

# Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems

Gonzalo J. Anaya-López, José P. González-Coma and F. Javier López-Martínez

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

This is the author's accepted version of the article:

G. J. Anaya-López, J. P. González-Coma, and F. J. López-Martínez, "Leakage Subspace Precoding and Scheduling for Physical Layer Security in Multi-User XL-MIMO Systems," *IEEE Communications Letters*, vol. 27, no. 2, pp. 467–471, Feb. 2023, doi: 10.1109/LCOMM.2022.3225881.

The final published version is available in IEEE Xplore.

**Abstract**—We investigate the achievable secrecy spectral efficiency in a multi-user extra-large multiple-input multiple-output (XL-MIMO) system. In these beyond-5G scenarios, seen as the natural evolution of conventional massive MIMO systems, the distances from the mobile users to the base station become comparable to the antenna array dimensions. We show that the consideration of spherical-wavefront propagation inherent to these set-ups is beneficial for physical-layer security, as it provides immunity against eavesdroppers located in similar angular directions that would otherwise prevent secure communication under classical planar-wavefront propagation. A leakage subspace precoding strategy is also proposed for joint secure precoding and user scheduling, which allows to improve the secrecy spectral efficiency over a 40% compared to conventional zero-forcing methods, under different eavesdropper collusion strategies.

**Index Terms**—Antenna array, XL-MIMO, near-field, physical layer security, secrecy, spectral efficiency, scheduling.

## I. INTRODUCTION

Extra-large aperture arrays (ELAAs) or extra-large (XL) multiple-input multiple-output (MIMO) systems are the natural evolution of massive MIMO systems [1], bringing the opportunity to deploy base stations (BSs) with an even larger number of antenna elements to serve a larger set of users. Since antenna sizes in XL-MIMO deployments become comparable to user distances, new channel features that differ from classical planar-wavefront (PW) [2, 3] and stationarity [4] assumptions have to be incorporated into the precoding design.

Manuscript received July 20, 2022, revised October 24, 2022. The review was coordinated by Dr. Ramón Agüero. The work of G. J. Anaya-López and F. J. López-Martínez was funded by MCIN/AEI/10.13039/501100011033 through grant PID2020-118139RB-I00, by European Social and Regional Funds and by Junta de Andalucía (P18-RT-3175, SNGJ5Y6-57, EMERGIA20 00297). The authors thank the Defense University Center at the Spanish Naval Academy (CUD-ENM) for the support provided for this research.

G.J. Anaya-López and F.J. López-Martínez are with the Communications and Signal Processing Lab, Telecommunication Research Institute (TELMA), Universidad de Málaga, Málaga 29010, Spain. J.P. González-Coma is with Defense University Center at the Spanish Naval Academy, Universidade de Vigo, Marín 36920, Spain. F.J. López-Martínez is also with Dept. Signal Theory, Networking and Communications, Universidad de Granada, Granada 18071, Spain. (contact e-mail: gjal@ic.uma.es.)

One remarkable feature that arises when assuming spherical-wavefront (SW) propagation is the possibility of separating users in the spatial domain using both the angular direction *and* the distance with respect to the BS [5].

In the roadmap to 6G, several new use cases that enhance data security are being proposed [6], and physical layer security (PLS) is identified as a top contender to enable these secure features [7]. The literature of PLS is rich when assuming conventional multi-user MIMO settings [8, 9]. While several strategies have been proposed for secure precoding design [10] and user scheduling [11] in massive MIMO setups, their adequacy to adapt to even larger antenna array deployments has not been addressed. Specifically, to the best of our knowledge the effect of spherical propagation inherent to the channel of XL-MIMO systems has been overlooked so far when analyzing PLS. This fact, together with the idea of using the characteristics of the SW propagation to carry out scheduling based on PLS, are the key aspects to be considered. Hence, in this work we seek to find answers to two key questions: (i) *how does SW propagation impact the secrecy performance in XL-MIMO systems?* (ii) *how can user scheduling be improved when incorporating security constraints into the XL-MIMO set-up?* We show that the user decorrelation with distance experienced under SW propagation [5] can be leveraged to reduce information leakage to eavesdroppers. Thus, if the BS successfully exploits this feature, the achievable secrecy rate substantially increases compared to the conventional PW assumption. To that end, we also propose a joint scheduling and precoding scheme that improves the system secure performance compared to the state of the art.

