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
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 Bit Error Rate (BER) and 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, [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...
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 ($P_1$ and $P_2$) 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 minimization 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 $X$, $\text{tr}(X)$, $E\{X\}$, $X^H$, and $X^T$ denote trace, expectation, conjugate transpose, and transpose operator, respectively. $X_1 \setminus X_2$ denote the set minus operation between the sets $X_1$ and $X_2$.

II. NETWORK AND TRANSCIEVER MODEL

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

1. **Input:** Locations of BSs and group users, $K_T \leq |S|$: minimum cluster size
2. **Init:** $S \leftarrow \emptyset$
3. **for** every user **do**
   4. Find the BS $t$ providing the highest receive power
   5. $S \leftarrow S \cup \{t\}$
5. **end for**
6. **if** $|S| < K_T$ **then**
7. Find the set $S'$ of $K_p - |S|$ BSs maximizing the sum SINR for group users
8. $S \leftarrow S \cup S'$
9. **end if**
10. **return** $S$

**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 $S$ 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 $d$ with transmit power $P_T$, where $N_s$ is the number of parallel data streams transmitted by the BS. The data $d$ is considered to be mutually independent, so that $E[dd^H] = I_{N_s}$. Before transmission, the data vector is processed by a $(N_T \times N_s)$ dimensional precoder matrix $V_t$ at the $t$-th BS, $t = 1, \ldots, K_T$. In order to improve security, we introduce an additional AN vector $z_t$ of size $(N_T \times 1)$ with zero mean and variance $E[z_tz_t^H] = \sigma_z^2 I_{N_T}$ at the $t$-th transmitter. The presence of AN has the goal of depleting the information leak to eavesdroppers. Furthermore, an AN-shaping matrix $W_t$ 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:

$$x_t = V_t d + W_t z_t$$

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

$$P_t \triangleq E[\|x_t\|^2].$$

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 $C_{tl}$ (with dimension $N_R \times N_T$) and $G_{te}$ 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 $y_l$ at legitimate UE $l$ is given by:

$$y_l = \sum_{t=1}^{K_T} C_{tl} V_t d + \sum_{t=1}^{K_T} C_{tl} W_t z_t + n_l$$

where $n_l$ is the $N_R$-dimensional zero mean random white Gaussian noise vector at the $l$-th UE’s receiver antennas with $E[n_l n_l^H] = \sigma_n^2 I_{N_R}$. The random noise vector is uncorrelated with the data vector, so that $E[n_l d^H] = 0$. The received signal at the UE $l$ is estimated as $\hat{d}_l$ (of dimension $N_s \times 1$) after passing through a $N_R \times N_s$ dimensional receive filter $R_l$. The estimated data is given by:

$$\hat{d}_l = R_l \sum_{t=1}^{K_T} C_{tl} V_t d + R_l \sum_{t=1}^{K_T} C_{tl} W_t z_t + R_l n_l.$$  

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

$$\epsilon_l \triangleq E[\|d - \hat{d}_l\|^2].$$

Similarly at the eavesdroppers, the received signal $y_e$ at the $e$-th eavesdropper is given as:

$$y_e = \sum_{t=1}^{K_T} (G_{te} V_t d + G_{te} W_t z_t) + n_e$$

where $n_e$ 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 $E[n_e n_e^H] = \sigma_n^2 I_{N_E}$. The random noise vector is uncorrelated with data vector such that $E[n_e d^H] = 0$. In this work, we assume that eavesdropper implements a classical MMSE linear receive filter. However, it can be 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:

$$E_e = \left( \sum_{t=1}^{K_T} V_t G_{te}^H \right) \left( \sum_{t=1}^{K_T} G_{te} V_t V_t^H G_{te}^H + \sigma_n^2 I_{N_E} \right)^{-1}.$$  

Eavesdroppers do not have the information about the presence of AN in the received signal and hence $W_t z_t$ is not considered in the MMSE receive filter design. After passing $y_e$ through the $N_E \times N_s$ receive filter $E_e$, the estimated data $\hat{d}_e$ at the $e$-th eavesdropper is given by:

$$\hat{d}_e = E_e \sum_{t=1}^{K_T} (G_{te} V_t d) + E_e \sum_{t=1}^{K_T} G_{te} W_t z_t + E_e n_e.$$  

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

$$\epsilon_e \triangleq E[\|d - \hat{d}_e\|^2].$$
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:

$$G_{te} = \hat{G}_{te} + \Delta_{te} \tag{10}$$

where $\hat{G}_{te}$ is the available erroneous estimate of CSI and $\Delta_{te}$ 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 errors for both legitimate UEs and eavesdropper are modeled as Gaussian random variables such that $E[\Delta_{te}] = \sigma_t^2 I$ and $E[\Delta_{tl}\Delta_{tl}^H] = \sigma_{tl}^2 I$.

