Anti-jamming beam alignment in millimeter-wave MIMO systems

Donatella Darsena, *Senior Member, IEEE* and Francesco Verde, *Senior Member, IEEE*

***Abstract*—In millimeter-wave (MMW) multiple-input multiple-output (MIMO) communications, users and their corresponding base station (BS) have to align their beam during both initial access and data transmissions to compensate for the high propagation loss. The beam alignment (BA) procedure specified for 5th Generation (5G) New Radio (NR) has been designed to be fast and precise in the presence of non-malicious interference and noise. A smart jammer might exploit this weakness and may launch an attack during the BA phase in order to degrade the accuracy of beam selection and, thus, adversely impacting the end-to-end performance and quality-of-service experienced by the users. In this paper, we study the effects of a jamming attack at MMW frequencies during the BA procedure used to perform initial access for idle users and adaptation/recovery for connected users. We show that the BA procedure adopted in 5G NR is extremely vulnerable to a smart jamming attack and, consequently, we propose a countermeasure based on the idea of randomized probing, which consists of randomly corrupting the probing sequence transmitted by the BS in order to reject the jamming signal at the UE via a subspace-based technique based on orthogonal projections and jamming cancellation. Numerical results corroborate our theoretical findings and show the very satisfactory accuracy of the proposed anti-jamming approach.**

***Index Terms*—Beam alignment, jamming, millimeter-wave, multiple-input multiple-output (MIMO), orthogonal projection, physical-layer security, randomized probing, subspace-based jamming suppression.**

I. Introduction

THE evolution of wireless radio-frequency (RF) communications has been basically driven by the unremitting pursuit of large portions of unexplored spectrum to boost the available data rates as much as possible. Unlike Long Term Evolution (LTE) systems, which mainly work below 3 GHz, 5th Generation (5G) New Radio (NR) are allowed to also operate in the *millimeter-wave (MMW)* band, with operating frequency from 24250 MHz to 52600 MHz [1], [2]. However, MMW communications are *power-limited*, because of higher path losses and blockage phenomena [3], which demand a significant technical breakthrough over the LTE system. Beamforming techniques are the standard way to provide the necessary signal-to-noise ratio (SNR) gain and provide spatial multiplexing, by using highly-directional beams [4], [5], especially in local coverage scenarios. Directional links are realized by antenna arrays with a large number of elements, which are feasible at MMW signaling since, due to the small wavelength, it is possible to package a large number of antenna elements at both the base station (BS) side and the user equipment (UE) side, implementing a massive multiple-input multiple-output (MIMO) system. All the lower layer functions are designed in NR on the basis of a *beam-centric* philosophy: in particular, unlike LTE, not only the user-plane channels, but also the control-plane channels are beamformed.

A problem arising in directional communications is how to establish, track and possibly reconfigure beams as the UE moves, or even when the UE device is simply rotated. Due to mobility and blockage, the current beam pair between the BS and UE may be blocked, resulting in a *beam failure event*. Beam failure could lead to *radio link failure (RLF)* already defined in LTE, which is managed by a costly higher-layer reconnection procedure. To deal with this issue, a new set of procedures, collectively referred to as *beam alignment (BA)* techniques, have been introduced in NR specifications, aimed at supporting possible fast beam reconfiguration and tracking, preferably working at the layers $1-2$ of the protocol stack. The beam-centric design is a groundbreaking difference between LTE and NR, which makes BA strategic for control and performance of MMW networks. Hence, with a widespread adoption of 5G NR, it is not difficult to imagine that BA will become the target of all kinds of potential threats or attacks.

A. Deficiency of existing beam alignment procedure

The task of beam management is to acquire and maintain a reliable beam pair, i.e., a transmit angle-of-departure (AoD) and a corresponding receive angle-of-arrival (AoA) that jointly provides the best radio connectivity. The beam management procedures specified by the 3rd Generation Partnership Project (3GPP) in [6] and the subsequent works [7]–[25] are designed to be resilient to beam failure events due to mobility and blockage *only*. A noticible exception is represented by [26], where the beam training duration, training power, and data transmission power are optimized to maximize the throughput between two legitimate nodes, while ensuring a covertness constraint at a third-part node that attempts to detect the existence of the communication.

One serious threat to MMW network is the *jamming attack during the BA phase*, for which a jammer may transmit high-power RF signals to induce a beam failure event and, thus,

Manuscript received September 28, 2021; revised April 11, 2022; accepted June 8, 2022. The associate editor coordinating the review of this paper and approving it for publication was Prof. N. Gonzalez-Prelcic.

D. Darsena is with the Department of Engineering, Parthenope University, Naples I-80143, Italy (e-mail: darsena@uniparthenope.it).

F. Verde is with the Department of Electrical Engineering and Information Technology, University Federico II, Naples I-80125, Italy (e-mail: f.verde@unina.it).

The authors are also with National Inter-University Consortium for Telecommunications (CNIT).

a RLF that prevents either idle users from accessing the network or connected users from reconfiguration and tracking. Jamming attacks might dramatically increase the occurrence frequency of RLFs, thus lowering the quality of service of users and increasing costs for system management. To the best of our knowledge, the jamming attack specifically targeting at MMW links has not been considered yet and the synthesis of effective anti-jamming schemes is an open problem.

B. Contribution and organization

Although other solutions are possible [6], [12], we focus in this paper on *mobile-controlled BA (MCBA)* [11] to perform initial access for idle users and adaptation/recovery for connected users, which can be summarized as follows:

- *Beam sweeping*: while all UEs stay in listening mode, the BS actively probes the channel by periodically broadcasting a beamforming codebook and a probing sequence over reserved beacon slots in the downlink.
- *Beam measurement*: the UE measures the quality of the received beamformed signals by using the received power or more sophisticated metrics, such as the SNR.
- *Beam determination*: the UE locally and independently identify the best beam.
- *Beam reporting*: the UE reports information regarding the best beam for successive data/control transmission or possible beam refinement over a control uplink channel.

MCBA is highly scalable and its overhead and complexity do not grow with the number of active users in the system. In this paper, due to the rapid development of software-defined radio techniques, we explicitly account for the presence of a *smart* jammer that is able to mimic the BS signal, which is formed by the transmit beamforming codebook and probing symbols.

Our study includes the main peculiar features of MMW networks. Specifically, according to NR physical-layer specifications, we consider orthogonal frequency-division multiplexing (OFDM) with cyclic prefix (CP) as a modulation format. Moreover, we exploit the fact that, at MMW frequencies, propagation in dense-urban non-line-of-sight (NLOS) environments is only based on a few scattering clusters, with relatively little delay/angle spreading within each cluster [27]. In this case, the MMW channel tends to exhibit a sparse structure in both angle and delay domains, which can be conveniently exploited to obtain anti-jamming alignment solutions. Finally, due to implementation/cost constraints of fully-digital architectures, we rely on a realistic MMW transmit implementation [28], according to which the number of RF chains is strictly smaller than the number of antennas. Within such a framework, our contributions are the following ones:

(i) We develop a detailed model of a smart jamming attack in MMW networks, which represents an important, yet open research problem. The novelty of the proposed modeling approach rests mainly on the application to BA of jamming transmission techniques, which previous works attribute to communications based on centimetre-wave (CMW) communications [29].

(ii) Existing beam sweeping procedures [6]–[25] rely on a publicly known protocol where the probing symbols are known to all UEs. As a countermeasure against the jamming attack, we propose the idea of *randomized probing*, which consists of superimposing a random sequence on the known probing symbols transmitted by the BS during the beam-sweeping phase. Such a random sequence is unknown to both the user and the jammer, but its subspace properties can be exploited at the UE to reject the contribution of the jamming signal. The idea of randomly corrupting the input data during the transmission has been used in other contexts with different aims, such as, to decentralize the transmission of a space time code from a set of distributed relays [30], to boost the performance or efficiency of neural networks [31], or to overcome the problem of pilot spoofing in CMW cellular systems [32].

(iii) Performance of the proposed anti-jamming methods are validated using a number of system parameters. It is demonstrated that a smart jamming attack leads to frequent beam failure events if no adequate countermeasures are taken. On the other hand, exploitation at the UE of randomized probing avoids beam misalignment, in such a way that costly beam recovery procedures are avoided while using lower-layer signaling.

The paper is organized as follows. The system model of the BA phase under a jamming attack is described in Section II. The study of the adverse effects of the jamming attack on a conventional BA algorithm is reported in Section III. The proposed countermeasure based on randomized probing is developed in Section IV. Numerical results are reported in Section V. Finally, conclusions are drawn in Section VI.

C. Notations

Upper- and lower-case bold letters denote matrices and vectors; the superscripts $*$, T, H, and -1 denote the conjugate, the transpose, the Hermitian (conjugate transpose), and the inverse of a matrix; $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$ are the fields of complex, real, integer, and natural numbers; $\mathbb{C}^n$ $[\mathbb{R}^n]$ denotes the vector-space of all n-column vectors with complex [real] coordinates; similarly, $\mathbb{C}^{n \times m}$ $[\mathbb{R}^{n \times m}]$ denotes the vector-space of all the $n \times m$ matrices with complex [real] elements; $\delta(\tau)$ is the Dirac delta; δ_n is the Kronecker delta, i.e., $\delta_n = 1$ when $n = 0$ and zero otherwise; $\jmath \triangleq \sqrt{-1}$ denotes the imaginary unit; $\max(x, y)$ returns the maximum between $x \in \mathbb{R}$ and $y \in \mathbb{R}$; $\lceil x \rceil$ rounds $x \in \mathbb{R}$ to the nearest integer greater than or equal to x; the (linear) convolution operator is denoted with $*$; $\otimes$ stands for the Kronecker product; $|\mathcal{A}|$ is the cardinality of the set $\mathcal{A}$; $\mathbf{0}_n$, $\mathbf{O}_{n \times m}$ and $\mathbf{I}_n$ denote the n-column zero vector, the $n \times m$ zero matrix and the $n \times n$ identity matrix; $\mathbf{x} \geq \mathbf{0}_n$ $[\mathbf{x} > \mathbf{0}_n]$ denotes a vector $\mathbf{x} \in \mathbb{R}^n$ with non-negative [positive] entries; $\mathbf{W}_n \in \mathbb{C}^{n \times n}$ is the unitary symmetric n-point inverse discrete Fourier transform (IDFT) matrix, whose $(m+1, p+1)$-th entry is given by $\frac{1}{\sqrt{n}} e^{\jmath \frac{2\pi}{n} mp}$ for $m, p \in \{0, 1, \ldots, n-1\}$, and its inverse $\mathbf{W}_n^{-1} = \mathbf{W}_n^{\text{H}}$ is the n-point discrete Fourier transform (DFT) matrix; $\{\mathbf{a}\}_\ell$ is the ℓ-th entry of $\mathbf{a} \in \mathbb{C}^n$, for $\ell \in \{1, 2, \ldots, n\}$; $\{\mathbf{A}\}_{\ell_1, \ell_2}$ is the (ℓ_1, ℓ_2)-th entry of $\mathbf{A} \in \mathbb{C}^{n \times m}$, for $\ell_1 \in \{1, 2, \ldots, n\}$ and $\ell_2 \in \{1, 2, \ldots, m\}$; matrix $\mathbf{A} = \text{diag}(a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^{n \times n}$ is diagonal;

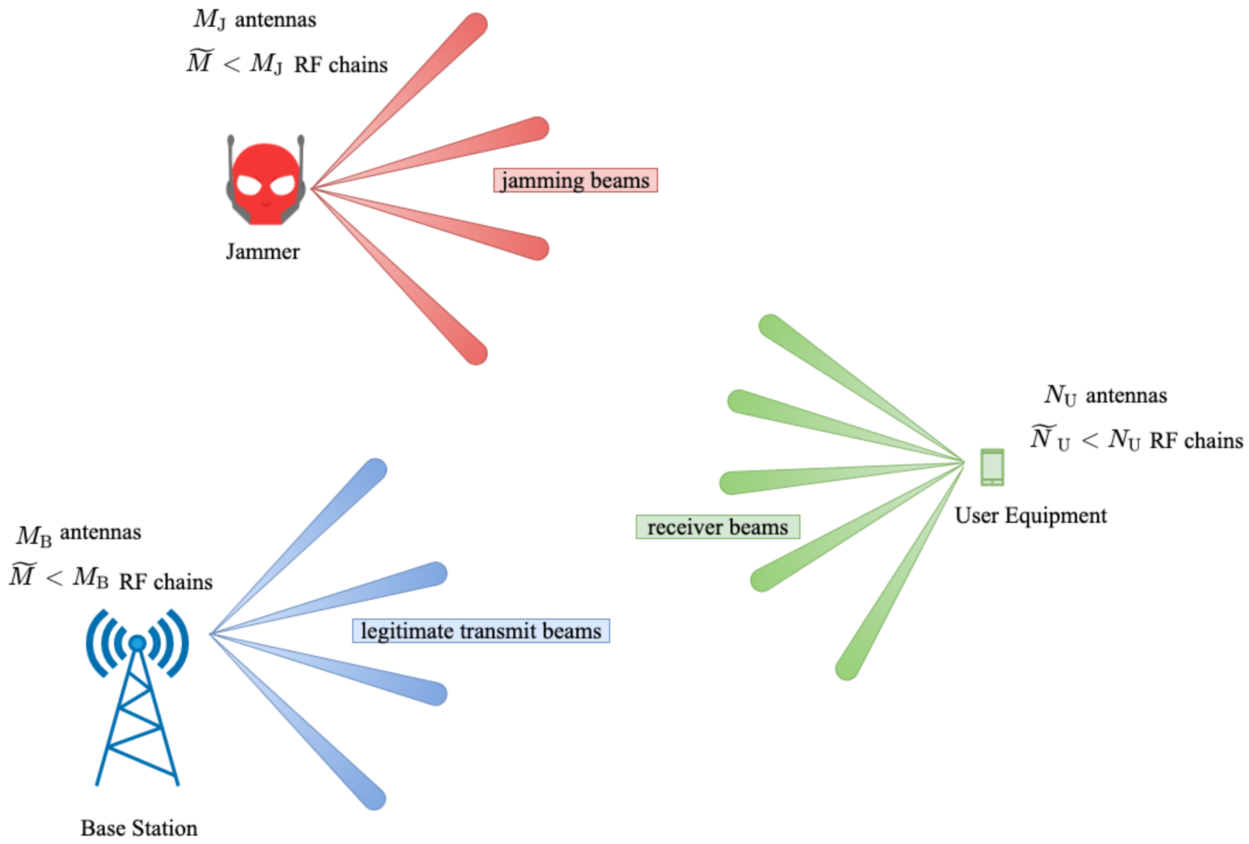

M_{J} antennas
$\widetilde{M} < M_{\mathrm{J}}$ RF chains
jamming beams
Jammer
N_{U} antennas
$\widetilde{N}_{\mathrm{U}} < N_{\mathrm{U}}$ RF chains
receiver beams
User Equipment
M_{B} antennas
$\widetilde{M} < M_{\mathrm{B}}$ RF chains
legitimate transmit beams
Base Station

Fig. 1. The jamming attack on the BA procedure in MMW MIMO systems.

vector $\mathbf{a} = \mathrm{vec}(\mathbf{A}) \in \mathbb{C}^{n \cdot m}$ is obtained by vertically stacking the columns of $\mathbf{A} \in \mathbb{C}^{m \times n}$; let $p \geq 1$ be a real number, the p-norm (also called ℓ_p-norm) of vector $\mathbf{x} \in \mathbb{C}^n$ is defined as $\|\mathbf{x}\|_p \triangleq \left(\sum_{i=1}^{n} |\{\mathbf{x}\}_i|^p\right)^{1/p}$; $\mathbf{1}_{\mathcal{A}} \in \mathbb{R}^n$ denotes a vector whose i-th entry is equal to one if i is contained in the set $\mathcal{A} \subseteq \{1, 2, \dots, n\}$, otherwise is zero; $\mathbf{1}_n \in \mathbb{R}^n$ is the all-ones vector; the support of $\mathbf{x} \in \mathbb{R}^n$ is the set of its nonzero entries, i.e., $\mathrm{supp}(\mathbf{x}) \triangleq \{i \in \{1, 2, \dots, n\} : \{\mathbf{x}\}_n \neq 0\}$; the operator $\mathscr{F}[x(n)] = \sum_{n \in \mathbb{Z}} x(n)\, e^{-\jmath 2\pi \nu n}$ ($\nu \in \mathbb{R}$) returns the Fourier transform of $x(n)$; $\mathbb{E}[\cdot]$ denotes ensemble averaging.

II. Beam alignment model under jamming attack

With reference to Fig. 1, we consider a MMW system employing OFDM signaling, with F subcarriers and a CP of length L_{cp}, which encompasses a legitimate BS (referred to as node B), equipped with M_{B} antennas and $\widetilde{M} \ll M_{\mathrm{B}}$ RF chains, a generic user (referred to as node U), with N_{U} antennas and $\widetilde{N}_{\mathrm{U}} \ll N_{\mathrm{U}}$ RF chains, and a jammer (referred to as node J) equipped with M_{J} antennas and $\widetilde{M} \ll M_{\mathrm{J}}$ RF chains. We study the worst case in which the jammer is perfectly aware of the BA protocol and tries to almost perfectly replicate the legitimate communication between the BS and the UE, with the scope to hinder their corresponding beam matching, by sending *smart* jammer signals. Such an attack is hard to be detected using network monitoring tools, since legitimate traffic on the medium will be sensed in this case [33]. All the notations are defined in Section I-C and the main symbols are summarized in Table I.

A. Transmit signal model

For the sake of simplicity, we assume that the BS and the jammer share the same number $\widetilde{M}$ of RF chains and, thus, they can transmit up to $\widetilde{M}$ different *probing* streams. The extension to the case in which the jammer and the BS have a different number of RF chains is straightforward. Let $\mathcal{F}_i \triangleq \{k_{i,0}, k_{i,1}, \dots, k_{i,F_i-1}\}$ denote the set gathering the F_i subcarriers assigned to the i-th stream, with $i \in \{1, 2, \dots, \widetilde{M}\}$ and $\sum_{i=1}^{\widetilde{M}} F_i \leq F$. Such sets $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_{\widetilde{M}}$ are disjoint, i.e., $\mathcal{F}_{i_1} \cap \mathcal{F}_{i_2} = \emptyset$, for $i_1 \neq i_2$. We denote with

$$\mathbf{d}_{\mathrm{TX}}^{(i)}(s) \triangleq [d_{\mathrm{TX}}^{(k_{i,0})}(s), d_{\mathrm{TX}}^{(k_{i,1})}(s), \dots, d_{\mathrm{TX}}^{(k_{i,F_i-1})}(s)]^{\mathrm{T}} \in \mathbb{C}^{F_i} \tag{1}$$

the *probing symbol vector* whose entry $d_{\mathrm{TX}}^{(k_{i,\ell})}(s)$ corresponds to the i-th stream, transmitted in the s-th symbol interval on subcarrier $k_{i,\ell}$, with TX $\in \{\mathrm{B}, \mathrm{J}\}$. Since the focus is on the BA phase only, we assume that the remaining subcarriers $F^{\mathrm{c}} \triangleq F - \sum_{i=1}^{\widetilde{M}} F_i$ are virtual carriers, i.e., subcarriers that are not used by the BS.[1] After OFDM precoding, one has

$$\mathbf{z}_{\mathrm{TX}}^{(i)}(s) \triangleq [z_{\mathrm{TX}}^{(i,0)}(s), z_{\mathrm{TX}}^{(i,1)}(s), \dots, z_{\mathrm{TX}}^{(i,P-1)}(s)]^{\mathrm{T}}$$

[1] In practice, the BS can use the remaining F^{c} subcarriers to transmit control and data information, which is orthogonally multiplexed in frequency with the probing symbols for BA alignment.