## II. SYSTEM MODEL

We consider a general downlink (DL) scenario, where a BS equipped with an XL antenna array with  $M \gg 1$  elements gives service to a set  $\mathcal{U}$  of single-antenna users, with  $|\mathcal{U}| = K$ . We assume an uniform linear array (ULA) as the antenna arrangement for the BS. The BS operates in two modes [12]: in *normal* mode, the BS acquires the channel state information (CSI) for the  $K$  DL users and serves them [13] according to some rate maximization criterion; we consider that CSI available at the BS is error-free; in *secure* mode, a set  $\mathcal{B}$  of legitimate users (i.e., Bobs) with  $|\mathcal{B}| = K_B < K$  is served according to a secrecy performance criterion using the CSI acquired in *normal* mode, whereas the remaining set of users  $\mathcal{V}$ , with  $|\mathcal{V}| = K_E = K - K_B$ , are considered as potential eavesdroppers (i.e., Eves). The data intended to each legitimate receiver potentially experiences an amount of

TABLE I: Variables and notation summary.

| Description           | Notation                  | Description                  | Notation                  |
|-----------------------|---------------------------|------------------------------|---------------------------|
| Number of antennas    | $M$                       | Users set                    | $\mathcal{U}$             |
| Number of users       | $K$                       | Legitimate users set         | $\mathcal{B}$             |
| Eavesdroppers set     | $\mathcal{V}$             | Clustered eavesdr. set       | $\mathcal{E}_k$           |
| User distance         | $r_k$                     | User angle                   | $\theta_k$                |
| Antenna spacing       | $d$                       | Wavelength                   | $\lambda$                 |
| Ref. channel power    | $\beta_0$                 | Reference distance           | $r_{\text{ref}}$          |
| Response vector       | $\mathbf{a}_k$            | Precoding vector             | $\mathbf{w}_k$            |
| Data symbol           | $s_k$                     | User power                   | $p_k$                     |
| Noise                 | $n_k$                     | Noise variance               | $\sigma_w^2$              |
| Secrecy spectral eff. | $R_s$                     | User priority                | $q_k$                     |
| Leakage subspace      | $\mathcal{L}$             | Interference subspace        | $\mathcal{I}_{\bar{k}}$   |
| Joint channel matrix  | $\mathbf{A}$              | $k$ -th joint channel matrix | $\mathbf{B}_k$            |
| Selected users set    | $\mathcal{S}$             | Orthogonal projector         | $\mathbf{II}$             |
| Cardinality of a set  | $ \mathcal{C} $           | Complex numbers set          | $\mathbb{C}$              |
| Diagonal matrix       | $\text{diag}(\mathbf{x})$ | Span of matrix columns       | $\text{span}(\mathbf{X})$ |
| Intersection operator | $\cap$                    | Subset operator              | $\subseteq$               |
| Transpose             | $(\cdot)^T$               | Hermitian transpose          | $(\cdot)^H$               |
| Transmitted signal    | $x_k$                     | Received signal              | $y_k$                     |

information leakage, which may be used by the eavesdroppers to compromise the transmission [8].

We consider that the array is centered at the coordinate origin and deployed along the vertical axis of a 2-D plane,  $r_k$  is the distance from the origin to user  $k$ , and  $\theta_k$  the angle formed by a vector starting at the origin and ending at user's  $k$  position. The distance between a given user, indexed by  $k$ , and the  $m$ -th element of the antenna array is defined as

$$r_{k,m} = r_k \sqrt{1 - 2md_k \sin \theta_k + d_k^2 m^2}, \quad m \in \left[-\frac{M}{2}, \frac{M}{2}\right], \quad (1)$$

so that  $r_{k,0} = r_k$ . Moreover,  $d_k = \frac{d}{r_k}$  is determined by the separation between two consecutive antenna elements,  $d = \frac{\lambda}{2}$ , with  $\lambda$  being the wavelength. From (1), we obtain the array response vector for each user as

$$\mathbf{a}_k = [a_1(r_k, \theta_k), a_2(r_k, \theta_k), \dots, a_M(r_k, \theta_k)]^T, \quad (2)$$

where the  $m$ -th element of the vector is expressed, depending on the assumed propagation model, as

$$a_m^{\text{SW}}(r_k, \theta_k) = \frac{\sqrt{\beta_0}}{r_{k,m}} e^{-j\frac{2\pi}{\lambda} r_{k,m}} \quad (3)$$

and

$$a_m^{\text{PW}}(r_k, \theta_k) = \frac{\sqrt{\beta_0}}{r_k} e^{-j\frac{2\pi}{\lambda} r_k} e^{-j2\pi m \sin \theta_k}, \quad (4)$$

respectively, and  $\beta_0$  denotes the channel power at the reference distance  $r_{\text{ref}} = 1$  m [3].

