Direction Estimation of the Attacked Signal in PBCH of 5G NR

Mohsen Kazemian, *Member, IEEE,* Tasos Dagiuklas, and Jürgen Jasperneite, *Senior Member, IEEE*

***Abstract*—This letter investigates the jamming attack in the physical broadcast channel (PBCH) of the fifth generation (5G) new radio (NR) that conveys critical information of the cell called master information block (MIB). Since smart attack on PBCH is simply possible using the information of synchronization signal block (SSB) that is unencrypted during the initial access, this channel is one of the most effective choices from a jammer's point of view. In this study, we propose a hypothesis test to detect the presence of a jamming attack in the PBCH block and, furthermore, we estimate the principal direction of the attacked PBCH demodulation reference signal (PBCH DMRS) that significantly deviates under that attack. These achievements are also presented in the form of semi-definite programming (SDP) relaxation. PBCH DMRS is located at 25% of the PBCH block and is vital for PBCH extraction to initiate a radio connection between user and an appropriate cell. Simulation results evaluate the proposed method in various aspects and prove its superiority over the recent competing methods.**

***Index Terms*—SPCA, smart jamming, 5G NR, PBCH DMRS, physical layer.**

I. Introduction

5TH generation (5G) new radio (NR) is the current technology released by third generation partnership project (3GPP), which has accelerated in recent years. Physical channels and signals in the physical layer of 5G NR are vulnerable to external attacks with different levels of feasibility [1], [2], [3]. In this technology, primary synchronization signal (PSS), secondary synchronization signal (SSS) and physical broadcast channel (PBCH) are wrapped altogether as an synchronization signal block (SSB), and transmitted in various patterns depending on the network settings such as channel bandwidth and subcarrier spacing. SSB is always 4 OFDM symbol wide and 240 subcarriers (i.e., 20 resource blocks (RBs)) long [1].

User equipment (UE) performs the cell search process to provide time and frequency synchronization with a cell and to detect the cell ID (CID) using $N_{ID}^{cell} = 3N_{ID}^{(1)} + N_{ID}^{(2)}$, where $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$ are carried by the strongest detected SSS and PSS sequences, respectively. UE finds out the CID, and then acquires the index of PBCH DMRS sequence, which describes the assigned resource elements (REs) in the PBCH block. PBCH DMRS specifies parameters such as half-frame bit and SSB index, depending on the maximum number of SSBs within a SSB set, and determines the least significant bits of system frame number (SFN). UE estimates the PBCH block, and then decodes the master information block (MIB) using SFN, to receive the other system information transmitted on physical downlink shared channel (PDSCH). Since SSB is unencrypted during the initial access and will be transmitted periodically within the broadcast channel transmission time interval (BCH TTI), it is easy for a malicious jammer to detect the PBCH DMRS REs, which follow N_{ID}^{cell}, by sniffing, and then attack the PBCH DMRS sequence with the aim of causing a failure in PBCH extraction and MIB information decoding.

By the development of 5G NR and beyond, researchers are now attracted to study on the physical layer security. However, thus far, a limited number of works has been accomplished in the particular area of 5G NR physical channels. Some energy efficiency (EE) based works such as [4] and [5] rely on the prior knowledge of the channels and even the jammers. Thus, they are not feasible in a real-time network. The methods in [6], [7], and [8] are basically designed using machine learning algorithms. In the absence of sufficient training samples, these methods fail to deal with unknown jamming patterns (JPs). However, zero-shot learning (ZSL) based method in [7] achieves some acceptable results. Moreover, [7] and [8] are ineffective when multiple jammers attack with distinct policies. The methods such as [9] add a designed and manufactured hardware to the network and, thus, require a high startup cost. Finally, the authors in [10] use sparse principal component analysis (SPCA) conceptual idea for jamming detection, which deserves more research efforts in the field of physical layer security.

Jamming attack on the PBCH DMRS REs forces the principal direction of its dominant subspace and, thus, that of PBCH dominant space to deviate from the normal state. The vulnerability of SSB and the importance of PBCH DMRS in delivering data from gNB to UE, in addition to considering the aforementioned issues, motivate us to study the sparsity in the structure of PBCH DMRS sequence, which is occurred by a jamming attack, at the user side. In this letter, we detect the targeted attack similar to the detection of a sparse direction with a significantly higher variance than any other direction, which is the main concept of SPCA. Furthermore, the principal component of the attacked signal is estimated. Thanks to investigating the sparsity on the structure of the attacked signal at the user side, this method does not rely on the number of attackers. Besides, the proposed adaptive detection procedure makes our method independent of any

M. Kazemian is with the Institute Industrial IT (inIT) of the Technische Hochschule OWL, Lemgo, Germany, e-mail: (mohsen.kazemian.my@ieee.org).

T. Dagiuklas is with the Department of Computer Science and Informatics, London South Bank University, United Kingdom, (e-mail: tdagiuklas@lsbu.ac.uk).

J. Jasperneite is with the Institute Industrial IT (inIT) of the Technische Hochschule OWL, and Fraunhofer IOSB-INA, Lemgo, Germany, (e-mail: juergen.jasperneite@th-owl.de).

jammer's information. The main contributions of this work that make this letter different from [10] are as follows: 1) we study the testing problem for jamming detection and compute the high probability deviation bounds using a semi-definite programming (SDP) relaxation, 2) the minimum jamming power for a successful detection is determined, and 3) the principal direction of the attacked PBCH DMRS is estimated, and then presented using a polynomial-time semi-definite relaxation technique. This is a fundamental requirement for jamming cancellation.

