Secure and Robust MIMO Transceiver for Multicast Mission Critical Communications

Deepa Jagyasi and Marceau Coupechoux
LTCI, Telecom Paris, Institut Polytechnique de Paris, France
{deepa.jagyasi,marceau.coupechoux}@telecom-paris.fr

***Abstract*—Mission-critical communications (MCC) involve all communications between people in charge of the safety of the civil society. MCC have unique requirements that include improved reliability, security and group communication support. In this paper, we propose secure and robust Multiple-Input-Multiple-Output (MIMO) transceivers, designed for multiple Base Stations (BS) supporting multicast MCC in presence of multiple eavesdroppers. We formulate minimization problems with the Sum-Mean-Square-Error (SMSE) at legitimate users as an objective function, and a lower bound for the MSE at eavesdroppers as a constraint. Security is achieved thanks to physical layer security mechanisms, namely MIMO beamforming and Artificial Noise (AN). Reliability is achieved by designing a system which is robust to two types of channel state information errors: stochastic and norm-bounded. We propose a coordinate descent-based algorithm and a worst-case iterative algorithm to solve these problems. Numerical results at physical layer and system level reveal the crucial role of robust designs for reliable MCC. We show the interest of both robust design and AN to improve the security gap. We also show that full BS cooperation in preferred for highly secured and reliable MCC but dynamic clustering allows to trade-off security and reliability against capacity.**

***Index Terms*—mission critical communication (MCC), physical layer security, robust transceiver design**

I. Introduction

Mission critical communications (MCC) are all communications between people in charge of the security and the safety of the civil society. Employees of public safety services, like policemen, firemen, rescue teams and ambulance nurses, but also from large companies managing critical infrastructures in the energy or transportation sectors require MCC for their operations [1]. MCC are conveyed by dedicated Private Mobile Radio (PMR) networks [2] that offer a group (or multicast) communication service. This is a one-to-many or many-to-many communication [3], which is one of the most important features of PMR networks and is essential to manage teams of employees. In 5G New Radio, group communication will be supported for MCC from Release R17 onwards [4]. Due to the critical aspects of their missions, MCC users also inherently require highly reliable and secure communication. In particular, sensitive information should not leak to unintended receivers although the broadcast nature of the wireless channel makes the network vulnerable to malicious eavesdroppers. Multiple-Input-Multiple-Output (MIMO) technique appear to be essential to address these MCC requirements. In this context, we propose a physical layer secured MIMO transceiver design for reliable multi-Base Stations (BS) multicast communication in the presence of malicious eavesdroppers.

In the 3rd Generation Partnership Project (3GPP), group communication is based on Multimedia Broadcast/Multimedia Service (MBMS) standards [2]. It thus naturally benefits from the multicast transmission techniques [5]. In MBMS, the reliability is improved by coordinating multiple BSs within a so called synchronization area. When all BSs of the area cooperate, we have a Multimedia Multicast/Broadcast Single Frequency Network (MBSFN) transmission [6]. On the contrary, when BSs transmit independently, we have a Single-Cell Point-to-Multipoint (SC-PTM) transmission [7]. Dynamic clustering, offering a good trade-off between MBSFN and SC-PTM is gaining popularity in the literature [8]–[10]. This motivates our scenario of a multicast transmission from multiple BSs towards a group of users and provides us with a framework for system level evaluations.

In order to ensure secure communication in the presence of eavesdroppers, we rely on physical layer security [11] mechanisms. They have the advantage of being independent of the secret key generation and distribution [12]. Although the use of long and complex keys is considered as one of the important techniques against eavesdroppers, the advent of powerful computational devices makes this approach indeed vulnerable in the long term [13]. In this paper, we consider physical layer security-based transceiver design for MCC by exploring signal processing methodologies in the presence of multiple eavesdroppers. Specifically, we incorporate security in two ways: MIMO beamforming is used to achieve the desired performance gain at legitimate users while degrading eavesdroppers channel; and artificial noise (AN) is added at the transmitter to guarantee additional security over the designed transceivers.

In our design, we formulate a problem in which the Sum-Mean-Square-Error (SMSE) is minimized at legitimate users while ensuring a Minimum-Mean-Square-Error (MMSE) at the eavesdroppers. This estimation-theoretic viewpoint is different from the information-theoretic one, usually adopted in the literature [14]. The approach is motivated by the fact that it leads to practical designs, while information-theoretic works rely on random codes, which are not practical except in very few cases. Further, in MCC, we mainly consider services with fixed data rate like group video-conference [3], rate-based

Supported by the EXTRANGE4G project with company ETELM funded by DGA. This work has been performed at LINCS laboratory.

maximization is thus not a primary aim. At last, although the approach does not provide any guarantee in terms of secrecy capacity, it is well adapted to applications, like video-conferencing, that require low Bite Error Rate (BER) and so low Mean-Square-Error (MSE) to properly function [14]. To better understand the performance of the proposed system, we study the security gap which is the difference of the minimum Signal-to-Noise Ratio (SNR) to guarantee a low BER at legitimate users and the maximum SNR that guarantees high BER at the eavesdroppers. With the goal of ensuring reliable communication, we propose a design that is robust to Channel State Information (CSI) errors. CSI is indeed never perfectly known due to various reasons such as estimation errors, feedback delays or pilot contamination. CSI errors thus affect the reliability of the communication [15]. Hence, it is crucial to design schemes that are resilient to such CSI imperfections. In this paper, we design systems that are robust to either Stochastic Errors (SE) or Norm-Bounded Errors (NBE) [16], [17]. SE models are often used in the literature (see e.g. [18] for a recent reference) to model errors arising from pilot aided linear MMSE channel estimation [19]. NBE are considered to be bounded within an ellipsoid or spherical region without further information on the statistics of the errors [17]. We perform a comparative analysis of both models in terms of system performance.

A. Related Work

Physical layer security has been investigated for various communication applications, most of which assume a simple wiretap communication channel model [11], [20]. In this setting, one legitimate transmitter (Alice) communicates with one legitimate receiver (Bob) (thus in unicast) in the presence of a single eavesdropper (Eve). Information theoretic aspects of secrecy have been widely studied in the literature, see e.g. [21], [22], our work however deals with signal processing techniques to achieve secure communications [23]. From the signal processing perspective, physical layer security has been studied for simple wiretap channels in various contexts such as AN-aided security [24]–[26], secure beamforming techniques [27], [28], or diversity oriented security [29]. However, secured designs considering complex communication scenarios involving multiple transmitters, receivers and eavesdroppers have been observed in the literature only over the past decade. For example, uplink multiuser transmissions are considered in [30] and relay-assisted security is studied in [31]. The multicast scenario has been studied in [32]–[35], however always while assuming a single transmitting BS. To the best of our knowledge, secured multiple BS multicast system design has not been reported in the literature. Specifically in MCC, physical layer security has been considered in [36]–[38] in the context of resource allocation problem [36], or for authentication [37], [38], but only for machine-type communications[1]. It is however worthwhile noting that no instance addressing the design of secure transceivers for MCC group communications has been observed so far.

MCC group communications involve text, image, audio or video exchanges in multicast. In this context, maximizing the data rate or the secrecy rate, as it is done usually in the literature, is not the main objective of operators. Instead, together with the security, the correctness of the data is of utmost importance. In our work, we thus consider a secure SMSE minimization-based transceiver design in the presence of multiple eavesdroppers. In the literature, only two instances of MMSE-based secure precoder design have been respectively discussed in [14] and [39], however, for a simple wiretap communication scenario. These designs cannot be readily adapted for the proposed system due to increased complexity related to the presence of multiple coordinating BSs and eavesdroppers. Moreover, the multicast transmission, which consists of transmitting a common message to all legitimate users, makes the processing at eavesdroppers easier and thus requires a specific design.

The addition of AN for the secure design of communication is either done in the null space of legitimate users, see e.g. [24], [26], or is jointly designed with the precoder as in [31]. In this paper, we adopt a joint AN and transceiver design approach, where an AN shaping matrix is designed by solving the joint optimization problem and meet the overall design constraints specific to the MCC. We confirm the interest of such a technique in the specific scenario of MCC which includes multi-BS multicast communication in the presence of multiple eavesdroppers.

At last, to improve the system performance under realistic channel uncertainties, robustness needs to be incorporated as part of the design. Effectiveness of this approach is studied in the literature for various wireless communication applications [40]–[42]. However, many existing works on physical-layer secured transceiver design consider the availability of perfect CSI knowledge of both legitimate users and eavesdroppers. Robustness towards imperfect CSI has been considered in [43]–[48]. Physical layer security with imperfect CSI for a simple wiretap system is studied in [43]–[45] with an objective of secrecy rate maximization. Reference [46] considers a system with multiple MISO transmitter-receiver point-to-point communications in the presence of one single-antenna eavesdropper. Authors optimize the secrecy rate under a power constraint and the energy efficiency under a secrecy rate constraint. Authors of [47] assume a single BS with multiple single antenna users (a MISO system) and eavesdroppers. The Signal-to-Interference-plus-Noise Ratio (SINR) gap is taken as a metric for security. Finally, in [48], authors formulate a multi-objective multicast and unicast secrecy rate optimization problem for a single BS with multiple single antenna users (a MISO system) and eavesdroppers. In our paper, we extend the existing works to multiple BSs, users and eavesdroppers with multiple antennas at every equipment; we assume multicast traffic and formulate a MMSE minimization problem. A robust design is proposed for both SE (when the error statistics can be learned) and NBE models (when minimal prior knowledge is available).

A preliminary version of this paper has been published

[1]The expression ”mission-critical communications” has two acceptations in the literature: 1) machine-type communications with delay-sensitive requirements; 2) communications between people in charge of the security and the safety of the society. These two communication types are related to different use cases and may have different requirements.

in [49]. This reference neither include the security issue nor the NBE model. The system level performance evaluation is based on the work of [10], but this reference, which proposes a clustering algorithm for MCC, does not implement any MIMO transceiver design.

B. Contribution

In this paper, we propose a physical layer secured and robust MIMO transceiver design for multi-BS multicast MCC system in the presence of multiple eavesdroppers. The main contributions of this work are summarized as follows:

- We formulate novel SMSE-based minimization problems to capture the reliability and security requirements of multicast MCC. Specifically, two optimization problems ($\mathcal{P}_1$ and $\mathcal{P}_2$) are considered according to the type of CSI errors, i.e., SE (Assumption 1) and NBE (Assumption 2). Security aspects are tackled using MIMO beamforming and AN and accounted in the miminization problems as a lower bound constraint for the MSE of eavesdroppers.
- When SEs are assumed, we propose a coordinate descent-based iterative algorithm to solve the SMSE minimization problem (Algorithm 2). The algorithm is based on closed-form equations for the MSE (Lemma 1) and the derived gradients of the Lagrangian (Proposition 1).
- When NBEs are assumed, we adopt a worst-case approach and decompose the original problem into three sub-problems. Resultant robust filters and AN shaping matrix are obtained by sequentially solving individual sub-problems in an iterative way (Algorithm 3).
- We provide numerical results at physical layer and system level to gain insights for the proposed designs. Physical layer simulations show the importance of robust designs for ensuring highly reliable MCC, even when NBEs are present. We also show the interest of AN for multicast MCC to ensure secure communications. System level simulations reveal that a full cooperation of the BSs in the synchronization area is preferred for reliable and secured MCC. If capacity becomes an important consideration, dynamic clustering can be adopted at the expense of less secured and reliable communications.

The paper is structured as follows: Section II describes the network and transceiver models. The problem formulations and the design of the transceivers are presented in Section III. Physical layer and system level simulations are shown in Section IV. Section V concludes the paper.

Notations: We use bold-faced lowercase letters to denote column vectors and bold-faced uppercase letters to denote matrices. For any matrix $\mathbf{X}$, $\mathrm{tr}(\mathbf{X})$, $\mathbb{E}\{\mathbf{X}\}$, $\mathbf{X}^H$, and $\mathbf{X}^T$ denote trace, expectation, conjugate transpose, and transpose operator, respectively. $\mathcal{X}_1 \backslash \mathcal{X}_2$ denote the set minus operation between the sets $\mathcal{X}_1$ and $\mathcal{X}_2$.

II. Network and Transceiver Model

In this section, we present the network and transceiver models.

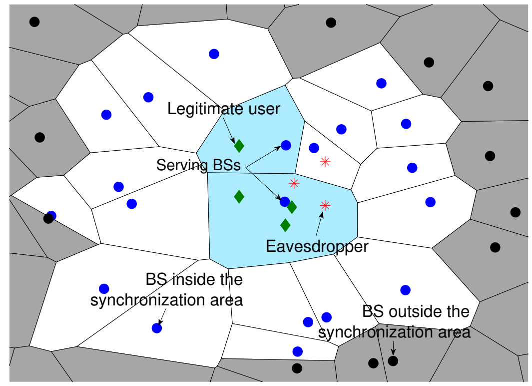


Fig. 1: Network model: White and blue cells form the MBSFN synchronization area; blue cells are serving a group of legitimate users (green diamonds) while a set of eavesdroppers (red crosses) overhear the multicast communication.