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

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

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

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

where $\tau_{te}$ and $\tau_{tl}$ 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., $E[d\Delta_{tl}] = 0$, $E[n_{l}\Delta_{tl}] = 0$ for all $t$, $l$ and $E[d\Delta_{te}] = 0$, $E[n_{e}\Delta_{te}] = 0$ 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 $V_t$, $R_t$, and $W_t$ 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:

$$\begin{align*}
\text{minimize} & \quad \sum_{t=1}^{K_T} \sum_{l=1}^{K_R} \epsilon_{l} \\
\text{subject to} & \quad C1: \quad \epsilon_{e} \geq \Gamma \quad \forall e \in \{1, \cdots, K_E\} \\
& \quad C2: \quad P_t \leq P_T \quad \forall t \in \{1, \cdots, K_T\}. \quad (P_1)
\end{align*}$$

The MSE $\epsilon_{l}$ and $\epsilon_{e}$ 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 $C1$, $\Gamma$ 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:

\[ P_t = \text{tr}(V_t^H V_t + \sigma^2_{\epsilon t} W_t W_t^H) \]  

(14)

\[ \epsilon_t = \text{tr}(I) - \text{tr}\left( \sum_{t=1}^{K_R} R_t \tilde{C}_{t_l} V_t \right) - \text{tr}\left( \sum_{t=1}^{K_T} V_t^H \tilde{C}_{t_l} R_t^H \right) \]

\[ + \text{tr}\left( \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} R_t \tilde{C}_{t_l} V_t V_t^H \tilde{C}_{t_l} R_t^H \right) \]

\[ + \text{tr}\left( \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} \sigma^2_{\epsilon e} \text{tr}(R_t R_t^H) \right) \]  

(15)

\[ \epsilon_e = \text{tr}(I) - \text{tr}\left( \sum_{t=1}^{K_T} V_t^H \tilde{G}_{te} E_e^H \right) - \text{tr}\left( \sum_{t=1}^{K_T} V_t^H \tilde{G}_{te} E_e^H \right) \]

\[ + \text{tr}\left( \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} E_e \tilde{G}_{te} W_t W_t^H \tilde{G}_{te} E_e^H \right) + \sigma^2_{\epsilon t} \text{tr}(E_e E_e^H) \]

\[ + \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} \sigma^2_{\epsilon e} \text{tr}(E_e E_e^H) \]  

(16)

Proof: See Appendix A.

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

\[ V_t = (A_t)^{-1} \left( \sum_{t=1}^{K_R} \tilde{C}_{t_l} R_t^H - \sum_{e=1}^{K_E} \lambda_e \tilde{G}_{te} E_e^H \right) \]  

(17)

\[ W_t = B_t / \sqrt{\text{tr}(B_t B_t^H)} \]  

(18)

\[ R_t = \left( \sum_{t=1}^{K_T} V_t^H \tilde{C}_{t_l} \right) \left( \sum_{t=1}^{K_T} \tilde{C}_{t_l} V_t V_t^H \tilde{C}_{t_l} \right) \]

\[ + \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} \tilde{C}_{t_l} W_t W_t^H \tilde{C}_{t_l} + \sigma^2_{\epsilon t} \sigma^2_{\epsilon e} \text{tr}(V_t V_t^H) \]

\[ + \sum_{t=1}^{K_T} \sigma^2_{\epsilon t} \sigma^2_{\epsilon e} \text{tr}(W_t W_t^H) \]  

(19)

where

\[ B_t = I - A_t^H (A_t A_t^H)^{-1} A_t \]  

(20)

\[ A_t = \sum_{t=1}^{K_R} \tilde{C}_{t_l} R_t R_t + \sum_{l=1}^{K_T} \sigma^2_{\epsilon t} \text{tr}(R_t R_t^H) \]
dodleg algorithm implemented in fsolve is an iterative algorithm which achieves a \( \varepsilon \)-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 (starting with a single fixed value); this is the worst-case cost. In the same way, constraint C1 is replaced by a robust counterpart C5, i.e., the worst-case MSE over all realizations of the error \( \Delta_{tl} \).