Symbol	**Meaning**
F	number of subcarriers
L_{cp}	CP length
P	OFDM symbol length
TX	subscript indicating the legitimate BS when TX $\equiv$ B or the jammer when TX $\equiv$ J
M_{TX}	number of antennas at the transmitter TX
N_{U}	number of antennas at the UE
$\widetilde{M}$	number of RF chains at the BS and jammer
$\widetilde{N}_{\text{U}}$	number of RF chains at the UE
T	OFDM symbol length related to the sampling period $T_{\text{c}} = T/P$
W	BA phase length (in OFDM symbols)
$\mathcal{F}_i$	set gathering the F_i subcarriers assigned to the i-th stream
$d_{\text{TX}}^{(k_{i,\ell})}(s)$	probing symbol of the i-th stream transmitted in the s-th symbol interval on subcarrier $k_{i,\ell}$
$\mathbf{u}_{\text{TX}}^{(i,s)}$	transmit beamforming vector used for the i-th stream in the s-th symbol interval
$\mathbf{H}_{\text{TX}}(\tau)$	impulse MIMO physical channel response between the transmitter TX and the UE
$\mathbf{v}^{(j,s)}$	receive beamforming vector of the j-th RF chain in the s-th symbol interval
$\overline{\mathbf{C}}_{\text{TX}}^{(k)}$	frequency-domain MIMO physical channel on subcarrier k
$\widetilde{\mathbf{C}}_{\text{TX}}^{(k)}$	frequency-domain MIMO virtual channel on subcarrier k
U_{TX}	cardinality of the angular support set probed by the transmitter TX
V	cardinality of the angular support set sensed by the UE
Q	number of beacon slots
$\mathbf{g}_{\text{TX}}^{(j,i)}(\widetilde{s})$	scaled version of the combined TX-UE beamforming vector $\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})$ during the $\widetilde{s}$ beacon slot
$\boldsymbol{\xi}_{\text{TX}}$	vector collecting all the unknown second-order moments of the TX-to-UE virtual channel
$\mathbf{G}_{\text{TX}}$	matrix collecting all the vectors $\mathbf{g}_{\text{TX}}^{(j,i)}(\widetilde{s})$, for $i \in \{1, 2, \ldots, \widetilde{M}\}$, $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, and $\widehat{s} \in \{0, 1, \ldots, Q-1\}$

TABLE I
LIST OF THE MAIN SYMBOLS USED THROUGHOUT THE PAPER.

$$= \mathbf{T}_{\text{cp}}\, \mathbf{W}^{(i)}\, \mathbf{d}_{\text{TX}}^{(i)}(s)$$

where $\mathbf{T}_{\text{cp}} \triangleq [\mathbf{I}_{\text{cp}}^{\text{T}}, \mathbf{I}_F]^{\text{T}} \in \mathbb{R}^{P \times F}$ accounts for CP insertion, with $\mathbf{I}_{\text{cp}} \in \mathbb{R}^{L_{\text{cp}} \times F}$ collecting the last L_{cp} rows of $\mathbf{I}_F$, and $P \triangleq F + L_{\text{cp}}$, whereas $\mathbf{W}^{(i)} \in \mathbb{C}^{F \times F_i}$ represents a submatrix of the F-point IDFT matrix $\mathbf{W}_F$ (see Subsection I-C), whose elements are given by

$$\{\mathbf{W}^{(i)}\}_{\ell_1+1, \ell_2+1} = \frac{1}{\sqrt{F}}\, e^{\jmath \frac{2\pi}{F} \ell_1 k_{i,\ell_2}}$$

for $\ell_1 \in \{0, 1, \ldots, F-1\}$ and $\ell_2 \in \{0, 1, \ldots, F_i - 1\}$. The vector $\mathbf{z}_{\text{TX}}^{(i)}(s)$ undergoes parallel-to-serial conversion, and the resulting sequence $z_{\text{TX}}^{(i)}(\ell)$ ($\ell \in \mathbb{Z}$), defined by $z_{\text{TX}}^{(i)}(sP + p) = z_{\text{TX}}^{(i,p)}(s)$, for $p \in \{0, 1, \ldots, P-1\}$, feeds a digital-to-analog converter (DAC) having impulse response $\psi_{\text{DAC}}(t)$, thus obtaining

$$x_{\text{TX}}^{(i,s)}(t) = \sum_{p=0}^{P-1} z_{\text{TX}}^{(i,p)}(s)\, \psi_{\text{DAC}}(t - sT - pT_c) \tag{2}$$

for $t \in [sT, (s+1)T)$, with T denoting the OFDM symbol length and $T_{\text{c}} \triangleq T/P$. For the BA phase, the beamforming is implemented in the analog RF domain. We consider fully-connected hybrid digital analog architecture, where each RF antenna port is connected to all antenna elements of the array, with identity baseband (digital) precoding matrix. To transmit the i-th probing stream, each transmitter applies an RF analog beamforming vector $\mathbf{u}_{\text{TX}}^{(i,s)} \in \mathbb{C}^{M_{\text{TX}}}$, which is assumed normalized such that $\|\mathbf{u}_{\text{TX}}^{(i,s)}\|_2 = 1$. Hence, the baseband transmitted signal by the generic transmit terminal TX during the s-th symbol interval is given by

$$\mathbf{x}_{\text{TX}}^{(s)}(t) = \sum_{i=1}^{\widetilde{M}} \mathbf{u}_{\text{TX}}^{(i,s)}\, x_{\text{TX}}^{(i,s)}(t)\,. \tag{3}$$

The BA phase spans a time window of length W OFDM symbols, i.e., WT seconds.

B. Physical channel model

During the BA phase, the $N_{\text{U}} \times M_{\text{TX}}$ MIMO physical channel matrix between the generic transmitter TX and the UE is modeled as

$$\mathbf{H}_{\text{TX}}(\tau) = \sum_{\ell=1}^{L_{\text{TX}}} \rho_{\text{TX}}(\ell)\, \mathbf{b}\left(\phi_{\text{TX}}(\ell)\right)\, \mathbf{a}_{\text{TX}}^{\text{H}}\left(\theta_{\text{TX}}(\ell)\right)\, \delta\left(\tau - \tau_{\text{TX}}(\ell)\right) \tag{4}$$

where $L_{\text{TX}} \ll \max\{M_{\text{TX}}, N_{\text{U}}\}$ denotes the number of *significant* propagation paths,[2] $\rho_{\text{TX}}(\ell)$, $\tau_{\text{TX}}(\ell)$, $\theta_{\text{TX}}(\ell) \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)$ and $\phi_{\text{TX}}(\ell) \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)$ are the channel gain, the time delay, the angle-of-departure (AoD), and angle-of-arrival (AoA) of the the ℓ-th multipath component, respectively, whereas $\mathbf{a}_{\text{TX}}\left(\theta_{\text{TX}}(\ell)\right) \in \mathbb{C}^{M_{\text{TX}}}$ and $\mathbf{b}\left(\phi_{\text{TX}}(\ell)\right) \in \mathbb{C}^{N_{\text{U}}}$ are the array responses of transmitter TX and UE, respectively, which depend on the array geometry and they are parameterized by the AoD and AoA, respectively. We have invoked the customary assumption that the communication bandwidth of the transmitted signals is much smaller than the carrier frequency f_0, such that the array responses can be assumed independent of frequency. We have also assumed that, for $\ell \in \{1, 2, \ldots, L_{\text{TX}}\}$, the channel gain $\rho_{\text{TX}}(\ell)$, AoD $\theta_{\text{TX}}(\ell)$ and AoA $\phi_{\text{TX}}(\ell)$ are time-invariant during the BA phase, i.e., over W OFDM symbols, since they typically vary on time intervals much longer than the channel coherence time.

Since each propagation path is approximately equal to the sum of independent micro-scatterers contributions, having same time delay and AoA-AoD, the channel gains $\rho_{\text{TX}}(\ell)$,

[2] After BA, multipath components conveying small amount of signal power can be neglected.

for $\ell \in \{1, 2, \dots, L_{\text{TX}}\}$ and TX $\in \{\text{B}, \text{J}\}$, can thus be modeled as independent zero-mean complex circular Gaussian random variables (RVs) (*uncorrelated Rayleigh scattering environment*), with variances $\sigma^2_{\text{TX}}(\ell)$, where $\rho_{\text{B}}(\ell)$ is statistically independent of $\rho_{\text{J}}(\ell)$.

C. Receive signal model

Since the noise in the receiver is mainly introduced by the RF chain electronics (filter, mixer, and A/D conversion), we neglect ambient noise external to the radio receiving system [34]. From (3) and (4), it follows that the baseband equivalent received signal at the UE antenna array during the BA phase reads as follows

$$\begin{aligned}\boldsymbol{\eta}(t) &= \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{h} \int \mathbf{H}_{\text{TX}}(\tau)\, \mathbf{x}^{(h)}_{\text{TX}}(t-\tau)\, \mathrm{d}\tau \\ &= \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{h} \sum_{\ell=1}^{L_{\text{TX}}} \sum_{i=1}^{\widetilde{M}} \rho_{\text{TX}}(\ell)\, g^{(i,h)}_{\text{TX}}(\ell) \\ &\qquad \cdot x^{(i,h)}_{\text{TX}}\left(t - \tau_{\text{TX}}(\ell)\right) \mathbf{b}\left(\phi_{\text{TX}}(\ell)\right) \qquad (5)\end{aligned}$$

where $g^{(i,h)}_{\text{TX}}(\ell) \triangleq \mathbf{a}^{\text{H}}_{\text{TX}}\left(\theta_{\text{TX}}(\ell)\right) \mathbf{u}^{(i,h)}_{\text{TX}} \in \mathbb{C}$ denotes the *beamforming gain* along the ℓ-th propagation path, in the h-th symbol interval, at the transmitter TX for the i-th RF chain.

Hereinafter, we assume perfect frequency and time synchronization. Recalling that the UE is equipped with $\widetilde{N}_{\text{U}}$ RF chains, after power splitting by a factor of $\widetilde{N}_{\text{U}}$ and anti-aliasing filtering, the baseband equivalent received signal at the output of the j-th RF chain can be written as

$$\begin{aligned} y^{(j,s)}_{\text{a}}(t) &= \frac{1}{\sqrt{\widetilde{N}_{\text{U}}}} \left\{ \left[\mathbf{v}^{(j,s)}\right]^{\text{H}} \boldsymbol{\eta}(t) \right\} * \psi_{\text{ADC}}(t) + w^{(j,s)}_{\text{a}}(t) \\ &= \frac{1}{\sqrt{\widetilde{N}_{\text{U}}}} \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{h=s-1}^{s} \sum_{\ell=1}^{L_{\text{TX}}} \sum_{i=1}^{\widetilde{M}} \sum_{p=0}^{P-1} \rho_{\text{TX}}(\ell)\, f^{(j,s)}_{\text{TX}}(\ell)\, g^{(i,h)}_{\text{TX}}(\ell) \\ &\qquad \cdot z^{(i,p)}_{\text{TX}}(h)\, \psi_{\text{a}}\left(t - \tau_{\text{TX}}(\ell) - hT - pT_{\text{c}}\right) + w^{(j,s)}_{\text{a}}(t) \qquad (6)\end{aligned}$$

for $t \in [sT, (s+1)T)$, with $s \in \{0, 1, \dots, W-1\}$, and $j \in \{1, 2, \dots, \widetilde{N}_{\text{U}}\}$, where we denote with $\mathbf{v}^{(j,s)} \in \mathbb{C}^{N_{\text{U}}}$ the beamforming vector of the jth RF chain at the UE side, normalized such that $\|\mathbf{v}^{(j,s)}\|_2 = 1$, $\psi_{\text{ADC}}(t)$ is the impulse response of the analog-to-digital converter (ADC), $f^{(j,s)}_{\text{TX}}(\ell) \triangleq \left[\mathbf{v}^{(j,s)}\right]^{\text{H}} \mathbf{b}\left(\phi_{\text{TX}}(\ell)\right) \in \mathbb{C}$ represents the *array gain* of the jth RF chain along the ℓ-th propagation path at the UE side, $w^{(j,s)}_{\text{a}}(t)$ is complex circular white Gaussian noise at the output of the jth RF chain, statistically independent of $\mathbf{d}^{(i)}_{\text{TX}}(h)$, for TX $\in \{\text{B}, \text{J}\}$, $h \in \{s-1, s\}$, and $i \in \{1, 2, \dots, \widetilde{M}\}$, and, finally, $\psi_{\text{a}}(t) \triangleq \psi_{\text{DAC}}(t) * \psi_{\text{ADC}}(t)$ is a unit-energy Nyquist pulse-shaping filter. We have also assumed in (6) that $L_\psi\, T_{\text{c}} + \tau_{\text{TX}}(\ell) < T$, for each $\ell \in \{1, 2, \dots, L_{\text{TX}}\}$ and TX $\in \{\text{B}, \text{J}\}$, with L_ψ being the duration of $\psi_{\text{a}}(t)$ (in sampling periods), so as the signal $y^{(j,s)}_{\text{a}}(t)$ is impaired only by the interblock interference (IBI) of the symbol transmitted in the previous signaling interval $t \in [(s-1)T, sT)$ and, thus, the integer h is restricted to the binary set $\{s-1, s\}$.

The continuous-time signal (6) is sampled with rate $1/T_c$ at time instants $t_{s,q} \triangleq sT + qT_{\text{c}}$, for $q \in \{0, 1, \dots, P-1\}$. Let $y^{(j,q)}(s) \triangleq y^{(j,s)}_{\text{a}}(t_{s,q})$ be the discrete-time counterpart of (6), one gets

$$\begin{aligned} y^{(j,q)}(s) &= \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{h=s-1}^{s} \sum_{i=1}^{\widetilde{M}} \sum_{p=0}^{P-1} z^{(i,p)}_{\text{TX}}(h) \\ &\qquad \cdot c^{(j,i,s,h)}_{\text{TX}}\left((s-h)P + q - p\right) + w^{(j,q)}(s) \qquad (7)\end{aligned}$$

with

$$\begin{aligned} c^{(j,i,s,h)}_{\text{TX}}(r) &\triangleq \frac{1}{\sqrt{\widetilde{N}_{\text{U}}}} \sum_{\ell=1}^{L_{\text{TX}}} \rho_{\text{TX}}(\ell)\, f^{(j,s)}_{\text{TX}}(\ell) \\ &\qquad \cdot g^{(i,h)}_{\text{TX}}(\ell)\, \psi_{\text{TX}}\left(r - \nu_{\text{TX}}(\ell), \ell\right) \qquad (8)\end{aligned}$$

where $r \in \mathbb{Z}$, we have defined $\psi_{\text{TX}}(r, \ell) \triangleq \psi_{\text{a}}\left(rT_c - \chi_{\text{TX}}(\ell)\right)$ and $\tau_{\text{TX}}(\ell) = \nu_{\text{TX}}(\ell)\, T_{\text{c}} + \chi_{\text{TX}}(\ell)$, with integer delay $\nu_{\text{TX}}(\ell)$ and fractional delay $\chi_{\text{TX}}(\ell) \in [0, T_{\text{c}})$, and noise sample $w^{(j,q)}(s) \triangleq w^{(j,s)}_{\text{a}}(t_{s,q})$. Under the assumption that the CP is sufficiently long, i.e., $L_{\text{cp}} \geq L_\psi + (\tau_{\max} - \tau_{\min})/T_{\text{c}}$, where $\tau_{\min} \triangleq \min_{\text{TX},\ell} \tau_{\text{TX}}(\ell)$ and $\tau_{\max} \triangleq \max_{\text{TX},\ell} \tau_{\text{TX}}(\ell)$, the IBI contributions in (7), which are represented by the addends corresponding to $h = s-1$, can be suppressed through CP removal. Therefore, by removing the first L_{cp} samples (corresponding to the CP), gathering the obtained data into the vector $\mathbf{y}^{(j)}(s) \triangleq [y^{(j,L_{\text{cp}})}(s), y^{(j,L_{\text{cp}}+1)}(s), \dots, y^{(j,P-1)}(s)]^{\text{T}} \in \mathbb{C}^F$, and accounting for (7), one obtains, for $j \in \{1, 2, \dots, \widetilde{N}_{\text{U}}\}$, the following IBI-free vector model

$$\mathbf{y}^{(j)}(s) = \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{i=1}^{\widetilde{M}} \text{circ}\left(\mathbf{c}^{(j,i)}_{\text{TX}}(s)\right) \mathbf{W}^{(i)}\, \mathbf{d}^{(i)}_{\text{TX}}(s) + \mathbf{w}^{(j)}(s) \qquad (9)$$

where $\text{circ}\left(\mathbf{c}^{(j,i)}_{\text{TX}}(s)\right) \in \mathbb{C}^{F \times F}$ is the circulant [35] channel matrix having

$$\begin{aligned} \mathbf{c}^{(j,i)}_{\text{TX}}(s) \triangleq [&c^{(j,i,s,s)}_{\text{TX}}(L_{\text{cp}}), c^{(j,i,s,s)}_{\text{TX}}(L_{\text{cp}}-1), \\ &\dots, c^{(j,i,s,s)}_{\text{TX}}(0), 0, \dots, 0] \in \mathbb{C}^{1 \times F}\end{aligned}$$

as its first row, whereas the additive noise is given by $\mathbf{w}^{(j)}(s) \triangleq [w^{(j,L_{\text{cp}})}(s), w^{(j,L_{\text{cp}}+1)}(s), \dots, w^{(j,P-1)}(s)]^{\text{T}} \in \mathbb{C}^F$. At this point, performing the DFT of $\mathbf{y}^{(j)}(s)$ and recalling that circulant matrices are diagonalized by the DFT [35], the frequency-domain received data vector assumes the form

$$\overline{\mathbf{y}}^{(j)}(s) = \sum_{\text{TX}\in\{\text{B},\text{J}\}} \sum_{i=1}^{\widetilde{M}} \text{diag}\left(\overline{\mathbf{c}}^{(j,i)}_{\text{TX}}(s)\right) \mathbf{R}^{(i)}\, \mathbf{d}^{(i)}_{\text{TX}}(s) + \overline{\mathbf{w}}^{(j)}(s) \qquad (10)$$

for $j \in \{1, 2, \dots, \widetilde{N}_{\text{U}}\}$, where $\overline{\mathbf{y}}^{(j)}(s) \triangleq \mathbf{W}^{\text{H}}_F\, \mathbf{y}^{(j)}(s) \in \mathbb{C}^F$, $\mathbf{W}^{\text{H}}_F$ is the F-point DFT matrix (see Subsection I-C), the vector $\overline{\mathbf{c}}^{(j,i)}_{\text{TX}}(s) \triangleq [\overline{c}^{(j,i,0)}_{\text{TX}}(s), \overline{c}^{(j,i,1)}_{\text{TX}}(s), \dots, \overline{c}^{(j,i,F-1)}_{\text{TX}}(s)]^{\text{T}} \in \mathbb{C}^F$ gathers the frequency-domain channel samples given by

$$\begin{aligned} \overline{c}^{(j,i,k)}_{\text{TX}}(s) &= \frac{1}{\sqrt{\widetilde{N}_{\text{U}}}} \sum_{\ell=1}^{L_{\text{TX}}} \rho_{\text{TX}}(\ell)\, f^{(j,s)}_{\text{TX}}(\ell)\, g^{(i,s)}_{\text{TX}}(\ell) \\ &\qquad \cdot e^{-\jmath \frac{2\pi}{F} k\, \nu_{\text{TX}}(\ell)}\, \Psi_{\text{TX}}\left(\frac{k}{F}, \ell\right) \qquad (11)\end{aligned}$$

for $k \in \{0,1,\dots,F-1\}$, with $\Psi_{\text{TX}}(\nu,\ell) = \mathscr{F}[\psi_{\text{TX}}(r,\ell)]$ being the Fourier transform of $\psi_{\text{TX}}(r,\ell)$ with respect to r, whereas $\mathbf{R}^{(i)} \triangleq \mathbf{W}_F^{\text{H}}\,\mathbf{W}^{(i)} \in \mathbb{R}^{F\times F_i}$ is a binary (0/1) matrix that extends the probing vector $\mathbf{d}_{\text{TX}}^{(i)}(s)$ with the insertion of $F-F_i$ zeros on the subcarriers belonging to the set $\mathcal{F}_i^{\text{c}}$, which is the complement of $\mathcal{F}_i$ with respect to the subcarrier set $\{0,1,\dots,F-1\}$, and, finally, $\overline{\mathbf{w}}^{(j)}(s) \triangleq \mathbf{W}_F^{\text{H}}\,\mathbf{w}^{(j)}(s)$ is modeled as zero-mean complex circular Gaussian with $\mathbb{E}[\overline{\mathbf{w}}^{(j_1)}(s_1)\,\overline{\mathbf{w}}^{(j_2)}(s_2)] = \sigma_w^2\,\delta_{j_1-j_2}\,\delta_{s_1-s_2}\,\mathbf{I}_F$.