A. Network Model

We consider the downlink of a cellular network dedicated to MCC with BSs serving legitimate users. Every legitimate user belongs to a multicast group, i.e., users of a given group receive the same information from the network. Every group is served by a cluster of coordinated BSs. In addition to legitimate users, we assume the potential presence of eavesdroppers, who listen to the transmitted information in a passive mode, i.e., without any tampering of the legitimate messages or active participation with the BSs. Fig. 1 shows such a cluster of BSs communicating with a set of group users. Among the BSs in the network, a set $\mathcal{B}$ of BSs are assumed to be synchronized: they operate at same frequency and utilize the same time/frequency resource block for communication. In the terminology of MBMS, $\mathcal{B}$ is called a *MBSFN synchronization area*. In Fig. 1, white and blue cells form the MBSFN synchronization area, while grey cells are outside. We also assume a perfect equalization at the receivers. Tight synchronization is provided by the SYNC protocol in MBMS systems [50], while equalization can be realized thanks to a linear MMSE [51].

In the proposed system, we consider a dynamic coordinated cluster of BSs $\mathcal{S} \subseteq \mathcal{B}$ (in blue in Fig. 1), for every group of users $\mathcal{U}$. When $\mathcal{S} = \mathcal{B}$, all BSs of the MBSFN synchronization area cooperate to serve the group, this is called a *full MBSFN transmission*. Cells outside $\mathcal{B}$ contribute to the co-channel interference. When $|\mathcal{S}| = 1$, we have a *SC-PTM transmission*. In general, a subset $\mathcal{S} \subseteq \mathcal{B}$ is dynamically selected for every group. In this case, cells in $\mathcal{S}$ cooperate, while cells in $\mathcal{B} \backslash \mathcal{S}$ and cells outside the MBSFN synchronization area contribute to the co-channel interference. In this paper, we consider a greedy clustering algorithm, where the cluster is formed by progressively selecting K_T' best BS on the basis of maximum Signal to Interference plus Noise Ratio (SINR) achieved at the group users (see Algorithm 1). We first include in $\mathcal{S}$ the BSs that provide the highest receive power to every user. If $|\mathcal{S}| \leq K_T'$, we complete with $K_T' - |\mathcal{S}|$ BSs providing the highest sum SINR to group users. K_T' is considered as a design parameter that controls the minimum cluster size. The greedy clustering algorithm and its variants are widely adopted in the literature related to multi-point cooperation, see e.g. [8], [52]. We denote K_T as the number of BSs eventually selected by Algorithm 1.

Algorithm 1: Greedy Clustering

Input: Locations of BSs and group users, $K'_T \leq |\mathcal{B}|$: minimum cluster size
Init: $\mathcal{S} \leftarrow \emptyset$
for every user **do**
  Find the BS t providing the highest receive power
  $\mathcal{S} \leftarrow \mathcal{S} \cup \{t\}$
end for
if $|\mathcal{S}| < K'_T$ **then**
  Find the set $\mathcal{S}'$ of $K'_T - |\mathcal{S}|$ BSs maximizing the sum SINR for group users
  $\mathcal{S} \leftarrow \mathcal{S} \cup \mathcal{S}'$
end if
return $\mathcal{S}$

B. Transceiver Model

To analyze the transmission towards a group of users, we consider the secure multi-user MIMO multicast wireless communication scenario as shown in Fig. 2, where the K_T BSs of cluster $\mathcal{S}$ multicast a common message to K_R legitimate user-equipments (UEs) in a group. The transmitted signal is assumed to be overheard by K_E passive eavesdroppers. All the nodes in the system are considered to be equipped with MIMO processing, where each BS, UE and Eve have N_T, N_R and N_E antennas respectively. Each BS multicasts a time-slotted N_s dimensional column vector $\mathbf{d}$ with transmit power P_T, where N_s is the number of parallel data streams transmitted by the BS. The data $\mathbf{d}$ is considered to be mutually independent, so that $\mathbb{E}[\mathbf{d}\mathbf{d}^H] = \mathbf{I}_{N_s}$. Before transmission, the data vector is processed by a $(N_T \times N_s)$ dimensional precoder matrix $\mathbf{V}_t$ at the t-th BS, $t = 1, \cdots, K_T$. In order to improve security, we introduce an additional AN vector $\mathbf{z}_t$ of size $(N_T \times 1)$ with zero mean and variance $\mathbb{E}[\mathbf{z}_t\mathbf{z}_t^H] = \sigma_{zt}^2\mathbf{I}_{N_T}$ at the t-th transmitter. The presence of AN has the goal of depleting the information leak to eavesdroppers. Furthermore, an AN-shaping matrix $\mathbf{W}_t$ of size $(N_T \times N_T)$ is considered to regulate the effect of AN in the overall design. Transceivers and AN-shaping matrix are jointly designed and this information is supposed to be shared between the transmitters and the legitimate users. Hence the signal transmitted from t-th BS is given by:

$$\mathbf{x}_t = \mathbf{V}_t\mathbf{d} + \mathbf{W}_t\mathbf{z}_t \tag{1}$$

and the total transmit power at t-th BS is given by:

$$P_t \triangleq \mathbb{E}[||\mathbf{x}_t\mathbf{x}_t^H||]. \tag{2}$$

We denote the true channel gain between the t-th BS and the l-th legitimate UE and between the t-th BS and the e-th eavesdropper by $\mathbf{C}_{tl}$ (with dimension $N_R \times N_T$) and $\mathbf{G}_{te}$ of dimension $N_E \times N_T$, respectively. We assume quasi-static Rayleigh fading channels that remain static over one transmission time-slot. Consequently, the received signal $\mathbf{y}_l$ at legitimate UE l is given by:

$$\mathbf{y}_l = \sum_{t=1}^{K_T} \mathbf{C}_{tl}\mathbf{V}_t\mathbf{d} + \sum_{t=1}^{K_T} \mathbf{C}_{tl}\mathbf{W}_t\mathbf{z}_t + \mathbf{n}_l \tag{3}$$

where $\mathbf{n}_l$ is the N_R-dimensional zero mean random white Gaussian noise vector at the l-th UE's receive antennas with $\mathbb{E}[\mathbf{n}_l\mathbf{n}_l^H] = \sigma_{nl}^2\mathbf{I}_{N_R}$. The random noise vector is uncorrelated with the data vector, so that $\mathbb{E}[\mathbf{n}_l\mathbf{d}^H] = 0$. The received signal at the UE l is estimated as $\widehat{\mathbf{d}}_l$ (of dimension $N_s \times 1$) after passing through a $N_R \times N_s$ dimensional receive filter matrix $\mathbf{R}_l$. The estimated data is given by:

$$\widehat{\mathbf{d}}_l = \mathbf{R}_l\sum_{t=1}^{K_T} \mathbf{C}_{tl}\mathbf{V}_t\mathbf{d} + \mathbf{R}_l\sum_{t=1}^{K_T} \mathbf{C}_{tl}\mathbf{W}_t\mathbf{z}_t + \mathbf{R}_l\mathbf{n}_l. \tag{4}$$

Thus, the MSE at the l-th legitimate UE is expressed as:

$$\epsilon_l \triangleq \mathbb{E}[||\mathbf{d} - \widehat{\mathbf{d}}_l||^2]. \tag{5}$$

Similarly at the eavesdroppers, the received signal $\mathbf{y}_e$ at the e-th eavesdropper is given as:

$$\mathbf{y}_e = \sum_{t=1}^{K_T} \big(\mathbf{G}_{te}\mathbf{V}_t\mathbf{d} + \mathbf{G}_{te}\mathbf{W}_t\mathbf{z}_t\big) + \mathbf{n}_e \tag{6}$$

where $\mathbf{n}_e$ is the random white Gaussian noise vector of size $N_E \times 1$ at the e-th eavesdropper's antenna elements with zero mean and covariance $\mathbb{E}[\mathbf{n}_e\mathbf{n}_e^H] = \sigma_{ne}^2\mathbf{I}_{N_E}$. The random noise vector is uncorrelated with data vector such that $\mathbb{E}[\mathbf{n}_e\mathbf{d}^H] = 0$. In this work, we assume that eavesdropper implements a classical MMSE linear receive filter. However, it can replaced with any other linear receiver models such as zero-forcing, matched filter, etc. In our previous work [49], we performed the comparative analysis of utilization of different filters for legitimate users and concluded that MMSE-based receiver was performing the best. With the intention to provide same benefits to the eavesdroppers and for the ease of readiness we assume the eavesdropper filters to be implemented as MMSE filter. The considered MMSE receive filter at e-th eavesdropper is given as:

$$\mathbf{E}_e = \Big(\sum_{t=1}^{K_T} \mathbf{V}_t^H\mathbf{G}_{te}^H\Big)\Big(\sum_{t=1}^{K_T} \mathbf{G}_{te}\mathbf{V}_t\mathbf{V}_t^H\mathbf{G}_{te}^H + \sigma_{ne}^2\mathbf{I}\Big)^{-1}. \tag{7}$$

Eavesdroppers do not have the information about the presence of AN in the received signal and hence $\mathbf{W}_t\mathbf{z}_t$ is not considered in the MMSE receive filter design. After passing $\mathbf{y}_e$ through the $N_E \times N_s$ receive filter $\mathbf{E}_e$, the estimated data $\overline{\mathbf{d}}_e$ at the e-th eavesdropper is given by:

$$\overline{\mathbf{d}}_e = \mathbf{E}_e\sum_{t=1}^{K_T} \mathbf{G}_{te}\mathbf{V}_t\mathbf{d} + \mathbf{E}_e\sum_{t=1}^{K_T} \mathbf{G}_{te}\mathbf{W}_t\mathbf{z}_t + \mathbf{E}_e\mathbf{n}_e. \tag{8}$$

Thus, the MSE at the e-th eavesdropper can be obtained as:

$$\epsilon_e \triangleq \mathbb{E}[||\mathbf{d} - \overline{\mathbf{d}}_{\mathbf{e}}||^{\mathbf{2}}]. \tag{9}$$

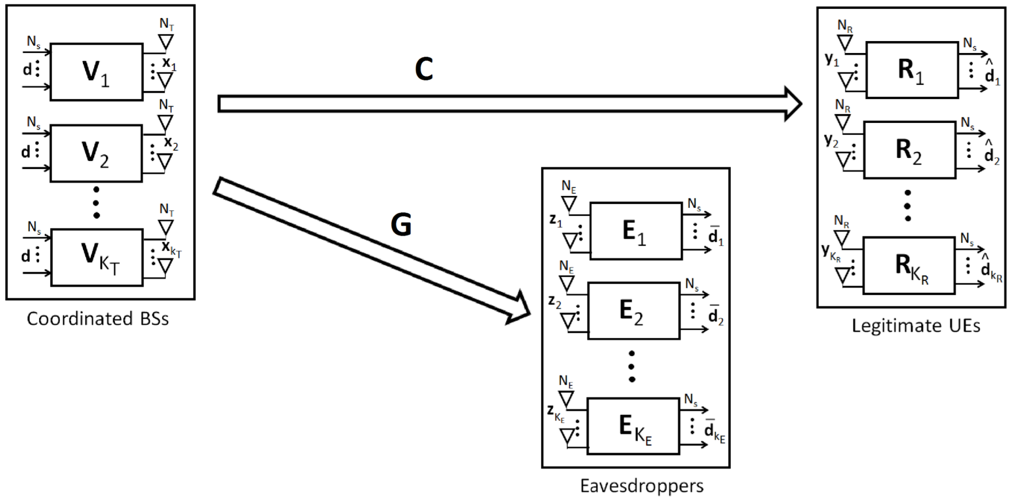


Fig. 2: System diagram for multi-BS multicast scenario in the presence of multiple passive eavesdroppers for MCC .

Furthermore, we incorporate imperfect CSI knowledge at the receivers as follows. The true channel between the t-th BS and the e-th Eve is modeled as:

$$\mathbf{G}_{te} = \widehat{\mathbf{G}}_{te} + \mathbf{\Delta}_{te} \tag{10}$$

where $\widehat{\mathbf{G}}_{te}$ is the available erroneous estimate of CSI and $\mathbf{\Delta}_{te}$ refers to the corresponding channel uncertainties. It is assumed here that a eavesdropper's CSI estimate have been obtained using some detection scheme, such as the ones described in [53] [54] and is thus available. In the same way, the CSI knowledge of legitimate users may not always be perfect, so that a robust transceiver design is required. The true channel between the t-th BS and the l-th user is modeled as:

$$\mathbf{C}_{tl} = \widehat{\mathbf{C}}_{tl} + \mathbf{\Delta}_{tl} \tag{11}$$

where $\widehat{\mathbf{C}}_{tl}$ is the erroneous channel estimate and $\mathbf{\Delta}_{tl}$ corresponds to channel uncertainties. We consider two ways of modeling the error $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$. The first one assumes that the errors statistics have been learned from previous measurements. The second is valid when only a rough estimate of the noise power is available. Hence, we define the following assumptions.

Assumption 1 (SE model)**.** *CSI errors $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ are modeled as Gaussian random variables such that $\mathbb{E}[\mathbf{\Delta}_{te}\mathbf{\Delta}_{te}^H] = \sigma_{te}^2\mathbf{I}$ and $\mathbb{E}[\mathbf{\Delta}_{tl}\mathbf{\Delta}_{tl}^H] = \sigma_{tl}^2\mathbf{I}$.*

Assumption 2 (NBE model)**.** *CSI errors $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ are modeled using the NBE model, also known as deterministic-bounded error model [42], where $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ are respectively taken in continuous sets, called uncertainty regions, defined by:*

$$\mathcal{G}_{te} = \{\mathbf{\Delta}_{te} : ||\mathbf{\Delta}_{te}||^2 \leq \tau_{te}\} \tag{12}$$

$$\mathcal{C}_{tl} = \{\mathbf{\Delta}_{tl} : ||\mathbf{\Delta}_{tl}||^2 \leq \tau_{tl}\} \tag{13}$$

where τ_{te} and τ_{tl} denote the radii of the uncertainty regions.

