user selection stage. In Section IV, we will see that this proposed strategy effectively nullifies user-sum rates in all unprotected cases.
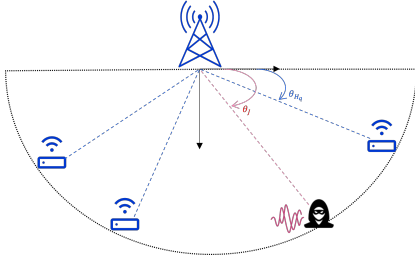
Fig. 1: Qualitative rendering of the considered scenario.

IV. SIMULATION RESULTS AND ANALYSIS

A. Wireless Setup and Methodology

Consider the setup depicted in Fig. 1, where both the UEs and the jammer are positioned on a circle in the xy-plane, with the BS at the center. The azimuth DoAs for the UEs are set up with a central angle θ_{H_q} spaced by $5°$ and an additional random disturbance ϕ_l drawn from a uniform distribution $\mathcal{U}(-5°, 5°)$. A similar method is applied for the jamming channel. We consider uniform linear arrays with $N_{T_q} = 8$ for all transmitters and $N_R = 16$ for the receiver. We model our slots similar to LTE, with $K = 14$ symbols and $N = 64$ subcarriers. The number of resource blocks per user B_q is set to $\lfloor \frac{NK}{Q} \rfloor$, and each user has a power budget of $P_q = 5$dBm. For this simulation, the number of users is $Q = 3$, the design hyperparameter $\eta = 10$, and the noise level $\sigma^2 = -3$dBm/Hz, with all channels computed using equations (3) and (4).

In the considered setup, the UEs calculate the surrogate noise covariance matrix $\tilde{C}_{z_{nk}}$ using equation (12). They then optimize their system parameters, which are subsequently utilized to determine the worst-case jamming strategy and to compute the user sum-rate R^B. Contrary to approaches as in [8], [9], our methodology assumes that while the jammer is aware of the optimized system parameters, the legitimate parties only have knowledge of the jamming signal's DoAs. Three baseline scenarios are considered for comparison:

1) *No Jammer*: Evaluating the system in the absence of any jamming activity.
2) *No Protection*: The jammer is active, but no specific protection is employed against it.
3) *Full Knowledge*: The system has complete knowledge of the jammer's channel and strategy, and optimizations are performed accordingly.

To showcase the effectiveness of our proposed jamming strategy, results also include scenarios with a barrage jammer, where $C_{u_{nk}} = P_J/(N_J NK)$.

B. Impact of Number of Antennas

The study first examines how the number of jammer antennas affects system resilience. As shown in Figure 2a, with protective measures in place, the sum user rate remains consistent, unaffected by the number of jammer antennas. This stability represents a significant rate improvement compared to worst-case scenarios. Moreover, optimizing transmit and receive parameters based on DoA information matches performance levels akin to scenarios with full knowledge of the jammer's setup. The proposed jamming strategy also demonstrates greater effectiveness than barrage jamming in unprotected scenarios, keeping user rates nearly zero across a wide range of antenna numbers.

C. Impact of Jamming Power

When varying the jamming power, our methods ensure resilience even at extremely high jamming power levels. However, a threshold exists beyond which the knowledge of jammer DoAs alone is insufficient, leading to a notable decline in user sum rates, observable in Fig. 2b. This decline happens at higher jamming powers when full jammer knowledge is available. In these scenarios, the proposed jamming strategy remains more effective than standard barrage jamming, effectively reducing communication rates to near zero with even modest jamming power budgets.