During the DL transmission in *secure* mode, the BS sends the data symbols  $s_k \sim \mathcal{N}_{\mathbb{C}}(0, 1)$  to each legitimate user  $k \in \mathcal{B}$ , by adapting the transmitted signal  $\mathbf{x}$  to the instantaneous CSI acquired in *normal* mode operation through the precoding matrix  $\mathbf{W} \in \mathbb{C}^{M \times K_{\text{B}}}$ , where we define the  $k$ -th column as  $\mathbf{w}_k$ , with  $\|\mathbf{w}_k\| = 1, \forall k \in \mathcal{B}$ . Therefore, it follows that the transmitted signal is  $\mathbf{x} = \sum_{k \in \mathcal{B}} p_k \mathbf{w}_k s_k$ , where  $p_k$  are the power allocation scale factors such that  $P_{\text{TX}} = \sum_{k \in \mathcal{B}} p_k$ , with  $P_{\text{TX}}$  the BS transmit power.

The received signal  $y_k$  for each legitimate user can be expressed in terms of the previously defined parameters as

$$y_k = \sqrt{p_k} s_k \mathbf{w}_k^H \mathbf{a}_k + \sum_{j \neq k; j \in \mathcal{B}} \sqrt{p_j} s_j \mathbf{w}_j^H \mathbf{a}_k + n_k, \quad (5)$$

where the first term in (5) is the desired signal for the legitimate user, the second one is the inter-user interference (IUI) due to legitimate users other than  $k$  being served simultaneously, and  $n_k \sim \mathcal{N}_{\mathbb{C}}(0, \sigma_w^2)$  is the additive white Gaussian noise (AWGN). The signal-to-interference-plus-noise ratio (SINR) for the legitimate users is defined as [14]

$$\text{SINR}_k = \frac{p_k |\mathbf{w}_k^H \mathbf{a}_k|^2}{\sigma_w^2 + \sum_{j \neq k; j \in \mathcal{B}} p_j |\mathbf{w}_j^H \mathbf{a}_k|^2}. \quad (6)$$

Now, the legitimate symbols also reach the remaining users  $v \in \mathcal{V}$ . From the point of view of these users (acting as eavesdroppers), such received signals are information leakage for the message  $s_k$ , not interference. Therefore, a leakage-to-interference-plus-noise ratio (LINR) can be defined as  $\text{LINR}_k(v) = \frac{p_k |\mathbf{w}_k^H \mathbf{a}_v|^2}{\sigma_w^2}$ , which can be seen as the SINR associated to the message  $s_k$  at the  $v$ -th eavesdropper. As in [8], we assume the worst-case scenario on which the eavesdroppers have the ability to separate the  $k$  symbols (either by means of collusion, or in a genie-aided fashion).

We consider two practical scenarios for eavesdropping: (i) total collusion (TC), on which all eavesdroppers  $v \in \mathcal{V}$  collaborate into jointly decoding the message targeted to user  $k$ ; (ii) partial collusion (PC), on which only the eavesdroppers in the vicinity of user  $k$  are able to collude, i.e.,  $v \in \mathcal{E}_k$ , where  $\mathcal{E}_k$  is the set of colluding clustered eavesdroppers for user  $k$ . Hence, by considering jointly interference cancellation for the eavesdroppers, as in [9], the overall LINR is expressed as

$$\text{LINR}_k^{\text{TC/PC}} = \sum_{v \in \mathcal{V}/\mathcal{E}_k} \frac{p_k |\mathbf{w}_k^H \mathbf{a}_v|^2}{\sigma_w^2}. \quad (7)$$

The amount of secure information is measured by the secrecy spectral efficiency, which is given from (6) and (7) as [8, 15]:

$$R_s = \sum_{k \in \mathcal{B}} R_{s,k} = \sum_{k \in \mathcal{B}} \log_2 \left[ \frac{1 + \text{SINR}_k}{1 + \text{LINR}_k^{\text{TC/PC}}} \right]^+. \quad (8)$$

### III. USER SCHEDULING AND PRECODING DESIGN

The aim is to maximize the secrecy spectral efficiency in (8) subject to the power constraint, i.e.,

$$\underset{\{\mathbf{w}_k, p_k\}_{k \in \mathcal{B}}}{\text{argmax}} \quad R_s \quad \text{s.t.} \quad \sum_{k \in \mathcal{B}} p_k \leq P_{\text{TX}}. \quad (9)$$

We note from (6) and (7) that the achievable secrecy spectral efficiency is limited by the interference caused by legitimate users, either because it decreases the SINR of legitimate users, or because it increases the LINR of eavesdroppers. In the XL-MIMO regime, it is known that IUI (and hence information leakage) can be palliated not only by separating users in the angular domain (i.e., through  $\theta_k$ ), but also in the distance domain even for users in the same direction [3]. Thus, this new feature for interference *and* leakage reduction must be considered in order to jointly design the precoder and scheduling for PLS purposes.