The channel errors for both legitimate UEs and eavesdroppers are considered to be uncorrelated with the transmitted data sequence as well as to the additive white noise vector, i.e., $\mathbb{E}[\mathbf{d}\mathbf{\Delta}_{t,l}] = 0$, $\mathbb{E}[\mathbf{n}_l\mathbf{\Delta}_{t,l}] = 0$ for all t, l and $\mathbb{E}[\mathbf{d}\mathbf{\Delta}_{t,e}] = 0$, $\mathbb{E}[\mathbf{n}_e\mathbf{\Delta}_{t,e}] = 0$ for all t, e. We now specify that the expectations in (5) and (9) are considered over data, channel matrix, noise and estimation errors.

III. Secure Transceiver design

In this section, we present our robust and secure transceiver design.

A. Stochastic CSI Errors

Our goal is to obtain the optimal precoder, receive filter, and AN-shaping matrices $\mathbf{V}_t$, $\mathbf{R}_l$, and $\mathbf{W}_t$ for secure communications at all the BSs and legitimate UEs while minimizing the overall SMSE of the legitimate UEs under the constraint of a maximum transmit power at every BS and a minimum MSE for every eavesdropper. In this sub-section, Assumption 1 is considered. Our joint optimization problem can thus be formulated as follows:

$$\begin{aligned} \underset{\substack{\mathbf{V}_t,\mathbf{W}_t,\mathbf{R}_l \\ t=1\ldots K_T, l=1\ldots K_R}}{\text{minimize}} \quad & \sum_{l=1}^{K_R} \epsilon_l \\ \text{subject to} \quad & C1: \ \epsilon_e \geq \Gamma \qquad \forall e \in \{1, \cdots, K_E\} \\ & C2: \ P_t \leq P_T \qquad \forall t \in \{1, \cdots, K_T\}. \end{aligned} \tag{$\mathcal{P}_1$}$$

The MSE ϵ_l and ϵ_e at the legitimate user l and eavesdropper e are obtained using (5) and (9), respectively. The transmit power P_t at t-th BS is given by (2). In $C1$, Γ is a design parameter that represents the lower bound on the achievable MSE expected at each eavesdropper. In $C2$, P_T is the maximum transmit power at every BS.

Lemma 1. *With Assumption 1, we have the following result:*

$$P_t = tr(\mathbf{V}_t\mathbf{V}_t^H + \sigma_{zt}^2\mathbf{W}_t\mathbf{W}_t^H) \quad (14)$$

$$\begin{aligned}\epsilon_l =& \operatorname{tr}(\mathbf{I}) - \operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t) - \operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H)\\ &+\operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H)\\ &+\operatorname{tr}(\sum_{t=1}^{K_T}\sigma_{zt}^2\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H)\\ &+\sigma_{nl}^2\operatorname{tr}(\mathbf{R}_l\mathbf{R}_l^H) + \sum_{t=1}^{K_T}\sigma_{tl}^2\sigma_{zt}^2\operatorname{tr}(\mathbf{R}_l\mathbf{R}_l^H)\operatorname{tr}(\mathbf{W}_t\mathbf{W}_t^H)\\ &+\sum_{t=1}^{K_T}\sigma_{tl}^2\operatorname{tr}(\mathbf{R}_l\mathbf{R}_l^H)\operatorname{tr}(\mathbf{V}_t\mathbf{V}_t^H) \quad (15)\end{aligned}$$

$$\begin{aligned}\epsilon_e =& \operatorname{tr}(\mathbf{I}) - \operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t) - \operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H)\\ &+\operatorname{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H)\\ &+\operatorname{tr}(\sum_{t=1}^{K_T}\sigma_{zt}^2\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{W}_t\mathbf{W}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) + \sigma_{ne}^2\operatorname{tr}(\mathbf{E}_e\mathbf{E}_e^H)\\ &+\sum_{t=1}^{K_T}\sigma_{te}^2\sigma_{zt}^2\operatorname{tr}(\mathbf{E}_e\mathbf{E}_e^H)\operatorname{tr}(\mathbf{W}_t\mathbf{W}_t^H)\\ &+\sum_{t=1}^{K_T}\sigma_{te}^2\operatorname{tr}(\mathbf{E}_e\mathbf{E}_e^H)\operatorname{tr}(\mathbf{V}_t\mathbf{V}_t^H). \quad (16)\end{aligned}$$

Proof: See Appendix A. ■

Proposition 1. *With Assumption 1, the optimal transceiver and AN shaping matrices verify:*

$$\mathbf{V}_t = (\mathbf{A}_t)^{-1}\Big(\sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H - \sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\Big) \quad (17)$$

$$\mathbf{W}_t = \mathbf{B}_t/\sqrt{\operatorname{tr}(\mathbf{B}_t\mathbf{B}_t^H)} \quad (18)$$

$$\begin{aligned}\mathbf{R}_l =& \Big(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\Big)\Big(\sum_{t=1}^{K_T}\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\\ &+\sum_{t=1}^{K_T}\sigma_{zt}^2\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H\widehat{\mathbf{C}}_{tl}^H + \sigma_{nl}^2\mathbf{I}\\ &+\sum_{t=1}^{K_T}\sigma_{tl}^2\operatorname{tr}(\mathbf{V}_t\mathbf{V}_t^H)\mathbf{I}\\ &+\sum_{t=1}^{K_T}\sigma_{tl}^2\sigma_{zt}^2\operatorname{tr}(\mathbf{W}_t\mathbf{W}_t^H)\mathbf{I}\Big)^{-1} \quad (19)\end{aligned}$$

where

$$\mathbf{B}_t = \mathbf{I} - \mathbf{A}_t^H(\mathbf{A}_t\mathbf{A}_t^H)^{-1}\mathbf{A}_t \quad (20)$$

$$\begin{aligned}\mathbf{A}_t =& \sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl} + \sum_{l=1}^{K_R}\sigma_{tl}^2\operatorname{tr}(\mathbf{R}_l\mathbf{R}_l^H)\\ &-\sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\mathbf{E}_e\widehat{\mathbf{G}}_{te} - \sum_{e=1}^{K_E}\lambda_e\sigma_{te}^2\operatorname{tr}(\mathbf{E}_e\mathbf{E}_e^H)\\ &+\lambda_t^{'}\mathbf{I} \quad (21)\end{aligned}$$

and where $\lambda_e \geq 0$, *and* $\lambda_t^{'} \geq 0$ *are the Lagrangian multipliers, which are calculated such that the constraints* $C1$, *and* $C2$ *are satisfied respectively.*

Proof: See Appendix B. ■

Algorithm 2: Iterative procedure to obtain transceiver filters for SEs

---

1: **Input:** β, K_T, K_R, K_E, $\widehat{\mathbf{C}}_{tl}$, $\widehat{\mathbf{G}}_{te}$, σ_{nl}, σ_{ne}, P_T, Γ $\forall$ $t \in \{1,\cdots,K_T\}$, $l \in \{1,\cdots,K_R\}$, and $e \in \{1,\cdots,K_E\}$
2: **Init:** Randomly generate $\mathbf{V}_t$, $\mathbf{W}_t$ $\forall t \in \{1,\cdots,K_T\}$, $\epsilon_l' \leftarrow 0$, $\epsilon_l \leftarrow 0$ $\quad\forall l \in \{1,\cdots,K_R\}$
3: **repeat**
4: $\quad\epsilon_l' \leftarrow \epsilon_l$ $\quad\forall l \in \{1,\cdots,K_R\}$
5: $\quad$Update $\mathbf{E}_e$ $\forall e \in \{1,\cdots,K_E\}$ using (7)
6: $\quad$Update $\mathbf{R}_l$ using $\mathbf{V}_t$, $\mathbf{W}_t$ in (19) $\forall l \in \{1,\cdots,K_R\}$
7: $\quad$Solve for λ_e and $\lambda_t^{'}$ using $C1$, $C2$ $\forall t \in \{1,\cdots,K_T\}$, and $\forall e \in \{1,\cdots,K_E\}$
8: $\quad$Update $\mathbf{V}_t$ using λ_e, $\lambda_t^{'}$, $\mathbf{R}_l$, $\mathbf{E}_e$ in (17) $\forall t = \{1,\cdots,K_T\}$
9: $\quad$Update $\mathbf{W}_t$ using $\mathbf{V}_t$ in (18) $\forall t = \{1,\cdots,K_T\}$
10: $\quad$Compute ϵ_l using $\mathbf{V}_t$, λ_e, $\lambda_t^{'}$, $\mathbf{W}_t$, and $\mathbf{R}_l$ in (15)
11: **until** $|\epsilon_l - \epsilon_l'| \leq \beta$ $\quad\forall l \in \{1,\cdots,K_R\}$
12: **return** $\mathbf{V}_t$, $\mathbf{W}_t$ $\quad\forall t \in \{1,\cdots,K_T\}$, $\mathbf{R}_l$, ϵ_l $\forall l \in \{1,\cdots,K_R\}$

From the lemma, we observe that the objective function is jointly non-convex. It is convex in every variable $\mathbf{V}_t$, $\mathbf{W}_t$ and $\mathbf{R}_l$ but includes $C1$, which is a concave constraint. The problem is thus non-convex. In order to simplify the resolution, we adopt a block coordinate descent approach [55]: in a cyclic way, a block of variable is optimized while keeping others as fixed, leading to the iterative resolution of sub-problems. As every sub-problem is non-convex, we look for a Karush-Kuhn-Tucker (KKT) solution. KKT is here a necessary condition, we don't have any guarantee on the local optimality or on the dual gap. The found solution is thus only a good stationary candidate. The resulting iterative procedure is shown in Algorithm 2. In step 7, the Lagrange multipliers $\lambda_e, \forall e$ and $\lambda_l, \forall l$ are obtained by solving the set of non-linear equations from constraints $C1$ and $C2$ by using the function `fsolve` from Matlab, which implements a dogleg trust-region algorithm [55].

Complexity analysis – Let us denote $N = \max(N_T, N_R, N_E, N_s)$ and $K = \max(K_T, K_R, K_E)$. N is an upper bound on the number of antennas per device and the number of data streams; K is related to the number of devices involved in the communication. The computation of $\mathbf{E}_e$ in (7), $\mathbf{R}_l$ in (19), $\mathbf{V}_t$ in (17), and $\mathbf{W}_t$ in (18) are dominated by K inversions of matrices of size N, so that their complexity is in $O(KN^3)$. The computation of ϵ_l involves a sum of matrix multiplications and is thus in $O(KN^3)$. The dodleg algorithm implemented in `fsolve` is an iterative algorithm which achieves a ε-approximation of the solution with complexity $O(K^3\varepsilon^{-3})$ when using fully quadratic models in the derivative-free case with $2K$ unknowns [56].

Lemma 2. *Let I_2 be the number of iterations of Algorithm 2 and $\varepsilon > 0$ the accuracy of* `fsolve`*. The complexity of Algorithm 2 is at most $O(I_2KN^3 + I_2K^3\varepsilon^{-3})$.*

Convergence analysis – The coordinate descent algorithm generate sequences whose limit points are stationary if the objective function is continuously differentiable and the minimum along every coordinate is uniquely attained [57]. In our case, the objective is indeed continuously differentiable but we are not able to ensure the uniqueness of the minimum in the sub-problems. We instead only look for a KKT solution in every sub-problem. As the global problem is non-convex, we cannot hope convergence towards a global optimum. We can however reach an epsilon approximation of a stationary point because the objective function is decreased at every iteration [58]. In our simulations, $I_2 = 10$ iterations are generally sufficient to achieve convergence (see Fig. 10 and the related discussion in Section IV-A).

B. Norm-bounded CSI errors

In this sub-section, we consider Assumption 2 for the system design, i.e., we assume that CSI errors are only norm bounded. In this case, the problem formulation can be written as:

$$\begin{aligned} \underset{\substack{\mathbf{V}_t,\mathbf{W}_t,\mathbf{R}_l \\ t=1\ldots K_T, l=1\ldots K_R}}{\text{minimize}} \quad & \sum_{l=1}^{K_R} \epsilon_l \\ \text{subject to} \quad & C1, C2 \\ & C3: \ \mathbf{\Delta}_{te} \in \mathcal{G}_{te}, \quad \forall t, \forall e \\ & C4: \ \mathbf{\Delta}_{tl} \in \mathcal{C}_{tl} \quad \forall t, \forall l. \end{aligned} \tag{$\mathcal{P}_2$}$$

Note that $C3$ and $C4$ can be seen as an infinite number of constraints. This problem is indeed a *robust optimization problem* in the sense that there is a *nominal problem* corresponding to $\mathbf{\Delta}_{te} = \mathbf{\Delta}_{tl} = 0$ and uncertainty sets $\mathcal{G}_{te}$ and $\mathcal{C}_{tl}$ for these two parameters.

