Coding-aware secure beamforming in cell-free networks

Guillaume Thiran, Luc Vandendorpe

ICTEAM, UCLouvain - Louvain-la-Neuve, Belgium
{guillaume.thiran,luc.vandendorpe}@uclouvain.be

***Abstract*—Secure beamforming methods are difficult to scale with the number of eavesdroppers and transmitters, as traditional security requires each transmitter-eavesdropper link to be secure. When messages are linearly coded together prior to the transmission, the communications are secure even if the eavesdropper receives all but one of the packets. As this fundamentally changes the way beamforming should be performed, this paper studies the coding-aware beamforming design in cell-free networks, with several transmitters, receivers, and eavesdroppers. A non-convex optimisation problem is formulated, which minimises the information leakage towards any eavesdropper while ensuring the receivers have a sufficient signal-to-interference-plus-noise ratio. A local optimum of this problem is obtained through sequential minimisation. The sub-problems which must be solved by the transmitters are shown to be convex, and they are tackled through conic optimisation. Numerical validations are performed, showing that secure communications are possible even when there are many eavesdroppers, and when some of them are located between the receivers and one of the transmitters. Trade-offs between security, rate, and the closeness of the eavesdroppers are moreover studied, demonstrating the improvements brought by the coding-aware beamformers.**

***Index Terms*—Secure communications, cell-free, near-field, beamforming design**

I. Introduction

Designing communication schemes which are able to simultaneously provide information to targeted users while preventing information leakage towards eavesdroppers is a challenging task. The bottom line of the concept of secure communication is that security can be achieved when the channel between the transmitter and the legitimate User Equipment (UE) is of superior quality than the one towards the eavesdropper. In that context, secure beamforming schemes try to degrade as much as possible the eavesdropper channel while guaranteeing a sufficient channel quality towards the targeted UE [1]. When multiple transmitters send unprotected data, and when there are several eavesdroppers, such a beamforming design becomes extremely challenging, as each transmitter must blind every eavesdropper. Moreover, the feasibility of such an approach depends on the scene geometry, since it is almost impossible to handle eavesdroppers located close to the receiver, or on the Line-of-Sight (LoS) communication paths.

To tackle these challenges, a coded security scheme has been designed in [2], working with parallel communication channels. In the original setting, a single transmitter operates on K orthogonal frequency bands. Instead of sending the raw signals on each band, the secure scheme sends K independent linear combinations of the K signals, one combination on each band. The targeted UE, upon reception of the K linear combinations, is able to recover the K signals. However, as soon as an eavesdropper misses one of the combinations, the recovery of the signals is impossible. This impossibility is proven in terms of zero mutual information between the received linear combinations and any of the raw signals.

When utilising such parallel coding scheme [2], the goal is to prevent the eavesdroppers from getting at least one of the signals, for instance by exploiting frequency-dependent antenna radiation patterns [3], or adaptive beamformers [4]. Both schemes however consider a single transmitter, and they thus fail to provide secure communications when eavesdroppers are aligned with the legitimate UE. By illuminating the scene from different directions, the distributed Access-Points (APs) of Cell-Free (CF) networks offer a unique opportunity to solve this challenge. Additionnally to the traditional array gain [5], a security gain can achieved by leveraging on the parallel coding scheme of [2], with beamformers ensuring that each eavesdropper does not receive one of the coded message.

To the authors' knowledge, designing such coding-aware beamformers ensuring physical layer security in a CF network, is an open challenge. This paper fills this gap by providing the following contributions:

- A coding-aware beamforming design problem is formulated, which leverages upon the secure parallel communication scheme of [2], for CF networks with multiple transmitters, receivers and eavesdroppers.
- Locally optimal beamformers are obtained as the output of a successive minimisation algorithm. The sub-problems which must be tackled are reformulated in a standard convex conic form, so that they can efficiently be solved at each iteration.
- The beamforming methods are validated numerically, showing significant gains with respect to traditional secure beamformers. In particular, the security-rate trade-off, as well as the security-eavesdropper closeness trade-off is emphasised.