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 \( \Delta_{te} \) and \( \Delta_{tl} \) (starting with a single fixed value); then the problem associated to the constraint (e.g. C5 above) is solved and optimal values of \( \Delta_{te} \) and \( \Delta_{tl} \) 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 \( \mathcal{P}_2' \)**: In the first sub-problem, we compute the optimal precoder \( \mathbf{V}_t \), receive filter \( \mathbf{R}_t \) and AN covariance matrix \( \mathbf{W}_t \) while the worst-case channel errors \( \Delta_{te} \) and \( \Delta_{tl} \) are supposed to be known. The first optimization sub-problem can be thus written as:

\[
\begin{align*}
\min_{\mathbf{V}_t, \mathbf{W}_t, \mathbf{R}_t} & \quad \sum_{l=1}^{K_R} \epsilon_l \\
\text{subject to} & \quad C1, C2, \\
& \quad C3 : \Delta_{te} \in \mathcal{G}_{te}, \quad \forall t, \forall e, \\
& \quad C4 : \Delta_{tl} \in \mathcal{C}_{tl}, \quad \forall t, \forall l.
\end{align*}
\]

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

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

\[
\begin{align*}
\min_{\mathbf{V}_t, \mathbf{W}_t, \mathbf{R}_t} & \quad \Delta_{tl}^{\text{opt}} - \sum_{l=1}^{K_R} \epsilon_l \\
\text{subject to} & \quad C4 : ||\Delta_{tl}||^2 \leq \tau_{tl}, \quad \forall t, \forall l.
\end{align*}
\]

The Lagrangian is given by:

\[
\mathcal{L}(\Delta_{tl}, \kappa_{tl}) = -\sum_{l=1}^{K_R} \epsilon_l + \sum_{t=1}^{K_T} \kappa_{tl} (||\Delta_{tl}||^2 - \tau_{tl})
\]

\[
= -\sum_{l=1}^{K_R} \epsilon_l + \sum_{t=1}^{K_T} \kappa_{tl} (\text{tr}(\Delta_{tl}^H \Delta_{tl}^{H_H}) - \tau_{tl})
\]

(22)
Algorithm 3: Iterative procedure to obtain transceiver filters for NBEs

1: Input: $\beta, K_T, K_R, K_E, \mathbf{E}_e, \mathbf{C}_l, \mathbf{G}_l, \tau_{tl}, \tau_{te}, P_T, \Gamma$, $\forall t \in \{1, \ldots, K_T\}, k \in \{1, \ldots, K_R\}$, and $e \in \{1, \ldots, K_E\}$
2: Init: Randomly generate $V_t, W_t \forall t \in \{1, \ldots, K_T\}$, $\Delta_t \in \mathbf{C}_t, \Delta_e \in \mathbf{G}_e, \epsilon_t \leftarrow 0 \forall t \in \{1, \ldots, K_T\}, l \in \{1, \ldots, K_R\}, e \in \{1, \ldots, K_E\}$.
3: repeat
4: $\epsilon'_t \leftarrow \epsilon_t \forall l \in \{1, \ldots, K_R\}$
5: Solve $P_t'$ and update $\Delta_t, l \in \{1, \ldots, K_T\}$, $W_t, R_l \forall t \in \{1, \ldots, K_T\}$, $e \in \{1, \ldots, K_E\}$
6: Solve $P_t''$ and update $\Delta_t$ using $V_t, W_t, R_l$ in (26) $\forall t \in \{1, \ldots, K_T\}, l \in \{1, \ldots, K_R\}$
7: Solve $P_t'''$ and update $\Delta_e$ using $V_t, W_t, E_e$ in (27) $\forall t \in \{1, \ldots, K_T\}, e \in \{1, \ldots, K_E\}$
8: Compute $\eta_t$ using $V_t, W_t$, and $R_l, \Delta_t, \Delta_e$ in (15).
9: until $|\epsilon_t - \epsilon'_t| \leq \beta \forall l \in \{1, \ldots, K_R\}$