In order to tackle this problem, we follow a worst-case approach, in which, the SMSE of legitimate users is minimized for the worst-case error $\mathbf{\Delta}_{tl}$ subject to the constraint and, with the worst-case error $\mathbf{\Delta}_{te}$, the MSE of the eavesdroppers is maintained above the predefined threshold. In other words, we try to minimize the maximum achievable SMSE at the legitimate users under the norm-bounds of CSI errors. While for the eavesdroppers, we optimize the system to achieve the threshold bound for the minimum achievable MSE. This leads to this new formulation:

$$\begin{aligned} \underset{\substack{\mathbf{V}_t,\mathbf{W}_t,\mathbf{R}_l \\ t=1\ldots K_T, l=1\ldots K_R}}{\text{minimize}} \quad & \max_{\mathbf{\Delta}_{tl}\in\mathcal{C}_{tl}} \sum_{l=1}^{K_R} \epsilon_l \\ \text{subject to} \quad & C2 \\ & C5: \ \min_{\mathbf{\Delta}_{te}\in\mathcal{G}_{te}} \epsilon_e \geq \Gamma \qquad \forall e. \end{aligned} \tag{$\bar{\mathcal{P}}_2$}$$

In this formulation, the objective function is replaced by its robust counterpart, i.e., the largest value of the original objective over all realizations of the error $\mathbf{\Delta}_{tl}$. Said differently, this is the worst-case cost. In the same way, constraint $C1$ is replaced by a robust counter part $C5$, i.e., the worst-case MSE over all realizations of the error $\mathbf{\Delta}_{te}$.

Robust counterpart problems can be efficiently solved in specific cases by deriving an explicit and tractable set of constraints, e.g., when the objective function is linear and the uncertainty sets are polytopic or ellipsoidal [59], [60]. However, the robust counterpart of convex problems is in general NP-hard [61]. In our work, the problem is not even convex.

A possible approach to deal with non-convex robust problems is the method of outer approximations [62], also known as the cutting-set method [63]. This approach proceeds by iterations: the problem is solved assuming a finite set of constraints for $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ (starting with a single fixed value); then the problem associated to the constraint (e.g. $C5$ above) is solved and optimal values of $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ are added to the finite set used in the first stage. This leads to a sequence of sub-problems. The method is known to be computationally intensive because the number of constraints increases at every iteration. In our case, the resolution of the sub-problems becomes even untractable. We thus retained in the constraint set only the latest optimal values for the uncertain parameters.

1) Sub-problem $\bar{\mathcal{P}}_2'$: In the first sub-problem, we compute the optimal precoder $\mathbf{V}_t$, receive filter $\mathbf{R}_l$ and AN covariance matrix $\mathbf{W}_t$ while the worst-case channel errors $\mathbf{\Delta}_{te}$ and $\mathbf{\Delta}_{tl}$ are supposed to be known. The first optimization sub-problem can be thus written as:

$$\begin{aligned} \underset{\substack{\mathbf{V}_t,\mathbf{W}_t,\mathbf{R}_l \\ t=1\ldots K_T, l=1\ldots K_R}}{\text{minimize}} \quad & \sum_{l=1}^{K_R} \epsilon_l \\ \text{subject to} \quad & C1, C2. \end{aligned} \tag{$\bar{\mathcal{P}}_2'$}$$

The optimization problem is similar to ($\mathcal{P}_1$) and can be solved using the proof given in Appendix B by replacing σ_{tl}^2 by $||\mathbf{\Delta}_{tl}||^2$, and σ_{te}^2 by $||\mathbf{\Delta}_{te}||^2$.

2) Sub-problem $\bar{\mathcal{P}}_2''$: In this sub-problem, the transceiver matrices and the worst-case error $\mathbf{\Delta}_{te}$ are supposed to be known and we look for the worst-case error $\mathbf{\Delta}_{tl}$. We can thus formulate the second sub-problem as:

$$\begin{aligned} \underset{\substack{\mathbf{\Delta}_{tl} \\ t=1\ldots K_T, l=1\ldots K_R}}{\text{minimize}} \quad & -\sum_{l=1}^{K_R} \epsilon_l \\ \text{subject to} \quad & C4: ||\mathbf{\Delta}_{tl}||^2 \leq \tau_{tl} \quad \forall t, \forall l. \end{aligned} \tag{$\bar{\mathcal{P}}_2''$}$$

The Lagrangian is given by:

$$\begin{aligned} \mathrm{L}(\mathbf{\Delta}_{tl}, \kappa_{tl}) &= -\sum_{l=1}^{K_R} \epsilon_l + \sum_{t=1}^{K_T}\sum_{l=1}^{K_R} (\kappa_{tl}(||\mathbf{\Delta}_{tl}||^2 - \tau_{tl})) \\ &= -\sum_{l=1}^{K_R} \epsilon_l + \sum_{t=1}^{K_T}\sum_{l=1}^{K_R} (\kappa_{tl}(\mathrm{tr}(\mathbf{\Delta}_{tl}\mathbf{\Delta}_{tl}^H) - \tau_{tl})) \end{aligned} \tag{22}$$

Algorithm 3: Iterative procedure to obtain transceiver filters for NBEs

1: **Input:** β, K_T, K_R, K_E, $\mathbf{E}_e$, $\widehat{\mathbf{C}}_{tl}$, $\widehat{\mathbf{G}}_{te}$, τ_{tl}, τ_{te}, P_T, $\Gamma \quad \forall\, t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, and $e \in \{1, \cdots, K_E\}$
2: **Init:** Randomly generate $\mathbf{V}_t$, $\mathbf{W}_t$ $\forall t \in \{1, \cdots, K_T\}$, $\mathbf{\Delta}_{tl} \in \mathcal{C}_{tl}$, $\mathbf{\Delta}_{te} \in \mathcal{G}_{te}$, $\epsilon_l \leftarrow 0 \quad \forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, $e \in \{1, \cdots, K_E\}$.
3: **repeat**
4: $\quad \epsilon_l' \leftarrow \epsilon_l \quad \forall l \in \{1, \cdots, K_R\}$
5: $\quad$ Solve $\bar{\mathcal{P}}_2'$ and update $\mathbf{V}_t$, $\mathbf{W}_t$, $\mathbf{R}_l$ using $\mathbf{\Delta}_{tl}$, $\mathbf{\Delta}_{te}$, $\mathbf{E}_e$ and Algorithm 2 $\forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, $e \in \{1, \cdots, K_E\}$.
6: $\quad$ Solve $\bar{\mathcal{P}}_2''$ and update $\mathbf{\Delta}_{tl}$ using $\mathbf{V}_t$, $\mathbf{W}_t$, $\mathbf{R}_l$ in (26) $\forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$.
7: $\quad$ Solve $\bar{\mathcal{P}}_2'''$ and update $\mathbf{\Delta}_{te}$ using $\mathbf{V}_t$, $\mathbf{W}_t$, $\mathbf{E}_e$ in (27) $\forall t \in \{1, \cdots, K_T\}$, $e \in \{1, \cdots, K_E\}$.
8: $\quad$ Compute ϵ_l using $\mathbf{V}_t$, $\mathbf{W}_t$, and $\mathbf{R}_l$, $\mathbf{\Delta}_{tl}$, $\mathbf{\Delta}_{te}$ in (15).
9: **until** $|\epsilon_l - \epsilon_l'| \leq \beta \quad \forall l \in \{1, \cdots, K_R\}$.

where $\kappa_{tl} \geq 0$ are the Lagrange multipliers associated to constraints $C4$. Considering (15), it is observed that solving ($\bar{\mathcal{P}}_2''$) is difficult. To simplify the solution, we consider an approximation of ϵ_l by ignoring the second and higher order terms of $\mathbf{\Delta}_{tl}$. With this approximation, the problem becomes convex and can be solved exactly (with zero dual gap). Taking the partial derivatives of the Lagrangian with respect to $\mathbf{\Delta}_{tl}^H$ and to κ_{tl}, respectively, and equating to zero we obtain:

$$\begin{aligned}\mathbf{\Delta}_{tl} &= \frac{1}{\kappa_{tl}}(\mathbf{R}_l^H\mathbf{V}_t^H + \mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H \\ &\quad +\sigma_{zt}^2\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H) \qquad (23)\\ \tau_{tl} &= \mathrm{tr}(\mathbf{\Delta}_{tl}\mathbf{\Delta}_{tl}^H). \qquad (24)\end{aligned}$$

Injecting (23) in (24), we obtain the Lagrange multipliers:

$$\begin{aligned}\kappa_{tl} &= \frac{1}{\sqrt{\tau_{tl}}}||(\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H + \sigma_{zt}^2\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H \\ &\quad +\mathbf{R}_l^H\mathbf{V}_t^H)||. \qquad (25)\end{aligned}$$

Using the value of κ_{tl} in (23), we get the following lemma.

Lemma 3. *The worst-case error $\mathbf{\Delta}_{tl}$ that provides the maximum SMSE at the legitimate UEs for given optimal transceivers and AN while satisfying the norm-bound constraint τ_{tl} is given by:*

$$\mathbf{\Delta}_{tl} = \sqrt{\tau_{tl}}\frac{\mathbf{\Upsilon}_{\mathbf{tl}}}{||\mathbf{\Upsilon}_{tl}||} \qquad (26)$$

where

$$\mathbf{\Upsilon}_{tl} = \mathbf{R}_l^H\mathbf{V}_t^H + \mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H + \sigma_{zt}^2\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H.$$

3) Sub-problem $\bar{\mathcal{P}}_2'''$: In this third sub-problem, the transceiver matrices and the worst-case error $\mathbf{\Delta}_{tl}$ are supposed to be known and we look for the worst-case error $\mathbf{\Delta}_{te}$. It can be found by solving the problem defined in constraint $C5$. The sub-problem can thus be written as:

$$\begin{aligned}&\underset{\mathbf{\Delta}_{te}, t=1\ldots K_T}{\text{minimize}} \quad \epsilon_e \geq \Gamma \\ &\text{subject to} \quad C3: ||\mathbf{\Delta}_{te}||^2 \leq \tau_{te} \quad \forall t.\end{aligned} \qquad (\bar{\mathcal{P}}_2''')$$

We adopt here the same approach as for (P2") and solve exactly the problem (with zero dual gap).

Lemma 4. *The worst-case error $\mathbf{\Delta}_{te}$ that provides the MMSE at the eavesdroppers for given optimal transceivers and AN while satisfying the norm-bound τ_{te} is given by:*

$$\mathbf{\Delta}_{te} = -\sqrt{\tau_{te}}\frac{\mathbf{\Upsilon}_{te}}{||\mathbf{\Upsilon}_{te}||} \qquad (27)$$

where

$$\mathbf{\Upsilon}_{te} = \mathbf{E}_e^H\mathbf{V}_t^H + \mathbf{E}_e^H\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t\mathbf{V}_t^H + \sigma_{zt}^2\mathbf{E}_e^H\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{W}_t\mathbf{W}_t^H.$$

A stationary solution for ($\bar{\mathcal{P}}_2$) is now obtained by a three step iterative process as given in Algorithm 3. We first obtain the optimal solution considering that the channel errors are known. Afterwards, the worst case channel errors are computed considering the optimal solution is known.

Complexity analysis – The computation of ϵ_l using (15) is again in $O(KN^3)$. The computation of $\mathbf{\Delta}_{tl}$ and $\mathbf{\Delta}_{te}$ involves K matrix multiplications and is thus $O(KN^3)$. The complexity of Algorithm 3 is thus dominated by the inner loop constituted by Algorithm 2.

Lemma 5. *Let I_3 be the number of iterations of Algorithm 3. The complexity of Algorithm 3 is at most $O(I_3I_2KN^3 + I_3I_2K^3\varepsilon^{-3})$.*

Convergence analysis – The cutting-set method is known to converge to a first-order stationary point [62]. In our case, we are not able to guarantee such a convergence because of the introduced simplification in the method. As suggested by [64], we can however interpret the robust problem as a dynamic game between two players. Player 1 tries to minimize the objective function by setting the optimization variables, while Player 2 tries to maximize it by setting the uncertainty realizations. In this framework, our algorithm can be interpreted as a *best response* algorithm and we know that if this algorithm converges, it converges to a Nash equilibrium of the game. Moreover, we observe in our simulation that generally $I_3 = 8$ iterations are sufficient to achieve convergence of the algorithm (see Fig. 10 and related discussion in Section IV).

IV. Numerical Results

In this section, we illustrate the performance of our designs with numerical simulations at physical layer and at system level.

A. Physical Layer Simulations

In physical layer simulations, there is no co-channel interference and both legitimate UEs and eavesdroppers experience the same path-loss. In results, we refer to the Non-Robust (NR) design, Robust (R) design, SE and NBE. Unless otherwise specified, the simulation parameters are the following: $K_T = 4$, $K_R = 8$, $K_E = 2$, $N_T = 16$, $N_R = 8$, $N_E = 4$, and $N_s = 2$; $P_T = 0$ dBm; $\sigma_{nl}^2 = P_T/\text{SNR}$, $l = 1, 2, .., K_R$, $\sigma_{ne}^2 = P_T/\text{SNR}$, $e = 1, .., K_E$, where

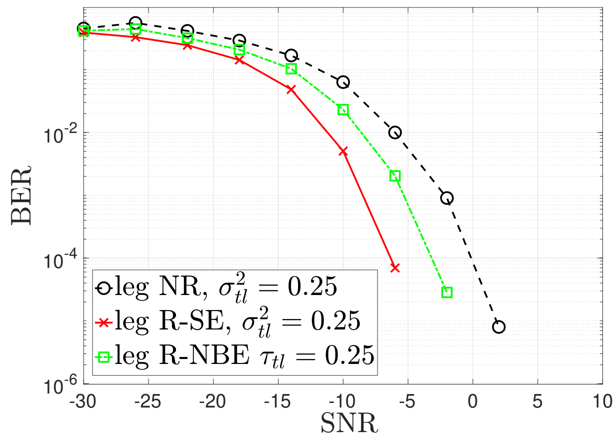


Fig. 3: BER at legitimate UEs (leg) vs. transmit SNR (in dB) with non-robust (NR), robust with SEs (R-SE) and robust with NBEs (R-NBE) designs ($K_T = 8$, $K_R = 16$, $K_E = 4$, eavesdroppers experience NBE with $\tau_{te} = 0.09$).

