On Linear Precoding Strategies for Secrecy Rate Maximization in Multiuser Multiantenna Wireless Networks

Muhammad Fainan Hanif, Le-Nam Tran, *Member, IEEE*, Markku Juntti, *Senior Member, IEEE*, and Savo Glisic, *Senior Member, IEEE*

***Abstract*—Revived interest in physical layer security has led to a cascade of information theoretic results for various system topologies under different constraints. In the present paper, we provide practically oriented solutions to the problem of maximizing achievable secrecy rates in an environment consisting of multiple legitimate and eavesdropping radio nodes. By assuming "genie" aided perfect channel state information (CSI) feedback for both types of nodes, we first study two scenarios of interest. When independent messages are intended for all legitimate users (called "broadcast" mode), provably convergent second-order cone programming (SOCP)-based iterative procedure is used for designing secrecy rate maximizing beamformers. In the same manner, when a common message is intended only for legitimate nodes (dubbed "multicast" mode), SOCP-based design is proposed for obtaining linear precoders that maximize the achievable secrecy rate. Subsequently, we leverage the analysis to the more real-world scenario, where the CSI of the malicious nodes has to be somehow estimated and that of the legitimate users is corrupted with unavoidable errors. For this case, we devise provably convergent iterative semidefinite programming (SDP) procedures that maximize the achievable secrecy rates for both the beamforming-based broadcast and the linearly precoded multicast modes. Finally, numerical results are reported that evaluate the performance of the proposed solutions as a function of different system parameters. The results presented in the paper are demonstrated to outperform the ones based on interference alignment strategies. We also ascertain superior performance of the proposed schemes in the realms of real world.**

***Index Terms*—Beamforming, channel uncertainties, degrees-of-freedom, interference alignment, multiantenna downlink, multicast systems, robust convex optimization, secrecy capacity.**

I. Introduction

SECRECY capacity was characterized in [1] for degraded broadcast channel where the eavesdropper receives a degraded version of legitimate user's received signal. Later, the seminal research effort [2] leveraged secrecy results to the general scenario and determined the capacity region for non-degraded broadcast channel. The secrecy model in [2] also assumed a common message to be decoded by both receivers in addition to transmitting a private message to one of them. Since then many results have appeared in the literature, and below we attempt to comprehensively (but by no means exhaustively) summarize the significant ones especially related to the problem we have considered.

The secrecy rates based on the results in [2] for Gaussian channel in a multi-input single-output (MISO) setting was evaluated in [3]. Later, achievable rates and upper bounds to the capacity were quantified in [4]. The system setup of [4] assumed that the legitimate transceiver had two antennas at both ends, while the eavesdropper was a single antenna device. Again the achievable rates were characterized using the results of [2]. Upper bounds to the capacity were obtained in [4] assuming unilateral cooperation between the wiretapper and the lawful receiver where the wiretapper's signal is made available to the legitimate node. Capacity was characterized in [5] under the assumptions that the legitimate transmitter and the eavesdropper both have multiple antenna elements, and the channel transfer functions are perfectly known at all nodes. The case of secrecy capacity of a general multiple-input multiple-output (MIMO) broadcast channel was considered in [6]. Results similar to those in the original work of [2] were derived for the MIMO setting as well. The natural extension to the case of multiple receivers was explored in [7], where the capacity region was obtained first for the degraded and then for so-called aligned broadcast setup in the presence of an eavesdropper. The case when error-free channel information to the eavesdropper is not available to the transmitter was studied in [8] by characterizing the outage probability, i.e., when the system is unable to support non-zero secrecy rates. Secrecy in conjunction with network coding was studied in [9], where the wiretapper is allowed a restricted access to a subset of links and the transmitted message is not revealed to it. Further [10] considers the most general setup of multiple legitimate users operating in the presence of several wiretappers. Apart from obtaining capacity results for the particular scenarios of degradedness in parallel channels, [10] has also evaluated the achievable secrecy rates in the most general scenario. For the special case of two legitimate users and one eavesdropper, improved inner bounds were obtained in [11]. The results for a similar case with multiple legitimate users and eavesdroppers were extended to the case of evaluating secure degrees of freedom (dof) in [12]. Some work pertaining to maximizing the secrecy rates in real world environments has also appeared in the recent literature. For instance, [13] has studied a single

Manuscript received September 17, 2013; revised December 05, 2013 and March 03, 2014; accepted May 15, 2014. Date of publication May 23, 2014; date of current version June 24, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Shuguang (Robert) Cui. The research was financially supported by the Academy of Finland.

The authors are with the Department of Communications Engineering, Centre for Wireless Communications, FI-90014, University of Oulu, Finland (e-mail: mfh21@uclive.ac.nz; fainanhanif@hotmail.com; ltran@ee.oulu.fi; markku.juntti@ee.oulu.fi; savo.glisic@ee.oulu.fi).

Digital Object Identifier 10.1109/TSP.2014.2326617

user system operating in the presence of a single wiretapper with statistical imperfections in the channel between the legitimate transmitter and the receiver. Subsequently, [14] studies the case of operation of a legitimate transceiver in the presence of several wiretappers. They arrive at the semidefinite program (SDP) formulations even with perfect channel information. For imperfect channel estimation, [14] models the errors to belong to the same types of uncertainty sets and arrives at an SDP formulation in this case as well.

Contributions: In this paper, we study the downlink of a mobile wireless system where the transmitting base station (BS) has multiple antenna elements while all legitimate nodes and the eavesdroppers are equipped with a single antenna. The goal is to maximize the number of bits per second per Hz to the legitimate nodes, and ensuring that the eavesdroppers remain as oblivious as they were before data transmission took place, i.e., we have perfect secrecy of the legitimate users' messages. Our specific contributions include: a) a *low-complexity* provably convergent iterative second-order cone programming (SOCP) based algorithm that assumes perfect channel estimation and solves the nonconvex problem of obtaining linear precoders for securely broadcasting and multicasting messages to the legitimate nodes; b) modeling the real world setting where the eavesdroppers do not share their channel information with the BS and there are unavoidable estimation errors in the channels of the legitimate nodes, and; c) finally, and most importantly, devising novel low complexity approximate solutions in the above mentioned real world setting by again devising a convergent iterative procedure based on solving SDPs in each of its steps. To the authors' knowledge this appears to be the first endeavor of its kind that studies multiuser environment with multiple antenna transmitting elements in conjunction with realistic assumptions on channel information, and also includes the possibility of handling a *mixture* of channel uncertainty sets from the perspective of maximizing achievable secrecy rates. As will be seen in the discussion to follow, the authors would like to note that the proposed approaches are neither high complexity global optimal solution yielding algorithms (as, for instance, considered in [15]), nor always suboptimal in the sense of work presented in [16].

The rest of the paper is organized as follows. Section II sets up the network model and formulates the problems. Section III proposes a solution to the problems when we assume that perfect channel estimating genie is available. In Section IV, we propose system and channel models for more practically oriented situations. Based on the models presented in Section IV, approximate solutions to the secrecy rate maximization problem are devised in Section V. Finally, numerical results and conclusions are described in Sections VI and VII, respectively.

Notation: We use conventional notation throughout. Bold lowercase and uppercase letters are reserved for vectors and matrices, respectively. For a vector $\mathbf{v}$, we use $[\mathbf{v}]_i$ to denote its i^{th} component. $\mathbf{M}^{\text{H}}$ and $\mathbf{M}^T$ denote the complex conjugate transpose and transpose of a matrix $\mathbf{M}$, respectively. For a complex number c the symbols $|c|, \Re(c)$ and $\Im(c)$ are used to represent its modulus, real and imaginary parts, respectively. $\|\cdot\|_1, \|\cdot\|_2$ and $\|\cdot\|_\infty$ denote the usual l_1, l_2 and l_∞ norms, respectively. $\mathcal{CN}(0, \mathbf{S})$ denotes a complex Gaussian random vector with zero mean and covariance matrix $\mathbf{S}$. Unless otherwise mentioned, all logarithms are to the base 2. Any new notation is defined at the point of its occurrence.

II. System Model and Problem Formulation

We consider the downlink of a multiuser system in which a multi-antenna transmitter with T elements is serving a set of M users, and each member of the set has a single receive antenna. The transmitter employs linear precoding for message transfer to the users. In addition, we assume that there is another set of N illegitimate single antenna nodes that can potentially 'overhear' (eavesdrop) on the message transmitted to an arbitrary legitimate node. The time domain baseband outputs at the two types of receivers are

$$y_u = \mathbf{h}_u \mathbf{x} + n_u, \quad u = 1, 2, \ldots, M \tag{1}$$

$$\check{y}_e = \mathbf{g}_e \mathbf{x} + \check{n}_e, \quad e = 1, 2, \ldots, N \tag{2}$$

where $\mathbf{x}$ is the channel input, $\mathbf{h}_u, \mathbf{g}_e$ are complex row vectors of dimension T representing channels to the u^{th} user and the e^{th} eavesdropper in the downlink channel, n_u and $\check{n}_e$ represent noise terms at the two types of receivers, respectively. It has been shown in [10], that in the above setup the following secrecy rate is achievable

$$R = \max_{P(\mathbf{u},\mathbf{x})} \min_{u,e} [I(\mathbf{u}; y_u) - I(\mathbf{u}; \check{y}_e)]^+ \tag{3}$$

where $[x]^+ \triangleq \max\{x, 0\}$, $\mathbf{u}$ is an auxiliary random variable that can be used to generate extra randomness to maintain secrecy, $P(\mathbf{u}, \mathbf{x})$ is the joint distribution of $\mathbf{u}$ and $\mathbf{x}$, and $I(x; y)$ denotes the mutual information of random variables x and y. Equipped with the above result, we will focus on the following two cases of interest with the *Gaussian* signalling assumption for the rest of the remaining paper.

A. Secure Broadcast Mode With Transmit Beamforming

In order to arrive at the Gaussian version of the secrecy rate in (3), we will assume $\mathbf{u} = \mathbf{x}$ so that $P(\mathbf{u}, \mathbf{x}) = P(\mathbf{x})$ follows the Gaussian probability law. Further, it is assumed that the input $\mathbf{x} = \sum_{i \le M} \mathbf{w}_i s_i = \mathbf{W}\mathbf{s}$, where the i^{th} column (beamformer $\mathbf{w}_i$) of matrix $\mathbf{W}$ corresponds to the i^{th} legitimate node, and the elements of the transmit vector $\mathbf{s}$ are s_i. In addition, the legitimate user under consideration treats signals of other users as noise. Further, the e^{th} eavesdropper can at best attempt to decode the signal of the u^{th} legitimate node while treating the signals of other nodes $j \neq u$ as noise. Similar in spirit to the approach in [17], we will assume the trace constraints on the input which for the case of unit precoders corresponding to the symbols of the receivers translate into $\sum_{i \le M} \|\mathbf{w}_i\|_2^2 \le P_a$. With this information, the achievable secrecy rate can be formulated as

$$\textbf{Problem a}: \max_{\sum_{i \le M} \|\mathbf{w}_i\|_2^2 \le P_a} \min_{\substack{1 \le u \le M, \\ 1 \le e \le N}} \alpha_{u,e} R^a_{u,e}(\mathbf{h}_u, \mathbf{g}_e, \mathbf{W}) \tag{4}$$

where

$$R^a_{u,e}(\mathbf{h}_u, \mathbf{g}_e, \mathbf{W}) \triangleq \left[\log\left(1 + \frac{|\mathbf{h}_u \mathbf{w}_u|^2}{\sigma_u^2 + \sum_{j \neq u} |\mathbf{h}_u \mathbf{w}_j|^2}\right) - \log\left(1 + \frac{|\mathbf{g}_e \mathbf{w}_u|^2}{\sigma_e^2 + \sum_{j \neq u} |\mathbf{g}_e \mathbf{w}_j|^2}\right) \right]^+ \tag{5}$$

$\alpha_{u,e} \in \mathbb{R}_{++}$ are arbitrary weighting factors, σ_u^2, σ_e^2 are noise variances[1] at the legitimate user and the eavesdropper, respectively. It is remarked here that the weights $\alpha_{u,e}$ may, for instance, be selected to prioritize users to accomplish a certain scheduling goal.[2] It is interesting to note that above achievable rate due to [10] is reminiscent of the well known SINR balancing problem in the communication theory literature [18].

B. Secure Multicast Mode

It is of practical interest to transmit the same message to a group of users. For instance, video broadcasting and similar applications rely on this principle. To formulate the problem in this case, we will again invoke the assumption $\mathbf{u} = \mathbf{x}$ so that $\mathbf{x} \sim \mathcal{CN}(0, \mathbf{Q})$, and following [17], the positive semidefinite covariance matrix of the input distribution satisfies $\mathrm{tr}(\mathbf{Q}) \leq P_b$. Hence, invoking (3), we obtain the following optimization problem

$$\textbf{Problem b}: \max_{\mathbf{Q}\succeq 0:\mathrm{tr}(\mathbf{Q})\leq P_b} \min_{\substack{1\leq u\leq M,\\ 1\leq e\leq N}} \alpha_{u,e} R_{u,e}^b(\mathbf{h}_u, \mathbf{g}_e, \mathbf{Q}) \quad (6)$$

where

$$R_{u,e}^b(\mathbf{h}_u, \mathbf{g}_e, \mathbf{Q}) \triangleq [\log(1+\mathbf{h}_u\mathbf{Q}\mathbf{h}_u^{\mathrm{H}}) - \log(1+\mathbf{g}_e\mathbf{Q}\mathbf{g}_e^{\mathrm{H}})]^+ \quad (7)$$

and without loss of generality unit variance noise is taken at both the legitimate and the eavesdropping nodes. It is pertinent to emphasize here that in the multicast scenario, we do not employ transmit beamforming. When transmit beamforming is used for multicasting purposes, the input covariance matrix takes the form $\mathbf{Q} = \mathbf{q}\mathbf{q}^{\mathrm{H}}$. However, in this case the optimization can be carried out by following a strategy that is very similar to the one used for solving **Problem a**. It is interesting to note that for the case $M = 1$, beamforming has been shown as an optimal strategy [14]. We remark that the present study can be straightforwardly extended to the case of multicellular settings. It should be pointed out here that in addition to the two case studies, **Problem a** and **Problem b**, presented here two more cases arise naturally. These scenarios are precoding in broadcasting and beamforming in the multicasting modes. Due to space constraints, these cases are not probed any further. However, the mathematical development presented below can be easily elevated to tackle these scenarios. Therefore, our study is without loss of generality.

III. Theoretical Benchmark Solutions With 'Genie' Aided Feedback

In this section, we devise reference solutions to both **Problem a** and **Problem b** given in (4) and (6), respectively. Here the fundamental assumption of our approach will involve relying on a 'genie' that provides perfect channel state information (CSI) of the eavesdropping nodes and other legitimate receivers to the main BS. This assumption is consistent with many existing works mainly devoted to information theoretic analysis of the type of problems under consideration, [4]–[6], [11], for instance.