To that aim, the system model is presented and the coding-aware beamforming optimisation problem is formulated in

Guillaume Thiran is a Research Fellow of the Fonds de la Recherche Scientifique - FNRS.

Section II. It is then solved in Section III, and numerically validated in Section IV.

II. System Model

A CF network is considered, with L UEs and M eavesdroppers, all equipped with a single-antenna. They are located respectively at $\{\mathbf{y}_l\}_l$, and $\{\mathbf{z}_m\}_m$, the notation $\{\cdot\}_l$ implicitely denoting $\{\cdot\}_{l=1}^{L}$, and similarly for the other indices. The eavesdroppers are associated with positive weights $\{\beta_{l,m}\}_{l,m}$ which depict the relative importance of the mth eavesdropper for the lth UE, $\beta_{l,m} = 0$ implying it is not considered as a malicious user. These weights enable among others to include the UEs in the eavesdroppers' set, but to have a 0 weight for each UE with respect to himself. In order to provide secure communications, the following strategy is investigated. The CF network splits its communication resources into K orthogonal Resource Elements (REs), typically in the time or frequency domain. For each lth UE, it processes blocks of K symbols denoted $\{s_{k,l}\}_{k=1}^{K}$, which are allocated to the K REs. As the UEs share the same resources, interference occur on each RE, and thus there different locations are exploited to separate them in the space domain thanks to the beamforming design. To that aim, each RE is served by N_k antennas of the CF network. These antennas might be identical for all REs, but they might also be different. The channel vector of the kth RE towards an antenna at location $\mathbf{p}$ is denoted $\mathbf{h}_{k,(\mathbf{p})}$. Considering LoS propagation, it is given by [6]

$$\mathbf{h}_{k,(\mathbf{p})}^{\mathrm{H}} = \left[L\left(r_{(k,\mathbf{p})}^{(1)}\right) e^{-j\frac{2\pi}{\lambda_k} r_{(k,\mathbf{p})}^{(1)}}, \ldots, L\left(r_{k,(\mathbf{p})}^{(N_k)}\right) e^{-j\frac{2\pi}{\lambda_k} r_{k,(\mathbf{p})}^{(N_k)}} \right],$$

with $r_{k,(\mathbf{p})}^{(n)}$ the distance between the nth antenna of the kth RE and the location $\mathbf{p}$, $L(r)$ the channel gain function, and λ_k the wavelength associated with the kth RE carrier frequency. The signal received on the kth RE at a location $\mathbf{p}$ reads thus as

$$r_{k,(\mathbf{p})} = \sum_{l=1}^{L} \mathbf{h}_{k,(\mathbf{p})}^{\mathrm{H}} \mathbf{w}_{k,l} s_{k,l} + n_k,$$

with $\mathbf{w}_{k,l} \in \mathbb{C}^{N_k}$ the beamforming vector of the symbol $s_{k,l}$, and n_k the Additive White Gaussian Noise (AWGN) realisation of the kth RE, with variance σ_n^2. Considering the Multi-User Interference (MUI) as noise, the Signal-to-Interference-plus-Noise Ratio (SINR) of the kth symbol of the lth UE is thus given by

$$\mathrm{SINR}_{k,l} = \frac{\left|\mathbf{h}_{k,l}^{\mathrm{H}} \mathbf{w}_{k,l}\right|^2}{\sigma_n^2 + \sum_{l' \neq l} \left|\mathbf{h}_{k,l}^{\mathrm{H}} \mathbf{w}_{k,l'}\right|^2}, \tag{1}$$

considering unit-energy symbols, and with $\mathbf{h}_{k,l} \triangleq \mathbf{h}_{k,(\mathbf{y}_l)}$. To mitigate the MUI, techniques such as successive interference cancellation could be employed. Yet, they are difficult to operate in practical settings. Thus, the above SINR expression is considered, providing in any case a lower bound to the actual SINR. On the contrary, to ensure secure communications, the eavesdroppers must be assumed to be performant enough to successfully suppress all MUI. The mth eavesdropper is thus impacted by the following Signal-to-Noise Ratio (SNR) for the symbol k of the lth user:

$$\mathrm{SNR}_{k,l,m} = \frac{\left|\mathbf{g}_{k,m}^{\mathrm{H}} \mathbf{w}_{k,l}\right|^2}{\sigma_n^2}, \tag{2}$$

with $\mathbf{g}_{k,m} \triangleq \mathbf{h}_{k,(\mathbf{z}_m)}$. The eavesdroppers are associated with an SNR sensitivity δ, or equivalently a power sensitivity $\delta\sigma_n^2$, under which they are unable to perform decoding [2].

Two possibilities are investigated for the symbols $s_{k,l}$. In the traditional case, the symbols $s_{k,l}$ are the information symbols $u_{k,l}$, and they are thus all sensitive to information leakage. In the second-case, the scheme of [2] is employed, meaning the K symbols of the lth UE are obtained as an invertible linear transform of its K information symbols. Such a rate-one linear coding has the following properties: i) upon reception of the K linear combinations, the linear system can be inverted to recover the information messages, and ii) as soon as one of the linear combinations is missing, none of the information messages cannot be recovered [2]. It should be emphasised that such an impossibility can be proven in terms of zero mutual information, and thus that it is an information-theoretic guarantee, stronger than a cryptographic one.

Given $\mathbf{w} \triangleq \{\mathbf{w}_{k,l}\}_{k,l}$, the information leakage metrics of the lth user towards the mth eavesdropper are defined, respectively in the traditional and coded case, as

$$\overline{\mathcal{L}}_{l,m}(\mathbf{w}) \triangleq \max_{k=1,\ldots K} \max\{\mathrm{SNR}_{k,l,m} - \delta, 0\}, \tag{3}$$

$$\underline{\mathcal{L}}_{l,m}(\mathbf{w}) \triangleq \min_{k=1,\ldots K} \max\{\mathrm{SNR}_{k,l,m} - \delta, 0\}. \tag{4}$$

In the traditional case, as all symbols contain uncoded sensitive information, the RE with the highest SNR impacts the information leakage. Contrarily, thanks to the linear coding scheme, the resource with the lowest SNR matters in the second case. In both cases, if the metric is equal to 0, then secure communications are guaranteed. As it will be discussed below, minimising $\underline{\mathcal{L}}_{l,m}(\mathbf{w})$ is difficult since it is neither convex, nor convex in the beamforming vectors of one RE, with those of the other REs fixed. Hence, even considering each RE sub-problem leads to a complicated optimisation. The metric $\underline{\mathcal{K}}_{l,m}$ is hence introduced as a proxy to the above as

$$\underline{\mathcal{K}}_{l,m}(\mathbf{w}) \triangleq \prod_{k=1}^{K} \max\{\mathrm{SNR}_{k,l,m} - \delta, 0\}. \tag{5}$$

From the generalised mean inequality, it satisfies $0 \leq \underline{\mathcal{L}}_{l,m} \leq \sqrt[K]{\underline{\mathcal{K}}_{l,m}}$, providing an upper-bound to the information leakage, and ensuring secure communications when $\underline{\mathcal{K}}_{l,m} = 0$. While the above is still not convex, its advantage is that it is convex in each RE beamforming vectors $\{\mathbf{w}_{k,l}\}_{l=1}^{L}$ when the others are considered fixed. This thus opens the way to decentralised methods reaching local optima, such as sequential minimisation [7].