D. Impact of Jamming DoAs

Exploring the dependency on adversarial signal DoAs involves analyzing three legitimate users with varying central DoAs, as depicted in 2c. User rates tend to decrease as jamming signals align more closely in direction. Yet, even with closely aligned jamming signals, the system maintains a transmission rate of about 2500 bits per slot in protected scenarios. Performance with full jammer knowledge parallels that achieved using only DoA knowledge. The proposed jamming strategy continues to stand out, reducing user rates to zero across all DoAs, demonstrating its efficacy in approximating the original semidefinite program solution.
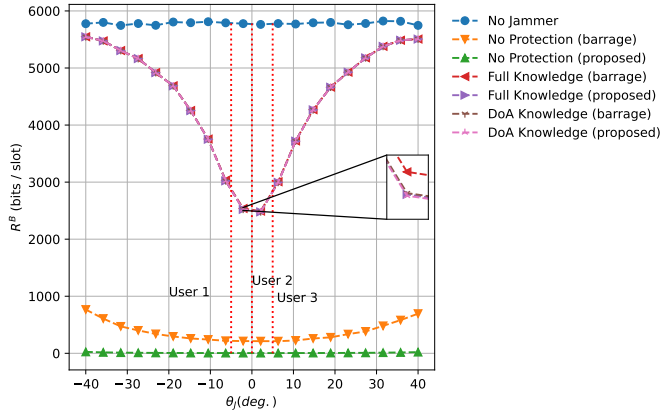
E. Impact of Number of Users

The final aspect of the study considers the effect of an increasing number of users. Results in Figure 2d confirm the advantages of our anti-jamming approaches, consistently outperforming unprotected scenarios. Notably, the proposed jamming strategy effectively nullifies user rates, regardless of the user count, underscoring its robustness against varying system scales.
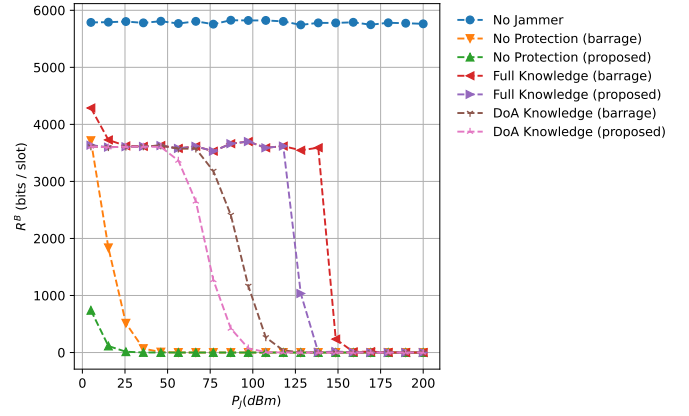
V. CONCLUSIONS

In this work, we have introduced a sensing-assisted and resilient-by-design approach for anti-jamming in MIMO-OFDM-MAC systems and have incorporated this methodology into the joint optimization of beamforming, scheduling, and power allocation. Our proposed method operates effectively and solely with information on the adversary's DoAs and significantly enhances system performance in various jamming scenarios, consistently outperforming unprotected setups under diverse channel conditions and jamming configurations. This holds even for the worst-case jammer, for which a computationally efficient approximation of the optimal startegy was derived. Future work will focus on the optimality and convergence properties of our resource allocation scheme, on a comparative analysis between our approximate jamming
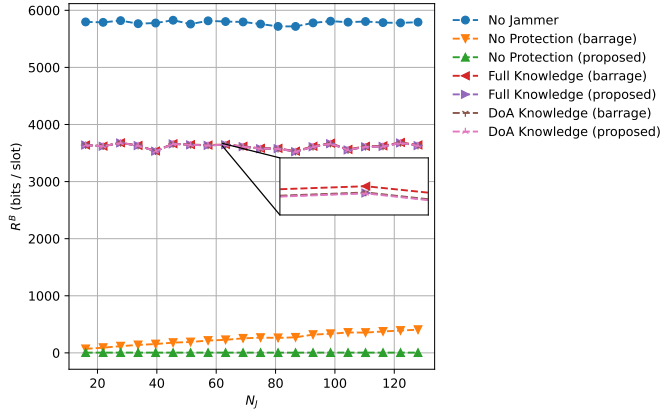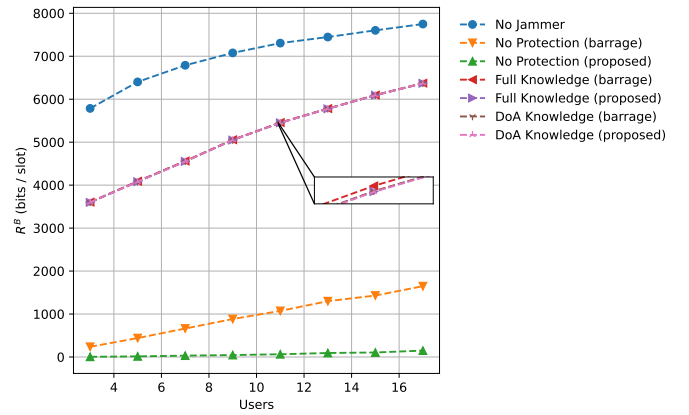
(a) User sum-rate vs. number of antennas. $P_J = 30$dBm, $\theta_J = 20°$.