[1]With slight abuse of notation, instead of using $\tilde{\sigma}_e^2$ to denote noise variance at the eavesdropper e, we use the symbol σ_e^2. This will not effect the generality of the ensuing analysis.

[2]We also note that no such weights have been explicitly shown in (3) to maintain generality of the achievable rate formula.

A. Solution of Problem a

As a first step, after straightforward algebra, **Problem a** is written in another equivalent form as

$$\begin{aligned}
\underset{\mathbf{w}_i, t_{u,e}, v_{u,e}}{\text{maximize}} \quad & \min_{u,e} \max\{\alpha_{u,e}\log t_{u,e}, 0\} \\
\text{subject to} \quad & \left(1 + \frac{|\mathbf{h}_u\mathbf{w}_u|^2}{\sigma_u^2 + \sum_{j\neq u}|\mathbf{h}_u\mathbf{w}_j|^2}\right) \geq t_{u,e}v_{u,e}, \forall u, e \\
& \left(1 + \frac{|\mathbf{g}_e\mathbf{w}_u|^2}{\sigma_e^2 + \sum_{j\neq u}|\mathbf{g}_e\mathbf{w}_j|^2}\right) \leq v_{u,e}, \quad \forall u, e \\
& \sum_{1\leq i\leq M} \|\mathbf{w}_i\|_2^2 \leq P_a. \qquad (8)
\end{aligned}$$

The equivalence of the above formulation with the initial problem can be proved by following standard procedure [19]. Observe that the objective function is monotonic in its arguments, hence, the above formulation can be further translated into its epigraph form as[3]

$$\begin{aligned}
\underset{\mathbf{w}_i, t_{u,e}, v_{u,e}, z}{\text{maximize}} \quad & z \qquad (9a) \\
\text{subject to} \quad & [t_{u,e}^{\alpha_{u,e}}]^+ \geq z \quad \forall u, e \qquad (9b) \\
& \left(1 + \frac{|\mathbf{h}_u\mathbf{w}_u|^2}{\sigma_u^2 + \sum_{j\neq u}|\mathbf{h}_u\mathbf{w}_j|^2}\right) \geq t_{u,e}v_{u,e}, \quad \forall u, e \qquad (9c) \\
& \left(1 + \frac{|\mathbf{g}_e\mathbf{w}_u|^2}{\sigma_e^2 + \sum_{j\neq u}|\mathbf{g}_e\mathbf{w}_j|^2}\right) \leq v_{u,e}, \quad \forall u, e \qquad (9d) \\
& \sum_{1\leq i\leq M} \|\mathbf{w}_i\|_2^2 \leq P_a. \qquad (9e)
\end{aligned}$$

Even after the above transformation the optimization problem in (9) is still nonconvex and very difficult to solve as only (9b) and (9e) can be cast into a tractable format. It does not appear possible to find a transformation that can convert the above problem into an equivalent convex one. Thus, we must find approximate solutions. To do so, we focus on the constraints given in (9c) and (9d). By introducing additional variables, program (9) can be transformed into the following

$$\begin{aligned}
\underset{\mathbf{w}_i, t_{u,e}, v_{u,e}, \alpha_u, \beta_{u,e}, z}{\text{maximize}} \quad & z \qquad (10a) \\
\text{s.t.} \quad & [t_{u,e}^{\alpha_{u,e}}]^+ \geq z \quad \forall u, e \qquad (10b) \\
& \sigma_u^2 + \sum_{1\leq j\leq M} |\mathbf{h}_u\mathbf{w}_j|^2 \geq t_{u,e}v_{u,e}\alpha_u, \\
& \quad \forall u, e \qquad (10c) \\
& \sigma_u^2 + \sum_{j\neq u} |\mathbf{h}_u\mathbf{w}_j|^2 \leq \alpha_u, \quad \forall u \qquad (10d) \\
& \sigma_e^2 + \sum_{1\leq j\leq M} |\mathbf{g}_e\mathbf{w}_j|^2 \leq v_{u,e}\beta_{u,e}, \quad \forall u, e \\
& \qquad (10e) \\
& \sigma_e^2 + \sum_{j\neq u} |\mathbf{g}_e\mathbf{w}_j|^2 \geq \beta_{u,e}, \quad \forall u, e \qquad (10f) \\
& \sum_{1\leq i\leq M} \|\mathbf{w}_i\|_2^2 \leq P_a. \qquad (10g)
\end{aligned}$$

[3]For numerical purposes, we assume nonzero secrecy rate i.e., $[r]^+ = \max\{r, 1\}$. Here we note that without the logarithmic function, the definition of $[r]^+$ is changed accordingly.

We are now in a position to determine the additional tractable convex constraints.

1) Transformation of (10d) and (10e): The constraints in (10d) and (10e) can both be expressed as second-order cone (SOC) constraints. Specifically, with the implicit assumptions $\alpha_u \geq 0, v_{u,e} \geq 0, \beta_{u,e} \geq 0$ for all u, e, the rights sides of (10d) and (10e) can be represented as $\alpha_u = 0.25\{(\alpha_u+1)^2 - (\alpha_u - 1)^2\}$ and $v_{u,e}\beta_{u,e} = 0.25\{(v_{u,e}+\beta_{u,e})^2 - (v_{u,e}-\beta_{u,e})^2\}$, respectively. Therefore, for all u, e both (10d) and (10e) can be expressed as the following SOC constraints

$$\sqrt{\sigma_u^2 + \sum_{j\neq u} |\mathbf{h}_u\mathbf{w}_j|^2 + \frac{1}{4}(\alpha_u - 1)^2} \leq \frac{1}{2}(\alpha_u + 1) \text{ and}$$
$$\sqrt{\sigma_e^2 + \sum_{j=1}^{M} |\mathbf{g}_e\mathbf{w}_j|^2 + \frac{1}{4}(v_{u,e} - \beta_{u,e})^2} \leq \frac{1}{2}(v_{u,e}+\beta_{u,e}) \quad (11)$$

respectively.

2) Approximation of (10c) and (10f): To deal with the nonconvex constraints given in (10c) and (10f), we need to approximate them with their convex counterparts. Let us focus on the more difficult constraints in (10c) and the strategy to handle the set of constraints in (10f) should be evident. For all u, e, note that by introducing slack variables, (10c) can take the form

$$\sigma_u^2 + \sum_{1\leq j\leq M} \gamma_{u,j} \geq t_{u,e}v_{u,e}\alpha_u, \ |\mathbf{h}_u\mathbf{w}_j| \geq \sqrt{\gamma_{u,j}}, \quad \forall j. \quad (12)$$

Still, the above set is composed of nonconvex constraints. For the second set of inequality constraints in (12), we make the following useful observation. For all u, j, the left side of this inequality constraint can be linearized by only taking the real part of $\mathbf{h}_u\mathbf{w}_j$ into consideration. The presence of similar constraints in an optimization problem are well known to render it NP-hard [20]. Since, for a complex number k, $\Re(k) \leq |k|$, a solution of the proposed approximation would guarantee a feasible solution to the original problem. Therefore, this constraint can be safely approximated as $\Re(\mathbf{h}_u\mathbf{w}_j) \geq \sqrt{\gamma_{u,j}}$. However, this constraint is still not in a convex form because of the concavity of the right side of the inequality.

The goal of our analysis is to arrive at an iterative solution to **Problem a**, which is primarily based on a recently introduced iterative scheme [21] that is used to approximately solve nonconvex problems. Let $\sqrt{\gamma_{u,j}} \triangleq f(\gamma_{u,j})$ be the nonconvex term, and suppose there is a function $g(\gamma_{u,j}, \theta_{u,j})$, which is *convex* in $\gamma_{u,j}$ for given *parameter* $\theta_{u,j}$, so that $f(\gamma_{u,j}) \leq g(\gamma_{u,j}, \theta_{u,j})$ holds for an appropriate range of $\theta_{u,j}$. Further, we determine $\bar{\theta}_{u,j}$ as a function of $\gamma_{u,j}$ that satisfies the following conditions

$$f(\gamma_{u,j}) = g(\gamma_{u,j}, \bar{\theta}_{u,j}), \nabla_{\gamma_{u,j}} f(\gamma_{u,j}) = \nabla_{\gamma_{u,j}} g(\gamma_{u,j}, \bar{\theta}_{u,j}) \quad (13)$$

where the gradient has been used in the second condition to emphasize that the procedure given in [21] is applicable to nonconvex functions of multiple variables as well. With the above conditions, Beck *et al.*. [21] and earlier Marks and Wright [22] derived an iterative procedure where the auxiliary variables (parameters) of bounding functions are prudently updated to meet the conditions (13) in every iteration. In our case, $f(\gamma_{u,j})$ is concave and in the n^{th} step of the iterative procedure, a convenient convex upper bound that satisfies the conditions in (13) is given by its first order Taylor series approximation, i.e.,

$$\sqrt{\gamma_{u,j}} \leq \sqrt{\gamma_{u,j}^{(n)}} + \frac{1}{2\sqrt{\gamma_{u,j}^{(n)}}}(\gamma_{u,j} - \gamma_{u,j}^{(n)}). \quad (14)$$

It is easy to see that if in the $n+1^{\text{st}}$ iteration the parameter $\gamma_{u,j}$ is updated as $\gamma_{u,j}^{(n+1)} = \gamma_{u,j}^{(n)}$, the conditions in (13) are satisfied. By providing this synopsis of the iterative scheme in [21], we have also dealt with the second inequality constraint in (12) and transformed it into a tractable approximation. The left side of the first inequality constraint in (12) is linear, and the only troublesome term is on the right side of this constraint. It is neither convex nor concave in its variables. First, notice the following equivalent transformation of this constraint for all u, e

$$\sigma_u^2 + \sum_{j=1}^{M} \gamma_{u,j} \geq t_{u,e}v_{u,e}\alpha_u \Leftrightarrow \begin{cases} \sigma_u^2 + \sum\limits_{j=1}^{M} \gamma_{u,j} \geq (\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{\frac{1}{3}} \\ t_{u,e}^3 \leq \vartheta_{u,e}^a, v_{u,e}^3 \leq \vartheta_{u,e}^b, \alpha_u^3 \leq \vartheta_u^c. \end{cases} \quad (15)$$

The first type of constraint in the equivalent formulation has got geometric mean of variables $\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c$ on its right side. Notice that the additional constraints introduced in the new transformation are all SOC representable. For example, consider the first of these constraints and observe that it can be rewritten as

$$(t_{u,e}^2)^2 \leq t_{u,e}\vartheta_{u,e}^a \Leftrightarrow \begin{cases} (\vartheta_{u,e}^{a_a})^2 \leq t_{u,e}\vartheta_{u,e}^a \\ t_{u,e}^2 \leq \vartheta_{u,e}^{a_a} \end{cases}$$
$$\Leftrightarrow \begin{cases} \sqrt{(\vartheta_{u,e}^{a_a})^2 + \frac{1}{4}(t_{u,e} - \vartheta_{u,e}^a)^2} \leq \frac{1}{2}(t_{u,e} + \vartheta_{u,e}^a) \\ \sqrt{t_{u,e}^2 + 0.25(\vartheta_{u,e}^{a_a} - 1)^2} \leq 0.5(\vartheta_{u,e}^{a_a} + 1) \end{cases} \quad (16)$$

where the implicit assumption that $t_{u,e}, \vartheta_{u,e}^a, \vartheta_{u,e}^{a_a}$ belong to the nonnegative orthant is understood to hold. In a similar way, the remaining constraints in (15) can be represented as a system of SOC constraints. Now recall that $(\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{1/3}$ is concave in its variables, and, hence, destroys the convexity of the first set of constraints provided in the equivalence relation (15). To handle this, we approximate it by again resorting to the convex upper bounding technique of [21]. As in the previous case, the first order Taylor approximation can be used to obtain the desired bound. Let $h(\mathbf{v}) \triangleq (\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{1/3}$, where $\mathbf{v} = [\vartheta_{u,e}^a, \vartheta_{u,e}^b, \vartheta_u^c]^T$ then in the n^{th} iteration the function can be bounded as follows

$$h(\mathbf{v}) \leq h(\mathbf{v}^{(n)}) + \nabla h(\mathbf{v}^{(n)})^T(\mathbf{v} - \mathbf{v}^{(n)}) \quad (17)$$

where

$$\nabla h(\mathbf{v}) = \left[\frac{\vartheta_{u,e}^b \vartheta_u^c}{3(\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{2/3}}, \ \frac{\vartheta_{u,e}^a \vartheta_u^c}{3(\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{2/3}}, \ \frac{\vartheta_{u,e}^a \vartheta_{u,e}^b}{3(\vartheta_{u,e}^a \vartheta_{u,e}^b \vartheta_u^c)^{2/3}} \right].$$

Finally, for the constraint in (10f) it is plain to see that after introducing the additional variables, we can approximate the quadratic terms by their linear counterparts as done in the case of (10c), albeit without worrying about the nonconvexity of the terms on the right side due to their linear nature. To summarize, the iterative algorithm for **Problem a** outlined below obtains the solution of the following convex optimization problem in its n^{th}

step (see (18) at the bottom of the page), where we have used the compact notation of (17). Now, we outline a simple iterative procedure needed to solve **Problem a**

Initialization: set $n := 0$ and randomly generate $(\gamma_{u,j}^{(n)}, \Gamma_{e,j}^{(n)}, \mathbf{v}^{(n)})$ so that the problem (18) is feasible.

repeat

- Solve (18).
- Denote the resulting optimal values of $(\gamma_{u,j}, \Gamma_{e,j}, \mathbf{v})$ by $(\gamma_{u,j}^{\star}, \Gamma_{e,j}^{\star}, \mathbf{v}^{\star})$.
- Set $(\gamma_{u,j}^{(n+1)}, \Gamma_{e,j}^{(n+1)}, \mathbf{v}^{(n+1)}) = (\gamma_{u,j}^{\star}, \Gamma_{e,j}^{\star}, \mathbf{v}^{\star})$ and update $n := n + 1$.

until convergence or required number of iterations

It is noteworthy that if the parameters to be updated in (18e) and (18i) tend to zero, a small nonzero constant can be added to these to ensure numerical stability.