Notations: Throughout the letter, $\lambda_{max}(\hat{\mathbf{\Sigma}})$ indicates the leading eigenvalue of matrix $\hat{\mathbf{\Sigma}}$, and $\mathbf{R}^{p\times p}$ is the set of $p\times p$ matrices with real numbers. We use $\mathbf{1}\{\cdot\}$, $\|\mathbf{v}_n\|_q$, and $\mathbf{V}\succeq 0$ to denote the indicator function, l_q norm of $\mathbf{v}_n$, and semi-definite positive $\mathbf{V}$, respectively.

II. System Model and Problem Formulation

The subcarriers that include the DMRS and the jamming signal are indexed by the set S with the cardinality $|S|=N_s$. Let $\mathbf{a}_n=[a_{(n,m)}]^T$ and $\mathbf{d}_n=[d_{(n,m)}]^T$, with $m\in S$, denote the jamming signal and the DMRS on the nth OFDM symbol time and mth subcarrier frequency, respectively. We formulate the received OFDM signal generated by the clustered delay line (CDL) channel model under the attacks of multiple jammers as follows

$$\mathbf{y}_n = diag(\mathbf{d}_n)\mathbf{F}(:,1:L)\mathbf{h}_n + \sum_{i=1}^{N_j}\sqrt{\theta^i}\; diag(\mathbf{a}_n^i)\mathbf{F}(:,1:L)\mathbf{g}_n^i + \mathbf{A}_n, \quad (1)$$

where $\mathbf{F}$ denotes the $N_s\times N_s$ square discrete Fourier transformation (DFT) matrix, and, $\mathbf{h}_n$ and $\mathbf{g}_n^i$ indicate the channel impulse response vectors with L channel taps, from the base station and the ith jammer to UE, respectively. Furthermore, N_j is the number of jammers, $\theta^i\geq 0$ is the ith jamming-to-signal ratio (JSR), and, finally, $\mathbf{A}_n\sim\mathcal{N}(0,\sigma^2)$ denotes the additive white Gaussian noise (AWGN) with mean zero and variance of σ^2 that is introduced to the channel.

III. Proposed Method

In the CDL channel model with different facing scatterers, each element of the channel impulse response vectors shows the gain distribution in a specific direction. Therefore, we can detect the presence of a jamming attack similar to sparse principal component detection in the SPCA approach. Referring to (1), the received signal $\mathbf{y}\sim\mathcal{N}_p(\mathbf{0},\mathbf{\Sigma})$ has the covariance of $\mathbf{\Sigma}=\mathbb{E}[\mathbf{y}\mathbf{y}^T]$, where $\mathbf{y}=\{\mathbf{y}_1,...,\mathbf{y}_{N_t}\}$, p denotes the number of dimensions and N_t is the total number of symbols. However, in accordance with the requirement of real-time systems, we consider only N symbols as the sample observations, which carry PBCH DMRS sequence, and reformulate $\mathbf{y}$ to $\hat{\mathbf{y}}\sim\mathcal{N}_p(\mathbf{0},\hat{\mathbf{\Sigma}})$, where $\hat{\mathbf{y}}=\{\hat{\mathbf{y}}_1,...,\hat{\mathbf{y}}_N\}$, $N>p$, and $\hat{\mathbf{\Sigma}}=\frac{1}{N}\sum_{n=1}^{N}\hat{\mathbf{y}}_n\hat{\mathbf{y}}_n^T\in\mathbf{R}^{p\times p}$ denotes the empirical covariance matrix of the received signal. In the following, a hypothesis testing problem is proposed to detect a jamming attack on the PBCH dominant space, and then the principal direction of $\mathbf{y}$ is estimated in the form of an efficient polynomial-time semi-definite relaxation.

A. Hypothesis Testing Problem

Phase 1: The largest k-sparse eigenvalue of $\hat{\mathbf{\Sigma}}$ is given by

$$\lambda_{max}^k(\hat{\mathbf{\Sigma}})\triangleq\max_{\mathbf{v}_n\in\mathcal{M}_{\mathbf{v}}}\mathbf{v}_n^T\hat{\mathbf{\Sigma}}\mathbf{v}_n, \quad (2)$$

where $\mathbf{v}_n$ denotes the unit norm sparse principal component of $\mathbf{\Sigma}$, which represents the deviation of PBCH DMRS under the jamming level $\theta=\sum_{i=1}^{N_j}\theta^i$ with $\mathcal{M}_{\mathbf{v}}\triangleq\Big\{\mathbf{v}_n=(v_{n_1},...,v_{n_p})^T\in\mathbf{R}^p:\sum_{j=1}^{p}\mathbf{1}\{v_{n_j}\neq 0\}\leq k,\|\mathbf{v}_n\|_2=1\Big\}$ as the set of k-sparse unit vectors. Equation (2) finds out the maximum eigenvalue of $\hat{\mathbf{\Sigma}}$ among different values corresponded to 2^p possible vectors for $\mathbf{v}_n$, considering the k sparsity level. The main objective in this phase is to compute the deviation bounds τ_0 and τ_1 for $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$ to be utilized in the test $\psi(\hat{\Sigma})\triangleq\mathbf{1}\{\lambda_{max}^k(\hat{\mathbf{\Sigma}})>\tau\}$, $\tau\in[\tau_0,\tau_1]$, with the probability of $1-\delta$, to discriminate between the normal and attacked states respectively denoted by $\mathcal{H}_0$ and $\mathcal{H}_1$, as follows [11]