Given these elements, the beamformers are designed to minimise the information leakage, while fulfilling SINR requirements ensuring that the symbols $s_{k,l}$ are correctly decoded,

and with a power constraint for each RE. In the traditional case, it reads thus as

$$\begin{aligned} \min_{\mathbf{w}} \quad & \textstyle\sum_{l=1}^{L}\sum_{m=1}^{M}\beta_{l,m}\overline{\mathcal{L}}_{l,m}(\mathbf{w}) \\ \text{s.t.} \quad & \text{SINR}_{k,l}\geq\theta_l,\forall k,\forall l, \\ & \textstyle\sum_{l=1}^{L}\|\mathbf{w}_{k,l}\|_2^2\leq 1,\forall k, \end{aligned} \tag{6}$$

with the weights $\beta_{l,m}$, and θ_l the SINR requirement of the lth UE. In the above, the notations $\forall k$ implicitly denote $\forall k = 1,\dots,K$, and similarly for the other indices. Similarly, the optimisation problem in the case of linear coding is obtained as

$$\begin{aligned} \min_{\mathbf{w}} \quad & \textstyle\sum_{l=1}^{L}\sum_{m=1}^{M}\beta_{l,m}\underline{\mathcal{L}}_{l,m}(\mathbf{w}) \\ \text{s.t.} \quad & \text{SINR}_{k,l}\geq\theta_l,\forall k,\forall l, \\ & \textstyle\sum_{l=1}^{L}\|\mathbf{w}_{k,l}\|_2^2\leq 1,\forall k, \end{aligned} \tag{7}$$

In the following, (7) will be termed the coding-aware beamforming design problem. In both cases, the optimisation problems require knowing the channel vectors $\mathbf{g}_{k,m}$, and thus the eavesdroppers' positions $\mathbf{z}_m$. If the eavesdroppers are active transmitters, such an information may come from their uplink transmissions to the CF network. Moreover, other systems such as camera's could give the locations of the users and equipments present in a scene, identifying them as potential eavesdroppers. Also, in areas such as warehouses, critical spots may be identified, for instance at locations at which visitors may be located. By considering these spots as potential eavesdropper locations, the above problems enable to create safe zones at which no information leakage is guaranteed. Such prior knowledge may moreover be fine-tuned with the weights $\beta_{l,m}$, by setting higher weights for positions which are more likely to be critical.

III. Beamforming algorithms

In this section, methods to solve the optimisation problems (6) and (7) are designed.

A. Convex real reformulation

A first challenge coming with problems (6) and (7) is that the SINR constraint is not convex. To circumvent this, it is noted that in both cases, the optimal beamforming vectors are defined up to a phase shift. Therefore, forcing the phase of $\mathbf{h}_{k,l}^{\mathrm{H}}\mathbf{w}_{k,l}$ to be zero for all k and l, the following constraints can be added to the optimisation problems without changing their optimal value:

$$\mathcal{R}\left\{\mathbf{h}_{k,l}^{\mathrm{H}}\mathbf{w}_{k,l}\right\}\geq 0,\qquad \mathcal{I}\left\{\mathbf{h}_{k,l}^{\mathrm{H}}\mathbf{w}_{k,l}\right\}=0. \tag{8}$$

In order to express the above inequalities into the real domain, the following notations are introduced. Given a vector $\mathbf{v}$, its real and imaginary parts are denoted as $\mathbf{v}_R\triangleq\mathcal{R}\{\mathbf{v}\}$ and $\mathbf{v}_I\triangleq\mathcal{I}\{\mathbf{v}\}$. The real vectors $\mathbf{b}_{k,l},\mathbf{c}_{k,l},\mathbf{x}_{k,l}\in\mathbb{R}^{2N_k}$ are furthermore defined as $\mathbf{b}_{k,l}^{\mathrm{T}}\triangleq\left[\mathbf{h}_{k,l;R}^{\mathrm{T}},\mathbf{h}_{k,l;I}^{\mathrm{T}}\right]$, $\mathbf{c}_{k,l}^{\mathrm{T}}\triangleq\left[-\mathbf{h}_{k,l;I}^{\mathrm{T}},\mathbf{h}_{k,l;R}^{\mathrm{T}}\right]$, and $\mathbf{x}_{k,l}^{\mathrm{T}}\triangleq\left[\mathbf{w}_{k,l;R}^{\mathrm{T}},\mathbf{w}_{k,l;I}^{\mathrm{T}}\right]$, the phase reference constraints (8) becoming

$$\mathbf{b}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}\geq 0,\qquad \mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}=0.$$