By substituting into (11) the beamforming gain $g_{\text{TX}}^{(i,s)}(\ell) = \mathbf{a}_{\text{TX}}^{\text{H}}(\theta_{\text{TX}}(\ell))\,\mathbf{u}_{\text{TX}}^{(i,s)}$ and array gain $f_{\text{TX}}^{(j,s)}(\ell) = \left[\mathbf{v}^{(j,s)}\right]^{\text{H}}\mathbf{b}(\phi_{\text{TX}}(\ell))$, one has the compact expression $\overline{c}_{\text{TX}}^{(j,i,k)}(s) = \left[\mathbf{v}^{(j,s)}\right]^{\text{H}}\overline{\mathbf{C}}_{\text{TX}}^{(k)}\,\mathbf{u}_{\text{TX}}^{(i,s)}$, where matrix $\overline{\mathbf{C}}_{\text{TX}}^{(k)} \in \mathbb{C}^{N_{\text{U}}\times M_{\text{TX}}}$ is given by

$$\overline{\mathbf{C}}_{\text{TX}}^{(k)} \triangleq \frac{1}{\sqrt{\widetilde{N}_{\text{U}}}}\sum_{\ell=1}^{L_{\text{TX}}}\rho_{\text{TX}}(\ell)\,\Psi_{\text{TX}}\left(\frac{k}{F},\ell\right) \cdot e^{-\jmath\frac{2\pi}{F}k\,\nu_{\text{TX}}(\ell)}\,\mathbf{b}(\phi_{\text{TX}}(\ell))\,\mathbf{a}_{\text{TX}}^{\text{H}}(\theta_{\text{TX}}(\ell)) \quad (12)$$

for $k \in \{0,1,\dots,F-1\}$. Consequently, after some straightforward manipulations, eq. (10) admits the equivalent form:

$$\overline{\mathbf{y}}^{(j)}(s) = \sum_{\text{TX}\in\{\text{B,J}\}}\sum_{i=1}^{\widetilde{M}}\left[\mathbf{I}_F\otimes\mathbf{v}^{(j,s)}\right]^{\text{H}}\overline{\mathbf{C}}_{\text{TX}}\left[\mathbf{I}_F\otimes\mathbf{u}_{\text{TX}}^{(i,s)}\right] \cdot \mathbf{R}^{(i)}\,\mathbf{d}_{\text{TX}}^{(i)}(s) + \overline{\mathbf{w}}^{(j)}(s) \quad (13)$$

for $j \in \{1,2,\dots,\widetilde{N}_{\text{U}}\}$, where we have defined the block-diagonal matrix

$$\overline{\mathbf{C}}_{\text{TX}} \triangleq \text{diag}\left(\overline{\mathbf{C}}_{\text{TX}}^{(0)},\overline{\mathbf{C}}_{\text{TX}}^{(1)},\dots,\overline{\mathbf{C}}_{\text{TX}}^{(F-1)}\right) \in \mathbb{C}^{(N_{\text{U}}F)\times(M_{\text{TX}}F)}\,. \quad (14)$$

D. Virtual channel model

The highly directional nature of propagation, together with the large number of antennas employed in MMW systems, makes *virtual* or *canonical model* of MIMO channel [11], [36], [37] a natural choice for our framework. Specifically, we assume that the BS, jammer and receiver are equipped with a *uniform linear array (ULA)* and we assume that the UE is in the far-field of both the transmitters. In this case, let d_{TX} and d_{U} denote the antenna spacing at the generic transmit node TX and the UE, respectively, the (normalized) array vectors are given by

$$\mathbf{a}_{\text{TX}}(\theta_{\text{TX}}(\ell)) \equiv \widetilde{\mathbf{a}}_{\text{TX}}(\vartheta_{\text{TX}}(\ell)) \triangleq \frac{1}{\sqrt{M_{\text{TX}}}}\left[1, e^{-\jmath\,2\pi\vartheta_{\text{TX}}(\ell)}, e^{-\jmath\,4\pi\vartheta_{\text{TX}}(\ell)},\dots,e^{-\jmath\,2\pi\vartheta_{\text{TX}}(\ell)(M_{\text{TX}}-1)}\right]^{\text{T}}$$
$$\mathbf{b}(\phi_{\text{TX}}(\ell)) \equiv \widetilde{\mathbf{b}}(\varphi_{\text{TX}}(\ell)) \triangleq \frac{1}{\sqrt{N_{\text{U}}}}\left[1, e^{-\jmath\,2\pi\varphi_{\text{TX}}(\ell)}, e^{-\jmath\,4\pi\varphi_{\text{TX}}(\ell)},\dots,e^{-\jmath\,2\pi\varphi_{\text{TX}}(\ell)(N_{\text{U}}-1)}\right]^{\text{T}} \quad (15)$$

where the *normalized spatial angles* $\vartheta_{\text{TX}}(\ell)$ and $\varphi_{\text{TX}}(\ell)$ are related to the physical AoD $\theta_{\text{TX}}(\ell)$ and physical AoA $\phi_{\text{TX}}(\ell)$ through the relations $\vartheta_{\text{TX}}(\ell) \triangleq (d_{\text{TX}}/\lambda_0)\sin\theta_{\text{TX}}(\ell)$ and $\varphi_{\text{TX}}(\ell) \triangleq (d_{\text{U}}/\lambda_0)\sin\phi_{\text{TX}}(\ell)$, respectively, whereas the wavelength is $\lambda_0 = c/f_0$, with c being the speed of the light in the medium. Hereinafter, we set $d_{\text{TX}} = d_{\text{U}} = \lambda_0/2$ for simplicity, which implies that $|\vartheta_{\text{TX}}(\ell)| \le 1/2$ and $|\varphi_{\text{TX}}(\ell)| \le 1/2$, for any $\ell \in \{1,2,\dots,L_{\text{TX}}\}$.

The virtual representation of the physical channel can be obtained [38] by uniformly sampling (12) in the AoD-AoA-delay 3-D domain at the Nyquist rate $(\Delta\vartheta_{\text{TX}},\Delta\varphi_{\text{TX}},\Delta\nu_{\text{TX}}) = (1/M_{\text{TX}},1/N_{\text{U}},T_{\text{c}})$, where $1/T_{\text{c}}$ is (approximately) the two-sided bandwidth of the OFDM signal. Therefore, the virtual representation of the channel matrix (12) is approximately given by[3]

$$\overline{\mathbf{C}}_{\text{TX}}^{(k)} = \sum_{n=0}^{N_{\text{U}}-1}\sum_{m=0}^{M_{\text{TX}}-1}\sum_{\widetilde{\ell}=0}^{\widetilde{L}_{\text{TX}}-1}\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}\,\widetilde{\mathbf{b}}\left(\frac{n}{N_{\text{U}}}-\frac{1}{2}\right) \cdot \widetilde{\mathbf{a}}_{\text{TX}}^{\text{H}}\left(\frac{m}{M_{\text{TX}}}-\frac{1}{2}\right)e^{-\jmath\frac{2\pi}{F}k\,\widetilde{\ell}\,T_{\text{c}}} \quad (16)$$

for $k \in \{0,1,\dots,F-1\}$, where the $N_{\text{U}}\,M_{\text{TX}}\,\widetilde{L}_{\text{TX}}$ *virtual channel coefficients* $\{\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}\}$ completely characterize the channel matrix (12), with N_{U}, M_{TX}, and $\widetilde{L}_{\text{TX}} \triangleq \lceil \nu_{\text{TX,max}}/T_{\text{c}}\rceil + 1$ denoting the maximum number of *resolvable* AoAs, AoDs, and delays in the AoD-AoA-delay 3-D domain, and, finally, $\nu_{\text{TX,max}} \triangleq \max_\ell \nu_{\text{TX}}(\ell)$. It is worth noting that each virtual coefficient $\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}$ is approximately equal to the sum of the complex gains of all the physical paths whose angles and delays belong to the resolution bin of dimension $\Delta\vartheta_{\text{TX}}\times\Delta\varphi_{\text{TX}}\times\Delta\nu_{\text{TX}}$ centered around the sampling point $(m/M_{\text{TX}}-1/2, n/N_{\text{U}}-1/2, \widetilde{\ell}\,T_{\text{c}})$ in the AoD-AoA-delay 3-D domain. We assume that each $\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}$ is a circularly symmetric complex Gaussian random variable. According to the central limit theorem, this is a reasonable assumption if there is a sufficiently large number of unresolvable physical paths contributing to each $\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}$. Moreover, if M_{TX}, N_{U}, and $1/T_{\text{c}}$ are sufficiently large, the virtual channel coefficients are approximately statistically independent (see [36] for details). Henceforth, we assume that the channel coefficients $\widetilde{C}_{\text{B}}^{(n,m,\widetilde{\ell})}$ and $\widetilde{C}_{\text{J}}^{(n,m,\widetilde{\ell})}$ are mutually independent zero-mean uncorrelated RVs, i.e., $\mathbb{E}[\widetilde{C}_{\text{TX}}^{(n_1,m_1,\widetilde{\ell}_1)}\{\widetilde{C}_{\text{TX}}^{(n_2,m_2,\widetilde{\ell}_2)}\}^*] = \widetilde{\sigma}_{\text{TX}}^2(n_1,m_1,\ell_1)\,\delta_{n_1-n_2}\,\delta_{m_1-m_2}\,\delta_{\widetilde{\ell}_1-\widetilde{\ell}_2}$, for TX $\in$ {B, J}, where $\widetilde{\sigma}_{\text{TX}}^2(n,m,\ell)$ is related to the variances of the physical channel gains via virtual partitioning of the paths [36].

Let $\mathbf{J}_r \triangleq \text{diag}(1, e^{\jmath\pi}, e^{\jmath 2\pi},\dots,e^{\jmath\pi(r-1)}) \in \mathbb{R}^r$, it is readily verified that $\widetilde{\mathbf{a}}_{\text{TX}}(m/M_{\text{TX}}-1/2) = \mathbf{J}_{M_{\text{TX}}}^*\,\widetilde{\mathbf{a}}_{\text{TX}}(m/M_{\text{TX}})$ and $\widetilde{\mathbf{b}}(n/N_{\text{U}}-1/2) = \mathbf{J}_{N_{\text{U}}}^*\,\widetilde{\mathbf{b}}(n/N_{\text{U}})$. By observing that $\mathbf{J}_{M_{\text{TX}}}^*\,\widetilde{\mathbf{a}}_{\text{TX}}(m/M_{\text{TX}})$ and $\mathbf{J}_{N_{\text{U}}}^*\,\widetilde{\mathbf{b}}(n/N_{\text{U}})$ in (16) turn out to be the $(m+1)$-th column and $(n+1)$-th column of the M_{TX}-point DFT matrix $\mathbf{W}_{M_{\text{TX}}}^{\text{H}}$ and the N_{U}-point DFT matrix $\mathbf{W}_{N_{\text{U}}}^{\text{H}}$ matrix, respectively, for $m \in \{0,1,\dots,M_{\text{TX}}-1\}$ and $n \in \{0,1,\dots,N_{\text{U}}-1\}$, the channel matrix (16) can be expressed in a more compact form as

$$\overline{\mathbf{C}}_{\text{TX}}^{(k)} = \mathbf{J}_{N_{\text{U}}}\,\mathbf{W}_{N_{\text{U}}}^{\text{H}}\,\widetilde{\mathbf{C}}_{\text{TX}}^{(k)}\,\mathbf{W}_{M_{\text{TX}}}\,\mathbf{J}_{M_{\text{TX}}}^* \quad (17)$$

[3] The effect of the frequency-domain coefficient $\Psi_{\text{TX}}(k/F,\ell)$ disappears in the sampled representation (16) of the physical model (12) if the pulse $\psi_{\text{a}}(t)$ satisfies the Nyquist criterion.

for $k \in \{0, 1, \ldots, F-1\}$, with

$$\widetilde{\mathbf{C}}_{\text{TX}}^{(k)} \triangleq \sum_{\widetilde{\ell}=0}^{\widetilde{L}_{\text{TX}}-1} \widetilde{\mathbf{C}}_{\text{TX}}^{(\widetilde{\ell})} \, e^{-\jmath \frac{2\pi}{F} k \, \widetilde{\ell} \, T_{\text{c}}} \tag{18}$$

where the $(n+1, m+1)$-th entry of $\widetilde{\mathbf{C}}_{\text{TX}}^{(\widetilde{\ell})} \in \mathbb{C}^{N_{\text{U}} \times M_{\text{TX}}}$ is given by $\widetilde{C}_{\text{TX}}^{(n,m,\widetilde{\ell})}$, for $n \in \{0, 1, \ldots, N_{\text{U}}-1\}$ and $m \in \{0, 1, \ldots, M_{\text{TX}}-1\}$. Representation (17) is of paramount importance since the *virtual channel matrix* $\widetilde{\mathbf{C}}_{\text{TX}}^{(k)}$ captures the *sparse* nature of the MMW MIMO channel: indeed, wireless channels with clustered multipath components tend to have far fewer than $N_{\text{U}} \, M_{\text{TX}} \, \widetilde{L}_{\text{TX}}$ virtual channel coefficients when operate at large bandwidths and symbol durations and/or with massive number of antennas. It can be verified numerically that, as the number of transmit M_{TX} and receive N_{U} antennas increases, the matrix $\widetilde{\mathbf{C}}_{\text{TX}}^{(k)}$ becomes more and more sparse.

At this point, substituting (17) into (13) and using the mixed-product property of the Kronecker product [35], the received signal can be conveniently rewritten in terms of the virtual channel as

$$\begin{aligned}\overline{\mathbf{y}}^{(j)}(s) = & \sum_{\text{TX} \in \{\text{B,J}\}} \sum_{i=1}^{\widetilde{M}} \left[\mathbf{I}_F \otimes \widetilde{\mathbf{v}}^{(j,s)}\right]^{\text{H}} \widetilde{\mathbf{C}}_{\text{TX}} \left[\mathbf{I}_F \otimes \widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)}\right] \\ & \cdot \mathbf{R}^{(i)} \, \mathbf{d}_{\text{TX}}^{(i)}(s) + \overline{\mathbf{w}}^{(j)}(s) \, , \quad \text{for } j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}\end{aligned} \tag{19}$$

where we have defined $\widetilde{\mathbf{v}}^{(j,s)} \triangleq \mathbf{J}_{N_{\text{U}}} \mathbf{W}_{N_{\text{U}}} \mathbf{v}^{(j,s)} \in \mathbb{C}^{N_{\text{U}}}$, $\widetilde{\mathbf{C}}_{\text{TX}} \triangleq \text{diag}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(0)}, \widetilde{\mathbf{C}}_{\text{TX}}^{(1)}, \ldots, \widetilde{\mathbf{C}}_{\text{TX}}^{(F-1)}\right) \in \mathbb{C}^{(N_{\text{U}} F) \times (M_{\text{TX}} F)}$, and $\widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)} \triangleq \mathbf{J}_{M_{\text{TX}}} \mathbf{W}_{M_{\text{TX}}} \mathbf{u}_{\text{TX}}^{(i,s)} \in \mathbb{C}^{M_{\text{TX}}}$.

The two sets

$$\left\{\widetilde{\mathbf{u}}_{\text{B}}^{(i,s)}, \text{for } i \in \{1, 2, \ldots, \widetilde{M}\} \text{ and } s \in \{0, 1, \ldots, W-1\}\right\}$$

and

$$\left\{\widetilde{\mathbf{u}}_{\text{J}}^{(i,s)}, \text{for } i \in \{1, 2, \ldots, \widetilde{M}\} \text{ and } s \in \{0, 1, \ldots, W-1\}\right\}$$

represent the *transmit beamforming codebooks* of the BS and the jammer, respectively, which define the directions along which the transmit beam patterns $\{\mathbf{u}_{\text{B}}^{(i,s)}\}$ and $\{\mathbf{u}_{\text{J}}^{(i,s)}\}$ send the legitimate and jamming signal power, respectively. On the other hand, the set

$$\left\{\widetilde{\mathbf{v}}^{(j,s)}, \text{for } j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\} \text{ and } s \in \{0, 1, \ldots, W-1\}\right\}$$

represents the *receive beamforming codebook* of the UE, which defines the directions from which the receiver beam patterns $\{\mathbf{v}^{(j,s)}\}$ collect the overall signal power.