where $\kappa_{tl} \geq 0$ are the Lagrange multipliers associated to constraints C4. Considering (15), it is observed that solving $P_t''$ is difficult. To simplify the solution, we consider an approximation of $\epsilon_t$ by ignoring the second and higher order terms of $\Delta_t$. 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 $\Delta_t^H$ and to $\kappa_{tl}$, respectively, and equating to zero we obtain:

$$
\Delta_t = \frac{1}{\kappa_{tl}} (R_t^H V_t^H + R_t^H R_l \mathbf{C}_l V_t^H \tau_{tl}^H + \sigma_z^2 R_t^H R_l \mathbf{C}_l^H W_t^H W_t^H) \forall t \in \{1, \ldots, K_T\}, l \in \{1, \ldots, K_R\}, e \in \{1, \ldots, K_E\}
$$

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

$$
\kappa_{tl} = \frac{1}{\sqrt{\tau_{tl}}} \|R_t^H R_l \mathbf{C}_l V_t^H V_t^H + \sigma_z^2 R_t^H R_l \mathbf{C}_l W_t^H W_t^H
$$

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

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

$$
\Delta_t = \sqrt{\tau_{tl}} \frac{\gamma_{tl}}{\|Y_{tl}\|}
$$

where

$$
Y_{tl} = R_t^H V_t^H + R_t^H R_l \mathbf{C}_l V_t^H V_t^H + \sigma_z^2 R_t^H R_l \mathbf{C}_l W_t^H W_t^H
$$

3) Sub-problem $P_t'''$: In this third sub-problem, the transceiver matrices and the worst-case error $\Delta_t$ are supposed to be known and we look for the worst-case error $\Delta_e$. It can be found by solving the problem defined in constraint C5. The sub-problem can thus be written as:

$$
\begin{align*}
\text{minimize} & \quad \Delta_{e,t} + 1 \ldots K_T^T \epsilon_e \geq \Gamma \\
\text{subject to} & \quad C3 : ||\Delta_{te}||^2 \leq \tau_{te} \quad \forall t
\end{align*}
$$

We adopt here the same approach as for $(P_2'')$ and solve exactly the problem (with zero dual gap).

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

$$
\Delta_{te} = -\sqrt{\tau_{te}} \frac{\gamma_{te}}{||Y_{te}||}
$$

where

$$
Y_{te} = E_t^H V_t^H + E_t^H E_e G_e V_t^H + \sigma_z^2 E_t^H E_e G_e W_t^H W_t^H
$$

A stationary solution for $(\tilde{P}_2)$ 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 $\epsilon_t$ using (15) is again in $O(KN^3)$. The computation of $\Delta_t$ and $\Delta_e$ 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 $O(I_3 I_2 N^3 + I_3^2 K^3 e^{-3})$.

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 $I_3$ is 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 $N_e = 2$; $P_T = 0$ dBm; $\sigma^2_{nl} = P_T / \text{SNR}, l = 1, 2, \ldots, K_R, \sigma^2_{ne} = P_T / \text{SNR}, e = 1, \ldots, K_E$, where
whereas other components are decreasing and tend towards are due to CSI errors and are increasing with the signal power, several components. In particular, the last two terms of (15) considered. The MSE at legitimate users is indeed made of the SNR after a certain threshold when NR designs are 10

Video conferencing requires a typical Bit Error Rate (BER) of 10

packet loss rate of 10

6

or

4

This can lead to typical BERs of 10

−3

for legitimate users.

1) Effect of CSI SNR: 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:

\[
\text{secrecy rate} = \sum_{l=1}^{K_e} \left( \log \left( 1 + \frac{\left| C_{tl} V_l \right|^2}{\sum_{t=1}^{K_T} \left| C_{tl} W_t \right|^2 + \sigma^2_{nl}} \right) \right) - \max_{1 \leq e \leq K_e} \log \left( 1 + \frac{\left| G_{te} V_l \right|^2}{\sum_{t=1}^{K_T} \left| G_{te} W_t \right|^2 + \sigma^2_{re}} \right)
\] (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.