Under the above, the SINR constraint reads as

$$\frac{\mathbf{b}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}}{\sqrt{\theta_l}}\geq\sqrt{\sigma_n^2+\sum_{l'\neq l}\left[\left(\mathbf{b}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l'}\right)^2+\left(\mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l'}\right)^2\right]}, \tag{9}$$

being now convex in the vectors $\{\mathbf{x}_{k,l}\}_{k,l}$. The power constraints are handled by noting that $\|\mathbf{w}_{k,l}\|_2=\|\mathbf{x}_{k,l}\|_2$. For the eavesdroppers' SNRs, the following is introduced

$$\mathbf{A}_{k,m}\triangleq\begin{bmatrix}\mathbf{g}_{k,m;R}^{\top} & \mathbf{g}_{k,m;I}^{\top}\\ -\mathbf{g}_{k,m;I}^{\top} & \mathbf{g}_{k,m;R}^{\top}\end{bmatrix}\in\mathbb{R}^{2\times 2N_k},$$

leading to $\left|\mathbf{g}_{k,m}^{\mathrm{H}}\mathbf{w}_{k,l}\right|^2=\|\mathbf{A}_{k,m}\mathbf{x}_{k,l}\|_2^2$, and concluding the translation of (6) and (7) into the real domain.

B. Traditional secure beamforming

Under the above transform, (6) becomes,

$$\min_{\{\mathbf{x}_{k,l}\}_{k,l}}\sum_{l,m}\beta_{l,m}\max_k\max\left\{\frac{\|\mathbf{A}_{k,m}\mathbf{x}_{k,l}\|_2^2}{\sigma_n^2}-\delta,0\right\} \tag{10}$$

$$\begin{aligned} \text{s.t.}\quad & (9), && \forall k,l,\\ & \mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}=0, && \forall k,l,\\ & \textstyle\sum_l\|\mathbf{x}_{k,l}\|_2^2\leq 1, && \forall k, \end{aligned}$$

with the inequality $\mathbf{b}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}\geq 0$ being encompassed by the SINR one. The above is a convex optimisation problem, which can be rewritten in a standard conic form to be solved by conic-programming solvers such as Mosek [8]:

$$\min_{\{\mathbf{x}_{k,l},\xi_{k,l}\}_{k,l},\{\eta_{l,m}\}_{l,m}}\sum_{l,m}\beta_{l,m}\eta_{l,m} \tag{11}$$

$$\begin{aligned} \text{s.t.}\quad & \eta_{l,m}\geq 0, && \forall l,m,\\ & \|\mathbf{A}_{k,m}\mathbf{x}_{k,l}\|_2^2-\delta\sigma_n^2\leq\eta_{l,m}\sigma_n^2, && \forall k,l,m,\\ & (9), && \forall k,l,\\ & \mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}=0, && \forall k,l,\\ & \textstyle\sum_l\xi_{k,l}\leq 1, && \forall k,\\ & \xi_{k,l}\geq\|\mathbf{x}_{k,l}\|_2^2, && \forall k,l. \end{aligned}$$

Apart from the above linear constraints, the third one is an instance of a quadratic cone, while the second and sixth ones correspond to a rotated quadratic cone.

C. Coding-aware secure beamforming

The real form of (7) reads as

$$\min_{\{\mathbf{x}_{k,l}\}_{k,l}}\sum_{l,m}\beta_{l,m}\prod_k\max\left\{\frac{\|\mathbf{A}_{k,m}\mathbf{x}_{k,l}\|_2^2}{\sigma_n^2}-\delta,0\right\} \tag{12}$$

$$\begin{aligned} \text{s.t.}\quad & (9), && \forall k,l,\\ & \mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l}=0, && \forall k,l,\\ & \textstyle\sum_l\|\mathbf{x}_{k,l}\|_2^2\leq 1, && \forall k, \end{aligned}$$