B. Solution of **Problem b**

Similar to the case in **Problem a**, let us begin with the following equivalently transformed version of the multicast problem

$$\underset{\mathbf{Q},t_{u,e},v_{u,e},z}{\text{maximize}} \quad z \tag{19a}$$

$$\text{subject to} \quad [t_{u,e}^{\alpha_{u,e}}]^{+} \geq z \quad \forall u,e \tag{19b}$$

$$\left(1+\mathbf{h}_u\mathbf{Q}\mathbf{h}_u^{\mathrm{H}}\right) \geq t_{u,e}v_{u,e}, \quad \forall u,e \tag{19c}$$

$$\left(1+\mathbf{g}_e\mathbf{Q}\mathbf{g}_e^{\mathrm{H}}\right) \leq v_{u,e}, \quad \forall u,e \tag{19d}$$

$$\mathrm{tr}(\mathbf{Q}) \leq P_b, \quad \mathbf{Q} \succeq 0 \tag{19e}$$

where we have introduced the same auxiliary variables as in (9) since being an independent problem this should not cause any confusion. Matrix $\mathbf{Q}$ belongs to the cone of positive semidefinite matrices.[4] We can decompose it as $\mathbf{Q} = \mathbf{B}\mathbf{B}^{\mathrm{H}}$ (for example, $\mathbf{B}$ could represent a lower triangular matrix in a Cholesky decomposition of $\mathbf{Q}$) and rewrite the above problem in terms of new optimization variables as

$$\underset{\mathbf{B},t_{u,e},v_{u,e},z}{\text{maximize}} \quad z \tag{20a}$$

$$\text{subject to} \quad [t_{u,e}^{\alpha_{u,e}}]^{+} \geq z \quad \forall u,e \tag{20b}$$

$$\|\mathbf{h}_u\mathbf{B}\|_2 \geq \sqrt{t_{u,e}v_{u,e}-1}, \quad \forall u,e \tag{20c}$$

$$\|\mathbf{g}_e\mathbf{B}\|_2^2 \leq v_{u,e}-1, \quad \forall u,e \tag{20d}$$

$$\|\mathrm{vec}(\mathbf{B})\|_2^2 \leq P_b \tag{20e}$$

where $\mathrm{vec}(\mathbf{B})$ stacks the columns of matrix $\mathbf{B}$.

1) Transformation of (20d): Although the constraint in (20d) is convex, it is still not explicitly expressed as an SOC constraint in the decision variables. To do so, we make a few key observations. Note that $\|\mathbf{g}_e\mathbf{B}\|_2^2 = \|[\mathbf{g}_e[\mathbf{B}]_1, \ldots, \mathbf{g}_e[\mathbf{B}]_T]\|_2^2 =$

[4]When required (for example, in a semidefinite program based solution), this constraint should be considered implicit.

$$\underset{\substack{\mathbf{W},t_{u,e},v_{u,e},\alpha_u,\\ \beta_{u,e},z,\mathbf{v},\gamma_{u,j},\Gamma_{e,j}\\ \vartheta_{u,e}^{a},\vartheta_{u,e}^{b},\vartheta_{u}^{c},\vartheta_{u,e}^{a_a},\\ \vartheta_{u,e}^{b_b},\vartheta_{u}^{c_c}}}{\text{maximize}} \quad z \tag{18a}$$

$$\text{subject to} \quad [t_{u,e}^{\alpha_{u,e}}]^{+} \geq z \quad \forall u,e \tag{18b}$$

$$\sigma_u^2 + \sum_{1\leq j\leq M} \gamma_{u,j} \geq h(\mathbf{v}^{(n)}) + \nabla h(\mathbf{v}^{(n)})^T(\mathbf{v}-\mathbf{v}^{(n)}), \quad \forall u,e \tag{18c}$$

$$\begin{cases} (16) \text{ and } \begin{cases} \sqrt{(\vartheta_{u,e}^{b_b})^2 + 0.25(v_{u,e}-\vartheta_{u,e}^{b})^2} \leq 0.5(v_{u,e}+\vartheta_{u,e}^{b}) \\ \sqrt{v_{u,e}^2 + 0.25(\vartheta_{u,e}^{b_b}-1)^2} \leq 0.5(\vartheta_{u,e}^{b_b}+1) \end{cases} \forall u,e \\ \begin{cases} \sqrt{(\vartheta_{u}^{c_c})^2 + 0.25(\alpha_u-\vartheta_{u}^{c})^2} \leq 0.5(\alpha_u+\vartheta_{u}^{c}) \\ \sqrt{\alpha_u^2 + 0.25(\vartheta_{u}^{c_c}-1)^2} \leq 0.5(\vartheta_{u}^{c_c}+1) \end{cases} \forall u \end{cases} \tag{18d}$$

$$\Re(\mathbf{h}_u\mathbf{w}_j) \geq \sqrt{\gamma_{u,j}^{(n)}} + \frac{1}{2\sqrt{\gamma_{u,j}^{(n)}}}(\gamma_{u,j}-\gamma_{u,j}^{(n)}), \quad \forall u,j \tag{18e}$$

$$\sqrt{\sigma_u^2 + \sum_{j\neq u} |\mathbf{h}_u\mathbf{w}_j|^2 + \frac{1}{4}(\alpha_u-1)^2} \leq \frac{1}{2}(\alpha_u+1), \ \forall u \tag{18f}$$

$$\sqrt{\sigma_e^2 + \sum_{j=1}^{M} |\mathbf{g}_e\mathbf{w}_j|^2 + \frac{1}{4}(v_{u,e}-\beta_{u,e})^2} \leq \frac{1}{2}(v_{u,e}+\beta_{u,e}), \ \forall u,e \tag{18g}$$

$$\sigma_e^2 + \sum_{j\neq u} \Gamma_{e,j} \geq \beta_{u,e}, \quad \forall u,e \tag{18h}$$

$$\Re(\mathbf{g}_e\mathbf{w}_j) \geq \sqrt{\Gamma_{e,j}^{(n)}} + \frac{1}{2\sqrt{\Gamma_{e,j}^{(n)}}}(\Gamma_{e,j}-\Gamma_{e,j}^{(n)}), \quad \forall e,j \tag{18i}$$

$$\sum_{1\leq i\leq M} \|\mathbf{w}_i\|_2^2 \leq P_a. \tag{18j}$$

$\sum_{k\leq T}|[\mathbf{g}_e\mathbf{B}]_k|^2$, where $[\mathbf{g}_e\mathbf{B}]_k$ and $[\mathbf{B}]_k$ denote the k^{th} coordinate and column of $\mathbf{g}_e\mathbf{B}$ and $\mathbf{B}$, respectively. Now for all u, e, the following equivalence relations are easy to see

$$\sum_{k=1}^{T}|[\mathbf{g}_e\mathbf{B}]_k|^2 \leq v_{u,e}-1 \Leftrightarrow \begin{cases} \sum\limits_{k=1}^{T}\varpi_{e,k}^2 \leq v_{u,e}-1 \\ |[\mathbf{g}_e\mathbf{B}]_k| \leq \varpi_{e,k}, \forall k \end{cases} \Leftrightarrow$$
$$\begin{cases} \sum\limits_{k=1}^{T}\varpi_{e,k}^2 + \frac{1}{4}(v_{u,e}-1)^2+1 \leq \frac{1}{4}(v_{u,e}+1)^2 \\ \|\Re([\mathbf{g}_e\mathbf{B}]_k), \Im([\mathbf{g}_e\mathbf{B}]_k)\|_2 \leq \varpi_{e,k}, \quad \forall k. \end{cases} \tag{21}$$

In the final step of (21), it is seen that all constraints are represented as SOC constraints.

2) Approximation of (20c): In order to handle the remaining constraints in (20c), we need to use tractable and safe approximations as done while solving **Problem a**. Again, for all u, e, consider the following transformations that render this set of constraints to a form suitable for obtaining convex approximations

$$\sum_{k=1}^{T}|[\mathbf{h}_u\mathbf{B}]_k|^2 \geq t_{u,e}v_{u,e}-1 \Leftrightarrow \begin{cases} \sum\limits_{k=1}^{T}\omega_{u,k}^2 \geq \sqrt{\zeta_{u,e}^a\zeta_{u,e}^b}-1 \\ \zeta_{u,e}^a \geq t_{u,e}^2, \zeta_{u,e}^b \geq v_{u,e}^2 \\ |[\mathbf{h}_u\mathbf{B}]_k| \geq \omega_{u,k}, \quad \forall k. \end{cases} \tag{22}$$

The middle inequality constraints in (22) are expressible as SOC constraints. The first set of inequality constraints in (22) involve a concave function on the right side of the inequality and hence, this term can be approximated with the following convex upperbound in the n^{th} iteration of the algorithm.

$$\sqrt{\zeta_{u,e}^a\zeta_{u,e}^b} \leq \sqrt{\{\zeta_{u,e}^a\zeta_{u,e}^b\}^{(n)}} + \underbrace{\left[\frac{\zeta_{u,e}^b}{2\sqrt{\zeta_{u,e}^a\zeta_{u,e}^b}}, \frac{\zeta_{u,e}^a}{2\sqrt{\zeta_{u,e}^a\zeta_{u,e}^b}}\right]}_{\text{gradient in the } n^{\text{th}} \text{ iteration}}$$
$$\times \left([\zeta_{u,e}^a, \zeta_{u,e}^b] - [\{\zeta_{u,e}^a\}^{(n)}, \{\zeta_{u,e}^b\}^{(n)}]\right)^T$$
$$\triangleq f^{(n)}(\zeta_{u,e}^a\zeta_{u,e}^b) \tag{23}$$

where it is easy to see that this bound satisfies the conditions stated in (13) when the variables in the $n+1^{\text{st}}$ iteration are updated with their values in the n^{th} step. The left side of this constraint is a convex function of variables $\omega_{u,k}$. To make it computationally amenable, it is required to upper bound the negative of this function in the n^{th} iteration as

$$-\sum_{k=1}^{T}\omega_{u,k}^2 \leq -\left[\sum_{k=1}^{T}(\omega_{u,k}^{(n)})^2 + \sum_{k=1}^{T}2\omega_{u,k}^{(n)}(\omega_{u,k}-\omega_{u,k}^{(n)})\right]. \tag{24}$$

With this, the first constraint in (22) is completely linearized. Finally, in the last set of the constraints in (22), the same conservative but safe approximation strategy as opted in the solution of **Problem a** is employed. Specifically, we replace the left side of this inequity with $\Re([\mathbf{h}_u\mathbf{B}]_k)$ for all k, and arrive at a linear formulation of this nonconvex constraint. Combining the manipulations presented above, the convex program solved in the n^{th} iteration of the algorithm proposed below, therefore, is shown in (25) at the bottom of the page. An algorithm that approximately solves **Problem b** is

Initialization: set $n := 0$ and randomly generate $\left(\omega_{u,k}^{(n)}, \{\zeta_{u,e}^a\}^{(n)}, \{\zeta_{u,e}^b\}^{(n)}\right)$ so that (25) is feasible.

repeat

- Solve (25).
- Denote the resulting optimal values of $\left(\omega_{u,k}, \zeta_{u,e}^a, \zeta_{u,e}^b\right)$ by $\left(\omega_{u,k}^\star, \{\zeta_{u,e}^a\}^\star, \{\zeta_{u,e}^b\}^\star\right)$.
- Set $\left(\omega_{u,k}^{(n+1)}, \{\zeta_{u,e}^a\}^{(n+1)}, \{\zeta_{u,e}^b\}^{(n+1)}\right) = \left(\omega_{u,k}^\star, \{\zeta_{u,e}^a\}^\star, \{\zeta_{u,e}^b\}^\star\right)$ and update $n := n+1$.

until convergence or required number of iterations

In the broadcast case we considered a beamforming system. After the above analysis for both **Problem a** and **Problem b**, we note that an approximation for **Problem a** with general linear precoding can be obtained analogously. Likewise, the interesting problem of showing the optimality of beamforming for **Problem a** may be tackled using the techniques proposed in [23], [24]. Before concluding this section, it should be mentioned that for a certain range of weighting vectors $\alpha_{u,e}$ for all u, e, the multicasting problem can be cast as a semidefinite program (SDP), cf. Lemma 1. A complexity and performance comparison of both approaches appears in Sections III-D and VI, respectively.

$$\underset{\substack{\mathbf{B}, t_{u,e}, v_{u,e}, z \\ \omega_{u,k}, \varpi_{e,k}, \zeta_{u,e}^a\zeta_{u,e}^b}}{\text{maximize}} \quad z \tag{25a}$$
$$\text{subject to} \quad [t_{u,e}^{\alpha_{u,e}}]^+ \geq z \quad \forall u, e \tag{25b}$$
$$\sum_{k=1}^{T}(\omega_{u,k}^{(n)})^2 + \sum_{k=1}^{T}2\omega_{u,k}^{(n)}(\omega_{u,k}-\omega_{u,k}^{(n)}) \geq f^{(n)}(\zeta_{u,e}^a\zeta_{u,e}^b) - 1, \quad \forall u, e \tag{25c}$$
$$\zeta_{u,e}^a \geq t_{u,e}^2, \zeta_{u,e}^b \geq v_{u,e}^2, \quad \forall u, e \tag{25d}$$
$$\Re([\mathbf{h}_u\mathbf{B}]_k) \geq \omega_{u,k}, \ \forall u, k = 1, \ldots, T \tag{25e}$$
$$\sum_{k=1}^{T}\varpi_{e,k}^2 + \frac{1}{4}(v_{u,e}-1)^2 + 1 \leq \frac{1}{4}(v_{u,e}+1)^2, \quad \forall u, e \tag{25f}$$
$$\|\Re([\mathbf{g}_e\mathbf{B}]_k), \Im([\mathbf{g}_e\mathbf{B}]_k)\|_2 \leq \varpi_{e,k}, \ \forall e, k = 1, \ldots, T \tag{25g}$$
$$\|\text{vec}(\mathbf{B})\|_2^2 \leq P_b. \tag{25h}$$

C. Improved Solutions for **Problem a** and **Problem b**

The above solutions for the case of genie supplied perfect CSI can be improved in terms of the objective achieved. The key to achieving this goal stems from noting the fact that for a complex number c the relation $\Re(c) \leq |c|$ holds true. This inequality renders conservatism to the solutions of both **Problem a** and **Problem b**. In order to obtain an improved objective, for all u, let us first revisit the second set of inequality constraints in (12) and note that it can be equivalently cast in the following form

$$\hat{r}_{u,j}^2 + \hat{i}_{u,j}^2 \geq \gamma_{u,j}, \quad \forall j \tag{26}$$

$$\Re(\mathbf{h}_u \mathbf{w}_j) = \hat{r}_{u,j}, \quad \Im(\mathbf{h}_u \mathbf{w}_j) = \hat{i}_{u,j}, \quad \forall j. \tag{27}$$

Indeed, the left side of the first constraint in (26) is convex in the variables involved and renders the constraint set intractable. This function can be iteratively approximated by its first order approximation in a manner very similar to the one used for the first inequality constraint in (22). Likewise, we can iteratively approximate the terms $|\mathbf{g}_e \mathbf{w}_j|^2$ and $|[\mathbf{h}_u \mathbf{B}]_k|^2$ appearing in (10f) and third inequality of (22), respectively to obtain new tractable formulations for **Problem a** and **Problem b**. Since the optimization variables are successively updated, the approximate solution is much better and less conservative in comparison to the one obtained by straightforwardly invoking the relation $\Re(c) \leq |c|$. To corroborate our finding, **Problem b** is solved and its solution is compared with the one obtained by using bisection search whose each iteration checks the feasibility of an SDP in $\mathbf{Q}$, and also with the formulation in [25]. Note that although the secrecy problem in [25] is represented as an SDP that achieves the same rate as obtained with bisection, [25] gives a more computationally efficient solution than simple bisection search. Extensive experimentation revealed that the improved SOCP solution produced the same objective as obtained from the SDP one. Fortunately, it is possible to provide a more mathematical statement in this regard. To this end, consider the following.