There are key differences between conventional joint scheduling and precoding designs [13, 14], and their secure counterparts targeting a secrecy spectral efficiency maximization as the ones here addressed: specifically, (i) the classical spectral efficiency metric is simpler, (ii) only users selected

---

**Algorithm 1** Leakage Subspace Precoding
 

---

```

1:  $i \leftarrow 0, \mathcal{S}^{(0)} \leftarrow \emptyset$ 
2: TC scenario
    $\Pi \leftarrow$  Compute the orthogonal projector into  $\mathcal{L}^\perp$ 
PC scenario
    $\Pi_k \leftarrow$  Compute the orthogonal projector into  $\mathcal{L}_k^\perp, \forall k \in \mathcal{B}$ 
3:  $q_k^{(0)} \leftarrow$  set initial priorities  $\forall k \in \mathcal{B}$ 
4: repeat
5:    $k^{(i)} \leftarrow$  Find highest priority (10),  $\mathcal{S}^{(i+1)} \leftarrow \mathcal{S}^{(i)} \cup \{k^{(i)}\}$ 
6:   TC scenario
      $\mathbf{A}^{(i)} \leftarrow$  Update using (12)
      $\boldsymbol{\omega}_{k^{(j)}} \leftarrow$  Compute TC-ZF precoders (11),  $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$ 
   PC scenario
      $\mathbf{B}_{k^{(j)}}^{(i)} \leftarrow$  Compute using (14),  $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$ 
      $\boldsymbol{\omega}_{k^{(j)}} \leftarrow$  Compute PC-ZF precoders (15),  $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$ 
7:    $\mathbf{w}_{k^{(j)}} \leftarrow$  Normalize  $\boldsymbol{\omega}_{k^{(j)}}, \forall k^{(j)} \in \mathcal{S}^{(i+1)}$ 
8:    $p_{k^{(j)}} \leftarrow$  Power allocation using waterfilling,  $\forall k^{(j)} \in \mathcal{S}^{(i+1)}$ 
9:    $q_k^{(i+1)} \leftarrow$  Update user priorities with (13)
10:   $\mathcal{B} \leftarrow \mathcal{B} \setminus \{k^{(i)}\}, i \leftarrow i + 1$ 
11: until  $\mathcal{B} = \emptyset$  or stopping criterion is met
  
```

---

by the scheduling procedure are considered to compute IUI, and (iii) information leakage to unscheduled users (i.e., Eves) is ignored. In the sequel, we describe a Leakage Subspace Precoding (LSP) approach for secure joint scheduling and precoding in this scenario (see Alg. 1), considering two collusion strategies for the eavesdroppers as detailed next:

1) *TC scenario*. This corresponds to the conventional worst-case collusion where all the eavesdroppers share information to decode data of the legitimate users. According to the LINR definition in (7), to avoid information leakage we propose to define a leakage subspace  $\mathcal{L}$ , spanned by the channel vectors of the eavesdroppers, i.e.,  $\mathcal{L} = \text{span}(\mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \dots, \mathbf{a}_{v_{K_E}})$ . Now, if the precoders associated to each legitimate user belong to the orthogonal subspace  $\mathcal{L}^\perp$ , we ensure that  $\text{LINR}_k^{\text{TC}} = 0$  in (8). Under this condition, it is simpler to decide which legitimate users will be allocated power.

The iterative procedure starts by setting an initial priority for each of the legitimate users  $q_k^{(0)}, \forall k \in \mathcal{B}$ , computed as  $q_k^{(0)} = \|\Pi \mathbf{a}_k\|$ , where  $\Pi$  is the orthogonal projector into the subspace  $\mathcal{L}^\perp$ . Next, similar to [14], we start an iterative procedure such that at the  $i$ -th iteration the user with higher priority, i.e.,

$$k^{(i)} = \underset{k \in \mathcal{B}}{\text{argmax}} (q_k^{(i)}) \quad (10)$$

is chosen as a candidate to receive a certain amount of the available power budget  $P_{\text{TX}}$ . To verify whether including the candidate user  $k^{(i)}$  increases the performance metric (8), we compute TC-zero-forcing (ZF) precoders for the set of users,  $\mathcal{S}^{(i)} \subseteq \mathcal{B}$ , comprising the previously selected users at iteration  $i$  plus the candidate user  $k^{(i)}$  as

$$[\boldsymbol{\omega}_{k^{(1)}}, \dots, \boldsymbol{\omega}_{k^{(i)}}] = \Pi^* (\mathbf{A}^{(i)})^H (\mathbf{A}^{(i)} \Pi^* (\mathbf{A}^{(i)})^H)^{-1}, \quad (11)$$

$$\text{where } \mathbf{A}^{(i)} = [\mathbf{a}_{k^{(1)}}, \mathbf{a}_{k^{(2)}}, \dots, \mathbf{a}_{k^{(i)}}]^T, \forall k \in \mathcal{S}^{(i)}. \quad (12)$$