In the above, the constraint set is convex, but the objective function is however not. While obtaining a global optimum is

extremely challenging, a local minimum can nevertheless be achieved through successive minimisation [7]. In such an algorithm, the beamforming vectors of each RE are sequentially optimised, considering the ones of the other REs as fixed. The sub-problem of the kth RE, denoted $(\mathcal{P}_k)$, is therefore given by

$$\min_{\{\mathbf{x}_{k,l}\}_l} \sum_{l,m} C_{k,l,m} \max\left\{\frac{\|\mathbf{A}_{k,m}\mathbf{x}_{k,l}\|_2^2}{\sigma_n^2} - \delta, 0\right\}$$

$$(\mathcal{P}_k) \quad \text{s.t.} \quad (9), \qquad \forall l,$$
$$\mathbf{c}_{k,l}^{\mathrm{T}}\mathbf{x}_{k,l} = 0, \qquad \forall l,$$
$$\textstyle\sum_l \|\mathbf{x}_{k,l}\|_2^2 \leq 1,$$

with $C_{k,l,m} \triangleq \beta_{l,m} \prod_{k' \neq k} \max\left\{\frac{\|\mathbf{A}_{k',m}\mathbf{x}_{k',l}\|_2^2}{\sigma_n^2} - \delta, 0\right\}$ modified weights taking into account the fact eavesdroppers might already be blinded on the other REs. The major advantage of the above is that each sub-problem $(\mathcal{P}_k)$ is convex in $\{\mathbf{x}_{k,l}\}_l$, and can thus efficiently be solved. Moreover, since it is known the optimal objective value is 0, if the successive minimisation algorithm, described in Algorithm 1, leads to this value, then it is known that a global optimum is achieved. The standard conic form associated with the problems $(\mathcal{P}_k)$'s can be obtained in a similar manner reads as for (11). at the difference that only the kth RE beamforming vectors are optimised, the others being considered fixed and included into the weights $C_{k,l,m}$. In Algorithm 1, the initial beamformers $\mathbf{w}_{k,l}^{(\text{init})}$ can be any beamformer fulfilling all the constraints of (7). Among others, a reasonable choice is to initialise the sequential minimisation algorithm with the beamformers found through the traditional optimisation problem (6).

Algorithm 1 Coding-aware beamforming design

Set $\mathbf{w}_{k,l} = \mathbf{w}_{k,l}^{(\text{init})}$ $\forall k, l$.
Transform the $\{\mathbf{w}_{k,l}\}_{k,l}$ into the $\{\mathbf{x}_{k,l}\}_{k,l}$
while No convergence **do**
  for $k = 1, \ldots, K$ **do**
    Update the $\{\mathbf{x}_{k,l}\}_l$ by solving $(\mathcal{P}_k)$
    Update the weights $\{C_{k,l,m}\}_{k,l,m}$
Obtain the beamformers $\{\mathbf{w}_{k,l}\}_{k,l}$ from the $\{\mathbf{x}_{k,l}\}_{k,l}$

IV. Numerical Analysis

The above section provides solution to the beamforming design problem, when the information symbols are sent (traditional scheme) or with linearly coded streams. In this section, the above solutions are illustrated and validated numerically. Unless stated otherwise, the parameters are as follows: $L = 2$ UEs are served on $K = 3$ REs, all with a carrier frequency $f_c = 5\,\text{GHz}$. The scene geometry is depicted in Figure 1, with the UE locations being $(-10, 5)$ and $(10, -10)\text{m}$. Each RE is associated with a different antenna set, each set being an antenna array with $N_k = 30$ antenna spaced by $\lambda/2$, respectively at $(-25, 0)$, $(0, 25)$, $(0, -25)\text{m}$. There are 3 eavesdroppers around each UE, located on a circle of radius $r_{\text{eve}} = 2\,\text{m}$. In total, this leads to $M = 8$, with 6 eavesdroppers and the two 2 UEs. All weights $\beta_{l,m}$ are set to 1, except the weights corresponding to a UE with himself. Considering the worst case scenario, the eavesdropper sensitivity is set to $\delta = 0$. The noise variance, normalised by the transmit power, is $\sigma_n^2 = 0.1$, and the path loss function is given by $L(r) = 625r^{-2}$. The rate threshold is set to $\theta_l = 14.7\,\text{dB}$.