$$\begin{cases}\mathcal{H}_0: & \hat{\mathbf{y}}\sim\mathcal{N}_p(0,\hat{\mathbf{\Sigma}}_0),\\ \mathcal{H}_1: & \hat{\mathbf{y}}\sim\mathcal{N}_p(0,\hat{\mathbf{\Sigma}}_0+\theta\mathbf{v}_n\mathbf{v}_n^T),\end{cases} \quad (3)$$

where $\hat{\mathbf{\Sigma}}_0$ is the covariance matrix of $\hat{\mathbf{y}}$ under $\mathcal{H}_0$. Let $\rho=\log(1/\delta)$ and $x=k\log(9ep/k)+\rho$. The upper and lower bounds of $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$, which are respectively denoted by quantiles τ_0 and τ_1, are computed by (see Appendix for the proof)

$$\begin{cases}\tau_0=1+4\sqrt{\frac{x}{N}}+4\frac{x}{N},\\ \tau_1=1+\theta-2(1+\theta)\sqrt{\frac{\rho}{N}}.\end{cases} \quad (4)$$

The condition $\tau_1>\tau_0$ holds for any $\theta>\check{\theta}$, where the minimum detection level $\check{\theta}$ is defined as follows

$$\check{\theta}\triangleq 4\sqrt{\frac{x}{N}}+4\frac{x}{N}+4\sqrt{\frac{\rho}{N}}. \quad (5)$$

Thus, for any $\theta>\check{\theta}$, we propose the test $\psi(\hat{\mathbf{\Sigma}})$ to detect the jamming attack with probability $1-\delta$ using an investigation on the behavior of $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$ such that

$$\mathbf{P}_{H_0}(\lambda_{max}^k(\hat{\mathbf{\Sigma}})>\tau_0)\leq\delta,\mathbf{P}_{H_1}(\lambda_{max}^k(\hat{\mathbf{\Sigma}})<\tau_1)\leq\delta. \quad (6)$$

Phase 2: Since computing $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$ is in general a hard computational problem, in this phase, the deviation bounds and the minimum detection level are computed using SDP relaxation technique. Thus, the largest k-sparse eigenvalue of $\hat{\mathbf{\Sigma}}$ can be written as

$$\lambda_{max}^k(\hat{\mathbf{\Sigma}})\triangleq\max_{\mathbf{V}\in\mathcal{M}_{\mathbf{V}}}\mathbf{Tr}(\hat{\mathbf{\Sigma}}\mathbf{V}), \quad (7)$$

where $\mathbf{V}\triangleq\mathbf{v}_n\mathbf{v}_n{}^T$ and $\mathcal{M}_{\mathbf{V}}\triangleq\Big\{\mathbf{Tr}(\mathbf{V})=1,\|\mathbf{V}\|_0\leq k^2,\mathbf{V}\succeq 0,\mathbf{Rank}(\mathbf{V})=1\Big\}$. Equation (7) contains l_0 norm and the rank one as the two sources of non-convexity. We use Cauchy–Schwarz inequality for matrix $\mathbf{V}$ to substitute $\|\mathbf{V}\|_1\leq k$ for $\|\mathbf{V}\|_0\leq k^2$, and then simply drop the rank-one constraint, in order to get a convex set. The SDP relaxation of $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$ is defined by

$$\tilde{\lambda}_{max}^k(\hat{\mathbf{\Sigma}})\triangleq\max_{\mathbf{V}\in\tilde{\mathcal{M}}_{\mathbf{V}}}\mathbf{Tr}(\hat{\mathbf{\Sigma}}\mathbf{V}), \quad (8)$$

where $\tilde{\mathcal{M}}_{\mathbf{V}} \triangleq \Big\{\mathbf{Tr}(\mathbf{V}) = 1, \|\mathbf{V}\|_1 \leq k, \mathbf{V} \succeq 0\Big\}$. Next, the behavior of $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}})$ under hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ will be studied.

We define the following inequality for any $\hat{\mathbf{\Sigma}} \succeq 0$ as a relaxation of the original problem

$$\lambda^k_{max}(\hat{\mathbf{\Sigma}}) \leq \tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}). \tag{9}$$

Referring to (6) and (9), $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}})$ takes the larger values under $\mathcal{H}_1$. Therefore, we can write (see (28) in Appendix)

$$\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \geq 1 + \theta - 2(1+\theta)\sqrt{\frac{\rho}{N}}. \tag{10}$$

To study $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}})$ under $\mathcal{H}_0$ state (i.e., the upper bound of $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}})$), we first use the duality of SDP defined by $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \triangleq \min_{\mathbf{\Phi} \in \tilde{\mathbf{S}}_p} \{\lambda_{max}(\hat{\mathbf{\Sigma}} + \mathbf{\Phi}) + k\|\mathbf{\Phi}\|_\infty\}$, where matrix $\mathbf{\Phi}$ belongs to the space of $p \times p$ symmetric real matrices indicated by $\tilde{\mathbf{S}}_p$. Using (9), for any $\mu \geq 0$ such that $\|\mathbf{\Phi}\|_\infty \leq \mu$, we have

$$\lambda^k_{max}(\hat{\mathbf{\Sigma}}) \leq \tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \leq \lambda_{max}(\hat{\mathbf{\Sigma}} + \mathbf{\Phi}) + k\mu. \tag{11}$$

Since $\hat{\mathbf{\Sigma}} \succeq 0$ is a k-sparse matrix, for any matrix $\mathbf{M}$ equation (11) yields

$$\begin{aligned} \lambda^k_{max}(\hat{\mathbf{\Sigma}} + \mathbf{M}) &\leq \lambda_{max}((\hat{\mathbf{\Sigma}} + \mathbf{M}) - \mathbf{M}) + k\|\mathbf{M}\|_\infty \\ &= \lambda^k_{max}(\hat{\mathbf{\Sigma}}) + k\|\mathbf{M}\|_\infty. \end{aligned} \tag{12}$$