*Lemma 1: For $t_{u,e} \geq 1$ and $\alpha_{u,e} \leq 1$ for all u, e, the **Problem b** can be equivalently cast as the following semidefinite program (SDP)*

$$\underset{\tilde{\mathbf{Q}}, t_{u,e}, \theta}{\text{maximize}} \quad t_{u,e}^{\alpha_{u,e}} \tag{28a}$$

$$\text{s.t.} \quad \left(\theta + \text{Tr}(\mathbf{h}_u \tilde{\mathbf{Q}} \mathbf{h}_u^{\text{H}})\right) \geq t_{u,e}, \quad \forall u, e,$$

$$\left(\theta + \text{Tr}(\mathbf{g}_e \tilde{\mathbf{Q}} \mathbf{g}_e^{\text{H}})\right) = 1 \tag{28b}$$

$$\text{tr}(\tilde{\mathbf{Q}}) \leq \theta P_b, \ \tilde{\mathbf{Q}} \succeq 0, \theta \geq 0 \tag{28c}$$

where $\mathbf{Q}\theta = \tilde{\mathbf{Q}}$.

Proof: The proof of this lemma readily follows from the concavity of $[t_{u,e}^{\alpha_{u,e}}]^+$ for the range of the parameters mentioned, and the arguments based on Charnes-Cooper transformation [25] that lead to the SDP given in (28). ■

Now we state the following striking result particularly relevant to **Problem b**.

Proposition 1: With the improved formulation given in (26) and (27)*, let $\mathbf{x}^{(n)}$ denote the sequence of Karush-Kuhn-Tucker (KKT) points of **Problem b** returned by the above sequential convex approximation procedure. Further, let $\mathbf{x}_{org}^{(n)}$ denote the KKT points of* (19)*. It can be shown that as n tends to infinity, $\|\mathbf{x}^{(n)} - \mathbf{x}_{org}^{(n)}\|$ tends to zero.*

Proof: The proof of the proposition is exactly the same as available in [21, Proposition 3.2] once we notice the fact that the problem under consideration satisfies the conditions needed to invoke [21, Proposition 3.2]. Indeed, from the formulation given in Lemma 1, it is straightforward to see that the objective is strictly concave when $0 < \alpha_{u,e} < 1$ for all u, e. Moreover, the feasible set is already convex due to the SDP representation of **Problem b**, cf. Lemma 1. Hence reproducing the same arguments as in [21, Proposition 3.2] we arrive at the desired conclusion. ■

TABLE I
AVERAGE RUN TIME (IN SECONDS) VERSUS THE NUMBER OF TRANSMIT ANTENNAS, T FOR TWO PROPOSED (IMPROVED AND SIMPLIFIED) DESIGNS FOR **PROBLEM b**. THE NUMBER OF LEGITIMATE USERS AND EAVESDROPPERS IS SET TO $M = 2$ AND $N = 3$, RESPECTIVELY. THE TOTAL TRANSMIT POWER IS SET TO $P_b = 12$ dB

Antennas, T	8	16	32	64	128
Simplified design	0.85	1.01	1.17	1.89	3.27
Improved design	0.95	1.25	1.49	2.46	4.19

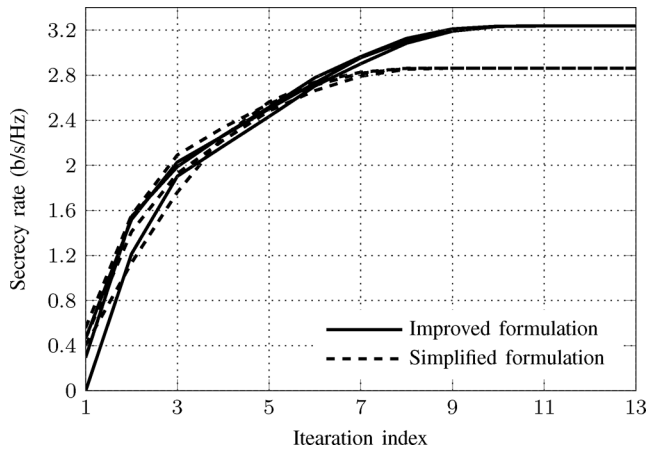


Fig. 1. Convergence results of the simplified and improved solutions of Problem b with randomly generated starting points. The number of antennas, legitimate users and eavesdroppers is set to $T = 8$, $M = 4$ and $N = 3$, respectively.

An interesting observation should be reported at this point. As mentioned previously, for the range of parameters given in Proposition 1, the SOCP solution converges to the SDP one. This can be attributed to the fact that convergence to KKT points (Proposition 1) is both necessary and sufficient when the original problem admits a convex representation (Lemma 1). A numerical demonstration of this results appears in Section VI. It is clear to see that the improvement in the SOCP based solution comes at the cost of increasing the number of variables and constraints, which naturally contributes to the computational complexity of the proposed solution. To demonstrate this we have produced Table I where, without loss of generality, we report computational times for **Problem b** with (26) and (27) (called improved design) and by the using the earlier real approximation (called simplified design). It is seen that expectedly the improved formulation consumes more time to obtain a solution for the given parameters.

In addition to this effect, the additional variables introduced in (26) and (27) are likely to contribute negatively to the convergence properties of the algorithm. However, this drawback comes with an immediate benefit of obtaining a much improved objective function i.e., the secrecy rate. We quantify this observation in Fig. 1 for a given scenario. It is clearly seen that the

improved solution yields a better objective at a deteriorated convergence behavior.

We further remark here that, unfortunately, the manipulation introduced in (26) and (27) does not carry to the case when the channels to the legitimate and eavesdropping nodes are corrupted with errors. This occurs since the presence of error vectors with continuous nature render unavoidable intractability to the equality constraints in (27). Therefore, in the sections to follow we will focus on the simplified approximations for both **Problem a** and **Problem b**.

D. Some Remarks on Complexity Estimate

In order to provide some complexity perspective of the proposed schemes, we will compare the complexity estimate of the formulation used to approximate genie-aided **Problem b** with the SDP formulation of the same problem refer to Lemma 1. We note that the algorithm used to solve **Problem b** is run for a few fixed number of iterations, and the convergence relies heavily on the initialization (please refer to Section VI). Therefore, we will need to provide the worst case complexity estimate of (25) solved in each of the runs of the algorithm. To do so, we will use the worst case complexity estimates of general interior point methods given in [20], [26]. The worst case complexity of a general interior point method for the SOCP problem (25) is $\mathcal{O}\left(MNT(MN+T^2)^2\right)$. The worst case complexity estimate for SDP version of **Problem b** amounts to $\mathcal{O}((M+N+T^2)^{3.5})$. It is seen that the number of transmit antennas do adversely affect the worst case complexity of SDP formulation. At the same time the numbers M, N enter into the worst case estimates of the SOCP formulation with less sensitivity in terms of the powers they are raised to. The good news is that T affects the worst case complexity of SOCP by almost a couple of orders of magnitude *lower* than it affects the SDP solution. Since very efficient solvers are available for SOCPs, so practically we expect it to perform even better. More on this appears in the section to follow. To conclude this subsection, we note that for **Problem a**, the formulation (18) admits a complexity estimate of $\mathcal{O}\left(T^3M^3N(1+N)^2\right)$ for the broadcast problem approximation.

IV. Secrecy Rate Maximization With Practical Considerations

To wiretap the message between the legitimate transceivers, the eavesdropping nodes require becoming part of the communication architecture. This enables them, at least, to know the channel in the downlink. However, to wiretap a channel without being removed from the system, the eavesdroppers have to protect their visibility from the proper communicating entities. Therefore, in the worst case scenario from the perspective of the lawful transmitter, the spying nodes succeed in keeping licensed users oblivious of their presence without exposing most of their parameters (like CSI, CQI etc.) to the transmitter by, for instance, not responding to its calls.

A. What if the Eavesdropper is Close to the Base Station?

As evident from the previous theoretical development, the secrecy rate is a function of the difference of the date rates at the legitimate user and the wiretapper (see for example, the expression for multicasting case with perfect CSI). From its mathematical formalism, it is evident that unless the SNR at the wiretapper is correlated with that of the legitimate user, the secrecy rate is an appreciable nonzero quantity. Therefore, close proximity of the eavesdropper to the base station, which in turn may imply greater signal strength, would only be meaningful (for the purpose of wiretapper) when the channel transfer function to it is correlated with that of the legitimate receiver.

B. CSI Model of Eavesdroppers

To this end, observe that in order to somehow decipher the private message of one of the M users, an eavesdropper has to be in close enough proximity of that user and notice a similar strength or more precisely SNR of the transmitted signal. This motivates approximating the channel estimate of that eavesdropper as a *function of the channel estimate* of the user whose message the wiretapper aims to decode. Indeed, spatial correlation between radio signals in cellular environments is known to exist, as experimentally demonstrated in [27]. Specifically, for an eavesdropper e, this amounts to modeling the estimate of its channel as

$$\mathbf{g}_e = f(\bar{\mathbf{h}}_u) + \boldsymbol{\delta}_{\mathbf{g}_e} \tag{29}$$

where $\bar{\mathbf{h}}_u$ is the channel estimate of a user u, and $f(\bar{\mathbf{h}}_u)$ and $\boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e}$ are elaborated in the sequel. A user u can, for example, be affected the most by the wiretapping node that has the minimum distance from it, i.e., the node that minimizes the metric $D_{eu} = \|\mathbf{d}_e - \mathbf{d}_u\|_2$ over all $e \in \{1, \ldots, N\}$ wiretappers, where the spatial coordinates of the eavesdropper e and the user u are denoted $\mathbf{d}_e$ and $\mathbf{d}_u$, respectively.

Coming back to our model presented in (29), we see that the function of the known channel estimate is a mapping of the form $f : \mathbb{C}^{1\times T} \times \mathbb{C}^{T\times T} \to \mathbb{C}^{1\times T}$. For example, this function can be affine in nature and representable as $f(\bar{\mathbf{h}}_u) = \bar{\mathbf{h}}_u\mathbf{A}_u + \mathbf{a}_u$, where $\mathbf{A}_u$ and $\mathbf{a}_u$ may be the parameters of the subspace in which the channel estimate of an eavesdropper lives. Now we model the error terms contained in $\mathcal{S}_{\mathbf{g}_e}$, the second term in (29). If the system relies on the RSS method of detecting the proximity user of an eavesdropper, it appears sensible to assume that the individual terms of the error vector (each of which is a complex number) lie inside a "box" of a specific dimension, say, $\rho_{\mathbf{g}_e}$ i.e.,

$$\begin{aligned}\mathcal{S}_{\mathbf{g}_e} &= \{\boldsymbol{\delta}_{\mathbf{g}_e} : |[\boldsymbol{\delta}_{\mathbf{g}_e}]_i|^2 \le \rho_{\mathbf{g}_e}^2, i = 1, \ldots, T\} \\ &= \{\boldsymbol{\delta}_{\mathbf{g}_e} : \|\boldsymbol{\delta}_{\mathbf{g}_e}\|_\infty \le \rho_{\mathbf{g}_e}\}.\end{aligned} \tag{30}$$

Although there is no specific motivation for modeling the errors using l_∞ norm, a scenario of interest may arise when, say, l_∞ norm based optimization criterion is used for estimating the legitimate user's channel [28]. Moreover, it will be later clear that uncertainty sets, $\mathcal{S}_{\mathbf{g}_e}$, parameterized by a constraint on a different norm (for instance, l_2 norm) can be handled conveniently based on the proposed development.

C. CSI Model of the Legitimate Users

The CSI of the legitimate nodes can be modeled in a traditional way. Upon estimating the channel of user u, the true channel seen at the transmitter is of the form

$$\mathbf{h}_u = \bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u}, \quad u = 1, \ldots, M \tag{31}$$

where $\bar{\mathbf{h}}_u$ denotes the estimated (known) value of the u^{th} user's channel and the second term characterizes the channel estima-

tion error contained in the uncertainty set $\mathcal{S}_{\mathbf{h}_u}$. The traditional assumption of Gaussian errors in the channel estimation process [29] motivates the following model for the uncertainty set

$$\mathcal{S}_{\mathbf{h}_u} = \{\boldsymbol{\delta}_{\mathbf{h}_u} : \|\boldsymbol{\delta}_{\mathbf{h}_u}\|_{\mathbf{E}_u} \leq \rho_{\mathbf{h}_u}\}, \quad u = 1, \ldots, M \tag{32}$$

where $\|\boldsymbol{\delta}_{\mathbf{h}_u}\|_{\mathbf{E}_u} = \sqrt{\boldsymbol{\delta}_{\mathbf{h}_u}\mathbf{E}_u\boldsymbol{\delta}_{\mathbf{h}_u}^{\mathrm{H}}}$ is the usual elliptic norm with a given nonsingular positive definite $\mathbf{E}_u$ and a suitably chosen constant $\rho_{\mathbf{h}_u}$. However, when there are dominant quantization effects, it is more convenient to model the error terms as [30]

$$\mathcal{S}_{\mathbf{h}_u} = \{\boldsymbol{\delta}_{\mathbf{h}_u} : \|\boldsymbol{\delta}_{\mathbf{h}_u}\|_{\infty} \leq q_{\mathbf{h}_u}\}, \quad u = 1, \ldots, M \tag{33}$$

which is similar to the model used for the eavesdropper presented in (30).

D. Optimization Problem Modeling

To ensure that the proposed precoders perform well at least against those error instances that lie inside the regions given in, for example (32), it is necessary to maximize the rates over all realizations of true channels. Clearly, this optimization process will also take into account those errors that most adversely affect the performance of the designed precoders. Such error realizations may be rare. Hence, this philosophy, dubbed as *worst case robust optimization* [31], can result in a rather conservative design. Despite being conservative, the worst case design either allows the problem to be equivalently transformed into a tractable one or admits good approximations [31].