Note that the projector  $\Pi$  is included in the computation of the TC-ZF precoders. Now, for  $k \in \mathcal{S}^{(i)}$  we denote by  $\mathcal{T}_k^{(i)} = \text{span}(\mathbf{a}_{j_1}, \mathbf{a}_{j_2}, \dots, \mathbf{a}_{j_{i-1}})$  the subspace spanned by the channels of the  $i-1$  legitimate users in  $\mathcal{S}^{(i)}$ , with  $j_1, \dots, j_{i-1} \neq k$ . Hence, the feasible subspace for user  $k$  precoding is given by  $(\mathcal{T}_k^{(i)})^\perp \cap \mathcal{L}^\perp$ . As the spatial characteristics of the channels strongly depend on the propagation

model [3], the interference *and* leakage reduction provided by the distance in the SW model [3] offers additional flexibility in the precoder design compared to the PW case. Finally, the precoders for each of the selected legitimate users is  $\mathbf{w}_k = \boldsymbol{\omega}_k / \|\boldsymbol{\omega}_k\|$ ,  $\forall k \in \mathcal{S}^{(i)}$  and the power allocation  $\mathbf{P}$  is chosen according to conventional waterfilling procedure [14], with  $P_{\text{TX}} = \sum_{k \in \mathcal{S}^{(i)}} p_k$ . Note that zero power allocation to artificial noise transmission is optimal for (8) in scenarios without fading or with multiple cooperative eavesdroppers [16], as the scenario under consideration. In addition, at each iteration  $i$ , it is important to update the priorities according to the interference caused by the user selected in previous iterations, that is

$$q_k^{(i)} = \left\| \left( \Pi - \sum_{j=1}^{i-1} \mathbf{w}_{k_j}^{(j)} (\mathbf{w}_{k_j}^{(j)})^H \right) \mathbf{a}_k \right\|, \quad (13)$$

where  $\mathbf{w}_{k_j}^{(j)}$  is the precoder obtained at the iteration  $j$  for the selected user  $k_j$ . The iterative procedure continues incorporating these candidate users as selected users if the new candidate improves the secrecy spectral efficiency; otherwise, it is discarded and the iterative procedure ends. Non-served users will be allocated in a different time/frequency resource.

2) *Partial colluding scenario*. Here, we consider a more practical situation where only the subset of eavesdroppers  $\mathcal{E}_k \subseteq \mathcal{V}$  located on the vicinity of the legitimate user  $k \in \mathcal{B}$  are likely to intercept its data, i.e.,  $\theta_v$  and  $r_v$  ( $\forall v \in \mathcal{E}_k$ ) are similar to  $\theta_k$  and  $r_k$ . These eavesdroppers belonging to  $\mathcal{E}_k$  collude to decode the information of legitimate user  $k$ . Since the set of eavesdroppers able to collude is smaller than in the TC case, this can be taken advantage of in the precoding design.

A glimpse of the procedure is captured in Alg. 1, since it follows the same lines as in the TC case. Nevertheless, the legitimate user priorities  $q_k$  and the precoder design have to incorporate the particularities of (7). Contrary to TC, in the PC case each user has its own leakage subspace defined by  $\mathcal{L}_k = \text{span}(\mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \dots, \mathbf{a}_{v_{|\mathcal{E}_k|}})$  and  $v_1, v_2, \dots, v_{|\mathcal{E}_k|} \in \mathcal{E}_k$ . Thus, we only need to guarantee that the precoder for the user  $k$  lies in the subspace  $\mathcal{L}_k^\perp$  to force the condition  $\text{LINR}_k^{\text{PC}} = 0$ , thereby simplifying the objective function in (9). To that end, we define the orthogonal projector into the subspace  $\mathcal{L}_k^\perp$  as  $\Pi_k$  and set the initial priorities as  $q_k^{(0)} = \|\Pi_k \mathbf{a}_k\|$ , such that only the eavesdroppers in  $\mathcal{E}_k$  affect whether user  $k$  is scheduled or not. Then, the iterative procedure starts and the candidate user selection at the  $i$ -th iteration is performed using (10). Notice that the TC-ZF precoding design in (11) is not valid in this scenario, as the leakage subspace is not common to all the users. As such, for each  $k \in \mathcal{S}^{(i)}$  we define the matrix

$$\mathbf{B}_k^{(i)} = [\mathbf{a}_k, \mathbf{a}_{j_1}, \mathbf{a}_{j_2}, \dots, \mathbf{a}_{j_{i-1}}, \mathbf{a}_{v_1}, \mathbf{a}_{v_2}, \dots, \mathbf{a}_{v_{|\mathcal{E}_k|}}]^T, \quad (14)$$

where we included the channel vectors for user  $k$ , for the  $i-1$  users in  $\mathcal{S}^{(i)}$  such that  $j_1, \dots, j_{i-1} \neq k$ , and the ones for the eavesdroppers  $v_1, v_2, \dots, v_{|\mathcal{E}_k|} \in \mathcal{E}_k$ . Then, the PC-ZF precoder is computed as

$$\boldsymbol{\omega}_k = \left[ (\mathbf{B}_k^{(i)})^H (\mathbf{B}_k^{(i)} (\mathbf{B}_k^{(i)})^H)^{-1} \right]_{:,1}, \quad (15)$$