E. Beacon slot model

Recalling that the probing vectors $\mathbf{d}_{\text{TX}}^{(1)}(s), \mathbf{d}_{\text{TX}}^{(2)}(s), \ldots, \mathbf{d}_{\text{TX}}^{(\widetilde{M})}(s)$ corresponding to the $\widetilde{M}$ streams are allocated to disjoint subcarrier sets, i.e., $\mathcal{F}_{i_1} \cap \mathcal{F}_{i_2} = \emptyset$ for $i_1 \neq i_2$, we focus on the F_i subcarriers assigned to the i-th stream, with $i \in \{1, 2, \ldots, \widetilde{M}\}$, by picking up only the entries $\overline{y}^{(j,k_{i,0})}(s), \overline{y}^{(j,k_{i,1})}(s), \ldots, \overline{y}^{(j,k_{i,F_i-1})}(s)$ of the received vector $\overline{\mathbf{y}}^{(j)}(s)$ at the output of the j-th RF chain with indices in the set $\mathcal{F}_i = \{k_{i,0}, k_{i,1}, \ldots, k_{i,F_i-1}\}$. On such subcarriers the contribution of the probing vectors $\mathbf{d}_{\text{TX}}^{(i')}(s)$ for $i' \neq i$ is zero. So doing, from (19), the i-th probing signal received during the s-th data block on subcarrier $k_{i,\ell}$ is

$$\begin{aligned}\overline{y}^{(j,k_{i,\ell})}(s) = & \sum_{\text{TX} \in \{\text{B,J}\}} [\widetilde{\mathbf{v}}^{(j,s)}]^{\text{H}} \, \widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})} \\ & \cdot \widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)} \, d_{\text{TX}}^{(k_{i,\ell})}(s) + \overline{w}^{(j,k_{i,\ell})}(s) \\ = & \sum_{\text{TX} \in \{\text{B,J}\}} [\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i,s)}]^{\text{H}} \, \text{vec}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})}\right) \\ & \cdot d_{\text{TX}}^{(k_{i,\ell})}(s) + \overline{w}^{(j,k_{i,\ell})}(s)\end{aligned} \tag{20}$$

with $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, $i \in \{1, 2, \ldots, \widetilde{M}\}$, and $\ell \in \{0, 1, \ldots, F_i - 1\}$, where $\overline{w}^{(j,k_{i,0})}(s), \overline{w}^{(j,k_{i,1})}(s), \ldots, \overline{w}^{(j,k_{i,F_i-1})}(s)$ are the entries of $\overline{\mathbf{w}}^{(j)}(s)$ with indices in the set $\mathcal{F}_i$, we have used the identity $[\widetilde{\mathbf{v}}^{(j,s)}]^{\text{H}} \, \widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})} \, \widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)} = \{[\widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)}]^{\text{T}} \otimes [\widetilde{\mathbf{v}}^{(j,s)}]^{\text{H}}\} \, \text{vec}(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})})$ [39], and $\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i,s)} \triangleq [\widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)}]^* \otimes \widetilde{\mathbf{v}}^{(j,s)} \in \mathbb{C}^{M_{\text{TX}} N_{\text{U}}}$ represents the combined TX-UE beamforming vector.

As depicted in Fig. 2 at the top of the next page, the BA phase is divided in Q *beacon slots* of duration equal to S consecutive OFDM blocks, i.e., $W = Q \, S$. At this point, let us denote with $\overline{y}^{(j,k_{i,\ell},s')}(\widetilde{s}) \triangleq \overline{y}^{(j,k_{i,\ell})}(\widetilde{s} \, S + s')$ the polyphase decomposition of the received data (20) with respect to S, for $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ and $s' \in \{0, 1, \ldots, S-1\}$. It assumed that the beamforming vectors $\widetilde{\mathbf{u}}_{\text{TX}}^{(i,s)}$ and $\widetilde{\mathbf{v}}^{(j,s)}$ are constant in each beacon slot, but they may vary from a beacon slot to another, i.e., $\widetilde{\mathbf{u}}_{\text{TX}}^{(i,\widetilde{s} \, S+s')} \equiv \widetilde{\mathbf{u}}_{\text{TX}}^{(i)}(\widetilde{s})$ and $\widetilde{\mathbf{v}}^{(j,\widetilde{s} \, S+s')} \equiv \widetilde{\mathbf{v}}^{(j)}(\widetilde{s})$. In this case, according to (20), one has

$$\begin{aligned}\overline{y}^{(j,k_{i,\ell},s')}(\widetilde{s}) = & \sum_{\text{TX} \in \{\text{B,J}\}} [\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})]^{\text{H}} \, \text{vec}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})}\right) \\ & \cdot d_{\text{TX}}^{(k_{i,\ell},s')}(\widetilde{s}) + \overline{w}^{(j,k_{i,\ell},s')}(\widetilde{s})\end{aligned} \tag{21}$$

where $\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s}) \triangleq [\widetilde{\mathbf{u}}_{\text{TX}}^{(i)}(\widetilde{s})]^* \otimes \widetilde{\mathbf{v}}^{(j)}(\widetilde{s}) \in \mathbb{C}^{M_{\text{TX}} N_{\text{U}}}$, $d_{\text{TX}}^{(k_{i,\ell},s')}(\widetilde{s}) \triangleq d_{\text{TX}}^{(k_{i,\ell})}(\widetilde{s} \, S + s')$, and noise sample $\overline{w}^{(j,k_{i,\ell},s')}(\widetilde{s}) \triangleq \overline{w}^{(j,k_{i,\ell})}(\widetilde{s} \, S + s')$. We are considering the case of perfect beacon synchronization between BS and UE, as well as between the jammer and UE. Such an assumption is reasonable in practice since beacon slots are periodically repeated and, thus, terminals can easily acquire perfect knowledge of the start epoch of each beacon slot [11].

F. Structure of the beamforming codebooks

To ensure spatial coverage, the size of the transmit and receive beamforming codebooks is proportional to the number of transmit and receive antennas. Therefore, for large-scale array in MMW communication, exhaustive search [40], although guaranteeing to select the optimal beam, introduces unacceptable beam training overhead. On the other hand, hierarchical schemes [41] require a non-trivial coordination among the UEs and the BS, which is difficult to have at the initial channel acquisition stage. Even though the proposed anti-jamming strategy can be applied to many available beamforming schemes, we resort herein to pseudo-random beamforming codebooks [10], [11], [42], which do not require interaction between the BS and each UE, and their overhead

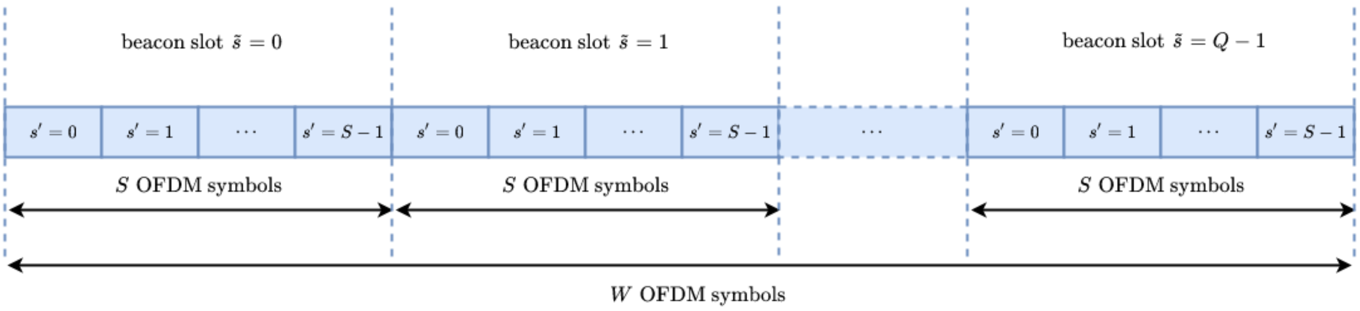

beacon slot $\tilde{s} = 0$
beacon slot $\tilde{s} = 1$
beacon slot $\tilde{s} = Q-1$
$s' = 0$
$s' = 1$
$\cdots$
$s' = S-1$
S OFDM symbols
W OFDM symbols

Fig. 2. The BA phase spans a time window of W OFDM symbols, which is divided into Q beacons slots of S OFDM symbols.

and complexity do not grow with the number of active users in the system. According to these schemes, the beamforming vectors of the transmitter TX and UE are

$$\widetilde{\mathbf{u}}_{\text{TX}}^{(i)}(\widetilde{s}) = \frac{\mathbf{1}_{\mathcal{U}_{\text{TX}}^{(i)}(\widetilde{s})}}{\sqrt{U_{\text{TX}}}} \quad \text{and} \quad \widetilde{\mathbf{v}}^{(j)}(\widetilde{s}) = \frac{\mathbf{1}_{\mathcal{V}^{(j)}(\widetilde{s})}}{\sqrt{V}} \tag{22}$$

respectively, where the *angular support sets* $\mathcal{U}_{\text{TX}}^{(i)}(\widetilde{s}) \subseteq \{1, 2, \ldots, M_{\text{TX}}\}$ and $\mathcal{V}^{(j)}(\widetilde{s}) \subseteq \{1, 2, \ldots, N_{\text{U}}\}$ of cardinality $U_{\text{TX}} \triangleq \left|\mathcal{U}_{\text{TX}}^{(i)}(\widetilde{s})\right|$ and $V \triangleq \left|\mathcal{V}^{(j)}(\widetilde{s})\right|$ collect the angles in the virtual beamspace channel representation that are probed by TX and sensed by the UE, respectively. So doing, the combined TX-UE beamforming vector in (21) reads as

$$\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s}) = \frac{\mathbf{1}_{\mathcal{U}_{\text{TX}}^{(i)}(\widetilde{s})} \otimes \mathbf{1}_{\mathcal{V}^{(j)}(\widetilde{s})}}{\sqrt{U_{\text{TX}}}\,\sqrt{V}} \tag{23}$$

whose entries are equal to 0 or 1 depending on the elements of the sets $\mathcal{U}_{\text{TX}}^{(i)}(\widetilde{s})$ and $\mathcal{V}^{(j)}(\widetilde{s})$.

The transmit beamforming codebook of the BS and the receive beamforming codebook of the UE are indeed pseudo-random since $\mathcal{U}_{\text{B}}^{(i)}(\widetilde{s})$, for $i \in \{1, 2, \ldots, \widetilde{M}\}$, and $\mathcal{V}^{(j)}(\widetilde{s})$, for $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, are generated in a pseudo-random manner, for each beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$. At each beacon slot, the subsets $\mathcal{U}_{\text{B}}^{(i)}(\widetilde{s})$, for $i \in \{1, 2, \ldots, \widetilde{M}\}$, are perfectly known at the UE, whereas $\mathcal{V}^{(j)}(\widetilde{s})$, for $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, are locally and independently generated by the UE. As regards the jammer, the transmit beamforming codebook $\mathcal{U}_{\text{J}}^{(i)}(\widetilde{s})$ is assumed to be unknown at the UE, for each beacon slot and $i \in \{1, 2, \ldots, \widetilde{M}\}$. The impact of the choice of the jamming codebook on the BA procedure between the BS and the UE is discussed in Section III.

G. Probing symbols of the BS in conventional schemes

Conventional BA schemes [6]–[25] do not account for jamming attacks. In such *jammer-unaware* methods, the BS transmits known probing symbols during each beacon slot:

$$d_{\text{B}}^{(k_{i,\ell})}(s) = \sqrt{\mathcal{P}_{\text{B}}}\, t^{(k_{i,\ell})}(s) \tag{24}$$

where $t^{(k_{i,\ell})}(s) \in \mathbb{C}$ is a publicly known symbol corresponding to the i-th stream in the s-th block on subcarrier $k_{i,\ell}$, with $|t^{(k_{i,\ell})}(s)|^2 = 1$, for $\ell \in \{0, 1, \ldots, F_i - 1\}$, and $\mathcal{P}_{\text{B}}$ is the available power per symbol at the BS. In Section IV, we will suitably modify the transmission scheme (24) to confer anti-jamming capabilities to the BA procedure.

H. Probing symbols of the jammer

The probing symbols transmitted by the jammer are essentially a noisy version of the publicly known probing symbols $\{t^{(k_{i,\ell})}(s)\}$ and they are modeled as

$$d_{\text{J}}^{(k_{i,\ell})}(s) = \sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, t^{(k_{i,\ell})}(s) + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, r_{\text{J}}^{(k_{i,\ell})}(s) \tag{25}$$

where $\mathcal{P}_{\text{J}}$ is the available power per symbol of the jammer and each stream $\{r_{\text{J}}^{(k_{i,\ell})}(s)\}$ is modeled as a sequence of zero-mean unit-variance independent and identically distributed (i.i.d.) complex circular RVs. For the sake of generality, we have introduced in (25) a power factor $0 \le \gamma_{\text{J}} \le 1$ that allows us to account for different jamming attacks. In extreme cases, the jammer may exclusively transmit known probing symbols, i.e., $\gamma_{\text{J}} = 0$ or, on the other hand, it might send in the air noise only, i.e., $\gamma_{\text{J}} = 1$. In the intermediate case $0 < \gamma_{\text{J}} < 1$, the jammer could decide to split its available power between known probing symbols and intentional noise.

III. Jammer-unaware beam alignment

In this section, we show what is the impact of transmit beamforming codebook of the jammer on the BA acquisition performance when the BS uses the conventional probing scheme (24) in the presence of the jamming attack. In this situation, the received signal by the UE is obtained by substituting (24) and (25) into (21), thus obtaining

$$\begin{aligned} \overline{y}^{(j,k_{i,\ell},s')}(\widetilde{s}) &= \sqrt{\mathcal{P}_{\text{B}}}\, \widetilde{h}_{\text{B}}^{(j,i,k_{i,\ell})}(\widetilde{s})\, t^{(k_{i,\ell},s')}(\widetilde{s}) \\ &\quad + \widetilde{h}_{\text{J}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left[\sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, t^{(k_{i,\ell})}(s)\right. \\ &\quad \left. + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, r_{\text{J}}^{(k_{i,\ell},s')}(\widetilde{s})\right] + \overline{w}^{(j,k_{i,\ell},s')}(\widetilde{s}) \end{aligned} \tag{26}$$

where $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ and $s' \in \{0, 1, \ldots, S-1\}$, with $\widetilde{h}_{\text{TX}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \triangleq [\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})]^{\text{H}} \operatorname{vec}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})}\right)$, $t^{(k_{i,\ell},s')}(\widetilde{s}) \triangleq t^{(k_{i,\ell})}(\widetilde{s}\,S + s')$, and $r_{\text{J}}^{(k_{i,\ell},s')}(\widetilde{s}) \triangleq r_{\text{J}}^{(k_{i,\ell})}(\widetilde{s}\,S + s')$. With reference to the beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ (see Fig. 2), by stacking S consecutive samples (26) into the vector

$$\begin{aligned} \overline{\mathbf{y}}^{(j,k_{i,\ell})}(\widetilde{s}) \triangleq [&\overline{y}^{(j,k_{i,\ell},0)}(\widetilde{s}), \overline{y}^{(j,k_{i,\ell},1)}(\widetilde{s}), \\ &\ldots, \overline{y}^{(j,k_{i,\ell},S-1)}(\widetilde{s})]^{\text{T}} \in \mathbb{C}^S \end{aligned}$$

one obtains

$$\begin{aligned}\overline{\mathbf{y}}^{(j,k_{i,\ell})}(\widetilde{s}) &= \sqrt{\mathcal{P}_{\text{B}}}\, \widetilde{h}_{\text{B}}^{(j,i,k_{i,\ell})}(\widetilde{s})\, \mathbf{t}^{(k_{i,\ell})}(\widetilde{s}) \\ &\quad + \widetilde{h}_{\text{J}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left[\sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, \mathbf{t}^{(k_{i,\ell})}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, \mathbf{r}_{\text{J}}^{(k_{i,\ell})}(\widetilde{s})\right] + \overline{\mathbf{w}}^{(j,k_{i,\ell})}(\widetilde{s}) \qquad (27)\end{aligned}$$

where

$$\begin{aligned}\mathbf{t}^{(k_{i,\ell})}(\widetilde{s}) &\triangleq [t^{(k_{i,\ell},0)}(\widetilde{s}), t^{(k_{i,\ell},1)}(\widetilde{s}), \\ &\qquad \ldots, t^{(k_{i,\ell},S-1)}(\widetilde{s})]^{\text{T}} \in \mathbb{C}^{S} \\ \mathbf{r}_{\text{J}}^{(k_{i,\ell})}(\widetilde{s}) &\triangleq [r_{\text{J}}^{(k_{i,\ell},0)}(\widetilde{s}), r_{\text{J}}^{(k_{i,\ell},1)}(\widetilde{s}), \\ &\qquad \ldots, r_{\text{J}}^{(k_{i,\ell},S-1)}(\widetilde{s})]^{\text{T}} \in \mathbb{C}^{S} \\ \overline{\mathbf{w}}^{(j,k_{i,\ell})}(\widetilde{s}) &\triangleq [\overline{w}^{(j,k_{i,\ell},0)}(\widetilde{s}), \overline{w}^{(j,k_{i,\ell},1)}(\widetilde{s}), \\ &\qquad \ldots, \overline{w}^{(j,k_{i,\ell},S-1)}(\widetilde{s})]^{\text{T}} \in \mathbb{C}^{S} .\end{aligned}$$

The strongest multipath components of the legitimate channel correspond to the entries with large variance of the channel matrix $\overline{\mathbf{C}}_{\text{B}}^{(k)}$, which is defined in (16) and represented by (17), for $k \in \{0, 1, \ldots, F-1\}$. To identify the variance of such components and, thus, achieve successfully BA, several objective functions can be used in a jammer-unaware approach [7]–[25]. Herein, we focus on the second-order objective function introduced in [11] that can be expressed as

$$P^{(j,i)}(\widetilde{s}) = \frac{1}{S\,F_i} \sum_{\ell=0}^{F_i-1} \mathbb{E}\left[\left\|\overline{\mathbf{y}}^{(j,k_{i,\ell})}(\widetilde{s})\right\|_2^2\right] \qquad (28)$$

which represents the *(normalized) mean received power* of the i-th data stream at the output of the j-th RF chain during the $\widetilde{s}$-th beacon slot, where the expectation is also evaluated with respect to the random probing symbols transmitted by the jammer. By substituting (27) into (28) and invoking the statistically independence among channels, random sequences, and noise, one has

$$P^{(j,i)}(\widetilde{s}) = [\mathbf{g}_{\text{B}}^{(j,i)}(\widetilde{s})]^{\text{T}}\, \boldsymbol{\xi}_{\text{B}} + [\mathbf{g}_{\text{J}}^{(j,i)}(\widetilde{s})]^{\text{T}}\, \boldsymbol{\xi}_{\text{J}} + \sigma_w^2 \qquad (29)$$

where we have additionally observed that

$$\begin{aligned}\mathbb{E}\left[|\widetilde{h}_{\text{TX}}^{(j,i,k_{i,\ell})}(\widetilde{s})|^2\right] &= [\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})]^{\text{H}}\, \mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}}\, \widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s}) \\ &= [\mathbf{g}_{\text{TX}}^{(j,i)}(\widetilde{s})]^{\text{T}}\, \boldsymbol{\xi}_{\text{TX}} \qquad (30)\end{aligned}$$

with

$$\mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}} \triangleq \mathbb{E}\left[\text{vec}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})}\right)\, \text{vec}^{\text{H}}\left(\widetilde{\mathbf{C}}_{\text{TX}}^{(k_{i,\ell})}\right)\right] \in \mathbb{C}^{(M_{\text{TX}} N_{\text{U}}) \times (M_{\text{TX}} N_{\text{U}})}$$

being the covariance matrix of the vectorized beamspace representation of the channel matrix. It is worth noting that, under the assumption that the virtual channel coefficients are uncorrelated., the matrix $\mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}}$ is diagonal with some dominant components along the diagonal and, according to (18), it turns out to be independent of the subcarrier index $k_{i,\ell}$. In (30), we set $\mathbf{g}_{\text{TX}}^{(j,i)}(\widetilde{s}) \triangleq \sqrt{U_{\text{TX}}}\,\sqrt{V}\,\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})$, with the combined TX-UE beamforming vector $\widetilde{\mathbf{g}}_{\text{TX}}^{(j,i)}(\widetilde{s})$ given by (23), whereas

$$\begin{aligned}\boldsymbol{\xi}_{\text{TX}} \triangleq \frac{\mathcal{P}_{\text{TX}}}{U_{\text{TX}}\,V} &\left[\{\mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}}\}_{1,1}, \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}}\}_{2,2}, \right. \\ &\left. \ldots, \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\text{TX}}}\}_{M_{\text{TX}} N_{\text{U}}, M_{\text{TX}} N_{\text{U}}}\right]^{\text{T}} \in \mathbb{R}^{M_{\text{TX}} N_{\text{U}}} . \qquad (31)\end{aligned}$$