With the above background, **Problem a** takes the form

$$\textbf{Problem a}: \max_{\sum_{i=1}^{M}\|\mathbf{w}_i\|_2^2 \leq P_a} \left\{ \min_{\substack{1\leq u\leq M,\\ 1\leq e\leq N}} \alpha_{u,e} \times R^a_{u,e}(\bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u}, \bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e}, \mathbf{W}),\ \forall(\boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e}, \boldsymbol{\delta}_{\mathbf{h}_u} \in \mathcal{S}_{\mathbf{h}_u}) \right\} \tag{34}$$

and **Problem b** can be written as

$$\textbf{Problem b}: \max_{\mathbf{Q}\succeq 0:\mathrm{tr}(\mathbf{Q})\leq P_b} \left\{ \min_{\substack{1\leq u\leq M,\\ 1\leq e\leq N}} \alpha_{u,e} \times R^b_{u,e}(\bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u}, \bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e}, \mathbf{Q}),\ \forall(\boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e}, \boldsymbol{\delta}_{\mathbf{h}_u} \in \mathcal{S}_{\mathbf{h}_u}) \right\} \tag{35}$$

where the uncertainty sets $\mathcal{S}_{\mathbf{g}_e}, \mathcal{S}_{\mathbf{h}_u}$ need not to be identical in (34) and (35). To complete the description of the problems in realistic scenarios, based on our earlier discussion, the uncertainty sets can be defined as

$$\begin{aligned} \mathcal{S}_{\mathbf{g}_e} &= \{\boldsymbol{\delta}_{\mathbf{g}_e} : \|\boldsymbol{\delta}_{\mathbf{g}_e}\|_{\infty} \leq \rho_{\mathbf{g}_e}\}, \quad \forall e, \\ \mathcal{S}_{\mathbf{h}_u} &= \{\boldsymbol{\delta}_{\mathbf{h}_u} : \|\boldsymbol{\delta}_{\mathbf{h}_u}\|_{\mathbf{E}_u} \leq \rho_{\mathbf{h}_u}\}, \quad \forall u. \end{aligned} \tag{36}$$

It is an immediate consequence that the above problems are *semi-infinite* in nature, i.e., with finite optimization variables and infinite constraints. This amounts to the fact that in the above form, the problems are intractable. Typically in the literature, the uncertainty sets are specified via simple Euclidean norm, for example, [32]. In some other works, like [33], one or two quadratic constraints have been considered where the focus has been on duality properties with reference to nonconvex quadratic problems. In order to distinguish between the genie aided benchmark solutions, and the ones obtained with more practical considerations above, we, in the next section, study the solution of secrecy rate maximization under the title of more realistic scenarios. Before outlining our approach to approximately solving the problems, we remark that the SOCP formulations can potentially be more useful than the SDP ones (as for instance outlined in Lemma 1) at least from two different aspects. Firstly, the perturbed SOCP formulations can handle a wider and more complex classes of uncertainty sets [31]. Secondly, for very diverse types of uncertainty sets, it is possible to rewrite an SOCP at the same level of conic complexity (i.e., as an SOCP) [34]. This clearly is more beneficial when complexity is a major concern in some design problem.

V. Solution in Realistic Scenarios

Based on our discussion in the previous section, unlike the traditional sensitivity analysis [35], which is a post-optimization tool, the proposed robust technique defined in (34) and (35) is a pre-optimization strategy. In addition, the sensitivity analysis is only capable of studying the affects of infinitesimally small perturbations on the achieved objective and is not a design tool.

A. Problem a *in Realistic Scenario*

The original form **Problem a** is intractable even when the uncertainty sets $\mathcal{S}_{\mathbf{g}_e}$ and $\mathcal{S}_{\mathbf{h}_u}$ are empty, and the task of obtaining a globally optimal equivalent tractable version of this problem appears hopeless. Therefore, we have to rely on the approximation obtained in (18). With the worst case robust optimization philosophy, the robust counterpart of this program can be written as follows

$$\underset{\mathcal{V}_a}{\text{maximize}} \quad z \tag{37a}$$

$$\text{subject to} \quad \Re(\mathbf{h}_u\mathbf{w}_u) \geq \chi_{u,e}, \quad \forall u, e, \quad \forall \boldsymbol{\delta}_{\mathbf{h}_u} \in \mathcal{S}_{\mathbf{h}_u} \tag{37b}$$

$$(\vartheta^a_{u,e}\vartheta^b_{u,e}\vartheta^c_u)^{\frac{1}{3}} \leq \mathrm{TA}(\chi^2_{u,e}) + \alpha_u, \quad \forall u, e \tag{37c}$$

$$\sigma_u^2 + \sum_{j\neq u} |\mathbf{h}_u\mathbf{w}_j|^2 \leq \alpha_u, \quad \forall u \quad \forall \boldsymbol{\delta}_{\mathbf{h}_u} \in \mathcal{S}_{\mathbf{h}_u} \tag{37d}$$

$$\sigma_e^2 + \sum_{1\leq j\leq M} |\mathbf{g}_e\mathbf{w}_j|^2 \leq v_{u,e}\beta_{u,e},\ \forall u, e\ \forall \boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e} \tag{37e}$$

$$\Re(\mathbf{g}_e\mathbf{w}_j) \geq f^{(n)}(\Gamma_{e,j}),\ \forall e, j = 1, \ldots, M \quad \forall \boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e} \tag{37f}$$

$$\text{constraints in (18b), (18d), (18h) and (18j).} \tag{37g}$$

where $\mathrm{TA}(g)$ is the first order Taylor approximation of function g at an appropriate point, and

$$f^{(n)}(\Gamma_{e,j}) \triangleq \sqrt{\Gamma^{(n)}_{e,j}} + \frac{1}{2\sqrt{\Gamma^{(n)}_{e,j}}}(\Gamma_{e,j} - \Gamma^{(n)}_{e,j}) \tag{38}$$

$$\mathcal{V}_a = \{\mathbf{W}, t_{u,e}, v_{u,e}, \alpha_u, \beta_{u,e}, z, \mathbf{v}, \chi_{u,e}, \Gamma_{e,j}\} \tag{39}$$

$$\mathbf{h}_u = \bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u}, \quad \forall u \tag{40}$$

$$\mathbf{g}_e = \bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e}, \quad \forall e. \tag{41}$$

1) Robust Transformation of (37b) and (37f): With the above description of the robust counterpart of **Problem a**, we first tackle the constraints in (37b) and (37f). For all e, u, j, it is immediate to note that both these sets of constraints are, respectively, equivalent to the following

$$\min_{\boldsymbol{\delta}_{\mathbf{h}_u}\in\mathcal{S}_{\mathbf{h}_u}} \Re(\mathbf{h}_u\mathbf{w}_u) \geq \chi_{u,e},\ \min_{\boldsymbol{\delta}_{\mathbf{g}_e}\in\mathcal{S}_{\mathbf{g}_e}} \Re(\mathbf{g}_e\mathbf{w}_j) \geq f^{(n)}(\Gamma_{e,j}). \tag{42}$$

Recall the fundamental result from basic convex analysis which states that for a vector $\mathbf{v}$ in a space equipped with the norm $\|\mathbf{v}\|$, its dual norm over a space of linear functionals $\mathbf{d}$ is defined as

$$\|\mathbf{d}\|_* \triangleq \max_{\|\mathbf{v}\|_2\leq 1} \Re(\mathbf{d}^{\mathrm{H}}\mathbf{v}) = \max_{\|\mathbf{v}\|_2\leq 1} |\mathbf{d}^{\mathrm{H}}\mathbf{v}|. \tag{43}$$

Further, the dual norm of the l_p norm[5] becomes [35]

$$\|\mathbf{d}\|_q \triangleq \left(\sum_i |[\mathbf{v}]_i|^q\right)^{\frac{1}{q}} \tag{44}$$

where $1/q = (p-1)/p$. The dual norms of l_∞, l_1 and l_2 norms are l_1, l_∞ and l_2 norms, respectively [35]. The minimization on the left side of the first inequality in (42), thus, can be treated as

$$\begin{aligned}\Re(\bar{\mathbf{h}}_u\mathbf{w}_u) &+ \min_{\boldsymbol{\delta}_{\mathbf{h}_u}:\|\boldsymbol{\delta}_{\mathbf{h}_u}\mathbf{E}_u^{1/2}\|_2\leq\rho_{\mathbf{h}_u}} \Re(\boldsymbol{\delta}_{\mathbf{h}_u}\mathbf{w}_u)\\ &= \Re(\bar{\mathbf{h}}_u\mathbf{w}_u) + \rho_{\mathbf{h}_u}\min_{\mathbf{u}:\|\mathbf{u}\|_2\leq 1} \Re(\mathbf{u}\mathbf{E}_u^{-1/2}\mathbf{w}_u)\\ &= \Re(\bar{\mathbf{h}}_u\mathbf{w}_u) - \rho_{\mathbf{h}_u}\|\mathbf{E}_u^{-1/2}\mathbf{w}_u\|_2 \end{aligned}\tag{45}$$

where we have used the fact that

$$\Re(\mathbf{u}\mathbf{E}_u^{-1/2}\mathbf{w}_u) \geq -|\mathbf{u}\mathbf{E}_u^{-1/2}\mathbf{w}_u| \geq -\|\mathbf{u}\|_2\|\mathbf{E}_u^{-1/2}\mathbf{w}_u\|_2 \tag{46}$$

and that equality in the relation $\Re(\mathbf{u}\mathbf{E}_u^{-1/2}\mathbf{w}_u) \geq -\|\mathbf{u}\|_2\|\mathbf{E}_u^{-1/2}\mathbf{w}_u\|_2$ under the constraint $\|\mathbf{u}\|_2 \leq 1$ is attained with $\mathbf{u} = -\mathbf{w}_u^{\mathrm{H}}\mathbf{E}_u^{-1/2}/\|\mathbf{E}_u^{-1/2}\mathbf{w}_u\|_2$. In a similar manner, the left side of the second inequality in (42) can be manipulated as

$$\begin{aligned}&\Re(\bar{\mathbf{g}}_e\mathbf{w}_j) + \min_{\boldsymbol{\delta}_{\mathbf{g}_e}:\|\boldsymbol{\delta}_{\mathbf{g}_e}\|_\infty\leq\rho_{\mathbf{g}_e}} \Re(\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{w}_j) =\\ &\Re(\bar{\mathbf{g}}_e\mathbf{w}_j) + \rho_{\mathbf{g}_e}\min_{\mathbf{v}:\|\mathbf{v}\|_\infty\leq 1} \Re(\mathbf{v}\mathbf{w}_j) = \Re(\bar{\mathbf{g}}_e\mathbf{w}_j) - \rho_{\mathbf{g}_e}\|\mathbf{w}_j\|_1\end{aligned}\tag{47}$$

where we have employed the fact that the dual norm of the l_∞ norm is the l_1 norm. Hence, with this move, tractable, convex and equivalent formulations for the constraints in (42) are obtained.

2) Robust Approximation of (37e): Next let us turn our attention to the uncertain constraints in (37e). For arbitrary u, e the constraint can be shaped to take the following form

$$\begin{cases}\sigma_e^2 + \sum\limits_{1\leq j\leq M} v'_{e,j} \leq v_{u,e}\beta_{u,e},\\ \max\limits_{\boldsymbol{\delta}_{\mathbf{g}_e}:\|\boldsymbol{\delta}_{\mathbf{g}_e}\|_\infty\leq\rho_{\mathbf{g}_e}} |(\bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e})\mathbf{w}_j|^2 \leq v'_{e,j}, \quad \forall j.\end{cases}\tag{48}$$

The first set of inequality constraints in (48), although not corrupted with errors, is still nonconvex. The approximation strategy to handle this set of constraints is similar to the one introduced earlier. To this end, note that for all j, the system

$$\sigma_e^2 + \bar{v}_e^2 \leq v_{u,e}\beta_{u,e}, \qquad \sum_{1\leq j\leq M} v'_{e,j} \leq \bar{v}_e^2 \tag{49}$$

equivalently represents the first set of constraints in (48). Clearly, the first of the constraints in (49) is SOC representable. To tackle the second inequality constraint, owing to its concavity, we can iteratively approximate the term $\bar{v}_e^2$ with its first order Taylor approximation such that the parameter update in the $n+1^{\mathrm{st}}$ run follows $\bar{v}_e^{(n+1)} = \bar{v}_e^{(n)}$, where $\bar{v}_e^{(n)}$ is the value of $\bar{v}_e$ in the n^{th} iteration.

The next step, for all j, is to note another equivalent formulation of the second inequality in (48) that involves the constrained error vector as follows

$$\begin{aligned}\max_{\boldsymbol{\delta}_{\mathbf{g}_e}:\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{B}_k\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}}\leq\rho_{\mathbf{g}_e}^2,k=1,\ldots,K} &\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}}\\ &+2\Re(\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}}) + \bar{\mathbf{g}}_e\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} \leq v'_{e,j}\end{aligned}\tag{50}$$

where $\mathbf{P}_j = \mathbf{w}_j\mathbf{w}_j^{\mathrm{H}}$, l_∞ norm of vector $\boldsymbol{\delta}_{\mathbf{g}_e}$ has been rewritten as a quadratic form where $\mathbf{B}_k$ are diagonal matrices with one nonzero entry (1 in our case) at the k^{th} position and K is equal to the dimension of $\boldsymbol{\delta}_{\mathbf{g}_e}$. Unfortunately, even in this form, the problem is still not tractable, as tools similar to those used while dealing with constraints in (37b) and (37f) cannot be applied. At this point, we have to resort to some carefully chosen approximation to deal with the inequality in (50). Here some of the seminal techniques presented in [31] are required. Following similar strategy, the constraint under consideration implies

$$\begin{aligned}&\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{B}_k\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}} \leq \rho_{\mathbf{g}_e}^2, k=1,\ldots,K \Rightarrow \boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}}\\ &\qquad +2\Re(\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}}) + \bar{\mathbf{g}}_e\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} \leq v'_{e,j} \qquad (51)\\ \Leftrightarrow &\{f_{e,j}^2 \leq 1, \boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{B}'_k\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}} \leq 1, k=1,\ldots,K\} \Rightarrow \boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}}\\ &\qquad +2f_{e,j}\Re(\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}}) + \bar{\mathbf{g}}_e\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} \leq v'_{e,j} \qquad (52)\end{aligned}$$

where $\mathbf{B}'_k = \mathbf{B}_k\rho_{\mathbf{g}_e}^{-2}$ and we remind the reader that K is the dimension of the error vector which in our case is T. For all e, k, j such that $\mu_{e,k,j} \geq 0$, the above can be relaxed to the following

$$\begin{aligned}\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}} + 2f_{e,j}\Re(\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}}) + \Bigg(&\bar{\mathbf{g}}_e\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} - v'_{e,j}\\ &+ \sum_{k=1}^K \mu_{e,k,j}\Bigg)f_{e,j}^2 - \sum_{k=1}^K \mu_{e,k,j}\boldsymbol{\delta}_{\mathbf{g}_e}\mathbf{B}'_k\boldsymbol{\delta}_{\mathbf{g}_e}^{\mathrm{H}} \leq 0.\end{aligned}\tag{53}$$

It is important to remark here that (53) is a safe approximation of the original statement in (52). The safety arises in a sense that the optimization variables satisfying (53) would also be feasible to (52) (or equivalently to (51)). In turn, (53) amounts to its equivalence with

$$\begin{pmatrix}\bar{\mathbf{g}}_e\mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} - v'_{e,j} + \sum\limits_{k=1}^K \mu_{e,k,j} & \bar{\mathbf{g}}_e\mathbf{P}_j^{\mathrm{H}}\\ \mathbf{P}_j\bar{\mathbf{g}}_e^{\mathrm{H}} & \mathbf{P}_j - \sum\limits_{k=1}^K \mu_{e,k,j}\mathbf{B}'_k\end{pmatrix} \preceq 0\tag{54}$$

which clearly corroborates with the definition of robust or safe approximation presented above. However, the matrix inequality is still not in a tractable form. To arrive at a tractable version, a straightforward application of Schur's complement lemma [31] produces the LMI

$$\begin{aligned}&\exists \mu_{e,j} \triangleq [\mu_{e,1,j},\ldots,\mu_{e,K,j}]^T \in \mathbb{R}_+^K\\ &: \begin{pmatrix}v'_{e,j} - \sum\limits_{k=1}^K \mu_{e,k,j} & & -\bar{\mathbf{g}}_e\mathbf{w}_j\\ & \sum\limits_{k=1}^K \mu_{e,k,j}\mathbf{B}'_k & \mathbf{w}_j\\ -\mathbf{w}_j^{\mathrm{H}}\bar{\mathbf{g}}_e^{\mathrm{H}} & \mathbf{w}_j^{\mathrm{H}} & 1\end{pmatrix} \succeq 0, \ \forall j.\end{aligned}\tag{55}$$

[5]The l_p norm of a vector $\mathbf{v}$ is defined as $\|\mathbf{v}\|_p = (\sum_i |[\mathbf{v}]_i|^p)^{1/p}$ where $p \geq 1$.