(b) User sum-rate vs. jammer powers, $N_J = 64$, $\theta_J = 20°$.

(c) User sum-rate vs. jamming DoAs, $N_J = 64$, $P_J = 30$dBm.

(d) User sum-rate vs. number of users, $N_J = 64$, $P_J = 30$dBm.

Fig. 2: Simulation results for all considered scenarios.

strategy and its globally optimal but not scalable counterpart, as well as on the practical validation of our approaches in field tests.

REFERENCES

[1] P. Schwenteck, G. T. Nguyen, H. Boche, W. Kellerer, and F. H. P. Fitzek, "6G Perspective of Mobile Network Operators, Manufacturers, and Verticals," *IEEE Networking Letters*, pp. 1–1, 2023.

[2] G. P. Fettweis and H. Boche, "6G: The Personal Tactile Internet—And Open Questions for Information Theory," *IEEE BITS the Information Theory Magazine*, vol. 1, no. 1, pp. 71–82, 2021.

[3] ——, "On 6G and Trustworthiness," *Commun. ACM*, vol. 65, no. 4, p. 48–49, Mar 2022.

[4] H. Boche, R. F. Schaefer, and H. V. Poor, "On the Algorithmic Solvability of Channel Dependent Classification Problems in Communication Systems," *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1155–1168, 2021.

[5] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," Jan. 2021, arXiv:2101.00292 [cs].

[6] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314, 2015.

[7] T. T. Do, E. Bjornson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-Resistant Receivers for the Massive MIMO Uplink," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.

[8] G. Marti, T. Kölle, and C. Studer, "Mitigating Smart Jammers in Multi-User MIMO," *IEEE Transactions on Signal Processing*, vol. 71, pp. 756–771, 2023, arXiv:2208.01453 [cs, eess, math].

[9] G. Marti and C. Studer, "Universal MIMO Jammer Mitigation via Secret Temporal Subspace Embeddings," May 2023, arXiv:2305.01260 [cs, eess, math].

[10] Q. Liu, M. Li, X. Kong, and N. Zhao, "Disrupting MIMO Communications With Optimal Jamming Signal Design," *IEEE Transactions on Wireless Communications*, vol. 14, no. 10, pp. 5313–5325, 2015.

[11] J. Gao, S. A. Vorobyov, H. Jiang, and H. V. Poor, "Worst-Case Jamming on MIMO Gaussian Channels," *IEEE Transactions on Signal Processing*, vol. 63, no. 21, pp. 5821–5836, 2015.

[12] A. Kashyap, T. Basar, and R. Srikant, "Correlated Jamming on MIMO Gaussian Fading Channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 2119–2123, 2004.

[13] M. H. Brady, M. Mohseni, and J. M. Cioffi, "Spatially-correlated Jamming in Gaussian Multiple Access and Broadcast Channels," in *40th Annual Conference on Information Sciences and Systems*. IEEE, 2006, pp. 1635–1639.

[14] W. Yu, W. Rhee, S. Boyd, and J. M. Cioffi, "Iterative Water-Filling for Gaussian Vector Multiple-Access Channels," *IEEE Transactions on Information Theory*, vol. 50, no. 1, pp. 145–152, 2004.

[15] H. Wolkowicz, R. Saigal, and L. Vandenberghe, *Handbook of Semidefinite Programming: Theory, Algorithms, and Applications*. Springer Science & Business Media, 2012, vol. 27.

[16] V. C. Andrei, X. Li, U. J. Mönich, and H. Boche, "Sensing-Assisted Receivers for Resilient-By-Design 6G MU-MIMO Uplink," in *2023 IEEE 3rd International Symposium on Joint Communications and Sensing*, 2023, pp. 1–6.