Within this section, we assume that σ_w^2 is known at the UE for beam determination. We remember that the vector $\mathbf{g}_{\text{B}}^{(j,i)}(\widetilde{s})$ is known at the UE, for all values of $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, $i \in \{1, 2, \ldots, \widetilde{M}\}$, and $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$. On the other hand, $\mathbf{g}_{\text{J}}^{(j,i)}(\widetilde{s})$ is *unknown* at the UE, since it does not have knowledge of both the transmit number of antennas M_{J} and beamforming codebook $\mathcal{U}_{\text{J}}^{(i)}(\widetilde{s})$ of the jammer. The unknown vector $\boldsymbol{\xi}_{\text{B}}$ has to be estimated to identify the AoA-AoD directions of the strongest scatterers regarding the BS-to-UE channel. To this aim, the UE can collect all the available power measurements in the vector

$$\begin{aligned}\mathbf{p} \triangleq{} & [P^{(1,1)}(0), \ldots, P^{(\widetilde{N}_{\text{U}},\widetilde{M})}(0), \\ & P^{(1,1)}(1), \ldots, P^{(\widetilde{N}_{\text{U}},\widetilde{M})}(1), \ldots, \\ & P^{(1,1)}(Q-1), \ldots, P^{(\widetilde{N}_{\text{U}},\widetilde{M})}(Q-1)]^{\text{T}} \\ &= \mathbf{G}_{\text{B}}\, \boldsymbol{\xi}_{\text{B}} + \mathbf{G}_{\text{J}}\, \boldsymbol{\xi}_{\text{J}} + \sigma_w^2\, \mathbf{1}_{\widetilde{M}\widetilde{N}_{\text{U}}Q} \qquad (32)\end{aligned}$$

with

$$\begin{aligned}\mathbf{G}_{\text{TX}} \triangleq{} & [\mathbf{g}_{\text{TX}}^{(1,1)}(0), \ldots, \mathbf{g}_{\text{TX}}^{(\widetilde{N}_{\text{U}},\widetilde{M})}(0), \\ & \mathbf{g}_{\text{TX}}^{(1,1)}(1), \ldots, \mathbf{g}_{\text{TX}}^{(\widetilde{N}_{\text{U}},\widetilde{M})}(1), \ldots, \\ & \mathbf{g}_{\text{TX}}^{(1,1)}(Q-1), \ldots, \mathbf{g}_{\text{TX}}^{(\widetilde{N}_{\text{U}},\widetilde{M})}(Q-1)]^{\text{T}} \\ & \in \mathbb{R}^{(\widetilde{M}\widetilde{N}_{\text{U}}Q) \times (M_{\text{TX}} N_{\text{U}})} . \qquad (33)\end{aligned}$$

The model (32) represents a high-dimensional system in which the number of unknowns $M_{\text{B}}\,N_{\text{U}}$ is at least of the same order of magnitude as the number of observations $\widetilde{M}\,\widetilde{N}_{\text{U}}\,Q$ or, even, $M_{\text{B}}\,N_{\text{U}} \gg \widetilde{M}\,\widetilde{N}_{\text{U}}\,Q$, in which case one cannot hope to recover the desired vector $\boldsymbol{\xi}_{\text{B}}$ if it does not exhibit any particular structure. However, the vector $\boldsymbol{\xi}_{\text{B}}$ is sparse and its entries are non-negative, i.e., $\boldsymbol{\xi}_{\text{B}} \geq \mathbf{0}_{M_{\text{B}} N_{\text{U}}}$. If the UE is unaware of the jamming attack, an estimate of $\boldsymbol{\xi}_{\text{B}}$ can be obtained by solving the *non-negative least-squares (NNLS)* problem:

$$\begin{aligned}\widehat{\boldsymbol{\xi}}_{\text{B}} = \arg \min_{\boldsymbol{\xi}_{\text{B}}^{\star} \in \mathbb{R}^{M_{\text{B}} N_{\text{U}}}} \left\|\mathbf{p} - \mathbf{G}_{\text{B}}\, \boldsymbol{\xi}_{\text{B}}^{\star} - \sigma_w^2\, \mathbf{1}_{\widetilde{M}\widetilde{N}_{\text{U}}Q}\right\|_2^2 , \\ \text{subject to } \boldsymbol{\xi}_{\text{B}}^{\star} \geq \mathbf{0}_{M_{\text{B}} N_{\text{U}}} \qquad (34)\end{aligned}$$

which is a convex optimization problem that can be solved efficiently [43]. In the absence of the jamming attack, under mild conditions on the matrix $\mathbf{G}_{\text{B}}$, the non-negativity constraint $\boldsymbol{\xi}_{\text{B}}^{\star} \geq \mathbf{0}_{M_{\text{B}} N_{\text{U}}}$ alone suffices for sparse recovery of $\boldsymbol{\xi}_{\text{B}}$, without the need to employ sparsity-promoting regularization terms [44]. The minimization program (34) is directly implemented in MATLAB as the function `lsqnonneg`, which executes the active-set algorithm of Lawson and Hanson [45].

In practice, the NNLS problem to be solved comes from replacing $\mathbf{p}$ in (34) with the corresponding estimate

$$\begin{aligned} \widehat{\mathbf{p}} \triangleq [&\widehat{P}^{(1,1)}(0), \ldots, \widehat{P}^{(\widetilde{N}_{\rm U},\widetilde{M})}(0), \\ &\widehat{P}^{(1,1)}(1), \ldots, \widehat{P}^{(\widetilde{N}_{\rm U},\widetilde{M})}(1), \ldots, \\ &\widehat{P}^{(1,1)}(Q-1), \ldots, \widehat{P}^{(\widetilde{N}_{\rm U},\widetilde{M})}(Q-1)]^{\rm T} \end{aligned} \quad (35)$$

where

$$\widehat{P}^{(j,i)}(\widetilde{s}) = \frac{1}{S\,F_i} \sum_{\ell=0}^{F_i-1} \left\| \overline{\mathbf{y}}^{(j,k_{i,\ell})}(\widetilde{s}) \right\|_2^2 \quad (36)$$

for $j \in \{1, 2, \ldots, \widetilde{N}_{\rm U}\}$ and $i \in \{1, 2, \ldots, \widetilde{M}\}$, within beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$.

A. Error analysis

As it is apparent from (32), the impact of the jamming attack on the BA procedure between the BS and the UE is determined by the transmit beamforming codebook of the jammer, which appears in the matrix $\mathbf{G}_{\rm J}$, and the second-order statistics of the channel between the jammer and the UE, i.e., the sparse vector $\boldsymbol{\xi}_{\rm J}$. The solution of (34) approximates $\boldsymbol{\xi}_{\rm B}$ with an error

$$\mathcal{E}(\widehat{\boldsymbol{\xi}}_{\rm B}) \triangleq \|\boldsymbol{\xi}_{\rm B} - \widehat{\boldsymbol{\xi}}_{\rm B}\|_2 \quad (37)$$

which depends not only on the jamming contribution $\mathbf{G}_{\rm J}\,\boldsymbol{\xi}_{\rm J}$, but also on the fact that $\boldsymbol{\xi}_{\rm B}$ is not exactly sparse, i.e., only a small number of its entries are nonzero, but $\boldsymbol{\xi}_{\rm B}$ is only close to a sparse vector. More precisely, a vector $\mathbf{s}_{\rm TX} \in \mathbb{R}^{M_{\rm TX} N_{\rm U}}$is called *$\kappa_{TX}$-sparse* [46, Def. 2.1] if at most $\kappa_{\rm TX}$ of its entries are nonzero, i.e., $|{\rm supp}(\mathbf{s}_{\rm TX})| \le \kappa_{\rm TX}$, for TX $\in \{{\rm B}, {\rm J}\}$. The *best κ_{TX}-term approximation* of $\boldsymbol{\xi}_{\rm TX}$ is defined as (see, e.g., [46, Def. 2.2])

$$\sigma_{\kappa_{\rm TX}}(\boldsymbol{\xi}_{\rm TX}) \triangleq \inf \Big\{ \|\boldsymbol{\xi}_{\rm TX} - \mathbf{s}_{\rm TX}\|_1, \text{where } \mathbf{s}_{\rm TX} \in \mathbb{R}^{M_{\rm TX} N_{\rm U}} \text{ is } \kappa_{\rm TX}\text{-sparse} \Big\}. \quad (38)$$

The infimum is achieved in (38) by a $\kappa_{\rm TX}$-sparse vector $\mathbf{s}_{\rm TX} \in \mathbb{C}^{M_{\rm TX} N_{\rm U}}$ whose nonzero entries equal the $\kappa_{\rm TX}$ largest absolute entries of $\boldsymbol{\xi}_{\rm TX}$. As regards to the transmit beamforming codebook of the jammer, we study the two different cases $\mathbf{G}_{\rm J} \neq \mathbf{G}_{\rm B}$ and $\mathbf{G}_{\rm J} = \mathbf{G}_{\rm B}$ separately.

1) $\mathbf{G}_J \neq \mathbf{G}_B$: In principle, the transmit beamforming codebooks of the BS and jammer may be different. For instance, the jamming codebook $\widetilde{\mathbf{u}}_{\rm J}^{(i)}(\widetilde{s})$ might be chosen in a pseudo-random manner similarly to the BS or, if the jammer is a high-power device that has a large amount of power to be spent, another option for the jammer could consist of probing the channel along *all* the possible directions (referred to as *omnidirectional beamforming*) and, consequently, setting $\widetilde{\mathbf{u}}_{\rm J}^{(i)}(\widetilde{s}) = \mathbf{1}_{\widetilde{M}}/\sqrt{\widetilde{M}}$. In the case of $\mathbf{G}_{\rm J} \neq \mathbf{G}_{\rm B}$, the jamming contribution $\mathbf{G}_{\rm J}\,\boldsymbol{\xi}_{\rm J}$ appears as additional noise of arbitrary nature and the reconstruction error (37) can be upper bounded [47] as follows

$$\mathcal{E}(\widehat{\boldsymbol{\xi}}_{\rm B}) \le \frac{A_1}{\sqrt{\kappa_{\rm B}}}\, \sigma_{\kappa_{\rm B}}(\boldsymbol{\xi}_{\rm B}) + A_2\, \|\mathbf{G}_{\rm J}\,\boldsymbol{\xi}_{\rm J}\|_2 \quad (39)$$

for some constants $A_1, A_2 > 0$, provided that the matrix $\mathbf{G}_{\rm B}$ satisfies the conditions summarized in the Appendix. By resorting to the sub-multiplicative property of the ℓ_2 norm [35], one has

$$\begin{aligned} \|\mathbf{G}_{\rm J}\,\boldsymbol{\xi}_{\rm J}\|_2 &\le \sqrt{{\rm trace}(\mathbf{G}_{\rm J}\,\mathbf{G}_{\rm J}^{\rm T})}\, \|\boldsymbol{\xi}_{\rm J}\|_2 \\ &= \frac{\mathcal{P}_{\rm J}}{U_{\rm J}\,V} \sqrt{\sum_{\substack{i \in \{1,2,\ldots,\widetilde{M}\} \\ j \in \{1,2,\ldots,\widetilde{N}_{\rm U}\} \\ \widetilde{s} \in \{0,1,\ldots,Q-1\}}} \left\| \mathbf{1}_{\mathcal{U}_{\rm J}^{(i)}(\widetilde{s})} \otimes \mathbf{1}_{\mathcal{V}^{(j)}(\widetilde{s})} \right\|_2^2} \\ &\quad \cdot \sqrt{\sum_{n=1}^{M_{\rm J} N_{\rm U}} \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\rm J}}\}_{n,n}^2} \\ &\le \frac{\mathcal{P}_{\rm J}}{U_{\rm J}\,V} \sqrt{\widetilde{M}\,\widetilde{N}_{\rm U}\,Q\,M_{\rm J}\,N_{\rm U}} \sqrt{\sum_{n=1}^{M_{\rm J} N_{\rm U}} \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\rm J}}\}_{n,n}^2} \end{aligned} \quad (40)$$

where we have also used (23) and (33), and remembered that $\mathbf{g}_{\rm J}^{(j,i)}(\widetilde{s}) = \sqrt{U_{\rm J}}\,\sqrt{V}\,\widetilde{\mathbf{g}}_{\rm J}^{(j,i)}(\widetilde{s})$. It is apparent from (40) that probing more directions simultaneously (i.e., increasing $U_{\rm J}$) has the detrimental effect from the jammer's viewpoint of spreading the total power over all such directions, thereby obtaining a worse power concentration in the angle domain.

2) $\mathbf{G}_J = \mathbf{G}_B$: The jammer might transmit by using the same beamforming codebook of the BS that we remember to be known to all UEs a priori, i.e., $\mathcal{U}_{\rm J}^{(i)}(\widetilde{s}) \equiv \mathcal{U}_{\rm B}^{(i)}(\widetilde{s})$, for any $i \in \{1, 2, \ldots, \widetilde{M}\}$ and $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$, which necessarily requires that $M_{\rm J} = M_{\rm B} \equiv M$. In this case, one has $\mathbf{G}_{\rm J} = \mathbf{G}_{\rm B} \equiv \mathbf{G}$ and, consequently, eq. (32) ends up to

$$\mathbf{p} = \mathbf{G}\,(\boldsymbol{\xi}_{\rm B} + \boldsymbol{\xi}_{\rm J}) + \sigma_w^2\, \mathbf{1}_{\widetilde{M}\widetilde{N}_{\rm U} Q} \quad (41)$$

which shows that the UE sees the sum of two sparse vectors $\boldsymbol{\xi}_{\rm B}$ and $\boldsymbol{\xi}_{\rm J}$ under the same measurement matrix $\mathbf{G}$. This case is worse than the previous one when $\mathbf{G}_{\rm J} \neq \mathbf{G}_{\rm B}$ since $\widehat{\boldsymbol{\xi}}_{\rm B}$ turns out to be an estimate of $\boldsymbol{\xi}_{\rm B} + \boldsymbol{\xi}_{\rm J}$. In this worst case, successful BA between the BS and the UE is achieved if

$$\frac{\mathcal{P}_{\rm B}}{\mathcal{P}_{\rm J}} \gg \frac{\max_{n \in \{1,2,\ldots,M N_{\rm U}\}} \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\rm J}}\}_{n,n}}{\max_{n \in \{1,2,\ldots,M N_{\rm U}\}} \{\mathbf{R}_{\widetilde{\mathbf{C}}_{\rm B}}\}_{n,n}}. \quad (42)$$

Condition (42) is violated when the jammer transmits with a power $\mathcal{P}_{\rm J}$ sufficiently greater than $\mathcal{P}_{\rm B}$ and/or, compared to the BS, it has a more favorable propagation towards the UE.

IV. The proposed anti-jamming beam alignment scheme

In this section, we modify the transmit scheme of the BS in order to allow the UE to cancel the jamming contribution. A key ingredient of our proposed anti-jamming scheme is the random probing symbols transmitted by the BS, which follow the model

$$d_{\rm B}^{(k_{i,\ell})}(s) = \sqrt{[1-\gamma_{\rm B}(s)]\,\mathcal{P}_{\rm B}}\; t^{(k_{i,\ell})}(s) + \sqrt{\gamma_{\rm B}(s)\,\mathcal{P}_{\rm B}}\; r_{\rm B}^{(k_{i,\ell})}(s) \quad (43)$$

where each stream $\{r_{\rm B}^{(k_{i,\ell})}(s)\}$ is modeled as a sequence of zero-mean unit-variance i.i.d. complex circular RVs, with $r_{\rm B}^{(k_{i,\ell})}(s)$ and (25) mutually independent and statistically independent of noise $\overline{w}^{(j,k_{i,\ell})}(s)$, for each OFDM block, and for any $i \in \{1, 2, \ldots, \widetilde{M}\}$ and $\forall j \in \{1, 2, \ldots, \widetilde{N}_{\rm U}\}$. The

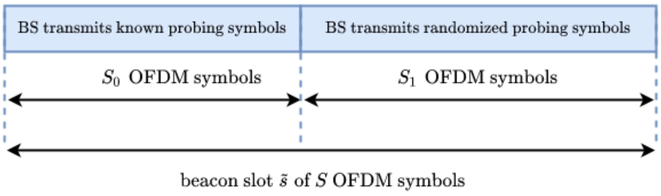

BS transmits known probing symbols
BS transmits randomized probing symbols
S_0 OFDM symbols
S_1 OFDM symbols
beacon slot $\tilde{s}$ of S OFDM symbols

Fig. 3. Each beacon slot is divided into two subslots: during the first S_0 OFDM symbols, the BS transmits a known probing sequence, whereas a random sequence is superimposed to the known symbols in the remaining S_1 OFDM blocks, with $S_0 + S_1 = S$.

BS allocates a different fraction $0 \le \gamma_{\text{B}}(s) \le 1$ of $\mathcal{P}_{\text{B}}$ to the random symbols $r_{\text{B}}^{(k_{i,\ell})}(s)$. Since $\{r_{\text{B}}^{(k_{i,\ell})}(s)\}$ is randomly generated at the BS, it is unknown at the UE. However, the UE knows that the BS has superimposed the random sequence $\{r_{\text{B}}^{(k_{i,\ell})}(s)\}$ on the known sequence $\{t^{(k_{i,\ell})}(s)\}$ and it can use such a knowledge to undo the jamming attack. The conventional probing scheme (24) can be obtained from (43) by setting $\gamma_{\text{B}}(s) = 0$, $\forall s \in \{0, 1, \ldots, W-1\}$.

In the sequel, we assume that $\gamma_{\text{B}}(s)$ does not vary from a beacon slot to another, but it might assume different values within a beacon slot, i.e, $\gamma_{\text{B}}(\widetilde{s}\, S + s') \equiv \gamma_{\text{B}}^{(s')}$, for any $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ and $s' \in \{0, 1, \ldots, S-1\}$. To counteract the detrimental effect of the jamming attack, we additionally propose to divide each beacon slot $\widetilde{s}$ in two subslots (see Fig. 3): in the former one, which lasts S_0 OFDM symbols, the BS transmits only the known symbols $t^{(k_{i,\ell},s')}$ defined in Section III, i.e., $\gamma_{\text{B}}^{(s')} = 0$, for $s' \in \{0, 1, \ldots, S_0 - 1\}$; whereas in the remaining $S_1 \triangleq S - S_0$ OFDM symbols of each beacon slot, the BS superimposes the random sequence $r_{\text{B}}^{(k_{i,\ell},s')}(\widetilde{s}) \triangleq r_{\text{B}}^{(k_{i,\ell})}(\widetilde{s}\, S + s')$ to the known symbols $t^{(k_{i,\ell},s')}$, with a fixed power fraction $\gamma_{\text{B}}^{(s')} \equiv \gamma_{\text{B}} \in (0, 1]$, for all $s' \in \{S_0, S_0 + 1, \ldots, S-1\}$.