3) Robust Transformation of (37d): Finally, as a remaining constraint given in (37d), first rewrite it equivalently for all u in the form

$$\sigma_u^2 + \sum_{j\neq u} \alpha'_{u,j} \leq \alpha_u,$$
$$\max_{\boldsymbol{\delta}_{\mathbf{h}_u}:\|\boldsymbol{\delta}_{\mathbf{h}_u}\mathbf{E}_u^{1/2}\|_2\leq\rho_{\mathbf{h}_u}} |(\bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u})\mathbf{w}_j|^2 \leq \alpha'_{u,j}, \ \ \forall j. \quad (56)$$

We can use the similar procedure as above to note that the second inequality in (56) admits the following representation

$$\exists \nu_{u,j} \in \mathbb{R}_+ : \begin{pmatrix} \alpha'_{u,j} - \nu_{u,j} & & -\bar{\mathbf{h}}_u\mathbf{w}_j \\ & \nu_{u,j}\mathbf{E}'_u & \mathbf{w}_j \\ -\mathbf{w}_j^{\mathrm{H}}\bar{\mathbf{h}}_u^{\mathrm{H}} & \mathbf{w}_j^{\mathrm{H}} & 1 \end{pmatrix} \succeq 0, \ \ \forall j. \quad (57)$$

where $\mathbf{E}'_u = \mathbf{E}_u\rho_{\mathbf{h}_u}^{-2}$. It should be noted that, instead of being just a safe approximation, in this case, the above formulation is equivalent to the original constraint contaminated with uncertainties [31]. In fact, in addition to the representation in (57), the perturbed constraint represented by the second inequality in (56) can also be cast as a system of three SOC constraints. To this end, we recall similar manipulations as given in [36, Eq. 24] and note that for all j, the optimization problem in the second inequality of (56) admits the following equivalent representation

$$(|\bar{\mathbf{h}}_u\mathbf{w}_j| + \rho_{\mathbf{h}_u}\|\mathbf{E}_u^{-1/2}\mathbf{w}_j\|_2)^2 \leq \alpha'_{u,j} \quad (58)$$

which in turn yields the following system of SOC constraints

$$\begin{cases} \hat{\nu}_{u,j}^2 \leq \alpha'_{u,j} \\ |\bar{\mathbf{h}}_u\mathbf{w}_j| + \rho_{\mathbf{h}_u}\|\mathbf{E}_u^{-1/2}\mathbf{w}_j\|_2 \leq \hat{\nu}_{u,j} \end{cases}$$
$$\Leftrightarrow \begin{cases} \hat{\nu}_{u,j}^2 \leq \alpha'_{u,j} \\ \rho_{\mathbf{h}_u}\|\mathbf{E}_u^{-1/2}\mathbf{w}_j\|_2 \leq \hat{\nu}_{u,j} - \tilde{\nu}_{u,j} \\ |\bar{\mathbf{h}}_u\mathbf{w}_j| \leq \tilde{\nu}_{u,j} \end{cases} \quad (59)$$

where the first inequality in (59) is the well known hyperbolic constraint and the third inequality in (59) follows the SOC representation due to the fact that for a complex number κ, the constraint $|\kappa| \leq c$ is equivalent to $\sqrt{\Re(\kappa)^2 + \Im(\kappa)^2} \leq c$, which is an SOC constraint. It is interesting to note that the formulation in [36, Eq. 24] is valid for a limited range of the uncertainty parameter. However, no such restriction appears in our case as shown by the constraints in (59). Thus for an arbitrary j, instead of a single LMI constraint in (57), we are able to represent the same perturbed constraint in (56) with a system of three SOC constraints in (59).

With the above, the issue of channels being corrupted with unavoidable uncertainties as presented in the formulation given in (37) is dealt with. A tractable formulation of robust **Problem a** in the n^{th} step of successive convex approximation procedure, similar to the ones outlined above, is summarized in the following program (see (60) at the bottom of the page), where $\mathcal{V}'_a = \{\alpha'_{u,j}, \nu_{u,j}, \bar{v}_e, v'_{e,j}, \mu_{e,j}\}$, the LMI in (60e) can be replaced by the system in (59) for all j, and we stress the fact that the parameter update follows the same rule in the first order Taylor approximations of $\mathrm{TA}(\bar{v}_e^2)$ and $\mathrm{TA}(\chi_{u,e}^2)$. Before outlining a general iterative scheme that solves the problem with channel uncertainties, let us first also derive a tractable robust counterpart of **Problem b**.

B. **Problem b** *in Realistic Scenario*

Consider the following formulation of multicast secrecy rate maximization problem

$$\begin{aligned} \underset{\mathcal{V}_b}{\text{maximize}} \quad & z && (61a)\\ \text{subject to} \quad & [t_{u,e}^{\alpha_{u,e}}]^+ \geq z \quad \forall u,e && (61b)\\ & \omega_u \geq f^{(n)}(\zeta_{u,e}^a\zeta_{u,e}^b) - 1, \ \forall u,e && (61c)\\ & \omega_u - (\bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u})\mathbf{B}\mathbf{B}^{\mathrm{H}}(\bar{\mathbf{h}}_u + \boldsymbol{\delta}_{\mathbf{h}_u})^{\mathrm{H}} \leq 0, \\ & \forall u, \forall \boldsymbol{\delta}_{\mathbf{h}_u} \in \mathcal{S}_{\mathbf{h}_u} && (61d)\\ & (\bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e})\mathbf{B}\mathbf{B}^{\mathrm{H}}(\bar{\mathbf{g}}_e + \boldsymbol{\delta}_{\mathbf{g}_e})^{\mathrm{H}} \leq v_{u,e} - 1, \\ & \forall u,e, \forall \boldsymbol{\delta}_{\mathbf{g}_e} \in \mathcal{S}_{\mathbf{g}_e} && (61e)\\ & \text{constraints in (25d) and (25h)} && (61f) \end{aligned}$$

$$\begin{aligned} \underset{\mathcal{V}_a \cap \mathcal{V}'_a}{\text{maximize}} \quad & z && (60a)\\ \text{subject to} \quad & \Re(\bar{\mathbf{h}}_u\mathbf{w}_j) - \rho_{\mathbf{h}_u}\|\mathbf{E}_u^{-1/2}\mathbf{w}_j\|_2 \geq \chi_{u,e}, \quad \forall u,e,j = 1,\ldots,M && (60b)\\ & (\vartheta_{u,e}^a\vartheta_{u,e}^b\vartheta_u^c)^{\frac{1}{3}} \leq \mathrm{TA}(\chi_{u,e}^2) + \alpha_u, \quad \forall u,e && (60c)\\ & \sigma_u^2 + \sum_{j\neq u}\alpha'_{u,j} \leq \alpha_u, \quad \forall u && (60d)\\ & \exists \nu_{u,j} \in \mathbb{R}_+ : \begin{pmatrix} \alpha'_{u,j} - \nu_{u,j} & & -\bar{\mathbf{h}}_u\mathbf{w}_j \\ & \nu_{u,j}\mathbf{E}'_u & \mathbf{w}_j \\ -\mathbf{w}_j^{\mathrm{H}}\bar{\mathbf{h}}_u^{\mathrm{H}} & \mathbf{w}_j^{\mathrm{H}} & 1 \end{pmatrix} \succeq 0, \quad \forall j, u(u\neq j) && (60e)\\ & \sigma_e^2 + \bar{v}_e^2 \leq v_{u,e}\beta_{u,e}, \ \sum_{1\leq j\leq M} v'_{e,j} \leq \mathrm{TA}(\bar{v}_e^2), \quad \forall u,e && (60f)\\ & \exists \mu_{e,j} \in \mathbb{R}_+^K : \begin{pmatrix} v'_{e,j} - \sum_{k=1}^K \mu_{e,k,j} & & -\bar{\mathbf{g}}_e\mathbf{w}_j \\ & \sum_{k=1}^K \mu_{e,k,j}\mathbf{B}'_k & \mathbf{w}_j \\ -\mathbf{w}_j^{\mathrm{H}}\bar{\mathbf{g}}_e^{\mathrm{H}} & \mathbf{w}_j^{\mathrm{H}} & 1 \end{pmatrix} \succeq 0, \quad \forall e,j && (60g)\\ & \Re(\bar{\mathbf{g}}_e\mathbf{w}_j) - \rho_{\mathbf{g}_e}\|\mathbf{w}_j\|_1 \geq f^{(n)}(\Gamma_{e,j}), \quad \forall e,j = 1,\ldots,M && (60h)\\ & \text{constraints in (18b), (18d), (18h) and (18j).} && (60i) \end{aligned}$$

where $\mathcal{V}_b = \{\mathbf{B}, t_{u,e}, v_{u,e}, z, \omega_u, \zeta^a_{u,e}\zeta^b_{u,e}\}$ and $f^{(n)}(\zeta^a_{u,e}\zeta^b_{u,e})$ is given in (23). In the above formulation, a part from the set of constraints in (61d) and (61e) all other constraints do not depend upon channels of both the legitimate and eavesdropping nodes. Fortunately, both types of perturbed constraints in (61d) and (61e) can be tackled using a similar strategy as used to derive the formulation in (55). Invoking the same procedure, the constraints in (61e) can be safely approximated as:

$$\exists[\bar{\mu}^1_{u,e},\ldots,\bar{\mu}^K_{u,e}]^T \in \mathbb{R}^K_+ : \begin{pmatrix} (v_{u,e}-1)-\sum_{k=1}^{K}\bar{\mu}^k_{u,e} & & -\bar{\mathbf{g}}_e\mathbf{B} \\ & \sum_{k=1}^{K}\bar{\mu}^k_{u,e}\mathbf{B}'_k & \mathbf{B} \\ -\mathbf{B}^{\mathrm{H}}\bar{\mathbf{g}}^{\mathrm{H}}_e & \mathbf{B}^{\mathrm{H}} & \mathbf{I} \end{pmatrix} \succeq 0. \quad (62)$$

1) Robust Approximation of (61d): In a similar manner, following our previous manipulations, for all u, the type of uncertain constraint in (61d) can be safely approximated as

$$\begin{cases} \Re(\bar{\mathbf{h}}_u[\mathbf{B}]_k) - \rho_{\mathbf{h}_u}\|[\mathbf{B}]_k\|_2 \geq \bar{\nu}_{u,k}, \quad \forall u,k, \\ \mathrm{TA}\left(\sum_{1\leq k\leq T}\bar{\nu}^2_{u,k}\right) \geq \omega_u \end{cases} \quad (63)$$

where we recall that $\mathrm{TA}(\cdot)$ provides first order approximation of the function in its argument. After obtaining tractable formulations of (62) and (63), we are now in a position to present a tractable version of the uncertainty immune secure multicast problem. In particular, the tractable approximation of the robust counterpart of **Problem b**, in the n^{th} step of the iterative schemes discussed above, reads

$$\begin{aligned} \underset{\mathcal{V}_b\cap\mathcal{V}'_b}{\text{maximize}} \quad & z & (64a)\\ \text{subject to} \quad & [t^{\alpha_{u,e}}_{u,e}]^+ \geq z \quad \forall u,e & (64b)\\ & \omega_u \geq f^{(n)}(\zeta^a_{u,e}\zeta^b_{u,e}) - 1, \quad \forall u,e & (64c)\\ & \text{constraints in (25d), (62), (63) and (25h)} & (64d) \end{aligned}$$

where $\mathcal{V}'_b = \{\bar{\nu}_{u,1},\ldots,\bar{\nu}_{u,T},\bar{\mu}^1_{u,e},\ldots,\bar{\mu}^K_{u,e}\}$. Before concluding this subsection, it is pertinent to again mention that the formulations presented in (60) and (64) provide the optimization programs required in the n^{th} iterations of the algorithms that are, respectively, used to solve the secrecy rate maximization problems in the broadcast and the multicast modes with imperfect channel estimates. In particular, the parameters to be updated in the iterative algorithms for the two transmission approaches remain the same as in the case of genie aided perfect CSI feedback, and only the optimization problems formulations are changed to (60) and (64).

C. Note on Convergence

We present the convergence results in a unified way. To simplify affairs, let $\tilde{\mathcal{F}}_n$, $\tilde{f}_n$ and $\tilde{x}_n$ denote the feasible set, the *parameters* to be updated and the optimization variables in the n^{th} iteration of the proposed algorithm in any of the above four cases[6], respectively. Since the conditions stated in (13) are to be satisfied so that $g(\tilde{x}_n,\tilde{f}_{n+1}) = f(\tilde{x}_n)$,[7] it ensures that the decision variables $\tilde{x}_n \in (\tilde{\mathcal{F}}_n \cap \tilde{\mathcal{F}}_{n+1})$. From this inclusion relation, it follows that the optimal value in the $n+1^{\mathrm{st}}$ iteration of the program, $\mathsf{O}(\tilde{x}_{n+1})$, can be no worse than the value of the problem in the previous iteration $\mathsf{O}(\tilde{x}_n)$, i.e., mathematically $\mathsf{O}(\tilde{x}_n) \leq \mathsf{O}(\tilde{x}_{n+1})$. Further, since the optimization space is compact convex, the iterative procedure is guaranteed to converge. Based on these arguments, therefore, it is easy to conclude that both iterative algorithms proposed above are guaranteed to converge. This fact holds whether we deal with the genie aided case or the solution in realistic scenarios. In addition, following the arguments presented in Proposition 1, it can be shown that the proposed algorithm converges to a locally optimal point that satisfies the Karush-Kuhn-Tucker (KKT) conditions of the problem it approximates. Prior results based on a similar technique in [19] clearly indicate that the convergence point is of a good quality. Since the exact solution (or capacity in our case) is not known for the scenario considered in the paper, it does not appear computationally conducive to make such a comparison as provided in [19].