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 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 \(\Gamma\) 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,
0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

Fig. 9: MSE at eavesdropper vs eavesdropper (eve) MSE threshold $\Gamma$ 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 $\sigma_{zt}^2 = 0.04$.

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 $K'_T$ 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. 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.

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:

$$P_t \triangleq \mathbb{E}[||x_t^H||^2] = \mathbb{E}[\text{tr}(x_t x_t^H)]$$

$$= \text{tr}(V_t V_t^H + W_t).$$

(29)

The MSE $\epsilon_l$ at the legitimate user $l$ is computed as follows:

$$\epsilon_l \triangleq \mathbb{E}[||d - \hat{d}_l||^2]$$

$$= \mathbb{E}\left[||d - \left(\sum_{t=1}^{K_T} R_t(\hat{C}_{tl} + \Delta_{tl}) V_t d\right)\right.$$

$$\left.\sum_{t=1}^{K_T} R_t(\hat{C}_{tl} + \Delta_{tl}) w_t + R_t(n_t)||^2\right]$$

$$= \text{tr}(I) - \text{tr}\left(\sum_{t=1}^{K_T} R_t(\hat{C}_{tl} V_t) - \text{tr}\left(\sum_{t=1}^{K_T} V_t H_t^H \hat{C}_{tl}^H R_t^H\right)\right)$$

$$+ \text{tr}\left(\sum_{t=1}^{K_T} R_t(\hat{C}_{tl} V_t V_t^H \hat{C}_{tl}^H R_t^H)\right)$$

$$+ \text{tr}\left(\sum_{t=1}^{K_T} R_t(\hat{C}_{tl} W_t \hat{C}_{tl}^H R_t^H)\right) + \sigma^2 d \text{tr}(R_t R_t^H)$$

$$+ \mathbb{E}\left[\text{tr}\left(\sum_{t=1}^{K_T} R_t(\Delta_{tl} W_t \Delta_{tl}^H R_t^H)\right)\right]$$

$$+ \mathbb{E}\left[\text{tr}\left(\sum_{t=1}^{K_T} R_t(\Delta_{tl} W_t \Delta_{tl}^H R_t^H)\right)\right].$$

(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:

$$\epsilon_e \triangleq \mathbb{E}[||d - \bar{d}_e||^2]$$

$$= \mathbb{E}\left[||d - \left(\sum_{t=1}^{K_T} E_e(\hat{G}_{te} + \Delta_{te}) V_t d\right)\right.$$

$$\left.\sum_{t=1}^{K_T} E_e(\hat{G}_{te} + \Delta_{te}) w_t + E_e n_t)||^2\right]$$

$$= \text{tr}(I) - \text{tr}\left(\sum_{t=1}^{K_T} E_e(\hat{G}_{te} V_t) - \text{tr}\left(\sum_{t=1}^{K_T} V_t H_t^H \hat{G}_{te}^H E_e^H\right)\right)$$

$$+ \text{tr}\left(\sum_{t=1}^{K_T} E_e(\hat{G}_{te} V_t V_t^H \hat{G}_{te}^H E_e^H)\right)$$

$$+ \text{tr}\left(\sum_{t=1}^{K_T} E_e(\hat{G}_{te} W_t \hat{G}_{te}^H E_e^H)\right) + \sigma^2 d \text{tr}(E_e E_e^H)$$

(31)

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

**APPENDIX B**

**PROOF OF PROPOSITION 1**

We use here two binary slack variables $\chi_l$ and $\chi_e$ 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:

\[
\epsilon_t = \text{tr}(I) - \text{tr}(\sum_{t=1}^{K_T} R_t \hat{C}_{tt} V_t) - \text{tr}(\sum_{t=1}^{K_T} V_t^H \hat{C}_{tt}^H R_t^H)
\]

\[
+ \text{tr}(\sum_{t=1}^{K_T} R_t \hat{C}_{tt} V_t V_t^H \hat{C}_{tt}^H R_t^H)
\]

\[
+ \chi_t \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(R_t R_t^H) \text{tr}(V_t V_t^H)
\]

\[
+ \chi_t \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(R_t R_t^H) \text{tr}(W_t W_t^H).
\]