Next, we decompose $\hat{\mathbf{\Sigma}}$ to $\mathbf{A} = diag(\hat{\mathbf{\Sigma}}_{i,i})$ and $\mathbf{B} = \hat{\mathbf{\Sigma}} - \mathbf{A}$ matrices, with $i \in \{1, ..., p\}$, and then control the largest element of each one separately, in the following two steps:

Step 1: To control the largest element of $\mathbf{B}$, we use Lemma 1 in [12] to bound $\|\mathbf{B}\|_\infty$ with high probability. Therefore, for any $x_1 > 0$ we have

$$\mathbf{P}\Big(|\mathbf{B}_{ij}| \geq 2\sqrt{\frac{x_1}{N}} + 2\frac{x_1}{N}\Big) \leq 4e^{-x_1}, \tag{13}$$

where $|.|$ denotes the absolute value of its element, and $\mathbf{B}_{i,j} = 0.5\Big[\frac{1}{N}\sum_{n=1}^N [0.5(\hat{\mathbf{y}}_{n,i} + \hat{\mathbf{y}}_{n,j})^2 - 1] - \frac{1}{N}\sum_{n=1}^N [0.5(\hat{\mathbf{y}}_{n,i} - \hat{\mathbf{y}}_{n,j})^2 - 1]\Big]$, with $i, j \in \{1, ..., p\}$. Applying Boole's inequality on the off-diagonal terms, (13) yields

$$\mathbf{P}\Big(\max_{i<j} |\mathbf{B}_{ij}| \geq 2\sqrt{\frac{x_1}{N}} + 2\frac{x_1}{N}\Big) \leq 2p^2 e^{-x_1}. \tag{14}$$

Using disjoint support decomposition (DSD) of $\hat{\mathbf{\Sigma}}$, we write $\mathcal{S}_\mu(\hat{\mathbf{\Sigma}}) = \mathcal{S}_\mu(\mathbf{A}) + \mathcal{S}_\mu(\mathbf{B})$, where $\mathcal{S}_\mu$ is the soft-threshold function of its input with threshold μ. Referring to (14), and taking $x_1 \triangleq \log(4p^2/\delta)$ and $\mu \triangleq 2\sqrt{\frac{x_1}{N}} + 2\frac{x_1}{N}$, we have $\|\mathbf{B}\|_\infty \leq \mu$ and, thus, $\mathcal{S}_\mu(\mathbf{B}) = 0$ with probability $1 - \delta/2$. Therefore, here we get

$$\lambda_{max}(\mathcal{S}_\mu(\hat{\mathbf{\Sigma}})) = \lambda_{max}(\mathcal{S}_\mu(\mathbf{A})) \leq \lambda_{max}(\mathbf{A}) = \max_i \mathbf{A}_{ii}, \tag{15}$$

where $\mathbf{A}_{ii} = \frac{1}{N}\sum_{n=1}^N \hat{\mathbf{y}}^2_{n,i}$.

Step 2: In this step, we control $\|\mathbf{A}\|_\infty$ using the same procedure of step 1. Applying Lemma 1 in [12] and Boole's inequality on the diagonal terms, for any $x_2 > 0$ we have

$$\mathbf{P}\Big(\max_i \mathbf{A}_{ii} \geq 1 + 2\sqrt{\frac{x_2}{N}} + 2\frac{x_2}{N}\Big) \leq pe^{-x_2}. \tag{16}$$

Algorithm 1 The proposed anti-jamming scheme for PBCH

Input: $\mathbf{y} = \{\mathbf{y}_1, ..., \mathbf{y}_{N_t}\}$, N, p, and k,
Compute $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \triangleq \max_{\mathbf{V} \in \tilde{\mathcal{M}}_{\mathbf{V}}} \mathbf{Tr}(\hat{\mathbf{\Sigma}}\mathbf{V})$, $\tilde{\tau}_0$ and $\tilde{\tau}_1$,
if $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \leq \tilde{\tau}_0$ **then**
  Return: No jamming,
else
  if $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \geq \tilde{\tau}_1$ **then**
    Compute $\tilde{\mathbf{v}}^k_{max}$,
  else
    Return: Not successful. Update input values,
  end if
end if
Output: $\tilde{\mathbf{v}}^k_{max}$.

Let $x_2 \triangleq \log(2p/\delta)$. Then, the largest element of $\mathbf{A}_{ii}$ is bounded with probability $1 - \delta/2$ such that

$$\max_i \mathbf{A}_{ii} \leq 1 + \eta, \tag{17}$$

where $\eta \triangleq 2\sqrt{\frac{x_2}{N}} + 2\frac{x_2}{N}$. Referring to (11), $\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) \leq \lambda_{max}(\mathcal{S}_\mu(\hat{\mathbf{\Sigma}})) + k\mu$. Using DSD of $\hat{\mathbf{\Sigma}}$, for $\mu \geq 0$, we write

$$\begin{aligned} \tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) &\leq \lambda_{max}(\mathcal{S}_\mu(\mathbf{A}) + \mathcal{S}_\mu(\mathbf{B})) + k\mu \\ &\leq \lambda_{max}(\mathcal{S}_\mu(\mathbf{A})) + \lambda_{max}(\mathcal{S}_\mu(\mathbf{B})) + k\mu. \end{aligned} \tag{18}$$