By substituting (25) and (43) into (21), one has

$$\begin{aligned}\overline{y}^{(j,k_{i,\ell},s')}(\widetilde{s}) &= \widetilde{h}_{\text{B}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left\{ \sqrt{[1-\gamma_{\text{B}}^{(s')}]\,\mathcal{P}_{\text{B}}}\, t^{(k_{i,\ell},s')}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{B}}^{(s')}\,\mathcal{P}_{\text{B}}}\, r_{\text{B}}^{(k_{i,\ell},s')}(\widetilde{s}) \right\} \\ &\quad + \widetilde{h}_{\text{J}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left\{ \sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, t^{(k_{i,\ell},s')}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, r_{\text{J}}^{(k_{i,\ell},s')}(\widetilde{s}) \right\} + \overline{w}^{(j,k_{i,\ell},s')}(\widetilde{s}) \end{aligned} \tag{44}$$

where $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ and $s' \in \{0, 1, \ldots, S-1\}$, with $\widetilde{h}_{\text{TX}}^{(j,i,k_{i,\ell})}(\widetilde{s})$, and $r_{\text{J}}^{(k_{i,\ell},s')}(\widetilde{s})$ defined in Section III. According to the proposed protocol, the data block (27) received by the UE during the beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$ can be partitioned as

$$\overline{\mathbf{y}}^{(j,k_{i,\ell})}(\widetilde{s}) = \begin{bmatrix} \overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s}) \\ \overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s})] \end{bmatrix}, \quad \text{with } \overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_0} \text{ and } \overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_1} \tag{45}$$

for $j \in \{1, 2, \ldots, \widetilde{N}_{\text{U}}\}$, $i \in \{1, 2, \ldots, \widetilde{M}\}$, and beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$, with

$$\begin{aligned}\overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s}) &= \sqrt{\mathcal{P}_{\text{B}}}\, \widetilde{h}_{\text{B}}^{(j,i,k_{i,\ell})}(\widetilde{s})\, \mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s}) \\ &\quad + \widetilde{h}_{\text{J}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left\{ \sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, \mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, \mathbf{r}_{0,\text{J}}^{(k_{i,\ell})}(\widetilde{s}) \right\} + \overline{\mathbf{w}}_0^{(j,k_{i,\ell})}(\widetilde{s}) \end{aligned} \tag{46}$$

$$\begin{aligned}\overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s}) &= \widetilde{h}_{\text{B}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left\{ \sqrt{(1-\gamma_{\text{B}})\,\mathcal{P}_{\text{B}}}\, \mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{B}}\,\mathcal{P}_{\text{B}}}\, \mathbf{r}_{1,\text{B}}^{(k_{i,\ell})}(\widetilde{s}) \right\} + \widetilde{h}_{\text{J}}^{(j,i,k_{i,\ell})}(\widetilde{s}) \left\{ \sqrt{(1-\gamma_{\text{J}})\,\mathcal{P}_{\text{J}}}\, \mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s}) \right. \\ &\quad \left. + \sqrt{\gamma_{\text{J}}\,\mathcal{P}_{\text{J}}}\, \mathbf{r}_{1,\text{J}}^{(k_{i,\ell})}(\widetilde{s}) \right\} + \overline{\mathbf{w}}_1^{(j,k_{i,\ell})}(\widetilde{s}) \end{aligned} \tag{47}$$

where $\mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_0}$, $\mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_1}$, $\mathbf{r}_{0,\text{J}}^{(k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_0}$, $\mathbf{r}_{1,\text{J}}^{(k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_1}$, $\overline{\mathbf{w}}_0^{(j,k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_0}$, $\overline{\mathbf{w}}_1^{(j,k_{i,\ell})}(\widetilde{s}) \in \mathbb{C}^{S_1}$ are obtained by partitioning $\mathbf{t}^{(k_{i,\ell})}(\widetilde{s})$, $\mathbf{r}_{\text{J}}^{(k_{i,\ell})}(\widetilde{s})$, and $\overline{\mathbf{w}}^{(j,k_{i,\ell})}(\widetilde{s})$, respectively, in accordance with (45), and, moreover,

$$\begin{aligned}\mathbf{r}_{1,\text{B}}^{(k_{i,\ell})}(\widetilde{s}) \triangleq [r_{\text{B}}^{(k_{i,\ell},S_0)}(\widetilde{s}), r_{\text{B}}^{(k_{i,\ell},S_0+1)}(\widetilde{s}), \\ \ldots, r_{\text{B}}^{(k_{i,\ell},S-1)}(\widetilde{s})]^{\text{T}} \in \mathbb{C}^{S_1} \,. \end{aligned} \tag{48}$$

Starting from (46)-(47), accordingly to the modified transmit protocol of the BS depicted in Fig. 3, we additionally propose to modify the BA procedure implemented by the UE. In our proposal, the UE performs BA in three steps. In the first step, for any beacon slot, the received blocks $\overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s})$ and $\overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s})$ are projected onto the subspace that is orthogonal to the subspace generated by the corresponding known probing symbols. In the second step, the power of the jammer-plus-noise contribution is estimated in each beacon slot by processing the projected version of $\overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s})$. In the last step, the BA procedure is finalized by using the projected version of $\overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s})$, for each beacon slot, thus developing a "cleaned" NNLS optimization problem that is obtained by canceling out the previously estimated jammer-plus-noise power contribution.

A. Step 1: Subspace projections

Both the power estimation of the jammer-plus-noise contribution obtained from $\overline{\mathbf{y}}_0^{(j,k_{i,\ell})}(\widetilde{s})$ and the BA algorithm applied on $\overline{\mathbf{y}}_1^{(j,k_{i,\ell})}(\widetilde{s})$ are performed in the subspace that is orthogonal to the one-dimensional subspace generated by the known vectors $\mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s})$ and $\mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s})$, respectively. Specifically, for $\kappa \in \{0, 1\}$, let $\mathbf{P}^{\perp}_{\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})} \in \mathbb{C}^{S_\kappa \times S_\kappa}$ denote the orthogonal projector onto the subspace complementary to that spanned by $\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})$, it results that

$$\mathbf{P}^{\perp}_{\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})} = \mathbf{I}_{S_\kappa} - \frac{1}{S_\kappa}\, \mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})\, [\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})]^{\text{H}} \tag{49}$$

where we have used the fact that $\|\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})\|_2^2 = S_\kappa$. By construction the matrix $\mathbf{P}^{\perp}_{\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})}$ has rank equal to $S_\kappa - 1$. Therefore, the economy-size eigenvalue decomposition (EVD) of $\mathbf{P}^{\perp}_{\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})}$ is given by $\mathbf{P}^{\perp}_{\mathbf{t}_\kappa^{(k_{i,\ell})}(\widetilde{s})} = \mathbf{U}_\kappa^{(k_{i,\ell})}(\widetilde{s})\, \mathbf{\Sigma}_\kappa^{(k_{i,\ell})}(\widetilde{s})\, [\mathbf{U}_\kappa^{(k_{i,\ell})}(\widetilde{s})]^{\text{H}}$, where

$\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s}) \in \mathbb{C}^{S_\kappa\times(S_\kappa-1)}$ represents the semi-unitary eigenvector matrix, obeying $[\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s}) = \mathbf{I}_{S_\kappa-1}$, whereas the diagonal matrix $\boldsymbol{\Sigma}_\kappa^{(k_i,\ell)}(\widetilde{s}) \in \mathbb{R}^{(S_\kappa-1)\times(S_\kappa-1)}$ contains the nonzero eigenvalues of $\mathbf{P}^\perp_{\mathbf{t}_\kappa^{(k_i,\ell)}(\widetilde{s})}$.

The part of the BS and jamming contribution associated with the transmission of the known probing symbols can be canceled out by applying the linear operator $[\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s})]^{\rm H}$ on $\overline{\mathbf{y}}_\kappa^{(j,k_i,\ell)}(\widetilde{s})$ given by (46)-(47), for $\kappa \in \{0,1\}$, thus yielding

$$\begin{aligned}\overline{\mathbf{y}}_{0,\perp}^{(j,k_i,\ell)}(\widetilde{s}) &\triangleq [\mathbf{U}_0^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\overline{\mathbf{y}}_0^{(j,k_i,\ell)}(\widetilde{s}) \\ &= \sqrt{\gamma_{\rm J}\,\mathcal{P}_{\rm J}}\,\widetilde{h}_{\rm J}^{(j,i,k_i,\ell)}(\widetilde{s})\,[\mathbf{U}_0^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{r}_{0,{\rm J}}^{(k_i,\ell)}(\widetilde{s}) \\ &\quad + [\mathbf{U}_0^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\overline{\mathbf{w}}_0^{(j,k_i,\ell)}(\widetilde{s}) \qquad (50)\\ \overline{\mathbf{y}}_{1,\perp}^{(j,k_i,\ell)}(\widetilde{s}) &\triangleq [\mathbf{U}_1^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\overline{\mathbf{y}}_1^{(j,k_i,\ell)}(\widetilde{s}) \\ &= \sqrt{\gamma_{\rm B}\,\mathcal{P}_{\rm B}}\,\widetilde{h}_{\rm B}^{(j,i,k_i,\ell)}(\widetilde{s})\,[\mathbf{U}_1^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{r}_{1,{\rm B}}^{(k_i,\ell)}(\widetilde{s}) \\ &\quad + \sqrt{\gamma_{\rm J}\,\mathcal{P}_{\rm J}}\,\widetilde{h}_{\rm J}^{(j,i,k_i,\ell)}(\widetilde{s})\,[\mathbf{U}_1^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{r}_{1,{\rm J}}^{(k_i,\ell)}(\widetilde{s}) \\ &\quad + [\mathbf{U}_1^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\overline{\mathbf{w}}_1^{(j,k_i,\ell)}(\widetilde{s}) \qquad (51)\end{aligned}$$

for $j \in \{1,2,\ldots,\widetilde{N}_{\rm U}\}$, $i \in \{1,2,\ldots,\widetilde{M}\}$, and beacon slot $\widetilde{s} \in \{0,1,\ldots,Q-1\}$.

The projected vector $\overline{\mathbf{y}}_{0,\perp}^{(j,k_i,\ell)}(\widetilde{s})$ - from which the BS contribution has been removed - is used in Step 2 to estimate the jammer-plus-noise power, whereas the projected vector $\overline{\mathbf{y}}_{1,\perp}^{(j,k_i,\ell)}(\widetilde{s})$ is the input of the BA procedure in Step 3.

B. Step 2: Estimation of the jammer-plus-noise contribution

Having removed the BS contribution from the received data in the first part of each beacon slot, it is now possible to estimate from (50) the power of the jammer-plus-noise term at the output of the j-th RF chain of the UE due to the signal transmitted by i-th RF chain of the jammer in the $\widetilde{s}$-th beacon slot through the estimator

$$P_{0,\perp}^{(j,i)}(\widetilde{s}) = \frac{1}{(S_0-1)\,F_i}\sum_{\ell=0}^{F_i-1}\mathbb{E}\left[\left\|\overline{\mathbf{y}}_{0,\perp}^{(j,k_i,\ell)}(\widetilde{s})\right\|_2^2\right] \qquad (52)$$

for $j \in \{1,2,\ldots,\widetilde{N}_{\rm U}\}$, $i \in \{1,2,\ldots,\widetilde{M}\}$, and beacon slot $\widetilde{s} \in \{0,1,\ldots,Q-1\}$, where the expectation is also evaluated with respect to the random probing symbols transmitted by the jammer. Under our assumptions (52) can be explicated as

$$P_{0,\perp}^{(j,i)}(\widetilde{s}) = \gamma_{\rm J}\,[\mathbf{g}_{\rm J}^{(j,i)}(\widetilde{s})]^{\rm T}\,\boldsymbol{\xi}_{\rm J} + \sigma_w^2 \qquad (53)$$

where we have used (30) and the facts that

$$\begin{aligned}\mathbb{E}\left[\|[\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{r}_{\kappa,{\rm J}}^{(k_i,\ell)}(\widetilde{s})\|_2^2\right] &= (S_\kappa-1)\\ \mathbb{E}\left[\|[\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\overline{\mathbf{w}}_\kappa^{(j,k_i,\ell)}(\widetilde{s})\|_2^2\right] &= (S_\kappa-1)\,\sigma_w^2\end{aligned}$$

for $\kappa \in \{0,1\}$, due to the semi-unitary property of $\mathbf{U}_\kappa^{(k_i,\ell)}(\widetilde{s})$. The $P_{0,\perp}^{(j,i)}(\widetilde{s})$ also includes the noise variance σ_w^2, whose knowledge is thereby not required for beam determination. In practice, the power level $P_{0,\perp}^{(j,i)}(\widetilde{s})$ can be directly estimated from data as

$$\widehat{P}_{0,\perp}^{(j,i)}(\widetilde{s}) = \frac{1}{(S_0-1)\,F_i}\sum_{\ell=0}^{F_i-1}\left\|\overline{\mathbf{y}}_{0,\perp}^{(j,k_i,\ell)}(\widetilde{s})\right\|_2^2 . \qquad (54)$$

The obtained power estimates (54) are used in Step 3 to achieve the BA between the BS and the UE in an optimization process that is (nearly) free from the jammer-plus-noise contribution.

C. Step 3: BA with jammer-plus-noise cancellation

The BA process is based on (51) and exploits the power estimations provided in the previous step. Similarly to (28), the NNLS optimization process relies on the power measurements

$$\begin{aligned}P_{1,\perp}^{(j,i)}(\widetilde{s}) &= \frac{1}{(S_1-1)\,F_i}\sum_{\ell=0}^{F_i-1}\mathbb{E}\left[\left\|\overline{\mathbf{y}}_{1,\perp}^{(j,k_i,\ell)}(\widetilde{s})\right\|_2^2\right]\\ &= \gamma_{\rm B}\,[\mathbf{g}_{\rm B}^{(j,i)}(\widetilde{s})]^{\rm T}\,\boldsymbol{\xi}_{\rm B} + \mathcal{P}_{0,\perp}^{(j,i)}(\widetilde{s}) \qquad (55)\end{aligned}$$

for $j \in \{1,2,\ldots,\widetilde{N}_{\rm U}\}$, $i \in \{1,2,\ldots,\widetilde{M}\}$, and beacon slot $\widetilde{s} \in \{0,1,\ldots,Q-1\}$, where the expectation is also evaluated with respect to the random probing symbols transmitted by both the BS and the jammer, and the equality follows from arguments similar to those invoked in Sections III and IV-B, with the additional observation that $\mathbb{E}\left[\|[\mathbf{U}_1^{(k_i,\ell)}(\widetilde{s})]^{\rm H}\,\mathbf{r}_{1,{\rm B}}^{(k_i,\ell)}(\widetilde{s})\|_2^2\right] = (S_1-1)$ and $P_{0,\perp}^{(j,i)}(\widetilde{s})$ is given by (53). By defining

$$\begin{aligned}\mathbf{p}_\kappa^\perp \triangleq [&P_{\kappa,\perp}^{(1,1)}(0),\ldots,P_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(0),\\ &P_{\kappa,\perp}^{(1,1)}(1),\ldots,P_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(1),\ldots,\\ &P_{\kappa,\perp}^{(1,1)}(Q-1),\ldots,P_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(Q-1)]^{\rm T} \qquad (56)\end{aligned}$$

for $\kappa \in \{0,1\}$, one gets the vector model

$$\mathbf{p}_1^\perp = \mathbf{G}_{\rm B}\,\boldsymbol{\xi}_{\rm B}^\perp + \underbrace{\mathbf{G}_{\rm J}\,\boldsymbol{\xi}_{\rm J}^\perp + \sigma_w^2\,\mathbf{1}_{\widetilde{M}\widetilde{N}_{\rm U}Q}}_{\mathbf{p}_0^\perp} = \mathbf{G}_{\rm B}\,\boldsymbol{\xi}_{\rm B}^\perp + \mathbf{p}_0^\perp \qquad (57)$$

with $\boldsymbol{\xi}_{\rm TX}^\perp \triangleq \gamma_{\rm TX}\,\boldsymbol{\xi}_{\rm TX} \in \mathbb{R}^{M_{\rm TX}N_{\rm U}}$, where $\boldsymbol{\xi}_{\rm TX}$ and $\mathbf{G}_{\rm TX}$ are defined by (31) and (33), respectively. In the proposed anti-jamming BA procedure, the sparse vector $\boldsymbol{\xi}_{\rm B}^\perp$ can be reconstructed from the measurements of the form (57) via the *modified* NNLS optimization problem:

$$\widehat{\boldsymbol{\xi}}_{\rm B}^\perp = \arg\min_{\boldsymbol{\xi}_{\rm B}^\star\in\mathbb{R}^{M_{\rm B}N_{\rm U}}}\left\|\mathbf{p}_1^\perp - \mathbf{G}_{\rm B}\,\boldsymbol{\xi}_{\rm B}^\star - \mathbf{p}_0^\perp\right\|_2^2 , \qquad \text{subject to } \boldsymbol{\xi}_{\rm B}^\star \geq \mathbf{0}_{M_{\rm B}N_{\rm U}} \qquad (58)$$

for which the algorithm of Lawson and Hanson is particularly well adapted [45]. Strictly speaking, the effect of the jamming attack is counteracted by subtracting the contribution of the jammer-plus-noise from the received power. Practical implementation of the proposed NNLS problem mandates the replacement of $\mathbf{p}_\kappa^\perp$ in (58) with

$$\begin{aligned}\widehat{\mathbf{p}}_\kappa^\perp \triangleq [&\widehat{P}_{\kappa,\perp}^{(1,1)}(0),\ldots,\widehat{P}_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(0),\\ &\widehat{P}_{\kappa,\perp}^{(1,1)}(1),\ldots,\widehat{P}_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(1),\ldots,\\ &\widehat{P}_{\kappa,\perp}^{(1,1)}(Q-1),\ldots,\widehat{P}_{\kappa,\perp}^{(\widetilde{N}_{\rm U},\widetilde{M})}(Q-1)]^{\rm T} \qquad (59)\end{aligned}$$

for $\kappa \in \{0,1\}$, where $\widehat{P}_{0,\perp}^{(j,i)}(\widetilde{s})$ has been defined in (54) and

$$\widehat{P}_{1,\perp}^{(j,i)}(\widetilde{s}) = \frac{1}{(S_1-1)\,F_i}\sum_{\ell=0}^{F_i-1}\left\|\overline{\mathbf{y}}_{1,\perp}^{(j,k_i,\ell)}(\widetilde{s})\right\|_2^2 \qquad (60)$$

for $j \in \{1, 2, \ldots, \widetilde{N}_{\rm U}\}$, $i \in \{1, 2, \ldots, \widetilde{M}\}$, and beacon slot $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$.