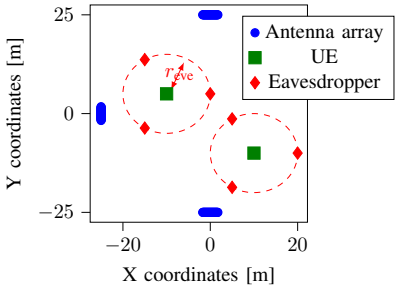

Fig. 1. Scene description (not to scale)

A. Beamformer analysis

First, the beamformers resulting from the optimisation are qualitatively analysed. Figure 2 depicts the SNR of the three REs of UE $l = 1$ in the region surrounding him, as well as the information leakage metrics. In the upper graphs, the traditional beamformer of each RE tries to avoid all the eavesdroppers. As some of the eavesdroppers are almost aligned with the UE, providing such security is impossible for each of the RE. In the bottom graphs, it can be observed the coding-aware beamformers act differently, since each eavesdropper must be in the blind region of only one of the RE. Hence, the beamformer of each RE 0 manages to blind two out of the three eavesdroppers, the remaining one being tackled by the beamformers of the other REs. These effects are also observed in the right panels of Figure 2, depicting the value of the metrics $\overline{\mathcal{L}}$ and $\sqrt[\kappa]{\underline{\mathcal{K}}}$ in the UE region. As it can be observed, many locations are unsecured in the traditional case, as at least one of the RE beamformer radiates power at that location. Thanks to the coding-aware beamformers, the unsecure region is significantly reduced, and the eavesdroppers get no information.

B. Security-rate-eavesdropper closeness trade-offs

The qualitative analysis can be complemented by quantitative security-rate trade-offs, by determining what is the highest possible security level which is achievable while fulfilling the rate constraint, for given eavesdropper locations. The upper panel of Figure 3 depicts such a trade-off, for the two beamforming designs, with 30 eavesdroppers located on each eavesdropper circle. Regarding the SINR axis, it is quantified as the loss with respect to the maximum achievable rate, i.e. when security is not a concern. For the security metrics, they have been normalised with the security value achieved with these security-unaware beamformers. As it can be observed,

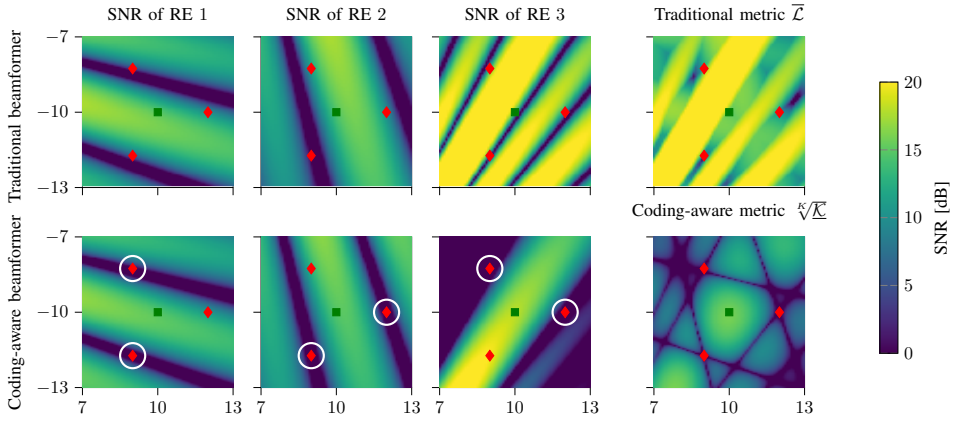

Fig. 2. SNR received by UE 1 on the three REs, with the traditional beamformers and with the coding-aware beamformers. The right panels depict the information leakage metrics in the two cases, for an eavesdropper located in (x, y). As in Figure 1, the green square denotes the UE location while the red points are the eavesdropper locations. The white circles highlight the eavesdroppers blinded by the coding-aware beamformers, emphasising the differences with respect to the traditional ones.