Finally, referring to equations (15) and (17) and with $\mathcal{S}_\mu(\mathbf{B}) = 0$, we reformulate equations (4) and (6) using SDP relaxation as follows

$$\begin{cases} \tilde{\tau}_0 = 1 + k\mu + \eta, \\ \tilde{\tau}_1 = 1 + \theta - 2(1+\theta)\sqrt{\frac{\rho}{N}}, \end{cases} \tag{19}$$

$$\mathbf{P}_{H_0}(\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) > \tilde{\tau}_0) \leq \delta, \mathbf{P}_{H_1}(\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) < \tilde{\tau}_1) \leq \delta. \tag{20}$$

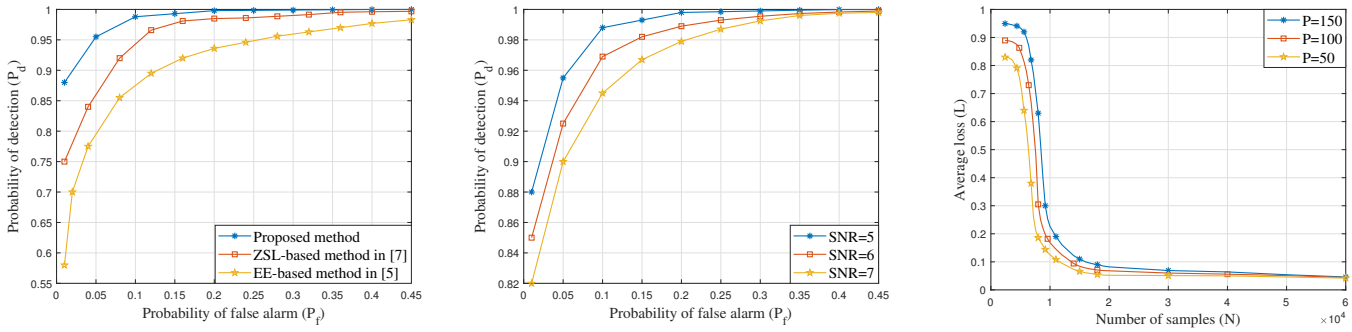
Same as phase 1, we compute the minimum detection level $\tilde{\theta} \triangleq k\mu + \eta + 4\sqrt{\frac{\rho}{N}}$, which for any $\theta > \tilde{\theta}$ the condition $\tilde{\tau}_1 > \tilde{\tau}_0$ holds. As a summary, in this phase, we proposed the computationally efficient test $\tilde{\varphi}(\hat{\mathbf{\Sigma}}) \triangleq \mathbf{1}\{\tilde{\lambda}^k_{max}(\hat{\mathbf{\Sigma}}) > \tilde{\tau}\}$ with $\tilde{\tau} \in [\tilde{\tau}_0, \tilde{\tau}_1]$ and $\tilde{\tau}_1 > \tilde{\tau}_0$, to discriminate between the normal and the attacked state of PBCH dominant space with probability $1 - \delta$.

B. Direction Estimation

In the preceding subsection, we detected the presence of a distinguished direction under $\mathcal{H}_1$ using the estimation of the largest eigenvalue of matrix $\hat{\mathbf{\Sigma}}$. Based on random matrix theory, the eigenvector $\mathbf{v}_n$ is associated to $\lambda^k_{max}(\mathbf{\Sigma})$ for any $\theta > 0$. Furthermore, if $\mathbf{\Sigma} \approx \hat{\mathbf{\Sigma}}$ in spectral norm, then the largest eigenvector of $\hat{\mathbf{\Sigma}}$ can be an acceptable approximation for $\mathbf{v}_n$, which will hereafter be denoted by $\hat{\mathbf{v}}_n$. Thus, in this subsection, our target is to find out the largest eigenvector of $\hat{\mathbf{\Sigma}}$ that is approximately equal to the attacked PBCH DMRS direction. The leading k-sparse eigenvector of $\hat{\mathbf{\Sigma}}$ is defined by

$$\hat{\mathbf{v}}^k_{max} \in \underset{\mathbf{u}_n \in \mathcal{M}_{\mathbf{u}}}{\operatorname{argmax}} \mathbf{u}_n^T \hat{\mathbf{\Sigma}} \mathbf{u}_n, \tag{21}$$

where $\hat{\mathbf{v}}$ is the set of all estimators, $\mathcal{M}_{\mathbf{u}} \triangleq \big\{\mathbf{u}_n \in$



(a) In comparison with the other methods. (b) With different SNR values. (c) In estimation of the principal direction.

Fig. 1. The performance of our proposed method.

$\mathbf{R}^p : \|\mathbf{u}_n\|_0 \leq k, \|\mathbf{u}_n\|_2 = 1\}$, and $\hat{\mathbf{v}}_n = \hat{\mathbf{v}}^k_{max}$. Since computing the estimator in (21) is a non-deterministic polynomial-time (NP)-hard problem, in the following, we compute $\hat{\mathbf{v}}_n$ using the polynomial-time SDP estimator $\tilde{\mathbf{v}}^k_{max}$. Let $\mathbf{U} \triangleq \mathbf{u}_n\mathbf{u}_n^T$, $\mathcal{U} \in \mathbf{R}^{p\times p}$ be the class of positive semi-definite real symmetric matrices, and $\tilde{\mathcal{M}}_{\mathbf{U}} \triangleq \{\mathbf{U} \in \mathcal{U}, \mathbf{Tr}(\mathbf{U}) = 1, \ \mathbf{Rank}(\mathbf{U}) = 1, \|\mathbf{U}\|_0 = K^2\}$, then we have

$$\max_{\mathbf{u}_n\in\mathcal{M}_{\mathbf{u}}} \mathbf{u}_n^T\hat{\mathbf{\Sigma}}\mathbf{u}_n = \max_{\mathbf{u}_n\in\mathcal{M}_{\mathbf{u}}} \mathbf{Tr}\big(\hat{\mathbf{\Sigma}}\mathbf{u}_n\mathbf{u}_n^T\big) = \max_{\mathbf{U}\in\tilde{\mathcal{M}}_{\mathbf{U}}} \mathbf{Tr}(\hat{\mathbf{\Sigma}}\mathbf{U}). \tag{22}$$