(32)

The $e$-th eavesdroppers MSE is simplified as:

\[
\epsilon_e = \text{tr}(I) - \text{tr}(\sum_{t=1}^{K_T} E_e \hat{G}_{te} V_t) - \text{tr}(\sum_{t=1}^{K_T} V_t^H \hat{G}_{te}^H E_e^H) + \sum_{t=1}^{K_T} \text{tr}\left(\sum_{e=1}^{K_E} E_e \hat{G}_{te} V_t V_t^H \hat{G}_{te}^H E_e^H\right) + \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(E_e E_e^H) + \chi_e \sum_{t=1}^{K_T} \sigma_{zt}^2
\]

\[
\text{tr}(E_e E_e^H) \text{tr}(V_t V_t^H) + \chi_t \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(E_e E_e^H) \text{tr}(W_t W_t^H).
\]

(33)

We solve the optimization problem $(P_1)$ by forming the Lagrangian $L$ as below:

\[
L(V_t, W_t, R_t, \lambda_e, \lambda'_e) = \sum_{t=1}^{K_T} \epsilon_t + \sum_{e=1}^{K_E} \lambda_e (\Gamma - \epsilon_e)
\]

\[
+ \sum_{t=1}^{K_T} \lambda'_t \text{tr}(V_t V_t^H)
\]

\[
+ \sum_{t=1}^{K_T} \lambda'_t \text{tr}(W_t W_t^H) - P_T
\]

(34)

where $\lambda_e$ and $\lambda'_e$ 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 $P_1$, 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 $P_1$ are as follows:

\[
\frac{\partial L}{\partial V_t^H} = 0
\]

\[
\frac{\partial L}{\partial R_t^H} = 0
\]

\[
\frac{\partial L}{\partial W_t^H} = 0
\]

\[
\Gamma - \epsilon_e \leq 0 \quad \forall e \in \{1, \ldots, K_E\}
\]

\[
\lambda_e \geq 0 \quad \forall e \in \{1, \ldots, K_E\}
\]

\[
\lambda_e (\Gamma - \epsilon_e) = 0 \quad \forall e \in \{1, \ldots, K_E\}
\]

\[
\text{tr}(V_t V_t^H + \sigma_{zt}^2 W_t W_t^H) - P_T \leq 0 \quad \forall t \in \{1, \ldots, K_T\}
\]

\[
\lambda'_t \geq 0 \quad \forall t \in \{1, \ldots, K_T\}
\]

\[
\lambda'_t (\text{tr}(V_t V_t^H + \sigma_{zt}^2 W_t W_t^H) - P_T) = 0 \quad \forall t \in \{1, \ldots, K_T\}.
\]

(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 $V_t$ is derived by taking the gradient of $L$ with respect to $V_t^H$, and is given as:

\[
\frac{\partial L}{\partial V_t^H} = -\sum_{l=1}^{K_R} \hat{C}_{tl}^H R_t^H + \sum_{l=1}^{K_R} \hat{C}_{tl}^H R_t R_t^H \hat{G}_{tt} V_t
\]

\[
+ \chi_t \sum_{l=1}^{K_R} \sigma^2_{zt} \text{tr}(R_t R_t^H) V_t + \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te}^H E_e^H
\]

\[
- \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te}^H E_e \hat{G}_{te} V_t
\]

\[
- \chi_t \sum_{e=1}^{K_E} \lambda_e \sigma_{zt}^2 \text{tr}(E_e E_e^H) V_t + \lambda'_t V_t.
\]

(36)

Equating to zero leads to:

\[
V_t = \left( \sum_{l=1}^{K_R} \hat{C}_{tl}^H R_t^H R_t \hat{G}_{tt} + \chi_t \sum_{l=1}^{K_R} \sigma^2_{zt} \text{tr}(R_t R_t^H) I \right)
\]

\[
- \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te}^H E_e \hat{G}_{te} - \chi_t \sum_{e=1}^{K_E} \lambda_e \sigma_{zt}^2 \text{tr}(E_e E_e^H) I
\]

\[
+ \lambda'_t \left( \sum_{l=1}^{K_R} \hat{C}_{tl}^H R_t^H - \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te}^H E_e^H \right).
\]