TABLE II: Simulation parameter settings.

| Parameter                            | Value                                      |
|--------------------------------------|--------------------------------------------|
| Channel realizations                 | 1000                                       |
| # legitimate users                   | $K_B = [10, 20]$                           |
| # eavesdroppers per Bob              | $k_e = [2^{TC}, 6^{PC}]$                   |
| Wavelength                           | $\lambda = 0.1249$ m                       |
| Distance between antennas            | $d = \frac{\lambda}{2}$ m                  |
| Number of antennas                   | $M = 100$                                  |
| Transmit signal-to-noise ratio (SNR) | $[0, 5, 10, 15, 20, 25]$ dB                |
| Rayleigh distance                    | $r_{\text{Rayl}} = \frac{2D^2}{\lambda}$ m |
| Critical distance [2]                | $r_{\text{Crit}} \approx 9D$ m             |
| Distance range                       | $[3r_{\text{Crit}}, r_{\text{Rayl}}]$ m    |
| Angular range                        | $[-\frac{\pi}{4}, \frac{\pi}{4}]$ rad      |

i.e., the first column of the former matrix computation. As such, we ensure that the precoder for each user  $k \in \mathcal{S}^{(i)}$  belongs to the intersection of the subspaces  $(\mathcal{T}_k^{(i)})^\perp \cap \mathcal{L}_k^\perp$ . Again, the precoders are normalized by  $\mathbf{w}_k = \boldsymbol{\omega}_k / \|\boldsymbol{\omega}_k\|$ ,  $\forall k \in \mathcal{S}^{(i)}$  and waterfilling is used for power allocation  $\mathbf{P}$ . Regarding the update of the priorities in (13), the same expression can be used but now including the projector  $\mathbf{I}_{\mathbf{k}}$ .

The key difference of this second scenario is that the legitimate user  $k$  is only forced to deal with the LINR corresponding to those eavesdroppers clustered around him, which in turn are known to be the more detrimental ones for physical layer security [17]. Therefore, the available degrees of freedom for precoding design are larger, in general, than in the TC scenario. This additional flexibility will be more effectively exploited under the SW model, taking advantage of the interference and leakage reduction provided by distance.

It is important to remark that the computational complexity of the iterations in Alg. 1 is  $\mathcal{O}(2Mi^2 + i^3 + 3M(|\mathcal{B}| - i))$  for TC and  $\mathcal{O}(2Mi(i + |\mathcal{E}_k|)^2 + i(i + |\mathcal{E}_k|)^3) + 3M(|\mathcal{B}| - i))$  for PC. That is, it scales linearly with  $M$  as in conventional ZF.

#### IV. NUMERICAL RESULTS

We now evaluate the performance of the joint secure precoding and scheduling LSP schemes, and investigate the impact of SW propagation in the XL-MIMO regime compared to the case of incorrectly assuming PW propagation. In addition, we compare LSP with a conventional scheme in the PLS literature: ZF precoding with waterfilling [8]. We consider a BS with  $M = 100$  antennas equispaced  $d = \lambda/2$ , giving service to a set of randomly located users as follows:  $K_B$  legitimate users are deployed randomly along the coverage region described in Table II at positions  $\theta_k$  and  $r_k$ ; then, a number of eavesdroppers  $k_e$  is deployed in the vicinity of each legitimate user at positions  $\theta_{e,k}$  and  $r_{e,k}$ , for  $e = 1 \dots k_e$ , so that  $K_E = K_B \cdot k_e$ . Specifically, one eavesdropper is always located approximately in the same angular direction as user  $k$  (i.e.,  $\theta_{1,k} = \theta_k + \Delta_k$ , with  $\Delta_k \sim \mathcal{U}[\pm 0.1^\circ]$ ), and  $r_p$  meters closer to the BS. The remaining  $e = 2 \dots k_e$  eavesdroppers are deployed at a distance  $r_q = r_{\text{Crit}}$  m from Bob (i.e.,  $r_q$  is the radius of a protected zone, on which no eavesdroppers are placed close to Bob) and a certain  $\theta_{e,k}$ .