To convert the non-convex optimization problem in (22) to a convex problem, we drop the rank 1 constraint and replace l_0 norm with l_1 penalty, as $\max_{\mathbf{U}\in\mathcal{U},\ \mathbf{Tr}(\mathbf{U})=1}\big\{\mathbf{Tr}\big(\hat{\mathbf{\Sigma}}\mathbf{U}\big) - \lambda\|\mathbf{U}\|_1\big\}$, for any $\lambda > 0$. Let $f(\mathbf{U}) \triangleq \mathbf{Tr}\big(\hat{\mathbf{\Sigma}}\mathbf{U}\big) - \lambda\|\mathbf{U}\|_1$. If there is an $\hat{\mathbf{U}}^\epsilon$ such that $f(\hat{\mathbf{U}}^\epsilon) \geq \max_{\mathbf{U}\in\mathcal{U},\ \mathbf{Tr}(\mathbf{U})=1} f(\mathbf{U}) - \epsilon$, with $\epsilon > 0$, the semi-definite relaxation for the estimator in (21) is computed by

$$\tilde{\mathbf{v}}^k_{max} \triangleq \tilde{\mathbf{v}}_{\lambda,\epsilon} \in \underset{\|\mathbf{u}_n\|_2=1}{\operatorname{argmax}} \mathbf{u}_n^T\hat{\mathbf{U}}^\epsilon\mathbf{u}_n. \tag{23}$$

In order to find $\hat{\mathbf{U}}^\epsilon$, we reformulate the aforementioned optimization problem as follows

$$\max_{\mathbf{U}\in\mathcal{U},\ \mathbf{Tr}(\mathbf{U})=1} f(\mathbf{U}) = \max_{\mathbf{U}\in\mathcal{U},\mathbf{Tr}(\mathbf{U})=1} \min_{\mathbf{Q}\in\mathcal{Q}} \mathbf{Tr}\big((\hat{\mathbf{\Sigma}} + \mathbf{Q})\mathbf{U}\big), \tag{24}$$

where $\mathcal{Q} \triangleq \{\mathbf{Q} \in \mathbf{R}^{p\times p} : \mathbf{Q}^T = \mathbf{Q}, \|\mathbf{Q}\|_\infty \leq \lambda\}$. Since the last term in (24) is linear in both $\mathbf{Q}$ and $\mathbf{U}$, the problem can be solved using the proximal methods (see Theorem 3.2 in [13]).

We summarize the design steps of our proposed method as the pseudo-code in Algorithm 1. Finally, in order to neutralize the jamming attack, the estimated $\tilde{\mathbf{v}}^k_{max}$ is simply projected onto the channel dominant subspace of the UE and, thus, the true information of the transmitted PBCH DMRS sequence can be extracted. The PCA conceptual idea has the potential for more research efforts on the jamming problem in any 5G NR physical channel. For example, finding the minimum of θ for different probabilities of detection, adopting the proposed method to the other classes of distributions, exploring the rate of convergence for different N values, and solving the problem for $N < p$, are left for the future.

IV. Simulation Results

In this letter, we consider non-line of sight (NLOS) CDL-B multiple-input multiple-output (MIMO) link-level fading channel with the parameters specified in 3GPP TR 38.901 Table 7.7.1-2 in [14], subcarrier spacing of 30 kHz, channel sampling rate = 10 kHz, 14 channel taps, and the maximum Doppler shift = 100 Hz. Our transmitter generates the sequence of PBCH DMRS symbols for CID = 910. Thus, using $2 \equiv 910 \mod 4$, DMRS symbols are allocated to the $(2+1)^{rd}$ RE of each 4 PBCH REs. Furthermore, $P = 100$, and signal-to-noise ratio (SNR) is set to 5dB, unless otherwise stated. The initial value for the sparsity level to start the iterative detection procedure is $k = floor(\sqrt{p})$, and, finally, the total jamming power of two employed jammers is set to $\theta = 0$dB.

We compare the detection performance of our method with the proposed algorithms in [5] and [7] due to their contributions to the adaptive detection problem. [5] formulates a regret minimization problem for each type of wireless environment, and then updates the transmit power towards the best values, using an online stochastic gradient descent approach. The algorithm in [7] consists of the following three steps: 1) to learn the latent feature representation of known JPs by a supervised learning procedure, 2) to recognize different JPs using an unsupervised classification approach, and 3) to classify both known and unknown JPs in latent space. Fig. 1(a) depicts the detection probability of different methods versus the probability of false alarm using receiver operating characteristic (ROC) curves, in the circumstances where all PBCH DMRS symbols are under jamming attack. This figure proves the superiority of our proposed method over the two competing algorithms.

We have defined a minimum value for the total jamming power in (5) for the probability of detection $1-\delta$. The behavior of our method, using different SNR values but the same noise and jamming power, is depicted in Fig. 1(b). It shows that, in the proposed method, the detection performance can be enhanced by decreasing the SNR value for a given P_f (e.g., almost 0.02 detection enhancement in 1db SNR reduction for $P_f = 0.1$). The possibility of reducing the transmitted signal power in order to improve the detection efficiency is the strong point of this method.