D. Remarks

Some remarks are now in order regarding the proposed anti-jamming BA approach.

Remark 1: Our general framework allows us to consider different jamming attacks. If the jammer transmits only known probing symbols, i.e., $\gamma_{\rm J} = 0$ in (25), its contribution disappears from the projected data $\overline{\mathbf{y}}_{0,\perp}^{(j,k_{i,\ell})}(\widetilde{s})$ and $\overline{\mathbf{y}}_{1,\perp}^{(j,k_{i,\ell})}(\widetilde{s})$, since the projections are performed onto the subspaces that are orthogonal to those spanned by the known probing vectors $\mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s})$ and $\mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s})$, for $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$. In this type of attack, the procedure in Step 2 provides estimation of the noise variance σ_w^2 only and the BA algorithm in Step 3 operates in a jammer-free scenario. On the other hand, when the jammer adds noise to the known probing symbols, i.e., $0 < \gamma_{\rm J} \leq 1$ in (25), the jammer also transmits into the subspace complementary to those generated by $\mathbf{t}_0^{(k_{i,\ell})}(\widetilde{s})$ and $\mathbf{t}_1^{(k_{i,\ell})}(\widetilde{s})$. In such an adversarial attack, the jammer-plus-noise power is estimated in Step 2 and, then, it is subtracted in Step 3. The impact of $\gamma_{\rm J}$ on the performance of the proposed anti-jamming BA scheme is studied in Section V (see Tab. II).

Remark 2: A distinguished feature of our BA technique is that neither a preventive detection of the jamming attack nor knowledge of the type of attack is required. Indeed, the proposed BA procedure successfully works even in the absence of the jammer. Such a case is akin to the previously discussed one when the jammer transmits known probing symbols only.

Remark 3: In the proposed BA procedure, the power transmitted by the BS in the subspace spanned by the known probing symbols is not used in Step 2 (see also Fig. 3), thus implying a possible waste of energy. One can argue that, in principle, the BS could not transmit in the first S_0 OFDM symbols of each beacon slot by powering-down its power amplifier(s). So doing, estimation of the jammer-plus-noise power in Step 2 could be obtained without performing the subspace projection at the UE. However, this option may not be feasible in practice for two basic reasons. First, current 3GPP specifications mandates the use of a continuous transmission during the beam-sweeping phase [6]. Second, the BS can enter a sleep mode with zero time delay; vice versa, going back from a sleep mode to the active transmission mode requires a certain delay and a certain amount of energy, which both depend on the sleep level. If the sleep level is arbitrarily close to zero, a somewhat reduced power saving may achieved and, moreover, the activation process of the BS might require an acceptable wake up time [48].

Remark 4: Similarly to Step 2, the known part of the probing signal transmitted by the BS is not exploited for beam determination in Step 3. Henceforth, one might set $\gamma_{\rm B} = 1$ in (47) in order not to squander energy at the BS: in this case, the BS transmits only random probing variables during the last S_1 OFDM symbols of each beacon slot (see again Fig. 3). However, the optimal choice of $\gamma_{\rm B}$ might also be dictated by other practical constraints, such as hardware complexity and impairments [49], as well as compliance with applicable standards, codes, and regulations. It is numerically shown in Section V (see Tab. III) that values of $\gamma_{\rm B}$ slightly smaller than one do not significantly affect the performance of the proposed anti-jamming BA scheme.

V. Numerical results

In this section, we provide numerical results aimed at evaluating the performance of the proposed jamming-resistant beam alignment technique. We consider an OFDM system, employing $F = 2048$ subcarriers and cyclic prefix of length $L_{\rm cp} = 128$. The system operates with carrier frequency $f_0 = 70$ GHz and bandwidth $1/T_{\rm c} = 1$ GHz. We assume that both the BS and jammer have $M_{\rm B} = M_{\rm J} = 32$ antennas and $\widetilde{M} = 3$ RF chains, and the UE has $N_{\rm U} = 32$ antennas and $\widetilde{N}_{\rm U} = 2$ RF chains. The number of subcarriers assigned to each probing stream is constant, i.e., $F_i = 3$, $\forall i \in \{1, 2, \ldots, \widetilde{M}\}$. The beacon slot contains $S = 28$ OFDM symbols. The number of paths of the BS-to-UE and jammer-to-UE links are fixed to $L_{\rm B} = L_J = 2$. The channel gains $\rho_{\rm TX}(\ell)$, for $\ell \in \{1, 2\}$ and TX $\in \{{\rm B}, {\rm J}\}$, are generated as circularly-symmetric statistically independent complex Gaussian RVs, with variance $\sigma^2(\ell)$ independent of TX, for $\ell \in \{1, 2\}$, and $\sigma^2(1) = 1$ and $\sigma^2(2)$ 3dB less. The delays $\tau_{\rm TX}(\ell)$ are randomly generated according to the one-sided exponentially decreasing delay power spectrum, i.e., $\tau_{\rm TX}(\ell) = -\tau_{\rm slope} \ln[1 - u_\ell(1 - e^{-\Delta_\ell/\tau_{\rm slope}})]$, where the maximum delay $\Delta_{\rm B} = \Delta_{\rm J} = 3$ and slop-time $\tau_{\rm slope} = 2$ (normalized to the sampling period), and u_k are independent RVs uniformly distributed in the interval $(0, 1)$. The AoAs and AoDs of both the BS and jammer are generated as independent RVs uniformly distributed into $(-\pi/2, \pi/2)$. The beamforming codebooks of the BS and UE are chosen in a pseudo-random manner as explained in Subsection II-F, with cardinality $U_{\rm B} = 4$ and $V = 4$, respectively. The signal-to-jamming ratio (SJR) is defined as SJR $\triangleq \mathcal{P}_{\rm B}/\mathcal{P}_{\rm J}$. Unless otherwise specified, the number of beacon slots is $Q = 100$ and we set $\gamma_{\rm B} = 1$ (i.e., the BS transmits only random probing variables during the last S_1 symbols of each beacon slot), $\gamma_{\rm J} = 1$ (i.e., the jammer transmits noise only), and $S_0 = S_1 = 14$ (i.e., each beacon slot is divided in two equal parts), and SJR $= -5$ dB.

In all the subsequent experiments, we consider three different cases regarding the choice of the transmit beamforming codebook of the jammer:

Case 1: For $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$, the jamming codebook $\widetilde{\mathbf{u}}_{\rm J}^{(i)}(\widetilde{s})$ is chosen in a pseudo-random manner, independently of the the BS and UE codebooks, with $U_{\rm J} = U_{\rm B} = V = 4$.

Case 2: The jammer carries out omnidirectional beamforming by probing the channel along all the possible directions, i.e., $\widetilde{\mathbf{u}}_{\rm J}^{(i)}(\widetilde{s}) = \mathbf{1}_{\widetilde{M}}/\sqrt{\widetilde{M}}$.

Case 3: For any $i \in \{1, 2, \ldots, \widetilde{M}\}$ and $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$, the jammer transmits by using the same beamforming codebook of the BS, i.e., $\mathcal{U}_{\rm J}^{(i)}(\widetilde{s}) \equiv \mathcal{U}_{\rm B}^{(i)}(\widetilde{s})$.

					γ_{J}			
$\mathrm{P_{BA}}$	0.0	0.1	0.2	0.3	0.4	0.5	0.6	
Case 1	0.889	0.886	0.885	0.885	0.885	0.884	0.881	0
Case 2	0.890	0.887	0.884	0.884	0.884	0.883	0.879	0
Case 3	0.890	0.885	0.883	0.881	0.879	0.879	0.873	0

TABLE II
P_{BA} VERSUS γ_{J} ($\gamma_{\mathrm{B}} = 1$, $Q = 100$, AND $\mathrm{SJR} = -5\,\mathrm{dB}$).

					γ_{B}			
$\mathrm{P_{BA}}$	0.1	0.2	0.3	0.4	0.5	0.6	0.7	
Case 1	0.801	0.840	0.856	0.863	0.869	0.878	0.882	0
Case 2	0.789	0.829	0.854	0.868	0.872	0.877	0.879	0
Case 3	0.758	0.807	0.826	0.839	0.852	0.859	0.865	0

TABLE III
P_{BA} VERSUS γ_{B} ($\gamma_{\mathrm{J}} = 1$, $Q = 100$, AND $\mathrm{SJR} = -5\,\mathrm{dB}$).

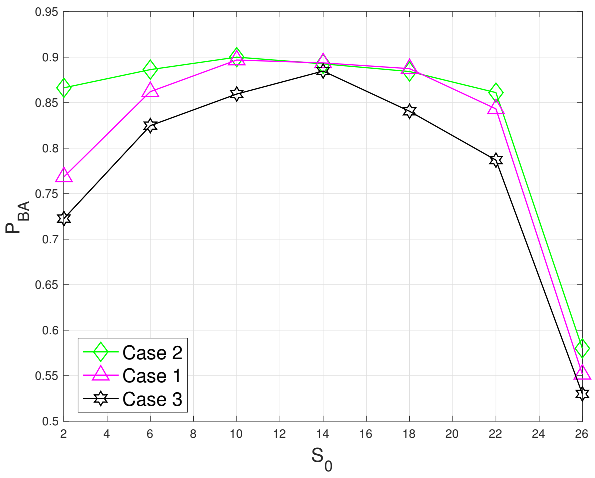


Fig. 4. P_{BA} versus S_0 ($\gamma_{\mathrm{B}} = \gamma_{\mathrm{J}} = 1$, $Q = 100$, and $\mathrm{SJR} = -5$ dB).

We implement the jammer-unaware BA strategy based on (34) and the proposed anti-jamming BA procedure based on (58). As an ideal reference, we also report the performance of NNLS BA in the absence of the jamming attack by assuming perfect knowledge of the noise power σ_w^2, which is referred to as "w/o jamming". As a performance metric, we evaluate the *probability P_{BA} of successful BA*, which is defined as the probability that the index of the largest component of $\widehat{\boldsymbol{\xi}}_{\mathrm{B}}$ [resp. $\widehat{\boldsymbol{\xi}}_{\mathrm{B}}^{\perp}$] coincides with the index of the actual largest entry of $\boldsymbol{\xi}_{\mathrm{B}}$ [resp. $\boldsymbol{\xi}_{\mathrm{B}}^{\perp}$]. In each Monte Carlo run, a new set of random probing symbols, random codebooks, noise, and channel parameters is randomly generated. The number of Monte Carlo runs is 1000 in all the experiments.

A. Probability of successful BA versus γ_J and γ_B

Tabs. II and III report the BA performance of the proposed procedure as a function of γ_{J} and γ_{B}, respectively. The proposed anti-jamming BA scheme is slightly influenced by the way in which the jammer splits its available power between known probing symbols and intentional noise. We remember that, when $\gamma_{\mathrm{J}} = 0$, i.e., the jammer transmits only known probing symbols, the jamming contribution is completely rejected via orthogonal projection. Therefore, the fact that the performance does not appreciably vary for $\gamma_{\mathrm{J}} > 0$ indirectly corroborates the satisfactory jamming rejection capabilities of the proposed modified NNLS optimization problem. On the other hand, as expected, the optimal value of γ_{B} is equal to one. However, values of γ_{B} slightly smaller than one lead to a negligible performance degradation.

B. Probability of successful BA versus S_0

The performance of the proposed anti-jamming BA scheme as a function of S_0 is reported in Fig. 4. We remember that $S_1 = 28 - S_0$ in our simulation setting. Results show that there is a significant performance degradation for $S_0 < 10$ and $S_0 > 18$. The value of S_0 impacts on the estimation accuracy of the jammner-plus-noise power (see Step 2). Values too small of S_0 lead to an unreliable estimate $\widehat{P}_{0,\perp}^{(j,i)}(\widetilde{s})$ of $P_{0,\perp}^{(j,i)}(\widetilde{s})$ [see eqs. (52) and (54)] and, thus, involve an inaccurate jamming-plus-noise cancellation in the proposed NNLS optimization problem (58). On the other hand, the value of S_1 represents the number of OFDM symbols (per each beacon slot and per each subcarrier) collected in Step 3 for building the estimates $\widehat{P}_{1,\perp}^{(j,i)}(\widetilde{s})$ in (60) to be used in (58). Values too large of S_0 implies values too small of S_1, hence providing poor NNLS performance.

C. Probability of successful BA versus number of beacon slots Q and SJR

We report in Figs. 5, 6, and 7 the BA performance as a function of the number of beacon slots Q. Additionally, Figs. 8, 9, and 10 depict the probability of successful BA as a function of the SJR. It is seen that, as predicted by our analysis, the performance of the jammer-unaware strategy (see Section III) is very poor when the jamming power is equal to or greater than the legitimate signal power, and successful BA is ensured only when SJR > 5 dB. Moreover, the adverse impact of the jamming attack is less burdensome in the case of omnidirectional jamming codebook, since each beam pattern of the jammer probes simultaneously all the directions, thereby spreading the total power in the spatial domain. Remarkably, the proposed anti-jamming strategy allows to achieve performance that is very close to that of the ideal case when there is no jamming attack, thus demonstrating that almost perfect jammer cancellation is obtained through the proposed three-step procedure developed in Section IV. Finally, it is apparent that, when the jammer transmits by using the same beamforming codebook of the BS (Case 3), the jamming-unaware BA approach is vulnerable to the jamming attack even when the SJR is as high as 5 dB. On the other hand, the proposed solution is completely robust with respect to the choice of the jamming codebook by being able to successfully reject the jamming contribution also in the worst Case 3.

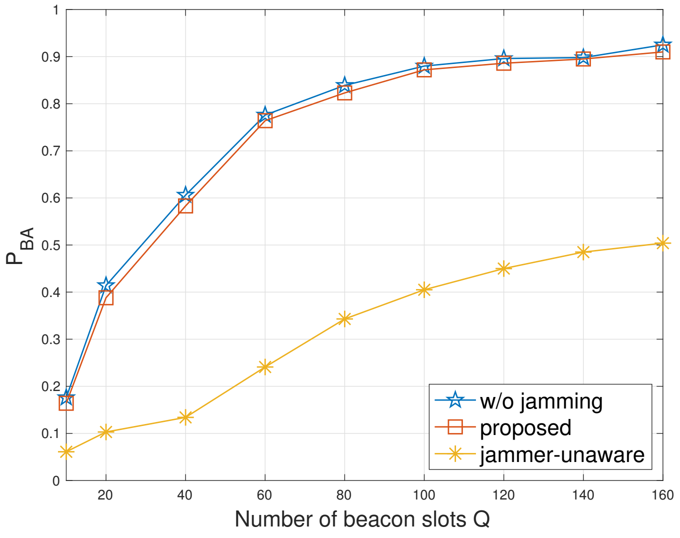


Fig. 5. P_{BA} versus number of beacon slots Q (Case 1, $\gamma_{\mathrm{B}} = \gamma_{\mathrm{J}} = 1$, and SJR $= -5$ dB).

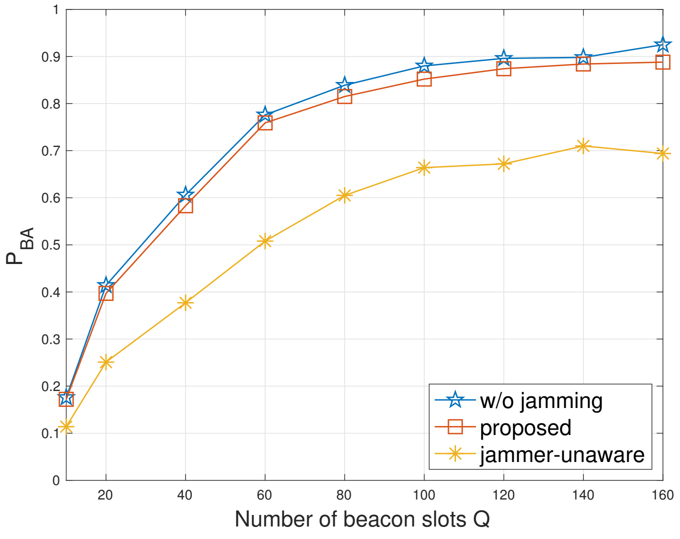


Fig. 6. P_{BA} versus number of beacon slots Q (Case 2, $\gamma_{\mathrm{B}} = \gamma_{\mathrm{J}} = 1$, and SJR $= -5$ dB).

VI. Conclusions and Directions for Future Work

We studied the problem of launching a jamming attack during the BA phase between the BS and users that wish to access the 5G MMW network. The considered jammer is smart in the sense that it is able to exploit the same spatial time-frequency resources that are publicly known to be used by the BS. In this case, a jamming-unaware approach is not able to ensure successful BA between the BS and the legitimate user. We proposed a novel BA procedure based on randomized probing and jammer cancellation, which guarantees performance very close to that achieved in the absence of a jamming attack.

An interesting research subject consists of considering a smart jammer that is able to modify the attack pattern according to the transmission features of the targeted communication links. For instance, the jammer might acquire information regarding the partition of each beacon slot and it may exploits such a knowledge to degrade the power estimation process in

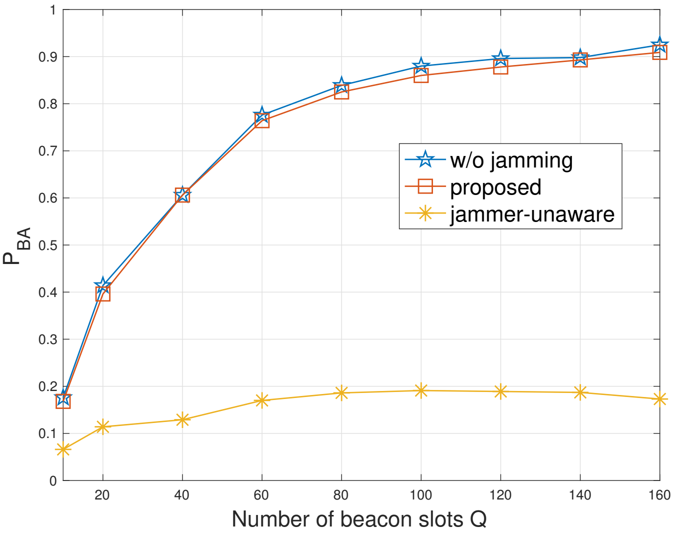


Fig. 7. P_{BA} versus number of beacon slots Q (Case 3, $\gamma_{\mathrm{B}} = \gamma_{\mathrm{J}} = 1$, and SJR $= -5$ dB).

Step 2. In this case, robust solutions have to be developed that allow to adaptively reconfigure beacon partition and/or to use more advanced interference cancellation techniques, e.g., independent component analysis.

Appendix

Several conditions on $\mathbf{G}_{\mathrm{B}}$ are known to ensure that the sparse vector $\boldsymbol{\xi}_{\mathrm{B}}$ can be estimated from the measurement vector $\mathbf{p}$. In general, the NNLS problem (34) can be ill-posed if the condition

$$\exists \boldsymbol{\alpha} \in \mathbb{R}^{\widetilde{M}\widetilde{N}_{\mathrm{U}}Q} \text{ such that } \mathbf{G}_{\mathrm{B}}^{\mathrm{T}}\boldsymbol{\alpha} > \mathbf{0}_{M_{\mathrm{B}}N_{\mathrm{U}}} \tag{61}$$

does not hold (see, e.g., [44]). Condition (61) requires the columns of $\mathbf{G}_{\mathrm{B}}$ be contained in the interior of a half-space containing the origin. Such a condition is fulfilled by the transmit beamforming codebook (23).