[6]Nominal (relying on genie feedback) data based and the robust versions of the broadcast and multicast secrecy problems.

[7]We follow the same notation for the function f and its convex upper bound g as introduced in (13).

VI. Numerical Results

In this section, for notational convenience, we use the symbolic notation (M,N,T) to represent a system consisting of M legitimate users, N eavesdroppers, and T transmit antennas. Throughout we assume that the transmit power is normalized with respect to noise variance. The channel estimate from the BS to legitimate user u is modeled as $\bar{\mathbf{h}}_u = \tilde{\mathbf{h}}_u\mathbf{R}^{1/2}_{\mathbf{h}_u}$ where $\tilde{\mathbf{h}}_u$ is a vector of i.i.d. complex Gaussian distribution with zero mean and unit variance, i.e., $[\tilde{\mathbf{h}}_u]_i \sim \mathcal{CN}(0,1)$ for $1\leq i\leq T$, and $\mathbf{R}_{\mathbf{h}_u}$ is a $T\times T$ transmit correlation matrix for user u. In our simulation setup, *exponential correlation model* [37] is used, i.e., the entries of the correlation matrix $[\mathbf{R}_{\mathbf{h}_u}]_{i,j} = r^{|i-j|}$, where the complex correlation coefficient of the neighboring transmit branches for the u^{th} user is $0\leq|r|\leq 1$. The channel estimates $\bar{\mathbf{g}}_e$ of eavesdroppers are generated similarly as $\bar{\mathbf{g}}_e = \tilde{\mathbf{g}}_e\mathbf{R}^{1/2}_{\mathbf{g}_e}$ with the correlation matrix following the same exponential model. The secrecy rates are averaged over several hundred realizations of the channels. All numerical results were generated using the parser YALMIP [38].

A. 'Genie' Aided Feedback

1) Average Secrecy Rate Versus Transmit Power: In the experiment reported in Fig. 2, we study the variation of the expected secrecy rates of the secure broadcast problem with transmit power. For the cases considered, identity transmit correlation matrices are used. Maximum achievable secrecy rate is obtained when the ratio M/T is minimum. It is also noteworthy that the gain in terms of the spectral efficiency tends to decrease as T increases for given M and N. In order to give some measure of the performance of proposed algorithm, we have superimposed simple upper bounds that correspond to the achievable rates of an ordinary broadcast channel. It is seen that the gap between the proposed algorithm and the broadcast rates appears acceptable, and it decreases as we increase T. Therefore, it gives a good indication of the fact that the proposed iterative strategy will yield results close to the optimal.

Fig. 3 plots average secrecy rate for the multicasting problem (**Problem b**) versus transmit power when $(M,N,T)=(4,3,8)$ and $(M,N,T)=(4,3,16)$. The rates achieved are compared with the ones predicated by [12, Theorem 1] and [12, Theorem

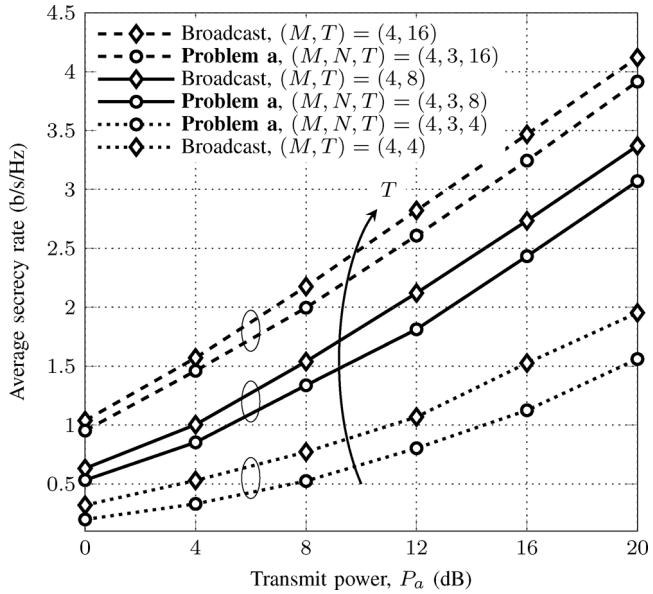


Fig. 2. Average secrecy rate for Problem a as a function of the transmit power P_a (dB).

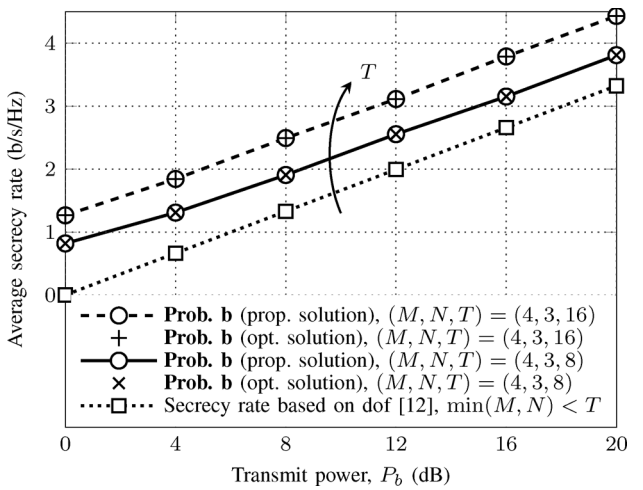


Fig. 3. Average secrecy rate for Problems b as a function of the transmit power P_b (dB) for two cases: $(M,N,T)=(4,3,8)$ and $(M,N,T)=(4,3,16)$. The curves show an increase in the achievable secrecy rate with the number of transmit antennas.

2] for $\min(M,N) < T$. The sub-optimality of the dof based achievable secrecy rates [12] is evident from the trend of the curves shown in this figure. We note that when $\min(M,N) \geq T$, [12, Theorem 1] computes the achievable dof via interference alignment technique for the special case of rationally independent channels, and hence, is not applicable to the scenarios we consider for our numerical investigations. In the same plot we have indicated that the proposed approach attains the global optimal solution as well. We discuss more on this aspect while describing the results of Fig. 5(a).

2) Average Secrecy Rate Versus Transmit Correlation: In Fig. 4, we study the secrecy rate for **Problems a and b** as function of the transmit correlation, r for two cases: $P_a = P_b = 8$dB and $P_a = P_b = 20$ dB. As noted above, the exponential correlation matrices are used to generate channel instances of the legitimate and eavesdropping nodes. The results show that the

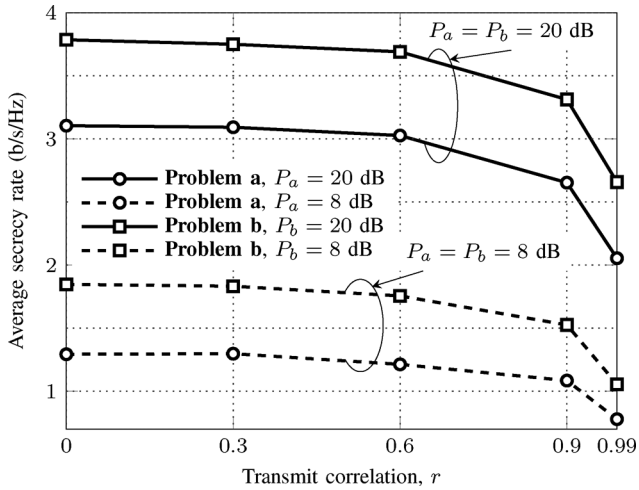


Fig. 4. Average secrecy rate for Problems a and b as a function of the transmit correlation r.

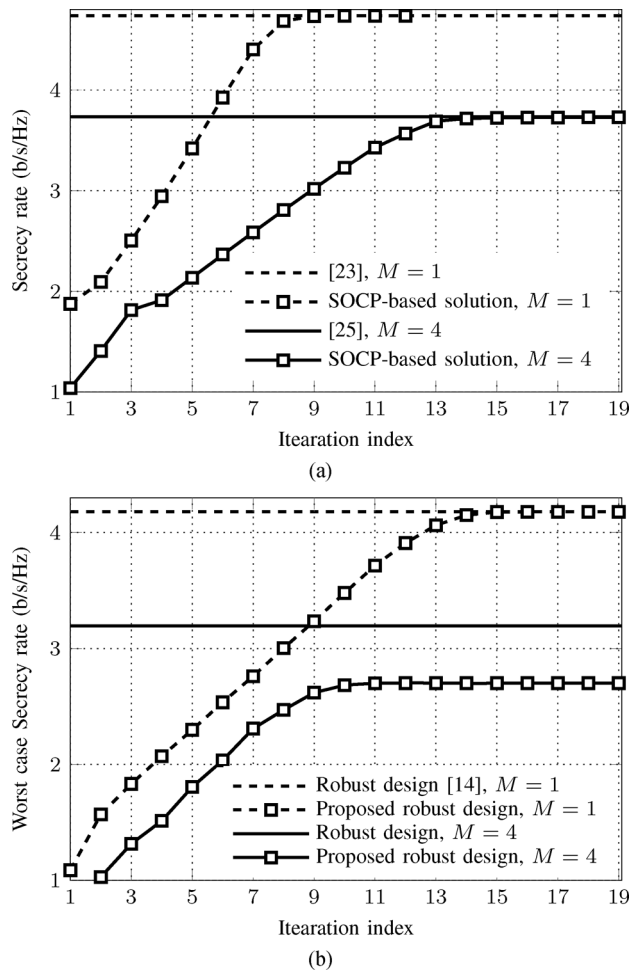


Fig. 5. Convergence behavior of algorithm for Problem b with genie-aided perfect and CSI and in realistic scenarios. We take $\alpha_{u,e} = 0.9$ for all u, e. (a) Convergence rate of the proposed solution for Problems b with $(M,N,T) = (4,3,8)$ and $(M,N,T) = (1,3,8)$ configurations. The total transmit power is set to $P_b = 10$ dB. (b) Convergence rate of the proposed robust solution for Problems b with the parameters taken From Fig. 5(a). The channel errors for eavesdropper e are assumed to be in a ball of radius ρ_e. The uncertainty parameters are taken as $\rho_u = \rho_e = 0.1$ for all u and e.

achievable secrecy rate of both **Problems a and b** decreases as the transmit correlation increases. As expected, this occurs

TABLE II
AVERAGE RUN TIME (IN SECONDS) VERSUS THE NUMBER OF TRANSMIT ANTENNAS, T. THE NUMBER OF EAVESDROPPERS IS SET TO $N = 3$. OTHER PARAMETERS ARE IDENTICAL TO THOSE FOR FIG. 5(A). THE SYMBOL $\times$ IN THE TABLE MEANS THAT WITH THE SETTINGS CONSIDERED, WE ARE NOT ABLE TO OBTAIN SOLUTION ON OUR WORKSTATIONS (FOR EXAMPLE, DUE TO NUMERICAL ISSUES THAT ARISE BECAUSE OF LARGE DIMENSIONS CONSIDERED)

	Antennas, T	8	16	32	64	128	256	512
$M = 1$	SDP [23], (SeDuMi)	0.18	0.54	0.87	3.21	15.24	92.88	489
	SOCP-based, (SeDuMi)	0.59	0.72	0.92	1.24	2.06	2.59	7.13
	SOCP-based, (ECOS)	0.01	0.02	0.035	0.062	0.12	0.31	0.68
$M = 4$	SDP [25], (SeDuMi)	0.09	0.13	0.35	1.35	7.06	39.48	$\times$
	SOCP-based, (SeDuMi)	0.08	1.01	1.21	2.26	6.24	20.92	77.24
	SOCP-based, (ECOS)	0.04	0.08	0.17	0.33	0.62	1.27	3.69

because a high value of r reduces the spatial diversity in the system. In addition, the gap between the curves for both problems is much bigger when higher normalized transmit power (20 dB) is used at the BS.

3) Convergence Results: To report our main findings we will concentrate on **Problems b**. We focus on two setups $(M, N, T) = (4, 3, 8)$ and $(M, N, T) = (1, 3, 8)$. Since the proposed algorithm is guaranteed to converge to a locally optimal solution of the problem,[8] it is interesting to evaluate the secrecy rate achieved and the number of iterations taken by the algorithm to stabilize. To do so, we compare our algorithm with the solution obtained by SDP based implementation presented in [23], [25]. Fig. 5(a) illustrates the convergence rate and the objective achieved by the proposed algorithm. For all u and e, the channels $\bar{\mathbf{h}}_u$ and $\bar{\mathbf{g}}_e$ are randomly generated with $\mathbf{R}_{\mathbf{h}_u} = \mathbf{I}$ and $\mathbf{R}_{\mathbf{g}_e} = \mathbf{I}$. The proposed algorithm converges to the same point as the one achieved by the SDP design in about 10 iterations for $M = 1$, and 15 runs for $M = 4$ legitimate users. **Problem a** showed very similar numerical convergence. The speed of convergence is sensitive to the initialization point. However, for the scenarios considered in the paper random initialization performed well. We stress that the SDP solution requires much more computational effort and has mostly been shown to serve the purpose of benchmark comparison. As reported next, we show that despite being iterative in nature, our SOCP based algorithm yields much less computational time.

To evaluate the numerical efficiency of our approach, we compare the computation time of the SOCP algorithm and the SDP based design derivable from [14], [23]. The results shown in Table II are obtained by solving the respective optimization programs with SeDuMi [39] as a solver in YALMIP on a 64-bit desktop that supports 8 Gbyte RAM and Intel CORE i7. Similarly for comparison we have also computed times with a more efficient SOCP solver ECOS (can be downloaded from https://github.com/ifa-ethz/ecos). It can be seen that for the settings shown, the computation times of the SOCP solutions are way less than those of the SDP based formulation. The solver tailor-made for SOCPs performs even better. This verifies our complexity predictions given in Section III-D. Indeed, such a large number of antennas, as shown in Table II, are being considered as a possibility for future generations of wireless systems [40].

[8]More on convergence related issues appears in Proposition 1 and Section V-C.