(37)

Receive filter $R_t$ is obtained in the same way, i.e. by differentiating the Lagrangian with respect to $R_t^H$, while considering
all other variables as fixed, and assigning it to zero:
\[
\frac{\partial L}{\partial R_t^H} = -\sum_{t=1}^{K_T} V_t^H \hat{C}_{tt}^H + \sum_{l=1}^{K_T} R_t \hat{C}_{il} V_t^H \hat{C}_{il}^H + \sum_{l=1}^{K_T} \sigma_{zt}^2 R_t \hat{C}_{il} W_t \hat{C}_{il}^H + \sigma_{n}^2 R_t \\
+ \chi l \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(V_t W_t^H) R_t \\
+ \chi l \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(W_t W_t^H) R_t \\
+ \chi l \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(V_t V_t^H) I \\
+ \chi l \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(W_t W_t^H) I \right]^{-1}. 
\]

(38)

Now, we differentiate the Lagrangian with respect to $W_t^H$ and setting it to zero:
\[
\frac{\partial L}{\partial W_t^H} = \sum_{t=1}^{K_T} \sigma_{zt}^2 \hat{C}_{tt}^H R_t \hat{C}_{tt} W_t \\
+ \chi l \sigma_{zt}^2 \sum_{t=1}^{K_T} \text{tr}(R_t R_t^H) W_t \\
- \sigma_{zt}^2 \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te} E_e^H E_e \hat{G}_{te} W_t \\
- \chi e \sigma_{zt}^2 \sum_{e=1}^{K_E} \lambda_e \sigma_{zt}^2 \text{tr}(E_e E_e^H) W_t + \chi l \sigma_{zt}^2 \text{tr}(W_t W_t^H) \right) 
\]

(40) 

This is equivalent to $A_t W_t = 0$ where
\[
A_t = \sum_{t=1}^{K_T} \hat{C}_{tt}^H R_t \hat{C}_{tt} + \chi l \sum_{t=1}^{K_T} \sigma_{zt}^2 \text{tr}(R_t R_t^H) \\
- \sum_{e=1}^{K_E} \lambda_e \hat{G}_{te} E_e^H E_e \hat{G}_{te} \\
- \chi e \sum_{e=1}^{K_E} \lambda_e \sigma_{zt}^2 \text{tr}(E_e E_e^H) + \chi l. 
\]

(42)

In the condition $A_t W_t = 0$, $A_t$ 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 $W_t$ should be taken in the null space of $A_t$ and $W_t = B_t / \sqrt{\text{tr}(B_t B_t^H)}$, where $B_t = I - A_t^H (A_t A_t^H)^{-1} A_t$. At last, differentiating the Lagrangian with respect to $\lambda_t$ and $\epsilon_t$ respectively and setting to zero we get:
\[
\frac{\partial L}{\partial \lambda_t} = \text{tr}(V_t V_t^H + \sigma_{zt}^2 W_t W_t^H) - P_t = 0 
\]

(43)

\[
\frac{\partial L}{\partial \epsilon_t} = \Gamma - \epsilon_t = 0. 
\]

(44)

The values for $\epsilon_t$, $\epsilon = \{1, 2, \cdots, K_E\}$ and $\lambda_t$, $t = \{1, 2, \cdots, K_T\}$ are jointly computed by inserting the values of $V_t$ and $W_t$ in (43) and (44) so as to satisfy the thresholds $P_t$ for all $t$ and $\epsilon_t$ for all $e$. The Lagrange multipliers are obtained such that they satisfy the KKT conditions in (35) which result in positive values for $\lambda_t$ and $\epsilon_t$ or zeros otherwise.

\section*{References}

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

[2] Y. Lair and M. 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. Kuz, and G. Vellev, “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. Coupéchoix, P. Godlewski, J.-M. Kelik, P. Ngouat, and P. Minot, “SIRN 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. Coupéchoix, P. Godlewski, P. Ngouat, and P. Minot, “A Dynamic Clustering Algorithm for Multi-Point Transmissions in Mission-Critical Communications,” in 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), June 2019, pp. 1–3.

[11] N. Yang, L. Wang, G. Geraci, M. Elkaslan, 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.

[12] 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.
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.