Let $\boldsymbol{\beta} \in \mathbb{R}^{M_{\mathrm{B}}N_{\mathrm{U}}}$ and $\mathcal{N} \subset \{1, 2, \ldots, M_{\mathrm{B}}N_{\mathrm{U}}\}$ be a subset. We denote with $\boldsymbol{\beta}_{\mathcal{N}} \in \mathbb{R}^{M_{\mathrm{B}}N_{\mathrm{U}}}$ the restriction of $\boldsymbol{\beta}$ to $\mathcal{N}$, i.e., $\{\boldsymbol{\beta}_{\mathcal{N}}\}_n = \{\boldsymbol{\beta}\}_n$ for $n \in \mathcal{N}$ and $\{\boldsymbol{\beta}_{\mathcal{N}}\}_n = 0$ otherwise. The matrix $\mathbf{G}_{\mathrm{B}}$ is said [46, Def. 4.21] to satisfy the ℓ_2-*robust nullspace property of order* κ_B with parameters $\rho \in (0, 1)$ and $\varsigma > 0$ if

$$\|\boldsymbol{\beta}_{\mathcal{N}}\|_2 \le \frac{\rho}{\sqrt{\kappa_{\mathrm{B}}}}\,\|\boldsymbol{\beta}_{\overline{\mathcal{N}}}\|_1 + \varsigma\,\|\mathbf{G}_{\mathrm{B}}\,\boldsymbol{\beta}\|_2 \quad \forall \boldsymbol{\beta} \in \mathbb{R}^{M_{\mathrm{B}}N_{\mathrm{U}}} \tag{62}$$

for any subset $\mathcal{N} \subset \{1, 2, \ldots, M_{\mathrm{B}}N_{\mathrm{U}}\}$ with $|\mathcal{N}| \le \kappa_{\mathrm{B}}$, where $\overline{\mathcal{N}}$ is the complement of $\mathcal{N}$ in $\{1, 2, \ldots, M_{\mathrm{B}}N_{\mathrm{U}}\}$. Property (62) implies that no κ_{B}-sparse vectors lie in the nullspace of $\mathbf{G}_{\mathrm{B}}$. It is readily seen from (23) and (33) that a (nonzero) vector $\boldsymbol{\beta} \in \mathbb{R}^{M_{\mathrm{B}}N_{\mathrm{U}}}$ does not belong to the nullspace of $\mathbf{G}_{\mathrm{B}}$ if and only if $\left(\mathbf{1}_{\mathcal{U}_{\mathrm{B}}^{(i)}(\widetilde{s})} \otimes \mathbf{1}_{\mathcal{V}^{(j)}(\widetilde{s})}\right)^{\mathrm{T}} \boldsymbol{\beta} \neq 0$ or, equivalently,

$$\sum_{n \in \mathrm{supp}\left(\mathbf{1}_{\mathcal{U}_{\mathrm{B}}^{(i)}(\widetilde{s})} \otimes \mathbf{1}_{\mathcal{V}^{(j)}(\widetilde{s})}\right)} \{\boldsymbol{\beta}\}_n \neq 0 \tag{63}$$

for at least one $i \in \{1, 2, \ldots, \widetilde{M}\}$, $j \in \{1, 2, \ldots, \widetilde{N}_{\mathrm{U}}\}$, and $\widetilde{s} \in \{0, 1, \ldots, Q-1\}$. This condition is fulfilled with

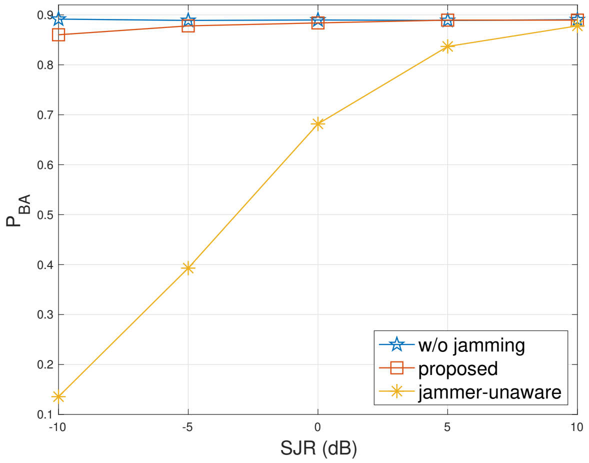


Fig. 8. P_{BA} versus SJR (Case 1, $\gamma_{\text{B}} = \gamma_{\text{J}} = 1$, and $Q = 100$).

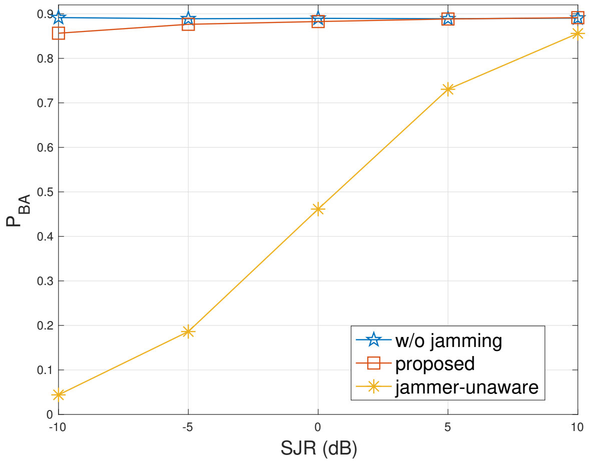


Fig. 10. P_{BA} versus SJR (Case 3, $\gamma_{\text{B}} = \gamma_{\text{J}} = 1$, and $Q = 100$).

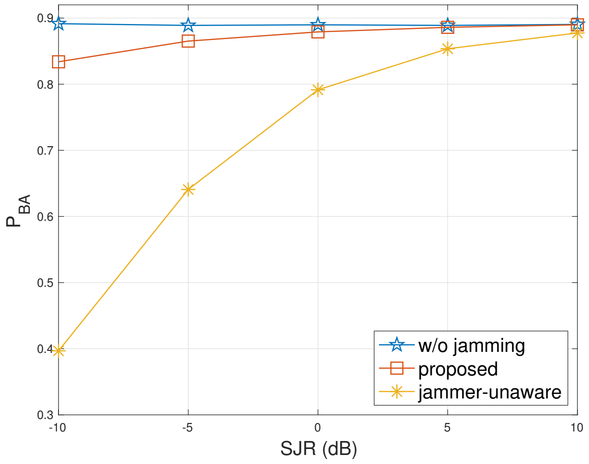


Fig. 9. P_{BA} versus SJR (Case 2, $\gamma_{\text{B}} = \gamma_{\text{J}} = 1$, and $Q = 100$).

overwhelming probability for a κ_{B}-sparse vector $\boldsymbol{\beta}$. We refer to [47] for a rigorous proof in the case of $0/1$-Bernoulli matrices.

REFERENCES

[1] 3GPP TS 38.104 (2019), "NR; Base Station (BS) Radio Transmission and Reception (Release 15)", V15-6.0 (2019-6).

[2] 3GPP TR 21.916 (2019), "Release 16 Description; Summary of Rel-16 Work Items (Release 16)", V0.2.0 (2019-12).

[3] T.S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!", *IEEE Access*, vol. 1, pp. 335-349, May 2013.

[4] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-Time Wireless Communications*. Cambridge University Press, 2003.

[5] D. Darsena, G. Gelli, and F. Verde, "Beamforming and precoding techniques," *Wiley 5G Ref: The Essential 5G Reference Online*, 2020.

[6] 3GPP TR 38.912 (2018), "Study on New Radio (NR) access technology (Release 15)", V15.0.0 (2018-06).

[7] T. Nitsche, C. Cordeiro, A.B. Flores, E.W. Knightly, E. Perahia, and J.C. Widmer, "IEEE 802.11 ad: Directional 60 GHz communication for multi-gigabit-per-second Wi-Fi," *IEEE Commun. Mag.*, vol. 52, pp. 132-141, Dec. 2014.

[8] J. Wang *et al.*, "Beam codebook based beamforming protocol for multi-Gbps millimeter-wave WPAN systems," *IEEE J. Select. Areas Commun.*, vol. 27, pp. 1390-1399, Oct. 2009.

[9] S. Hur, T. Kim, D.J. Love, J.V. Krogmeier, T.A. Thomas, and A. Ghosh, "Millimeter wave beamforming for wireless backhaul and access in small cell networks," *IEEE Trans. Commun.*, vol. 61, pp. 4391-4403, Oct. 2013.

[10] M. Kokshoorn, H. Chen, P. Wang, Y. Li, and B. Vucetic, "Millimeter wave MIMO channel estimation using overlapped beam patterns and rate adaptation,"*IEEE Trans. Signal Process.*, vol. 65, pp. 601-616, Feb. 2017.

[11] X. Song, S. Haghighatshoar, and G. Caire, "A scalable and statistically robust beam alignment technique for millimeter-wave systems," *IEEE Trans. Wireless Commun.*, vol. 17, pp. 4792-4805, July 2018.

[12] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi, "A tutorial on beam management for 3GPP NR at mmwave frequencies," *IEEE Commun. Surv. Tutor.*, vol. 21, pp. 173-196, First Quarter 2019.

[13] N.J. Myers, A. Mezghani, and R.W. Heath, "Swift-link: A compressive beam alignment algorithm for practical mmWave radios," *IEEE Trans. Signal Process.*, vol. 67, pp. 1104-1119, Feb. 2019.

[14] M. Hussain and N. Michelusi, "Energy-efficient interactive beam alignment for millimeter-wave networks," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 838-851, Feb. 2019.

[15] D. Zhang, A. Li, M. Shirvanimoghaddam, Y. Li, and B. Vucetic, "Exploring AoA/AoD dynamics in beam alignment of mobile millimeter wave MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 68, pp. 6172-6176, June 2019.

[16] M. Li, C. Liu, S.V. Hanly, I.B. Collings, and P. Whiting, "Explore and eliminate: Optimized two-stage search for millimeter-wave beam alignment," *IEEE Trans. Wireless Commun.*, vol. 18, pp. 4379-4393, Sept2019.

[17] V. Suresh and D.J. Love, "Single-bit millimeter wave beam alignment using error control sounding strategies," *IEEE J. Select. Topics Signal Process.*, vol. 13, pp. 1032-1045, Sept. 2019.

[18] X. Li, J. Fang, H. Duan, Z. Chen, and H. Li, "Fast beam alignment for millimeter wave communications: A sparse encoding and phaseless decoding approach," *IEEE Trans. Signal Process.*, vol. 67, pp. 4402-4417, Sept. 2019.

[19] M. Morales-Céspedes, O.A. Dobre, and A. García-Armada, "Semi-blind interference aligned NOMA for downlink MU-MISO systems," *IEEE Trans. Commun.*, vol. 68, pp. 1852-1865, Mar. 2020.

[20] C. Liu, M. Li, L. Zhao, P. Whiting, S.V. Hanly and I.B. Collings, "Millimeter-wave beam search with iterative deactivation and beam shifting," *IEEE Trans. Wireless Commun.*, vol. 19, pp. 5117-5131, Aug. 2020.

[21] R. Gupta, K. Lakshmanan, and A.K. Sah, "Beam alignment for mmWave using non-stationary bandits," *IEEE Commun. Lett.*, vol. 24, pp. 2619-2622, Nov. 2020.

[22] I. Chafaa, E.V. Belmega, and M. Debbah, "One-bit feedback exponential learning for beam alignment in mobile mmWave," *IEEE Access*, vol. 8, pp. 194575-194589, 2020.

[23] H. Echigo, Y. Cao, M. Bouazizi, and T. Ohtsuki, "A deep learning-based low overhead beam selection in mmWave communications," *IEEE Trans. Veh. Technol.*, vol. 70, pp. 682-691, Jan. 2021.

[24] M. Wang, C. Zhang, X. Chen, and S. Tang, "Performance analysis of millimeter wave wireless power transfer with imperfect beam alignment," *IEEE Trans. Veh. Technol.*, vol. 70, pp. 2605-2618, Mar. 2021.

[25] J. Zhang and C. Masouros, "Learning-based predictive transmitter-receiver beam alignment in millimeter wave fixed wireless access links," *IEEE Trans. Signal Process.*, vol. 69, pp. 3268-3282, 2021.

[26] J. Zhang *et al.*, "Joint beam training and data transmission design for covert millimeter-wave communication,"IEEE Trans. Inf. Foren. Sec., vol. 16, pp. 2232-2245, 2021.

[27] M. Akdeniz, Y. Liu, S. Sun, S. Rangan, T. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Select. Areas Commun.*, vol. 32, pp. 1164-1179, June 2014.

[28] A.F. Molisch, V.V. Ratnam, S. Han, Z. Li, S.L.H. Nguyen, L. Li, and K. Haneda, "Hybrid Beamforming for Massive MIMO," *IEEE Commun. Magazine*, vol. 55, pp. 134-141, Sept. 2017.

[29] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of Jamming attacks in time-critical wireless applications," IEEE Trans. Mobile Comput., vol. 13, pp. 1746-1759, Aug. 2014.

[30] B. Sirkeci-Mergen and A. Scaglione, "Randomized space-time coding for distributed cooperative communication," *IEEE Trans. Signal Process.*, vol. 55, pp. 5003-5017, Oct. 2007.

[31] L. Zhang, P.N. Suganthan, "A survey of randomized algorithms for training neural networks," *Information Sciences*, vol. 364-365, pp. 146-155, Oct. 2016.

[32] J.K. Tugnait, "Pilot spoofing attack detection and sountermeasure," *IEEE Trans. Commun.*, vol. 66, pp. 2093-2106, May 2018.

[33] K. Pelechrinis, M. Iliofotou, and S.V. Krishnamurthy, "Denial of service attacks in wireless networks: The Case of jammers," *IEEE Commun. Surveys & Tutorials*, vol. 13, pp. 245-57, 2011.

[34] "Radio noise", Recommendation ITU-R P.372-13, Sep. 2016.

[35] R.A. Horn and C.R. Johnson, *Matrix Analysis*. New York: Cambridge Univ. Press, 1990.

[36] A. M. Sayeed, "Deconstructing multiantenna fading channels," *IEEE Trans. Signal Process.*, vol. 50, pp. 2563-79, 2002.

[37] R. W. Heath Jr., N. Gonzàlez-Prelcic, S. Rangan, W. Roh, and A.M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Select. Areas Commun.*, vol. 10, pp. 436-53, 2016.

[38] W. U. Bajwa, J. Haupt, A. M. Sayeed, and R. Nowak, "A new approach to estimating sparse multipath channels," *Proc. IEEE*, vol. 98, pp. 1058-76, 2010.

[39] J. W. Brewer, "Kronecker products and matrix calculus in system theory," *IEEE Transactions on circuits and systems*, vol. CAS-25, pp. 772-81, 1978.

[40] M.R. Akdeniz *et al.*, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. Select. Areas Commun.*, vol. 32, pp. 1164-1179, June 2014.

[41] A. Alkhateeb, O. El Ayach, G. Leus, and R.W. Heath, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. Select. Topics Signal Process.*, vol. 8, pp. 831–846, Oct. 2014.

[42] K. Venugopal, A. Alkhateeb, N.G. Prelcic, and R.W. Heath, "Channel estimation for hybrid architecture based wideband millimeter wave systems," *IEEE J. Select. Areas Commun.*, vol. 35, pp. 1996-2009, Sep. 2017.

[43] D. Kim, S. Sra, and I. Dhillon, "Tackling box-constrained convex optimization via a new projected quasi-Newton approach," *SIAM Journal on Scientific Computing*, vol. 32, pp. 3548-3563, 2010.

[44] M. Slawski and M. Hein, "Non-negative least squares for high-dimensional linear models: Consistency and sparse recovery without regularization," *Electron. J. Statist.*, vol. 7, pp. 3004-3056, 2013.

[45] A. Björck, *Numerical Methods for Least Squares Problems*. SIAM: Philadelphia, PA, 1996.

[46] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. Springer Science+Business Media New York 2013.

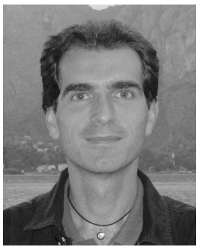
[47] R. Kueng and P. Jung, "Robust nonnegative sparse recovery and the nullspace property of $0/1$ measurements," *IEEE Trans. Inf. Theory*, vol. 64, pp. 689-703, Feb. 2018.

[48] P. Frenger, P. Moberg, J. Malmodin, Y. Jading, and I. Godor, "Reducing energy consumption in LTE with cell DTX," *Proc. of 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, 2011, pp. 1-5.

[49] A. Zaidi, F. Athley, and J. Medbo, *5G Physical Layer: Principles, Models and Technology Components*. Elsevier Science Publishing Co Inc, 2018 .

Donatella Darsena (M'06-SM'16) received the Dr. Eng. degree summa cum laude in telecommunications engineering in 2001, and the Ph.D. degree in electronic and telecommunications engineering in 2005, both from the University of Napoli Federico II, Italy. From 2001 to 2002, she worked as embedded system designer in the Telecommunications, Peripherals and Automotive Group, STMicroelectronics, Milano, Italy. Since March 2005, she has been with the University of Napoli Parthenope, Italy. She first served as an Assistant Professor of probability theory and, since January 2022, she has served as an Associate Professor of telecommunications with the Department of Engineering.

Her research interests are in the broad area of signal processing for communications, with current emphasis on backscattering communications, space-time techniques for cooperative and cognitive networks, green communications for IoT. Dr. Darsena was an Associate Editor for the IEEE COMMUNICATIONS LETTERS from December 2016 to July 2019. She has served as Associate Editor for IEEE ACCESS since October 2018, Senior Area Editor for IEEE COMMUNICATIONS LETTERS since August 2019, and Associate Editor for IEEE SIGNAL PROCESSING LETTERS since 2020.



Francesco Verde (M'10-SM'14) was born in Santa Maria Capua Vetere, Italy, on June 12, 1974. He received the Dr. Eng. degree *summa cum laude* in electronic engineering from the Second University of Napoli, Italy, in 1998, and the Ph.D. degree in information engineering from the University of Napoli Federico II, in 2002. Since December 2002, he has been with the University of Napoli Federico II, Italy. He first served as an Assistant Professor of signal theory and mobile communications and, since December 2011, he has served as an Associate Professor of telecommunications with the Department of Electrical Engineering and Information Technology. His research activities include reflected-power communications, orthogonal/non-orthogonal multiple-access techniques, wireless systems optimization, and physical-layer security.

Prof. Verde has been involved in several technical program committees of major IEEE conferences in signal processing and wireless communications. He has served as Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS since 2017 and Senior Area Editor of the IEEE SIGNAL PROCESSING LETTERS since 2018. He was an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING (from 2010 to 2014) and IEEE SIGNAL PROCESSING LETTERS (from 2014 to 2018), as well as Guest Editor of the EURASIP Journal on Advances in Signal Processing in 2010 and SENSORS MDPI in 2018-2022.