B. Numerical Investigations in More Realistic Scenarios

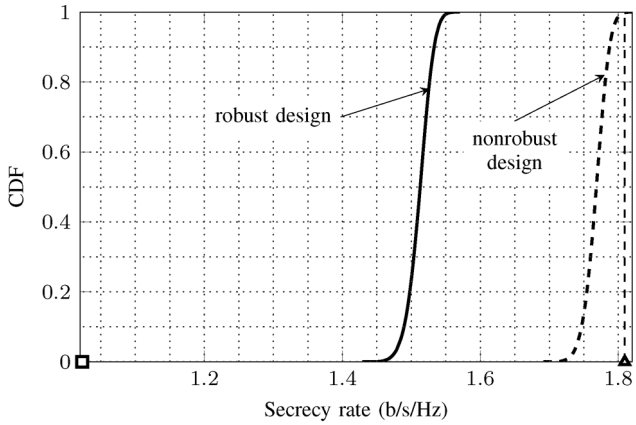
In the experiments to follow, we will without loss of generality assume that for all u, e the uncertainty parameters $\rho_{\mathbf{h}_u} = \rho_u$ and $\rho_{\mathbf{g}_e} = \rho_e$. We recall that the uncertainty set for the channel estimates of the eavesdroppers is modeled by a "box", while the error vectors affecting the channels of legitimate users are assumed to be present in a region defined by elliptic norm constraint. The solution for genie aided case is called "nonrobust" and that for corrupted channel estimates "robust". Before entering into detailed investigations of more realistic scenarios, let us briefly study companion figure of Fig. 5(a) shown in Fig. 5(b). We again note that thanks to the SDP formulation of [25] we can derive the exact robust counterpart of multicast secrecy problem for Euclidean norm uncertainty by a straightforward application of S-Lemma. It is seen in Fig. 5(b) that for $M = 1$ the proposed approach performs nearly optimally. However, for larger M the approximation used to obtain the robust version of the desired signal has a more pronounced impact. Hence, we see a slightly lower rate achieved compared to the optimal one.

1) A Comparative Study of Robust and Nonrobust Solutions: We generate cumulative distribution functions (CDFs) of the achievable rates in **Problems a** and **b** with uniformly distributed errors in the uncertainty regions of the legitimate users and the eavesdroppers parameterized by the values of ρ_u and ρ_e, respectively. As a benchmark we calculate the probability of exceeding the achieved secrecy rates, shown using square and triangle markers in CDF plots, by the robust (PE-R) and nonrobust (PE-NR) designs. The metrics PE-NR and PE-R (second and third columns of tables in Fig. 6(a) and (b)) are also evaluated when the errors follow the Gaussian law specified by its variance (the first column of both tables in Fig. 6). It is seen in both CDF plots that on account of a larger feasible set, the nonrobust linear precoders can promise a bigger secrecy rate. However, the probability of achieving that rate is very small in the nonrobust design, shown by the intersection point of vertical lines with the nonrobust CDFs. Further, in the tables provided in Fig. 6, PE-R and PE-NR show that as the variance of the Gaussian errors increases the exceedance probability tends to decrease for the robust design in both problems. However, the value of this probability is virtually zero with the nonrobust precoders.

2) Worst Case Secrecy Rate Versus ρ_e: For fixed ρ_u and a pair of BS powers, the average worst case secrecy rate achieved by **Problems a** and **b** is plotted against the parameter ρ_e, the dimension parameter of the box uncertainty set (see Fig. 7). As expected, the gap between the curves for the nonrobust and robust designs is considerably enhanced for larger ρ_e. A similar result was also observed in the case of **Problem b** (not shown here for reasons of space).

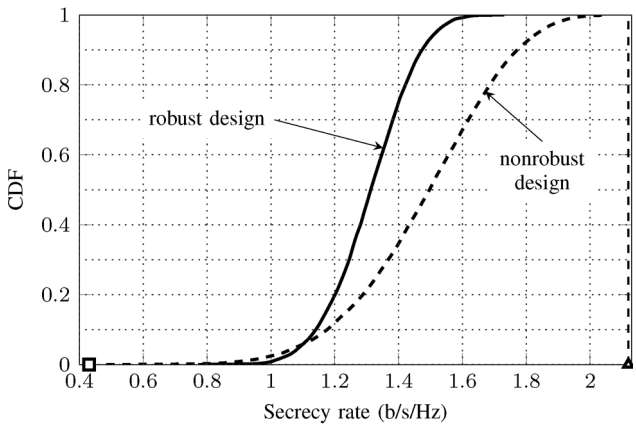
VII. CONCLUSION

In this paper, a system consisting of a linearly precoded multiantenna base station serving a set of legitimate users in the presence several wiretappers is studied. We explore beamforming for maximizing achievable rates when independent information is meant for legitimate users. Similarly, when a common message is to be multicast to a set of users in a cell, linear precoding with no rank constraints is investigated. For both sce-



Variance	PE-NR	PE-R
0.01	3×10^{-5}	1
0.02	0	0.99
0.04	0	0.72
0.06	0	0.37

(a)



Variance	PE-NR	PE-R
0.05	1.4×10^{-4}	0.99
0.1	9×10^{-5}	0.96
0.15	3×10^{-5}	0.79
0.2	2×10^{-5}	0.59

(b)

Fig. 6. CDF of the secrecy rate for Problems a and b for the system $(M, N, T) = (4, 3, 8)$. The transmit power is $P_a = P_b = 12$ dB, and $\mathbf{E}_u = \mathbf{I}$ for both a and b. Square and triangle markers show the secrecy rate of robust and nonrobust problems, respectively. (a) CDF of the secrecy rate for Problem a with $\rho_u = 0.1, \rho_e = 0.05$. (b) CDF of the secrecy rate for Problem b with $\rho_u = \rho_e = 0.3$.

narios, provably convergent iterative SOCP algorithms are derived. Subsequently, we leverage our analysis to the situation when the wiretappers are concealed and their channel information has be to indirectly estimated in an erroneous manner. To tackle this issue, we deal with semi-infinite instances of the broadcast and multicast secrecy rate maximization problems. We approximate both categories of the problems with tractable and safe optimization programs. Results reveal that the proposed algorithmic procedures are not only efficient complexity wise (for a certain range of parameters the proposed procedure is found at least 10 times quicker than the SDP based solution) but also provide much superior spectral efficiency compared to the known solutions.

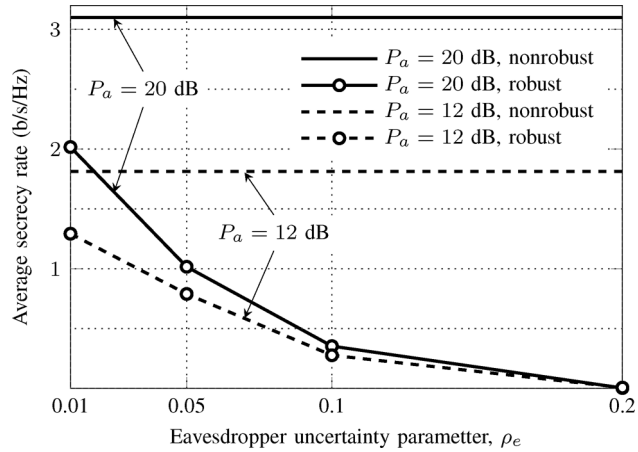


Fig. 7. Average worst case secrecy rate for Problem a as a function of the uncertainty parameter, ρ_e for the system $(M, N, T) = (4, 3, 8)$. ρ_u is taken as 0.1, and $\mathbf{E}_u = \mathbf{I}$ for all u.

ACKNOWLEDGMENT

The authors are grateful to Prof. Sennur Ulukus of the University of Maryland for her helpful comments.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 2466–2470.
[4] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[6] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[7] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[9] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.
[10] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw., Special Issue on Wireless Physical Layer Security*, vol. 142374, 2009.
[11] E. Ekrem and S. Ulukus, "On Gaussian MIMO compound wiretap channels," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2010, pp. 1–6.
[12] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.
[13] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[14] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.
[15] L. P. Qian, Y. J. A. Zhang, and J. Huang, "MAPEL: Achieving global optimality for a non-convex wireless power control problem," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1553–1563, Mar. 2009.
[16] M. Chiang, C. W. Tan, D. Palomar, D. O'Neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.
[17] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[18] M. Schubert and H. Boche, "Solution of the multiuser downlink beamforming problem with individual SINR constraints," *IEEE Trans. Veh. Technol.*, vol. 53, no. 1, pp. 18–28, Jan. 2004.

[19] L.-N. Tran, M. F. Hanif, A. Tölli, and M. Juntti, "Fast converging algorithm for weighted sum rate maximization in multicell MISO downlink," *IEEE Signal Process. Lett.*, vol. 19, no. 12, pp. 872–875, Dec. 2012.
[20] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.
[21] A. Beck, A. B. Tal, and L. Tetruashvili, "A sequential parametric convex approximation method with applications to nonconvex truss topology design problems," *J. Global Opt.*, vol. 47, no. 1, pp. 29–51, 2010.
[22] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, 1978.
[23] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, Jun. 2010.
[24] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
[25] Q. Li and W.-K. Ma, "Multicast secrecy rate maximization for MISO channels with multiple multi-antenna eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2011, pp. 1–5.
[26] M. S. Lobo, L. Vandenberghe, S. Boyd, and H. Lebret, "Applications of second-order cone programming," *Linear Algebra Appl., Special Issue on Linear Algebra in Control, Signals and Image Processing*, pp. 193–228, Nov. 1998.
[27] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron. Lett.*, vol. 27, no. 23, pp. 2145–2146, Nov. 1991.
[28] R. J. Baxley, J. E. Kleider, and G. T. Zhou, "Pilot design for OFDM with null edge subcarriers," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 396–405, Jan. 2009.
[29] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.
[30] L. Karray, P. Duhamel, and O. Rioul, "Image coding with an L^∞ norm and confidence interval criteria," *IEEE Trans. Image Process.*, vol. 7, no. 5, pp. 621–631, May 1998.
[31] A. B. Tal, L. E. Ghaoui, and A. Nemirovski, *Robust Optimization*. Princeton, NJ, USA: Princeton Univ. Press, 2009.
[32] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4871–4881, Dec. 2009.
[33] A. Beck and Y. C. Eldar, "Strong duality in nonconvex quadratic optimization with two quadratic constraints," *SIAM J. Optim.*, vol. 17, no. 3, pp. 844–860, Oct. 2006.
[34] D. Bertsimas, D. B. Brown, and C. Caramanis, "Theory and applications of robust optimization," *SIAM Rev.*, vol. 53, no. 3, pp. 464–501, 2011.
[35] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U. K.: Cambridge Univ. Press, 2004.
[36] S. A. Vorobyov, A. B. Gershman, and Z.-Q. Luo, "Robust adaptive beamforming using worst-case performance optimization: A solution to the signal mismatch problem," *IEEE Trans. Signal Process.*, vol. 51, no. 2, pp. 313–324, Feb. 2003.
[37] P. J. Smith, P. Dmochowski, M. Chiani, and A. Giorgetti, "On the number of independent channels in a diversity system," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2010, pp. 1–6.
[38] J. Löfberg, "YALMIP : A toolbox for modeling and optimization in MATLAB," presented at the CACSD Conf., Taipei, Taiwan, 2004.
[39] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optim. Methods Softw.*, vol. 11–12, pp. 625–653, 1999.
[40] F. Rusek, D. Persson, B. K. Lau, E. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, Jan. 2013.

Muhammad Fainan Hanif received the Ph.D. degree in electrical and electronic engineering from the University of Canterbury, Christchurch, New Zealand, in 2011. Later, he was a postdoctoral researcher at the Centre for Wireless Communications, Department of Communications Engineering, University of Oulu, Finland. His research interests include convex optimization applications in signal processing and modern communication systems.

Le-Nam Tran (M'09) received the B.S. degree in Electrical Engineering from Ho Chi Minh National University of Technology, Vietnam, in 2003, and M.S. and Ph.D. in Radio Engineering from Kyung Hee University, Republic of Korea, in 2006 and 2009, respectively.

In 2009, he joined the Department of Electrical Engineering, Kyung Hee University, Republic of Korea, as a lecturer. From September 2010 to July 2011, he was a postdoc fellow at the Signal Processing Laboratory, ACCESS Linnaeus Centre, KTH Royal Institute of Technology, Sweden. Since August 2011, he has been with Centre for Wireless Communications and Department of Communications Engineering, University of Oulu, Finland. His current research interests include multiuser MIMO systems, energy efficient communications, and full duplex transmission. He received the Best Paper Award from IITA in August 2005.

Markku Juntti (S'93–M'98–SM'04) received his M.Sc. (Tech.) and Dr.Sc. (Tech.) degrees in Electrical Engineering from University of Oulu, Oulu, Finland in 1993 and 1997, respectively.

Dr. Juntti was with University of Oulu in 1992–1998. In academic year 1994–1995 he was a Visiting Scholar at Rice University, Houston, Texas. In 1999–2000 he was a Senior Specialist with Nokia Networks. Dr. Juntti has been a professor of communications engineering at University of Oulu, Department of Communication Engineering and Centre for Wireless Communications (CWC) since 2000. His research interests include signal processing for wireless networks as well as communication and information theory. He is an author or co-author in some 200 papers published in international journals and conference records as well as in book *WCDMA for UMTS* published by Wiley. Dr. Juntti is also an Adjunct Professor at Department of Electrical and Computer Engineering, Rice University, Houston, Texas, USA.

Dr. Juntti is an Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and was an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2002–2008. He was Secretary of IEEE Communication Society Finland Chapter in 1996–1997 and the Chairman for years 2000–2001. He has been Secretary of the Technical Program Committee (TPC) of the 2001 IEEE International Conference on Communications (ICC'01), and the Co-Chair of the Technical Program Committee of 2004 Nordic Radio Symposium and 2006 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2006). He is the General Chair of 2011 IEEE Communication Theory Workshop (CTW 2011).

Savo Glisic (M'90–SM'94) is a Professor of Telecommunications at University of Oulu, Finland, head of the networking research group, and Director of Globalcomm Institute for Telecommunications. He was Visiting Scientist at Cranfield Institute of Technology, Cranfield, U.K.(1976–1977) and University of California, San Diego (1986–1987). He has been active in the field wireless communications for 30 years and has published a number of papers and books. The latest books *Advanced Wireless Networks: 4G Cognitive Opportunistic and Cooperative Technology*, 2nd ed. (Wiley, 2009) and *Advanced Wireless Communications and Future Internet*, 3rd ed. (Wiley, 2011) cover the enabling technologies for the definition of 4G and incoming 5G systems. He is also running an extensive doctoral program in the field of wireless networking (www.telecomlab.oulu.fi/kurssit/networks/). His research interest is in the area of network optimization theory, network topology control and graph theory, cognitive networks and game theory, radio resource management, QoS and queuing theory, networks information theory, protocol design, advanced routing and network coding, relaying, cellular, WLAN, ad hoc, sensor, active and bio inspired networks with emphasis on genetic algorithms. Dr. Glisic has served as the Technical Program Chairman of the third IEEE ISSSTA'94, the eighth IEEE PIMRC'97, and IEEE ICC'01. He was Director of IEEE ComSoc MD programs.