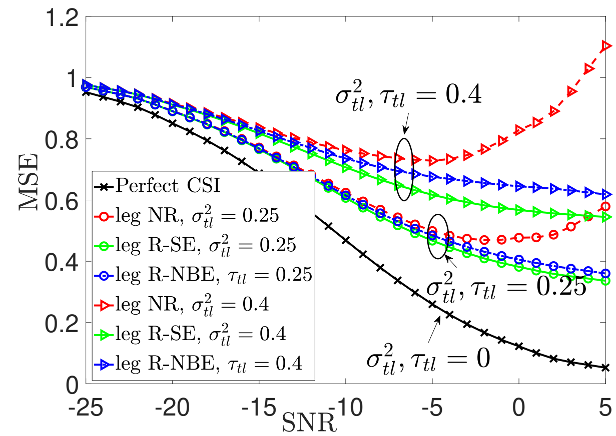


Fig. 4: MSE at legitimate UEs (leg) vs. transmit SNR (in dB) with perfect CSI, non-robust (NR) and robust (R) designs with SEs or NBEs ($P_T = 20$ dBm, eavesdroppers experience NBE with $\tau_{te} = 0.09$).

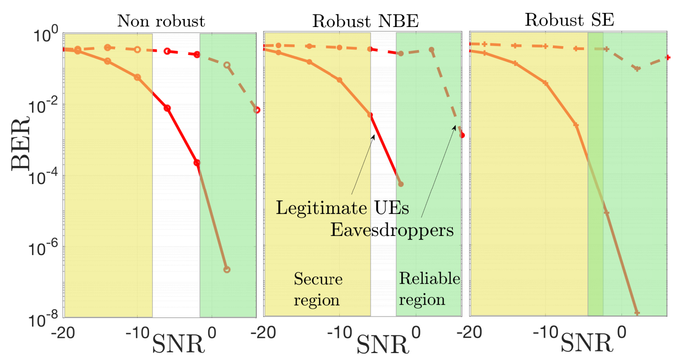


Fig. 5: BER vs. transmit SNR (dB) and BER Security gap for non-robust, robust with NBE and robust with SE (target BER of 0.3 for eavesdroppers, target BER of 10^{-4} for legitimate UEs).

SNR is the transmit SNR. For the R-SE design, $\sigma_{tl}^2 = 0.04$ and $\sigma_{te}^2 = 0.09$. For the R-NBE design, $\tau_{tl} = 0.04$ and $\tau_{te} = 0.09$. AN variance is $\sigma_{zt}^2 = 0.09$. The target MSE threshold at each eavesdropper is $\Gamma = 0.5$, a value that leads to high BERs according to our simulations. We assume a QPSK modulation and average performance metrics over 10^6 data samples for every simulation. In Algorithm 2 and 3, $\beta = 10^{-4}$. Video conferencing requires a typical Bit Error Rate (BER) of 10^{-4} [65]. In 5G NR, the MCC video service is mapped on the quality of service indicator QCI67 [66], which requires a packet loss rate of 10^{-3}. This can lead to typical BERs of 10^{-6} or 10^{-7} after channel decoding for a packet length of 1000 Bytes. In the numerical results below, we thus observe typical BERs between 10^{-4} and 10^{-6} for legitimate users.

1) Effect of CSI errors: Fig. 3 shows the BER as a function of the transmit SNR for robust and non-robust designs at legitimate UEs. We observe the interest of designing a system robust to CSI errors to improve the reliability of MCC: up to 6 dB gain can be achieved at low BER when assuming SEs. As expected, the performance in presence of NBEs is worse than with SEs. This is due to the higher noise uncertainty: noise is drawn in a sphere of known radius but there is no further statistical knowledge about it. Nevertheless, NBE-based robust design achieves a 3 dB gain at low BER.

Fig. 4 shows the effect of different channel error variances on the MSE at legitimate UEs, which is our objective in the proposed minimization problems. Obviously the scenario with perfect CSI performs the best. Then, as expected, the higher the channel errors the lower the performance. The knowledge of the probability distribution function of noise (SE) is a clear advantage over sole knowledge of an upper bound (NBE) for a robust design.

We observe in Fig. 4 that the MSE is increasing with the SNR after a certain threshold when NR designs are considered. The MSE at legitimate users is indeed made of several components. In particular, the last two terms of (15) are due to CSI errors and are increasing with the signal power, whereas other components are decreasing and tend towards zero. In NR designs, receive filters do not compensate for these terms because CSI is supposed to be perfect, so that the overall MSE starts increasing when the CSI error component becomes preponderant.

2) Security Gap: The security gap is a measure of the secrecy level based on the BER performance of legitimate UEs and eavesdroppers. The security gap is defined as $S_g = SNR_{min}^L - SNR_{max}^E$ where SNR_{min}^L is the minimum SNR at a legitimate UE to achieve high reliability (e.g. 10^{-4} in our simulations) and SNR_{max}^E is the maximum SNR that guarantees a high BER at a eavesdropper (e.g. 0.3). Below SNR_{max}^E at eavesdroppers, the communication is secure, above SNR_{min}^L at legitimate UEs, the communication is reliable. The gap quantifies the advantage a legitimate UE should have over eavesdroppers in order to have a secure and reliable communication. We see in Fig. 5 (left) that multi-user MIMO and AN leads already to a small security gap (4.5 dB) even with a non-robust design. Proposed robust designs allow an even smaller gap, especially with the negative security gap achieved with SE model design (2.5 dB with NBE in the center and -2.3 dB with SE on the right of the figure).

3) Secrecy Rate: Secrecy rate is a well-studied physical layer security metric and is defined as the difference between the achievable rate at the legitimate users and at the eavesdroppers. Following [67], [68], we adopt the following definition of the secrecy rate for the proposed multi-BS multicast system in presence of multiple eavesdroppers:

$$\text{secrecy rate} = \sum_{l=1}^{K_R}\Bigg(\log\big(1+\sum_{t=1}^{K_T}\frac{|\mathbf{C}_{tl}\mathbf{V}_t|^2}{|\mathbf{C}_{tl}\mathbf{W}_t|^2+\sigma_{tl}^2}\big) - \max_{1\le e\le K_E}\log\big(1+\sum_{t=1}^{K_T}\frac{|\mathbf{G}_{te}\mathbf{V}_t|^2}{|\mathbf{G}_{te}\mathbf{W}_t|^2+\sigma_{te}^2}\big)\Bigg) \quad (28)$$

In Fig. 6 and 7, we show the secrecy rate performance of the proposed R-NBE system as a function of the SNR. In Fig. 6, the performance is observed with different MSE thresholds ($\Gamma = 0.1, 0.3, 0.5$) at the eavesdroppers. As expected, the achievable secrecy rate increases with the SNR. Moreover, a positive secrecy rate is achieved, even at very low SNR. This validates the secure communication of the proposed system. At last, secrecy rate is increasing with the MSE threshold, which shows that we can control the secrecy rate outage by varying this parameter.

The secrecy rate performance of the proposed system with and without AN is shown in Fig 7. For both the cases, secrecy rate increases with increasing SNR. The proposed system design without AN is able to achieve positive secrecy rate for the whole SNR range and thus demonstrates a good performance. Adding AN is further deteriorating the signal at the eavesdroppers and hence achieving improved overall secrecy performance. Tuning AN variance is thus another means of controlling secrecy rate outage.

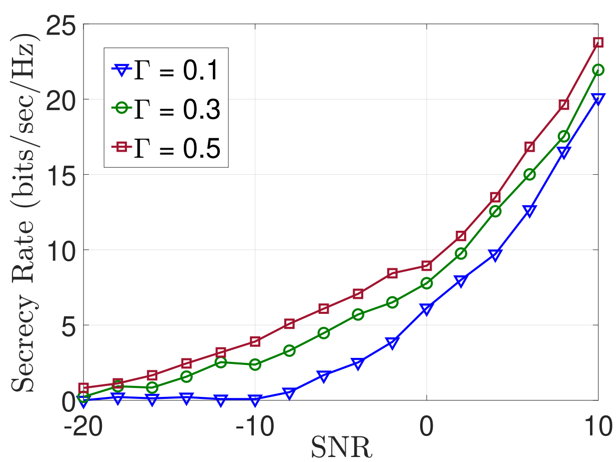


Fig. 6: Secrecy rate vs varying SNR for the proposed robust NBE design (R-NBE) for different values of MSE thresholds at the eavesdroppers (Γ.)

4) Effect of AN: Fig. 8 shows the effect of the AN variance on the BER of legitimate UEs and eavesdroppers for the R-NBE design. It is first observed that the BER of the legitimate UEs is significantly lower than the eavesdroppers BER, hence guaranteeing a reliable communication. The addition of AN lowers a bit the performance of legitimate UEs as some power

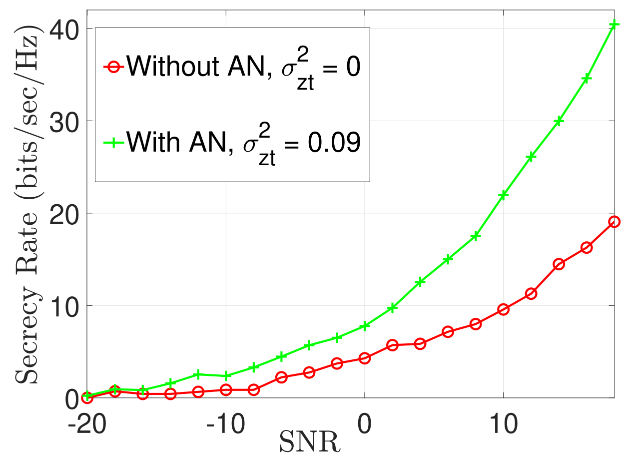


Fig. 7: Secrecy rate vs varying SNR for the proposed robust NBE (R-NBE) design by considering with and without the presence of AN.

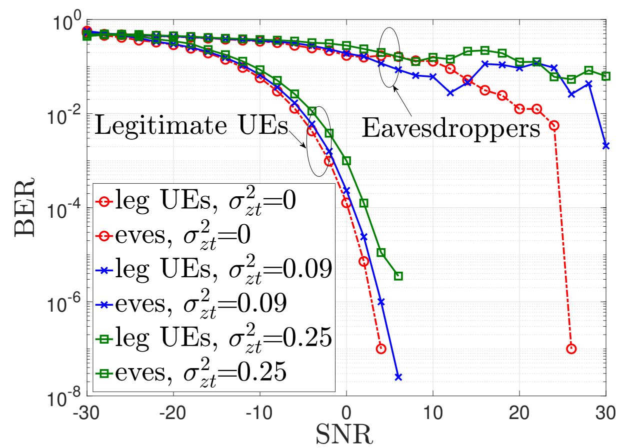


Fig. 8: BER vs. transmit SNR (dB) at legitimate UEs (leg) and eavesdroppers (eves) for varying AN variance for robust NBEs (R-NBE) design ($\tau_{tl} = 0.04$, $\tau_{te} = 0.09$).

is dedicated to it. On the contrary for eavesdroppers, there is a significant gap between the system performance with and without AN. For the specific case of multicast MCC, this confirms the interest of AN for secure communications shown in the literature in other contexts. Fig. 9 shows the MSE at eavesdroppers as a function of the threshold Γ considered in our optimization problems. It is observed that the system designed without the consideration of AN is not always able to satisfy the requirement, whereas all the thresholds are readily satisfied by the AN-aided system design. Further, with the increase in the variance of AN, the system is more likely to achieve higher thresholds and inherently provides enhanced security against eavesdroppers.

5) Convergence: The convergence of the proposed iterative algorithms is observed through simulations for the NR, R-SE, and R-NBE system designs and is shown in Fig. 10. The figure depicts the SMSE values for the legitimate UEs with respect to the number of iterations for two different SNR values. Even though the global convergence cannot be guaranteed,

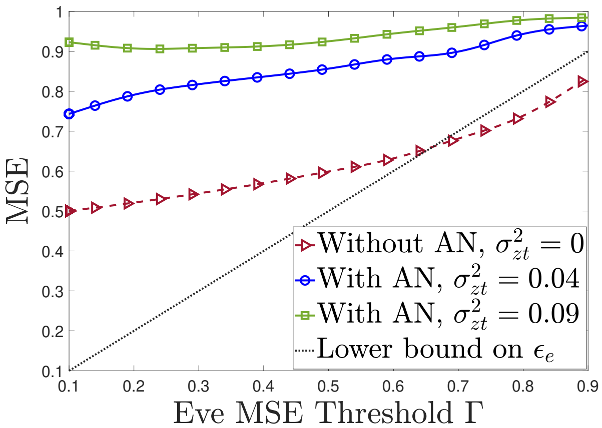


Fig. 9: MSE at eavesdropper vs eavesdropper (eve) MSE threshold Γ for varying AN at $SNR = -10$ dB for robust NBEs (R-NBE) design.