Let $L(\tilde{\mathbf{v}}_{max}^k, \mathbf{v}_n) \triangleq \sin\Big(\phi(\tilde{\mathbf{v}}_{max}^k, \mathbf{v}_n)\Big) = \Big(1 - \big((\tilde{\mathbf{v}}_{max}^k)^T \mathbf{v}_n\big)^2\Big)^{1/2} = \frac{1}{\sqrt{2}}\big\|\tilde{\mathbf{v}}_{max}^k(\tilde{\mathbf{v}}_{max}^k)^T - \mathbf{v}_n\mathbf{v}_n{}^T\big\|_2$ be the average loss of the estimator $\tilde{\mathbf{v}}_{max}^k$, where $\phi(\tilde{\mathbf{v}}_{max}^k, \mathbf{v}_n) \triangleq \cos^{-1}\Big(\big|(\tilde{\mathbf{v}}_{max}^k)^T \mathbf{v}_n\big|\Big)$ indicates the angle between $\tilde{\mathbf{v}}_{max}^k$ and $\mathbf{v}_n$. Taking $\lambda \triangleq 4\sqrt{\frac{\log p}{N}}$ and $\epsilon \triangleq \frac{\log p}{4N}$, Fig. 1(c) depicts $L(\tilde{\mathbf{v}}_{max}^k, \mathbf{v}_n)$ as a function of N for $p \in \{50, 100, 150\}$ over 100 repetitions. In large N, the estimator $\tilde{\mathbf{v}}_{max}^k$ converges to the same mean loss for different p values. It proves that our proposed estimator is independent of the k-sparsity level, in case adequate sample observations are available.

V. Conclusion

In this letter, we proposed a method to detect the jamming attack on PBCH in 5G NR and estimated the principal direction of the deviated signal, with zero startup cost. Firstly, a hypothesis testing problem was formulated to detect the presence of an attack. Then, in case of an attack detection, we estimated the leading eigenvector of the population covariance matrix as a fundamental phase prior to the jamming cancellation. Furthermore, these findings were also computed using the SDP technique. Simulation results prove the efficiency of the proposed method in various aspects. Vulnerability of 5G NR from this physical channel motivates researchers to further studies in this direction.

Appendix

Under $\mathcal{H}_0$: Let unit sphere $\mathbf{R}^\Omega$ be a subset of $\mathbf{R}^p$, i.e., $\Omega \subset \{1, ..., p\}$, with the cardinality $|\Omega| = k$, and $\hat{\mathbf{\Sigma}}_\Omega$ denotes the $k \times k$ submatrix of the finite set Ω, with elements $(\hat{\mathbf{\Sigma}}_{i,j})_{\{i,j\}\in\Omega}$. Then, we have $\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \triangleq \max_{\|\Omega\|=k} \lambda_{max}(\hat{\mathbf{\Sigma}}_\Omega) \triangleq \max_{\mathbf{v}_n \in \mathcal{M}_\mathbf{v}} \mathbf{v}_n^T \hat{\mathbf{\Sigma}} \mathbf{v}_n$ and $\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \triangleq 1 + \max_{\|\Omega\|=k} \{\lambda_{max}(\hat{\mathbf{\Sigma}}_\Omega) - 1\}$ for $\hat{\mathbf{\Sigma}} \succeq 0$. We denote $\dot{\mathbf{v}}_n$ and $\ddot{\mathbf{v}}_n$ respectively as the sparse principal components in the spaces $\mathbf{R}^\Omega$ and $\mathbf{R}^k$, such that $\dot{\mathbf{v}}_n = \ddot{\mathbf{v}}_n$ and $\|\dot{\mathbf{v}}_n\|_2 = \|\ddot{\mathbf{v}}_n\|_2 = 1$. Therefore, we have

$$\dot{\mathbf{v}}_n^T \hat{\Sigma}_\Omega \dot{\mathbf{v}}_n - 1 = \ddot{\mathbf{v}}_n^T \hat{\Sigma} \ddot{\mathbf{v}}_n - 1 = \frac{1}{N}\sum_{n=1}^N [(\dot{\mathbf{v}}_n^T \hat{\mathbf{y}}_n)^2 - 1]. \quad (25)$$

Referring to Lemma 1 in [12], the following tail bound holds for any positive x

$$\mathbf{P}\left(\frac{1}{N}\sum_{n=1}^N [(\dot{\mathbf{v}}_n^T \hat{\mathbf{y}}_n)^2 - 1] \geq 2\sqrt{\frac{x}{N}} + 2\frac{x}{N}\right) \leq e^{-x}. \quad (26)$$

Using a $1/4$-net over $\mathbf{R}^\Omega$, there is $\mathcal{N}_\Omega$ as a subset of $\mathbf{R}^\Omega$ with cardinality smaller than 9^k, such that the inequality $\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \leq 2 \max_{\mathbf{v}_n \in \mathcal{N}_\Omega} \mathbf{v}_n^T \hat{\mathbf{\Sigma}} \mathbf{v}_n$ holds for any $\hat{\mathbf{\Sigma}} \succeq 0$ [11]. Therefore, with the definition of $\Psi_\Omega = \big\{\lambda_{max}(\hat{\mathbf{\Sigma}}_\Omega) - 1 \geq 4\sqrt{\frac{x}{N}} + 4\frac{x}{N}\big\}$ and using Boole's inequality for any $x > 0$, we have

$$\mathbf{P}(\Psi_\Omega) \leq \mathbf{P}\left(\max_{\mathbf{v}_n \in \mathcal{N}_\Omega} \frac{1}{N}\sum_{n=1}^N (\mathbf{v}_n^T \hat{\mathbf{y}}_n)^2 - 1 \geq 2\sqrt{\frac{x}{N}} + 2\frac{x}{N}\right) \leq 9^k e^{-x}. \quad (27)$$