the coding-aware beamformers significantly improve the considered trade-off, providing security guarantees even in the presence of many eavesdroppers and high rate constraints. Another trade-off can be studied, which amounts to keeping the rate constraint constant while making the eavesdroppers closer through the value of r_{eve}. This is illustrated in the bottom panel of Figure 3. Again, the coding-aware beamforming design drastically improves the security guarantees.

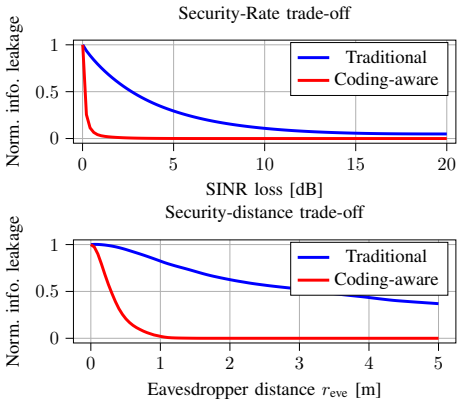

Fig. 3. Security-Rate (above) and Security-Distance (below) trade-offs

V. Conclusion

Motivated by the security improvements brought by the coding schemes over parallel communication links, traditional and coding-aware beamforming design problems have been formulated. In the first case, the problem has been rewritten as a convex optimisation problem, which can then be solved with conic-programming solvers. In the second case, as the problem is not convex, a locally optimal beamformer is reached through successive minimization. The sub-problems which must be tackled by each array have been reformulated as convex problems which can then efficiently be solved. The developed beamforming methods have been validated numerically, in a qualitative and quantitative way. Trade-offs have been studied, between the security, rate and eavesdropper locations, showing that the coding-aware beamforming design significant improves the security guarantees. Future works include scenarios in which several receivers must be served simultaneously, as well as the cases of multi-antenna eavesdroppers, and of eavesdroppers cooperating together.

References

[1] H. Sharma, N. Kumar, and R. Tekchandani, "Physical layer security using beamforming techniques for 5g and beyond networks: A systematic review," *Physical Communication*, vol. 54, p. 101791, 2022.

[2] A. Cohen, R. G. L. D'Oliveira, C.-Y. Yeh, H. Guerboukha, R. Shrestha, Z. Fang, E. W. Knightly, M. Médard, and D. M. Mittleman, "Absolute security in terahertz wireless links," 2023.

[3] Y. Shiri, C.-Y. Yeh, Z. Fang, R. Shrestha, H. Guerboukha, J. Malowicki, N. Thawdar, and D. M. Mittleman, "Absolute security with diffraction grating in terahertz communication links," in *2023 48th International Conference on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz)*, pp. 1–2, IEEE, 2023.

[4] C.-Y. Yeh, M. Médard, and D. M. Mittleman, "Absolute security with digital beamforming for high-frequency links," in *2023 48th International Conference on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz)*, pp. 1–2, 2023.

[5] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive mimo: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 492–523, 2021.

[6] E. Björnson, O. T. Demir, and L. Sanguinetti, "A primer on near-field beamforming for arrays and reconfigurable intelligent surfaces," in *2021 55th Asilomar Conference on Signals, Systems, and Computers*, pp. 105–112, 2021.

[7] R. Sargent and D. Sebastian, "On the convergence of sequential minimization algorithms," *Journal of Optimization Theory and Applications*, vol. 12, pp. 567–575, 1973.

[8] M. F. Anjos and J. B. Lasserre, *Handbook on semidefinite, conic and polynomial optimization*, vol. 166. Springer Science & Business Media, 2011.