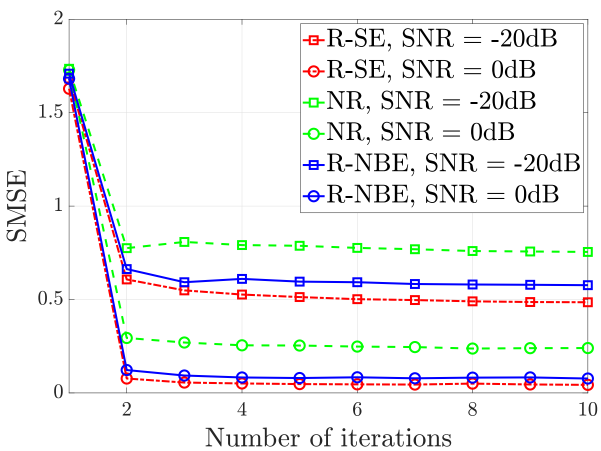
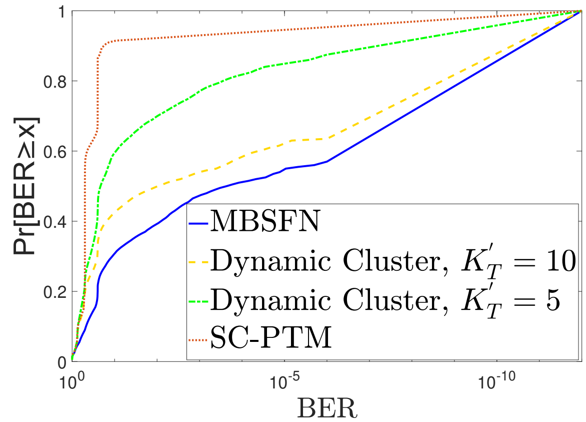


Fig. 10: Convergence behavior of the proposed iterative algorithms for NR, R-SE, and R-NBE system designs.

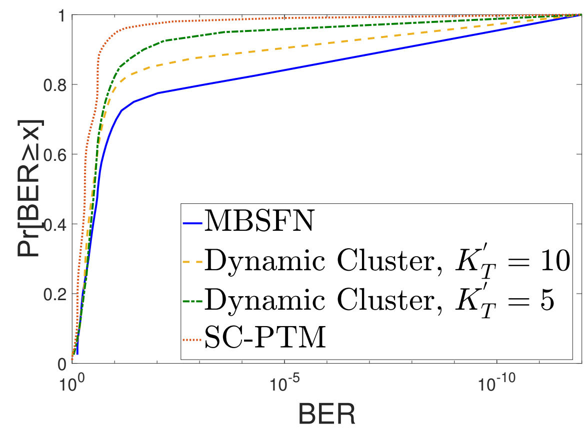
simulations illustrate the fact that SMSE values monotonically decreases with each iteration and achieves convergence to a stationary point. It can also be observed that the proposed iterative algorithms quickly converge in less than ten iterations for all the designs. Furthermore, as expected, lower SMSE value is achieved with higher SNR due to the enhanced signal quality.

B. System Level Simulations

System level simulations allow us to account for co-channel interference and random locations of the users. We consider 100 BSs, distributed over an area of 10 km^2, drawn according to a Poisson process. The synchronization area is made of 20 BSs (see Fig. 1). The path-loss between BSs and users is calculated as per Okumura-Hata model using a carrier frequency of 700 MHz as given in [69] (a typical frequency for MCC). We assume $N_T = 16$, $N_R = 8$, $N_E = 4$, $N_s = 2$, $P_T = 46$ dBm. The system considered is with robust-NBE at both legitimate UEs and eavesdroppers with $\tau_{tl} = 0.04$ and $\tau_{te} = 0.09$ respectively. AN at t-th BS is set to $\sigma_{zt}^2 = 0.04$.



(a) BER CDF for legitimate UEs.



(b) BER CDF for eavesdroppers.

Fig. 11: BER CDF with MBSFN, SC-PTM and dynamic clustering.

For a simulation, a team leader is uniformly drawn in the synchronization area and then 9 team members are selected within a distance of 500 m. Two eavesdroppers are randomly drawn within the same distance around the team leader. All the simulations are executed over 10^6 data streams. Simulations are performed for 100 groups.

Fig. 11 shows the BER CDF of legitimate UEs (a) and eavesdroppers (b) for different clustering approaches: MBSFN (the whole synchronization area serves the legitimate UEs), SC-PTM (only cells covering UEs multicast information without cooperation) and dynamic greedy clustering (Algorithm 1, where $K_T^{\prime}$ controls the minimum number of BSs involved in the cluster). As expected MBSFN provides the best performance, SC-PTM the worst and dynamic clustering offers a tradeoff[2]. This is true for both legitimate UEs and eavesdroppers but the gap between the two is much higher with MBSFN compared to SC-PTM. MBSFN should thus be preferred for secure and highly reliable MCC. However, a drawback of MBSFN is that it consumes radio resources in every BS of the synchronization area and thus suffers from low capacity. If an operator wants to increase its network

[2]SC-PTM provides however the best performance in terms of system capacity as studied in [10].

capacity, it should trade-off the security and reliability level against capacity by adopting a dynamic clustering scheme. Dynamic clustering with $K'_T = 10$ BSs, which is half of the synchronization area represents for example here a good trade-off.

Fig. 12 depicts the secrecy rate outage probability of the proposed system for different clustering methods: MBSFN, SCPTM, and dynamic greedy clustering with cluster sizes as 5 and 10. It is observed that MBSFN achieves the best secrecy performance, the SC-PTM demonstrates the worst whereas the performance of dynamic clustering is in between. For example, with a target secrecy rate of 10 bits/sec/Hz, 90% of the users observe outage with SC-PTM, while outage probability is 43% with dynamic clustering with a cluster size of 5, 38% with a cluster size of 10 and 30% with MBSFN. The performance thus increases with the number of BSs involved in the multicast transmission thanks to the combined effect of AN and beamforming.

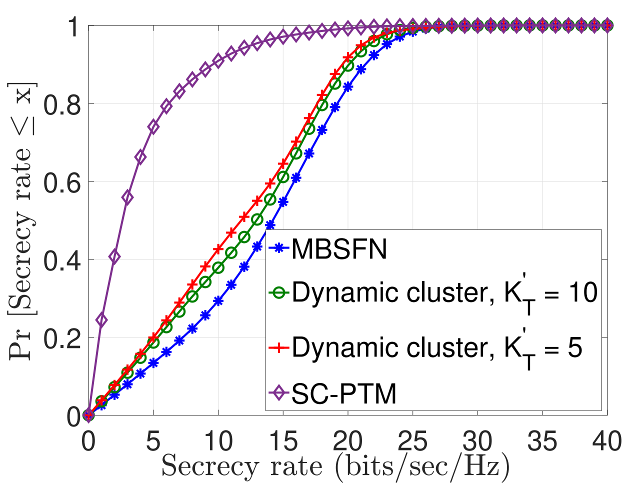


Fig. 12: Secrecy rate CDF for comparing system level performance among systems using MBSFN, SC-PTM and dynamic clustering.

V. CONCLUSION

We propose a secure MIMO transceiver design for multi-BS multicast MCC that are resilient towards CSI errors following stochastic and norm-bounded error models. SMSE minimization problems are formulated under the constraint of maximum transmit power at every BS and minimum MSE at every eavesdropper. The BSs forming the coordinating cluster are obtained dynamically by using a greedy algorithm. Security is added in the system by optimal MIMO beamforming and by introducing an additional AN at the transmitters. The desired AN filter is jointly designed along with the precoder and receiver filters by solving the considered optimization problems using iterative and worst-case approaches. The performance is evaluated in terms of various parameters including security gap, BER and MSE. The computational analysis is also conducted and presented for both error model-based proposed designs. Numerical results reveal the crucial role of robust designs for MCC, even in presence of norm-bounded errors. Adding AN degrades only slightly the performance of legitimate users but significantly improves the security of their communication. At last, we highlight the fact that increasing the number of cooperating BSs improves both reliability and security. However, dynamic clustering can represent a good trade-off if capacity becomes a requirement.

APPENDIX A
PROOF OF LEMMA 1

The transmit power can be expressed as follows:

$$\begin{aligned} P_t &\triangleq \mathbb{E}[||\mathbf{x}_t\mathbf{x}_t^H||] = \mathbb{E}[\mathrm{tr}(\mathbf{x}_t\mathbf{x}_t^H)] \\ &= \mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H + \mathbf{W}_t). \end{aligned} \tag{29}$$

The MSE ϵ_l at the legitimate user l is computed as follows:

$$\begin{aligned} \epsilon_l &\triangleq \mathbb{E}[||\mathbf{d} - \widehat{\mathbf{d}}_l||^2] \\ &= \mathbb{E}\Big[||\mathbf{d} - (\sum_{t=1}^{K_T}\mathbf{R}_l(\widehat{\mathbf{C}}_{tl} + \mathbf{\Delta}_{tl})\mathbf{V}_t\mathbf{d} \\ &\quad + \sum_{t=1}^{K_T}\mathbf{R}_l(\widehat{\mathbf{C}}_{tl} + \mathbf{\Delta}_{tl})\mathbf{w}_t + \mathbf{R}_l\mathbf{n}_l)||^2\Big] \\ &= \mathrm{tr}(\mathbf{I}) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H) \\ &\quad + \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H) \\ &\quad + \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H) + \sigma_{nl}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H) \\ &\quad + \mathbb{E}\big[\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\mathbf{\Delta}_{tl}\mathbf{V}_t\mathbf{V}_t^H\mathbf{\Delta}_{tl}^H\mathbf{R}_l^H)\big] \\ &\quad + \mathbb{E}\big[\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\mathbf{\Delta}_{tl}\mathbf{W}_t\mathbf{\Delta}_{tl}^H\mathbf{R}_l^H)\big]. \end{aligned} \tag{30}$$

The last two terms can be simplified by using the trace property as given in Lemma 1 in [40].
Incorporating the property will yields (15). Similarly, MSE at e-th eavesdropper is given as:

$$\begin{aligned} \epsilon_e &\triangleq \mathbb{E}\Big[||\mathbf{d} - \overline{\mathbf{d}}_e||^2\Big] \\ &= \mathbb{E}\Big[||\mathbf{d} - (\sum_{t=1}^{K_T}\mathbf{E}_e(\widehat{\mathbf{G}}_{te} + \mathbf{\Delta}_{te})\mathbf{V}_t\mathbf{d} \\ &\quad + \sum_{t=1}^{K_T}\mathbf{E}_e(\widehat{\mathbf{G}}_{te} + \mathbf{\Delta}_{te})\mathbf{w}_t + \mathbf{E}_e\mathbf{n}_e)||^2\Big] \\ &= \mathrm{tr}(\mathbf{I}) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) \\ &\quad + \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) \\ &\quad + \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{W}_t\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) + \sigma_{ne}^2\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H) \end{aligned}$$

$$+\mathbb{E}\big[\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\mathbf{\Delta}_{te}\mathbf{V}_t\mathbf{V}_t^H\mathbf{\Delta}_{te}^H\mathbf{E}_e^H)\big]$$
$$+\mathbb{E}\big[\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\mathbf{\Delta}_{te}\mathbf{W}_t\mathbf{\Delta}_{te}^H\mathbf{E}_e^H)\big]. \quad (31)$$

Again, the application of the trace property provides the result (16).