We define the new event $\Psi = \bigcup_{|\Omega|=k} \Psi_\Omega = \max_{|\Omega|=k} \{\lambda_{max}(\hat{\mathbf{\Sigma}}_\Omega) - 1\} \geq 4\sqrt{\frac{x}{N}} + 4\frac{x}{N}$. Let $C_{p,k}$ be the combinatorial number of parameters k and p. The Boole's inequality on the $C_{p,k}$ subsets of Ω yields $\mathbf{P}\Big(\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \geq 1 + 4\sqrt{\frac{x}{N}} + 4\frac{x}{N}\Big) = \mathbf{P}(\Psi) \leq C_{p,k} 9^k e^{-x}$. Finally, using the inequality $C_{p,k} \leq (ep/k)^k$, the upper bound for $\lambda_{max}^k(\hat{\mathbf{\Sigma}})$ is defined as $\tau_0 = 1 + 4\sqrt{\frac{x}{N}} + 4\frac{x}{N}$.

Under $\mathcal{H}_1$: Referring to (2), we have $\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \geq \mathbf{v}_n^T \hat{\mathbf{\Sigma}} \mathbf{v}_n = \frac{1}{N}\sum_{n=1}^N (\hat{\mathbf{y}}_n^T \mathbf{v}_n)^2$. Let $\hat{\mathbf{\Sigma}}_0 = \mathbf{I}_p$, which denotes a $p \times p$ identity matrix. Then, using (3), we have $\hat{\mathbf{y}}_n^T \mathbf{v}_n \sim \mathcal{N}(0, 1 + \theta)$. Let $Z \triangleq \frac{1}{N}\sum_{n=1}^N \left(\frac{(\hat{\mathbf{y}}_n^T \mathbf{v}_n)^2}{1+\theta} - 1\right)$ be a new random variable. Using Lemma 1 in [12], the inequality $\mathbf{P}(Z \leq -2\sqrt{\rho/N}) \leq e^{-\rho}$ holds for any $\rho > 0$. Thus, the following inequality can be simply proved

$$\lambda_{max}^k(\hat{\mathbf{\Sigma}}) \geq 1 + \theta - 2(1+\theta)\sqrt{\frac{\rho}{N}}. \quad (28)$$

References

[1] R. K. Saha and J. M. Cioffi, "Dynamic spectrum sharing for 5G NR and 4G LTE coexistence - a comprehensive review," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 795–835, Jan. 2024.

[2] Z. Lin, H. Niu, K. An, Y. Hu, D. Li, J. Wang, and N. Al-Dhahir, "Pain without gain: Destructive beamforming from a malicious RIS perspective in IoT networks," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7619–7629, Mar. 2024.

[3] Z. Lin, M. Lin, B. Champagne, W.-P. Zhu, and N. Al-Dhahir, "Secrecy-energy efficient hybrid beamforming for satellite-terrestrial integrated networks," *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6345–6360, Jun. 2021.

[4] J. Ma, Q. Li, Z. Liu, L. Du, H. Chen, and N. Ansari, "Jamming modulation: An active anti-jamming scheme," *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2730–2743, Apr. 2023.

[5] P. Zhou, Q. Wang, W. Wang, Y. Hu, and D. Wu, "Near-optimal and practical jamming-resistant energy-efficient cognitive radio communications," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2807–2822, Jun. 2017.

[6] A. Pourranjbar, G. Kaddoum, and W. Saad, "Recurrent-neural-network-based anti-jamming framework for defense against multiple jamming policies," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8799–8811, May 2023.

[7] H. Han, W. Li, Z. Feng, G. Fang, Y. Xu, and Y. Xu, "Proceed from known to unknown: Jamming pattern recognition under open-set setting," *IEEE Wireless Communications Letters*, vol. 11, no. 4, pp. 693–697, Apr. 2022.

[8] X. Chang, Y. Li, Y. Zhao, Y. Du, and D. Liu, "An improved anti-jamming method based on deep reinforcement learning and feature engineering," *IEEE Access*, vol. 10, pp. 69 992–70 000, Jun. 2022.

[9] K. Chen, J. Zhang, S. Chen, S. Zhang, and H. Zhao, "Active jamming mitigation for short-range detection system," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11 446–11 457, Apr. 2023.

[10] S.-D. Wang, H.-M. Wang, W. Wang, and V. C. M. Leung, "Detecting intelligent jamming on physical broadcast channel in 5G NR," *IEEE Communications Letters*, vol. 27, no. 5, pp. 1292–1296, May 2023.

[11] Q. Berthet and P. Rigollet, "Complexity theoretic lower bounds for sparse principal component detection," in *Proceedings of the 26th Annual Conference on Learning Theory*, vol. 30, Princeton, USA, 12-14 Jun. 2013, pp. 1046–1066.

[12] B. Laurent and P. Massart, "Adaptive estimation of a quadratic functional by model selection," *The Annals of Statistics*, vol. 28, no. 5, pp. 1302–1338, Oct. 2000.

[13] A. Nemirovski, "Prox-method with rate of convergence $O(1/t)$ for variational inequalities with lipschitz continuous monotone operators and smooth convex-concave saddle point problems," *SIAM Journal on Optimization*, vol. 15, no. 1, pp. 229–251, 2004.

[14] "Study on channel model for frequencies from 0.5 to 100 GHz, document 3GPP TR 38.901, release 17," Mar. 2022.