The secrecy spectral efficiency (Fig. 1) and the number of served legitimate users (Fig. 2) are shown for the case of the TC scenario, worst-case situation [8] where all the

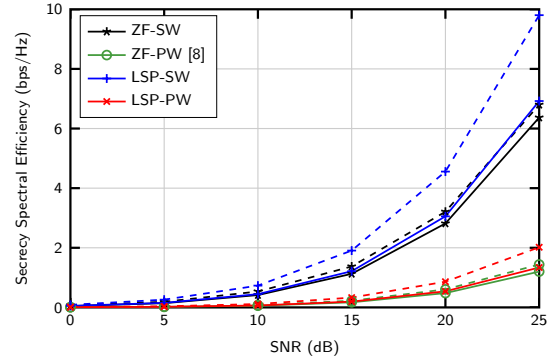


Fig. 1: Secrecy spectral efficiency in the TC scenario, considering SW and PW propagation and different precoding strategies. Solid/dashed lines correspond to ( $K_B = 10$ ) and ( $K_B = 20$ ), respectively.

eavesdroppers cooperate to decode the legitimate messages, under the PW and SW propagation models. Solid and dashed lines denote the cases with  $K_B = \{10, 20\}$  legitimate users, respectively, and the remaining set of parameters is listed in Table II, with  $r_p = 2r_q$  and  $D = Md$ . From the observation of Fig. 1, some remarks are in order: (i) under the PW model, the secrecy spectral efficiency is reduced due to the position of the eavesdroppers, and chiefly those located in similar angular directions as the legitimate users; (ii) the consideration of the SW model allows to improve the secure transmission spectral efficiencies up to 44.21% and to serve more users, since legitimate users and eavesdroppers with similar angular directions are decorrelated with distance [3]; (iii) increasing the number of legitimate users notably improves the secrecy spectral efficiency in the SW case, which is not the case when considering PW; (iv) although the number of served users is not the metric being optimized, we see that in this setting LSP manages to improve *both* the secrecy spectral efficiency and the average number of served users when  $K_B = 20$ , compared to conventional ZF precoding [8]. Note that both ZF and LSP resort to waterfilling to determine the power allocation. As a consequence, the use of this method is directly related to the number of legitimate users being allocated power. Indeed, users receive power only if their effective channel gain, i.e., the gain obtained when the information leakage and the interference from the other legitimate users are removed, are over a certain threshold, say  $\mu$ . The value of  $\mu$  increases with the number of users receiving power, and decreases with the SNR and the effective channel gains. Accordingly, since ZF approach gets, in general, more balanced effective gains as users are not prioritized as in LSP, we can expect that the number of served users is larger when using ZF compared to LSP. This intuition can, however, fail when the SNR and/or the effective channel gains are not large enough, as we can see in Fig. 2. Thus, the increase on  $\mu$  due to the number of served legitimate users cannot be compensated due the poor effective channel gains obtained in this scenario.

The secrecy spectral efficiency (Fig. 3) and the number of served legitimate users (Fig. 4) are shown for the case of the PC scenario, under the PW and SW propagation models. We increase  $k_e = 6$  so that each legitimate user is affected

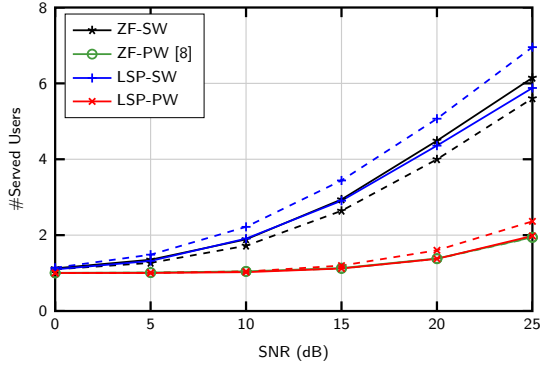


Fig. 2: Number of served users in the TC scenario, considering SW and PW propagation and different precoding strategies. Solid/dashed lines correspond to ( $K_B = 10$ ) and ( $K_B = 20$ ), respectively.

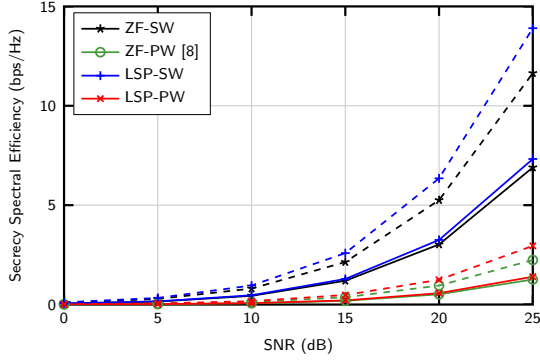


Fig. 3: Secrecy spectral efficiency in the PC scenario, considering SW and PW propagation and different precoding strategies. Solid/dashed lines correspond to ( $K_B = 10$ ) and ( $K_B = 20$ ), respectively.