Appendix B
Proof of Proposition 1

We use here two binary slack variables χ_l and χ_e in order to consider at once different problems introduced in the paper. $\chi_l = 1$ corresponds to a robust solution for legitimate users and $\chi_l = 0$ to a non-robust design. $\chi_e = 1$ corresponds to a perfect eavesdroppers CSI at the transmitter, otherwise $\chi_e = 0$. The generalized MSE equations are now reformulated as:

$$\begin{aligned}\epsilon_l \;=\;& \mathrm{tr}(\mathbf{I}) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H)\\
&+\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H)\\
&+\mathrm{tr}(\sum_{t=1}^{K_T}\sigma_{zt}^2\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{W}_t\mathbf{W}_t^H\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H) + \sigma_{nl}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H)\\
&+\chi_l\sum_{t=1}^{K_T}\sigma_{tl}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H)\mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H)\\
&+\chi_l\sum_{t=1}^{K_T}\sigma_{tl}^2\sigma_{zt}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H)\mathrm{tr}(\mathbf{W}_t\mathbf{W}_t^H). \quad (32)\end{aligned}$$

The e-th eavesdroppers MSE is simplified as:

$$\begin{aligned}\epsilon_e \;=\;& \mathrm{tr}(\mathbf{I}) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t) - \mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) +\\
&\mathrm{tr}(\sum_{t=1}^{K_T}\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t\mathbf{V}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) + \mathrm{tr}(\sum_{t=1}^{K_T}\sigma_{zt}^2\mathbf{E}_e\widehat{\mathbf{G}}_{te}\\
&\mathbf{W}_t\mathbf{W}_t^H\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H) + \sigma_{ne}^2\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H) + \chi_e\sum_{t=1}^{K_T}\sigma_{te}^2\\
&\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H)\mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H) + \chi_e\sum_{t=1}^{K_T}\sigma_{te}^2\sigma_{zt}^2\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H)\\
&\mathrm{tr}(\mathbf{W}_t\mathbf{W}_t^H). \quad (33)\end{aligned}$$

We solve the optimization problem ($\mathcal{P}_1$) by forming the Lagrangian L as below:

$$\begin{aligned}\mathrm{L}(\mathbf{V}_t,\mathbf{W}_t,\mathbf{R}_l,\lambda_e,\lambda_t^{'}) \;=\;& \sum_{l=1}^{K_R}\epsilon_l + \sum_{e=1}^{K_E}\lambda_e(\Gamma-\epsilon_e)\\
&+\sum_{t=1}^{K_T}\lambda_t^{'}\mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H\\
&+\sigma_{zt}^2\mathbf{W}_t\mathbf{W}_t^H) - P_T \quad (34)\end{aligned}$$

where λ_e and $\lambda_t^{'}$ are the Lagrange multipliers associated with e-th Eve's MSE constraint $C1$ and t-th BS's power constraint $C2$ respectively. The Lagrange multiplier approach is applicable for solving the optimization problems with equality conditions in the constraints. On the other hand, the Karush-Kuhn-Tucker (KKT) approach allows handling of the inequality constraints by generalizing the Lagrange multiplier based on the KKT conditions. In the formulated optimization problem $\mathcal{P}_1$, it can be seen that all the optimization constraints have inequality bounds. Hence, we utilize the KKT approach to restructure the constraints and solve the optimization problem. The KKT conditions for the problem $\mathcal{P}_1$ are as follows:

$$\begin{aligned}\frac{\partial \mathrm{L}}{\partial \mathbf{V}_t^H} &= 0\\
\frac{\partial \mathrm{L}}{\partial \mathbf{R}_l^H} &= 0\\
\frac{\partial \mathrm{L}}{\partial \mathbf{W}_t^H} &= 0\\
\Gamma-\epsilon_e &\leq 0\ \forall e\in\{1,\cdots,K_E\}\\
\lambda_e &\geq 0\ \forall e\in\{1,\cdots,K_E\}\\
\lambda_e(\Gamma-\epsilon_e) &= 0\ \forall e\in\{1,\cdots,K_E\}\\
\mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H+\sigma_{zt}^2\mathbf{W}_t\mathbf{W}_t^H)-P_T &\leq 0\ \forall t\in\{1,\cdots,K_T\}\\
\lambda_t^{'} &\geq 0\ \forall t\in\{1,\cdots,K_T\}\\
\lambda_t^{'}(\mathrm{tr}(\mathbf{V}_t\mathbf{V}_t^H+\sigma_{zt}^2\mathbf{W}_t\mathbf{W}_t^H)-P_T) &= 0\ \forall t\in\{1,\cdots,K_T\}.\end{aligned} \quad (35)$$

On taking these conditions into account, the desired transceivers are obtained by minimizing the Lagrangian with respect to each optimization variable while considering that the other variables as fixed. Hence, the precoder $\mathbf{V}_t$ is derived by taking the gradient of L with respect to $\mathbf{V}_t^H$, and is given as:

$$\begin{aligned}\frac{\partial \mathrm{L}}{\partial \mathbf{V}_t^H} \;=\;& -\sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H + \sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl}\mathbf{V}_t\\
&+\chi_l\sum_{l=1}^{K_R}\sigma_{tl}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H)\mathbf{V}_t + \sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\\
&-\sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\mathbf{E}_e\widehat{\mathbf{G}}_{te}\mathbf{V}_t\\
&-\chi_e\sum_{e=1}^{K_E}\lambda_e\sigma_{te}^2\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H)\mathbf{V}_t + \lambda_t^{'}\mathbf{V}_t. \quad (36)\end{aligned}$$

Equatting to zero leads to:

$$\begin{aligned}\mathbf{V}_t \;=\;& \Big(\sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H\mathbf{R}_l\widehat{\mathbf{C}}_{tl} + \chi_l\sum_{l=1}^{K_R}\sigma_{tl}^2\mathrm{tr}(\mathbf{R}_l\mathbf{R}_l^H)\mathbf{I}\\
&-\sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\mathbf{E}_e\widehat{\mathbf{G}}_{te} - \chi_e\sum_{e=1}^{K_E}\lambda_e\sigma_{te}^2\mathrm{tr}(\mathbf{E}_e\mathbf{E}_e^H)\mathbf{I}\\
&+\lambda_t^{'}\mathbf{I}\Big)^{-1}\Big(\sum_{l=1}^{K_R}\widehat{\mathbf{C}}_{tl}^H\mathbf{R}_l^H - \sum_{e=1}^{K_E}\lambda_e\widehat{\mathbf{G}}_{te}^H\mathbf{E}_e^H\Big). \quad (37)\end{aligned}$$

Receive filter $\mathbf{R}_l$ is obtained in the same way, i.e. by differentiating the Lagrangian with respect to $\mathbf{R}_l^H$, while considering all other variables as fixed, and assigning it to zero:

$$\begin{aligned}\frac{\partial \mathrm{L}}{\partial \mathbf{R}_l^H} &= -\sum_{t=1}^{K_T} \mathbf{V}_t^H \widehat{\mathbf{C}}_{tl}^H + \sum_{t=1}^{K_T} \mathbf{R}_l \widehat{\mathbf{C}}_{tl} \mathbf{V}_t \mathbf{V}_t^H \widehat{\mathbf{C}}_{tl}^H \\ &+ \sum_{t=1}^{K_T} \sigma_{zt}^2 \mathbf{R}_l \widehat{\mathbf{C}}_{tl} \mathbf{W}_t \mathbf{W}_t^H \widehat{\mathbf{C}}_{tl}^H + \sigma_{nl}^2 \mathbf{R}_l \\ &+ \chi_l \sum_{t=1}^{K_T} \sigma_{tl}^2 \mathrm{tr}(\mathbf{V}_t \mathbf{V}_t^H) \mathbf{R}_l \\ &+ \chi_l \sum_{t=1}^{K_T} \sigma_{tl}^2 \sigma_{zt}^2 \mathrm{tr}(\mathbf{W}_t \mathbf{W}_t^H) \mathbf{R}_l \qquad (38)\end{aligned}$$

$$\begin{aligned}\mathbf{R}_l &= \Big(\sum_{t=1}^{K_T} \mathbf{V}_t^H \widehat{\mathbf{C}}_{tl}^H\Big)\Big(\sum_{t=1}^{K_T} \widehat{\mathbf{C}}_{tl} \mathbf{V}_t \mathbf{V}_t^H \widehat{\mathbf{C}}_{tl}^H \\ &+ \sum_{t=1}^{K_T} \sigma_{zt}^2 \widehat{\mathbf{C}}_{tl} \mathbf{W}_t \mathbf{W}_t^H \widehat{\mathbf{C}}_{tl}^H + \sigma_{nl}^2 \mathbf{I} \\ &+ \chi_l \sum_{t=1}^{K_T} \sigma_{tl}^2 \mathrm{tr}(\mathbf{V}_t \mathbf{V}_t^H) \mathbf{I} \\ &+ \chi_l \sum_{t=1}^{K_T} \sigma_{tl}^2 \sigma_{zt}^2 \mathrm{tr}(\mathbf{W}_t \mathbf{W}_t^H) \mathbf{I}\Big)^{-1}. \qquad (39)\end{aligned}$$

Now, we differentiate the Lagrangian with respect to $\mathbf{W}_t^H$ and setting it to zero:

$$\begin{aligned}\frac{\partial \mathrm{L}}{\partial \mathbf{W}_t^H} &= \sum_{l=1}^{K_R} \sigma_{zt}^2 \widehat{\mathbf{C}}_{tl}^H \mathbf{R}_l^H \mathbf{R}_l \widehat{\mathbf{C}}_{tl} \mathbf{W}_t \\ &+ \chi_l \sigma_{zt}^2 \sum_{l=1}^{K_R} \sigma_{tl}^2 \mathrm{tr}(\mathbf{R}_l \mathbf{R}_l^H) \mathbf{W}_t \\ &- \sigma_{zt}^2 \sum_{e=1}^{K_E} \lambda_e \widehat{\mathbf{G}}_{te}^H \mathbf{E}_e^H \mathbf{E}_e \widehat{\mathbf{G}}_{te} \mathbf{W}_t \\ &- \chi_e \sigma_{zt}^2 \sum_{e=1}^{K_E} \lambda_e \sigma_{te}^2 \mathrm{tr}(\mathbf{E}_e \mathbf{E}_e^H) \mathbf{W}_t + \lambda_t^{'} \sigma_{zt}^2 \mathbf{W}_t \qquad (40)\end{aligned}$$

$$\begin{aligned}0 &= \sigma_{zt}^2 \Bigg[\sum_{l=1}^{K_R} \widehat{\mathbf{C}}_{tl}^H \mathbf{R}_l^H \mathbf{R}_l \widehat{\mathbf{C}}_{tl} + \chi_l \sum_{l=1}^{K_R} \sigma_{tl}^2 \mathrm{tr}(\mathbf{R}_l \mathbf{R}_l^H) \\ &- \sum_{e=1}^{K_E} \lambda_e \widehat{\mathbf{G}}_{te}^H \mathbf{E}_e^H \mathbf{E}_e \widehat{\mathbf{G}}_{te} \\ &- \chi_e \sum_{e=1}^{K_E} \lambda_e \sigma_{te}^2 \mathrm{tr}(\mathbf{E}_e \mathbf{E}_e^H) + \lambda_t^{'} \mathbf{I}\Bigg] \mathbf{W}_t. \qquad (41)\end{aligned}$$

This is equivalent to $\mathbf{A}_t \mathbf{W}_t = 0$ where

$$\begin{aligned}\mathbf{A}_t &= \sum_{l=1}^{K_R} \widehat{\mathbf{C}}_{tl}^H \mathbf{R}_l^H \mathbf{R}_l \widehat{\mathbf{C}}_{tl} + \chi_l \sum_{l=1}^{K_R} \sigma_{tl}^2 \mathrm{tr}(\mathbf{R}_l \mathbf{R}_l^H) \\ &- \sum_{e=1}^{K_E} \lambda_e \widehat{\mathbf{G}}_{te}^H \mathbf{E}_e^H \mathbf{E}_e \widehat{\mathbf{G}}_{te} \\ &- \chi_e \sum_{e=1}^{K_E} \lambda_e \sigma_{te}^2 \mathrm{tr}(\mathbf{E}_e \mathbf{E}_e^H) + \lambda_t^{'} \mathbf{I}. \qquad (42)\end{aligned}$$

In the condition $\mathbf{A}_t \mathbf{W}_t = 0$, $\mathbf{A}_t$ cannot be zero because otherwise effective components in the design of the precoder would be zero and the precoder matrix would be non-singular. This would invalidate the complete design. As a consequence, the AN shaping matrix $\mathbf{W}_t$ should be taken in the null space of $\mathbf{A}_t$ and $\mathbf{W}_t = \mathbf{B}_t / \sqrt{\mathrm{tr}(\mathbf{B}_t \mathbf{B}_t^H)}$, where $\mathbf{B}_t = \mathbf{I} - \mathbf{A}_t^H (\mathbf{A}_t \mathbf{A}_t^H)^{-1} \mathbf{A}_t$. At last, differentiating the Lagrangian with respect to $\lambda_t^{'}$ and λ_e respectively and setting to zero we get:

$$\begin{aligned}\frac{\partial \mathrm{L}}{\partial \lambda_t^{'}} &= \mathrm{tr}(\mathbf{V}_t \mathbf{V}_t^H + \sigma_{zt}^2 \mathbf{W}_t \mathbf{W}_t^H) - P_T = 0 \qquad (43) \\ \frac{\partial \mathrm{L}}{\partial \lambda_e} &= \Gamma - \epsilon_e = 0. \qquad (44)\end{aligned}$$

The values for λ_e, $e = \{1, 2, \cdots, K_E\}$ and $\lambda_t^{'}$, $t = \{1, 2, \cdots, K_T\}$ are jointly computed by inserting the values of $\mathbf{V}_t$ and $\mathbf{W}_t$ in (43) and (44) so as to satisfy the thresholds P_t for all t and ϵ_e for all e. The Lagrange multipliers are obtained such that they satisfy the KKT conditions in (35) which result in positive values for λ_e and $\lambda_t^{'}$ or zeros otherwise.

REFERENCES

[1] TCCA, "Critical Communications and Mobile Network Operators," The Critical Communications Association (TCCA), Tech. Rep., May 2018.

[2] Y. Lair and G. Mayer, "Mission Critical Services in 3GPP," 3rd Generation Partnership Project, Tech. Rep., Jun. 2017. [Online]. Available: https://www.3gpp.org/news-events/1875-mcservices

[3] 3GPP, "Mission Critical Services Common Requirements," 3rd Generation Partnership Project, Tech. Rep. TS 22.280, Jul. 2018.

[4] J. Li, K. K. Nagalapur, E. Stare, S. Dwivedi, S. A. Ashraf, P. Eriksson, U. Engström, W. Lee, and T. Lohmar, "5G New Radio for Public Safety Mission Critical Communications," *CoRR*, vol. abs/2103.02434, 2021.

[5] A. Prasad, A. Maeder, K. Samdanis, A. Kunz, and G. Velev, "Enabling Group Communication for Public Safety in LTE-Advanced Networks," *Journal of Network and Computer Applications*, vol. 62, pp. 41–52, Feb. 2016.

[6] A. Daher, M. Coupechoux, P. Godlewski, J.-M. Kelif, P. Ngouat, and P. Minot, "SINR Model for MBSFN Based Mission Critical Communications," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sept. 2017, pp. 1–5.