by a larger number of potentially detrimental eavesdroppers compared to the TC case. These new eavesdroppers are deployed at a distance  $r_q/2$  from Bob with the angles  $\theta_{e,k}$  uniformly distributed. From the new two figures, Fig. 3 and Fig. 4, we extract several remarks: (i) under the PW model, the secrecy spectral efficiency is low because close-by eavesdroppers have a dominant effect; (ii) this is not the case when considering SW propagation, under which the secrecy spectral efficiency improves by taking advantage of the attenuation of leakage with distance up to 19.41%; (iii) recall that ZF is forced to compute interference cancellation for *all* users, regardless whether they may not be allocated any power in the waterfilling procedure. As the information leakage is not as severe as in the TC case, the effective channel gains are larger than in the previous scenario. Therefore, LSP prioritizes users with large effective channel gains, whereas ZF distributes the power among legitimate users whose effective channel gains are more evenly distributed. Thus, LSP achieves better secrecy spectral efficiencies despite serving fewer users, an effect directly related to SNR, which is better appreciated in high-SNR regimes.

## V. CONCLUSION

We showed that considering SW propagation in XL-MIMO allows to significantly reduce information leakage to eavesdroppers in the same angular directions, compared to PW

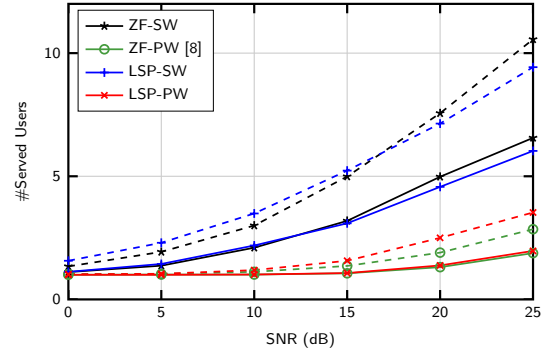


Fig. 4: Number of served users in the PC scenario, considering SW and PW propagation and different precoding strategies. Solid/dashed lines correspond to ( $K_B = 10$ ) and ( $K_B = 20$ ), respectively.

propagation. Higher secrecy rates and more served users can be achieved in DL multi-user scenarios under SW propagation, specially in the worst case scenario on which all eavesdroppers collude. We proposed a novel scheduling and precoding strategy that outperforms conventional ZF strategies, yielding a  $\sim 40\%$  improvement in terms of secrecy spectral efficiency. Future work will deal with practical channel estimation set-ups, including the effect of imperfect CSI and the cost of channel acquisition in the overall throughput.

## REFERENCES

- [1] E. D. Carvalho, A. Ali, A. Amiri, M. Angelichinoski, and R. W. Heath, "Non-Stationarities in Extra-Large-Scale Massive MIMO," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 74–80, 2020.
- [2] H. Lu and Y. Zeng, "How does performance scale with antenna number for extremely large-scale mimo?" in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.
- [3] —, "Communicating with Extremely Large-Scale Array/Surface: Unified Modelling and Performance Analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4039–4053, 2022.
- [4] A. Ali, E. D. Carvalho, and R. W. Heath, "Linear Receivers in Non-Stationary Massive MIMO Channels With Visibility Regions," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 885–888, 2019.
- [5] H. Lu and Y. Zeng, "Near-Field Modeling and Performance Analysis for Multi-User Extremely Large-Scale MIMO Communication," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 277–281, 2022.
- [6] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, 2020.
- [7] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 2021.
- [8] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy Sum-Rates for Multi-User MIMO Regularized Channel Inversion Precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, 2012.
- [9] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy Rates in Broadcast Channels with Confidential Messages and External Eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, 2014.
- [10] S. J. Maeng, Y. Yapıcı, İ. Güvenç, A. Bhuyan, and H. Dai, "Precoder Design for Physical-Layer Security and Authentication in Massive MIMO UAV Communications," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 2949–2964, 2022.
- [11] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-Aided Secure Communications With Cooperative Jamming," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9385–9392, 2018.
- [12] G. J. Anaya-Lopez, G. Gomez, and F. J. Lopez-Martinez, "A Product Channel Attack to Wireless Physical Layer Security," *IEEE Wireless Commun. Lett.*, vol. 10, no. 5, pp. 943–947, 2021.
- [13] J. P. González-Coma, F. J. López-Martínez, and L. Castedo, "Low-Complexity Distance-Based Scheduling for Multi-User XL-MIMO Sys-

tems," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2407–2411, 2021.

- [14] Taesang Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 528–541, 2006.
- [15] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.
- [16] M. Khojastehnia and S. Loyka, "To Jam or Not to Jam in Gaussian MIMO Wiretap Channels?: Invited Paper," in *2021 17th Int. Symp. on Wireless Communication Systems (ISWCS)*, 2021, pp. 1–6.
- [17] Á. Vázquez-Castro and M. Hayashi, "Physical layer security for rf satellite channels in the finite-length regime," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 981–993, 2018.