[7] MCC Work Plan Manager (Alain Sultan), "Release 13 analytical view," 3rd Generation Partnership Project, Tech. Rep. TSG RP-151569, Sept. 2015.

[8] A. Papadogiannis, D. Gesbert, and E. Hardouin, "A Dynamic Clustering Approach in Wireless Networks with Multi-Cell Cooperative Processing," in *2008 IEEE International Conference on Communications*, May 2008, pp. 4033–4037.

[9] A. Papadogiannis and G. C. Alexandropoulos, "The Value of Dynamic Clustering of Base Stations for Future Wireless Networks," in *International Conference on Fuzzy Systems*, July 2010, pp. 1–6.

[10] A. Daher, M. Coupechoux, P. Godlewski, P. Ngouat, and P. Minot, "A Dynamic Clustering Algorithm for Multi-Point Transmissions in Mission-Critical Communications," *IEEE Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4934–4946, July 2020.

[11] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[12] L. Mucchi, F. Nizzi, T. Pecorella, R. Fantacci, and F. Esposito, "Benefits of Physical Layer Security to Cryptography: Tradeoff and Applications," in *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, June 2019, pp. 1–3.

[13] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[14] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter Design With Secrecy Constraints: The MIMO Gaussian Wiretap Channel," *IEEE Transactions on Signal Processing*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[15] N. Lee, O. Simeone, and J. Kang, “The Effect of Imperfect Channel Knowledge on a MIMO System with Interference,” *IEEE Transactions on Communications*, vol. 60, no. 8, pp. 2221–2229, Aug. 2012.

[16] X. Zhang, D. P. Palomar, and B. Ottersten, “Statistically Robust Design of Linear MIMO Transceivers,” *IEEE Transactions on Signal Processing*, vol. 56, no. 8, pp. 3678–3689, Aug. 2008.

[17] M. B. Shenouda and T. N. Davidson, “Convex Conic Formulations of Robust Downlink Precoder Designs With Quality of Service Constraints,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 714–724, Dec. 2007.

[18] X. Yu, Q. Li, M. Xie, and H. Shi, “Performance of Uplink Multicell Multiuser Massive SM-MIMO Systems With Imperfect CSI and Pilot Contamination,” *IEEE Systems Journal*, vol. 15, no. 3, pp. 3573–3584, Sept. 2021.

[19] E. Björnson, J. Hoydis, and L. Sanguinetti, “Massive MIMO Networks: Spectral, Energy, and Hardware Efficiency,” *Foundations and Trends in Signal Processing*, vol. 11, no. 3-4, pp. 154–655, Nov. 2017.

[20] C. E. Shannon, “Communication Theory of Secrecy Systems,” *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[21] A. Khisti and G. W. Wornell, “Secure Transmission With Multiple Antennas—Part I: The MISOME Wiretap Channel,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[22] ——, “Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel,” *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[23] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Singapore: Springer, 2014.

[24] L. Zhang, Y. Cai, B. Champagne, and M. Zhao, “Non-Linear Transceiver Design for Secure Communications with Artificial Noise-Assisted MIMO relay,” *IET Communications*, vol. 11, no. 6, pp. 930–935, Mar. 2017.

[25] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, “Artificial-Noise-Aided Secure Transmission in Wiretap Channels With Transmitter-Side Correlation,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8286–8297, Dec. 2016.

[26] S. Xu, S. Han, Y. Du, W. Meng, L. He, and C. Zhang, “AN-Aided Secure Beamforming Design for Correlated MISO Wiretap Channels,” *IEEE Communications Letters*, vol. 23, no. 4, pp. 628–631, Apr. 2019.

[27] T. T. Vu and H. H. Kha, “Optimal Precoder Designs for Energy-Efficiency Maximization in Secure MIMO systems,” in *2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS)*, Sept. 2016, pp. 50–55.

[28] H.-M. Wang, Q. Yin, and X.-G. Xia, “Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks,” *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532–3545, July 2012.

[29] Y. Zou, X. Wang, and W. Shen, “Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[30] T. Allen, A. Tajer, and N. Al-Dhahir, “Secure Alamouti Multiple Access Channel Transmissions: Multiuser Transmission and Multi-Antenna Eavesdroppers,” *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1510–1513, Oct. 2019.

[31] Y. Cai, Q. Shi, B. Champagne, and G. Y. Li, “Joint Transceiver Design for Secure Downlink Communications Over an Amplify-and-Forward MIMO Relay,” *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3691–3704, Sept. 2017.

[32] L. You, J. Wang, W. Wang, and X. Gao, “Secure Multicast Transmission for Massive MIMO With Statistical Channel State Information,” *IEEE Signal Processing Letters*, vol. 26, no. 6, pp. 803–807, June 2019.

[33] X. Liu, F. Gao, G. Wang, and X. Wang, “Joint Beamforming and User Selection in Multicast Downlink Channel under Secrecy-Outage Constraint,” *IEEE Communications Letters*, vol. 18, no. 1, pp. 82–85, Jan. 2014.

[34] A. P. Shrestha, J. Jung, and K. S. Kwak, “Secure Wireless Multicasting in Presence of Multiple Eavesdroppers,” in *2013 13th International Symposium on Communications and Information Technologies (ISCIT)*, Sept. 2013, pp. 814–817.

[35] W. Kim, S. Ha, J. Koh, and J. Kang, “Artificial Noise-Aided Secure Beamforming for Multigroup Multicast,” in *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan. 2018, pp. 1–4.

[36] H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, “Resource Allocation for Secure URLLC in Mission-Critical IoT Scenarios,” *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5793–5807, Sept. 2020.

[37] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, “Physical Layer Authentication for Mission Critical Machine Type Communication Using Gaussian Mixture Model Based Clustering,” in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, June 2017, pp. 1–5.

[38] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, “Physical Layer Authentication in Mission-Critical MTC Networks: A Security and Delay Performance Analysis,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 4, pp. 795–808, Apr. 2019.

[39] M. Pei, L. Wang, and D. Ma, “Linear MMSE Transceiver Optimization for General MIMO Wiretap Channels with QoS Constraints,” in *2013 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug. 2013, pp. 259–263.

[40] P. Ubaidulla and A. Chockalingam, “Relay Precoder Optimization in MIMO-Relay Networks With Imperfect CSI,” *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5473–5484, Nov. 2011.

[41] J. Liu, F. Gao, and Z. Qiu, “Robust Transceiver Design for Downlink Multiuser MIMO AF Relay Systems,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 2218–2231, Apr. 2015.

[42] H. Shen, J. Wang, B. C. Levy, and C. Zhao, “Robust Optimization for Amplify-and-Forward MIMO Relaying From a Worst-Case Perspective,” *IEEE Transactions on Signal Processing*, vol. 61, no. 21, pp. 5458–5471, Nov. 2013.

[43] X. Li, W. Wang, M. Zhang, F. Zhou, and N. Al-Dhahir, “Robust Secure Beamforming for SWIPT-Aided Relay Systems With Full-Duplex Receiver and Imperfect CSI,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1867–1878, Feb. 2020.

[44] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin, “Robust Secure Beamforming in MIMO Wiretap Channels With Deterministically Bounded Channel Errors,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9775–9784, Oct. 2018.

[45] J. Huang and A. L. Swindlehurst, “Robust Secure Transmission in MISO Channels Based on Worst-Case Optimization,” *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[46] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, “Beamforming Optimization for Physical Layer Security in MISO Wireless Networks,” *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, July 2018.

[47] Y. Li, L. Zhang, Y. Wu, and D. Wei, “Robust Secure Beamforming for Multiuser MISO Wiretap Channels,” in *2020 3rd International Conference on Smart BlockChain (SmartBlock)*, Oct. 2020, pp. 69–74.

[48] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, “On Artificial-Noise-Aided Transmit Design for Multiuser MISO Systems With Integrated Services,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 8179–8195, Sept. 2017.

[49] D. Jagyasi, M. Coupechoux, and A. Daher, “Multi-Cell MIMO Transceiver Design for Mission-Critical Communication,” in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6.

[50] 3GPP, “Technical Specification Group Radio Access Network; MBMS synchronisation protocol (SYNC) ,” 3rd Generation Partnership Project (3GPP), TS 25.446.

[51] C. A. Jotten, C. Sgraja, and J. J. Blanz, “On the Impact of Coarse Synchronization on the Performance of Broadcast/Multicast Single Frequency Network Operation in WCDMA,” in *2008 IEEE 68th Vehicular Technology Conference*, Sept. 2008, pp. 1–6.

[52] Z. Zhang, N. Wang, J. Zhang, and X. Mu, “Dynamic User-Centric Clustering for Uplink Cooperation in Multi-Cell Wireless Networks,” *IEEE Access*, vol. 6, pp. 8526–8538, Jan. 2018.

[53] A. Mukherjee and A. L. Swindlehurst, “Detecting Passive Eavesdroppers in the MIMO Wiretap Channel,” in *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2012, pp. 2809–2812.

[54] G. Prasad, Y. Huo, L. Lampe, and V. C. M. Leung, “Machine Learning Based Physical-Layer Intrusion Detection and Location for the Smart Grid,” in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6.

[55] W. Sun and Y.-X. Yuan, *Optimization Theory and Methods. Nonlinear Programming*. New York, USA: Springer, 2006.

[56] S. Gratton, C. W. Royer, L. N. Vicente, and Z. Zhang, “Complexity and Global Rates of Trust-Region Methods Based on Probabilistic Models,” *IMA Journal of Numerical Analysis*, vol. 38, no. 3, pp. 1579–1597, Aug. 2017.

[57] D. P. Bertsekas, “Nonlinear Programming,” *Journal of the Operational Research Society*, vol. 48, no. 3, pp. 334–334, Dec. 1997.

[58] H. Shen, B. Li, M. Tao, and X. Wang, "MSE-Based Transceiver Designs for the MIMO Interference Channel," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3480–3489, Nov. 2010.
[59] A. Ben-Tal, L. El Ghaoui, and A. Nemirovski, *Robust optimization. Princeton series in applied mathematics*, 2009.
[60] A. Ben-Tal, ·. Dick, J.-P. Vial, A. Ben-Tal, D. Den Hertog, and J.-P. Vial, "Deriving Robust Counterparts of Nonlinear Uncertain Inequalities," *Math. Program., Ser. A*, vol. 149, pp. 265–299, 2015.
[61] D. Bertsimas, D. B. Brown, and C. Caramanis, "Theory and Applications of Robust Optimization," *SIAM Review*, vol. 53, no. 3, pp. 464–501, Aug. 2011.
[62] S. Leyffer, M. Menickelly, T. Munson, C. Vanaret, and S. M. Wild, "A Survey of Nonlinear Robust Optimization," *INFOR: Information Systems and Operational Research*, vol. 58, no. 4, pp. 342–373, Mar. 2020.
[63] A. Mutapcic and S. Boyd, "Cutting-set Methods for Robust Convex Optimization with Pessimizing Oracles," *Optimization Methods and Software*, vol. 24, no. 3, pp. 381–406, June 2009.
[64] N. Ho-Nguyen and F. Kilinç-Karzan, "Online First-Order Framework for Robust Convex Optimization," *Operations Research*, vol. 66, no. 6, pp. 1670–1692, Dec. 2018.
[65] T. Stockhammer, M. Hannuksela, and T. Wiegand, "H.264/AVC in Wireless Environments," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 7, pp. 657–673, July 2003.
[66] 3GPP, "Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 17) ," 3rd Generation Partnership Project, Tech. Rep. TS 23.203, June 2021.
[67] Y. Gu, Z. Wu, Z. Yin, and X. Zhang, "The secrecy capacity optimization artificial noise: A new type of artificial noise for secure communication in mimo system," *IEEE Access*, vol. 7, pp. 58 353–58 360, 2019.
[68] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, 2016.
[69] M. Hata, "Empirical Formula for Propagation Loss in Land Mobile Radio Services," *IEEE Transactions on Vehicular Technology*, vol. 29, no. 3, pp. 317–325, Aug. 1980.

Deepa Jagyasi (S'16) received the Bachelor of Engineering degree in Electronics and Telecommunication Engineering from the Pune University, Pune, India, in 2010, the Master of Engineering degree in Electronics and Communication Engineering from Mumbai University, Mumbai, India, in 2013, and the Ph.D. in Electronics and Communication Engineering from the International Institute of Information Technology (IIIT), Hyderabad, India in 2021. From November 2018 to June 2021, she was affiliated with the LTCI, Telecom Paris, Institut Polytechnique de Paris, France as a research engineer. Her research interests include transceiver design, robust optimization, physical layer security, mmWave communications, and machine learning for wireless communication.

Marceau Coupechoux received the Engineer degree from Telecom Paris in 1999 and University of Stuttgart in 2000, the Ph.D. degree from Institut Eurecom in 2004, the Habilitation degree from University Pierre et Marie Curie in 2015. He is a Professor at Telecom Paris and a Professeur Chargé de Cours at Ecole Polytechnique. From 2000 to 2005, he was with Alcatel-Lucent. In 2011-2012, he was a Visiting Scientist with the Indian Institute of Science, Bengaluru, India. He has been a General Co-Chair of WiOpt 2017 and Gamenets 2019. In the Computer and Network Science Department of Telecom Paris, he is working on wireless and cellular networks, focusing mainly on performance evaluation, optimization and resource allocation.