BIOBJECTIVE TRANSMITTER OPTIMIZATION FOR SERVICE INTEGRATION IN MIMO GAUSSIAN BROADCAST CHANNEL

Weidong Mei, Weiqing Kong, Zhi Chen, and Jun Fang

National Key Laboratory of Science and Technology on Communications
University of Electronic Science and Technology of China, Chengdu 611731, China
Emails: mwduestc@gmail.com; kongweiqing@std.uestc.edu.cn; {chenzhi, JunFang}@uestc.edu.cn

ABSTRACT

This paper considers a two-receiver multiple-input multiple-output (MIMO) Gaussian broadcast channel model with integrated services. Specifically, two sorts of service messages are combined and served simultaneously: one multicast message intended for both receivers and one confidential message intended for only one receiver and kept perfectly secure from the other receiver. Our goal is to jointly design the transmit covariances of the multicast message and confidential message, such that the secrecy capacity region is maximized. This maximization problem is a biobjective optimization problem, but can be converted into a general scalar optimization problem via our proposed method of scalarization. Nonetheless, the equivalent scalar problem is nonconvex by nature. To circumvent the nonconvex issue, a provably convergent difference-of-concave (DC) approach is introduced to solve it in an iterative fashion. In view of the high computational complexity of the DC approach, a power splitting method is also devised for fast implementation of service integration. The security performance and computational efficiency of our proposed algorithms are finally demonstrated by numerical results.

Index Terms— Physical-layer service integration (PHY-SI), DC program, broadcast channel (BC), secrecy capacity region

I. INTRODUCTION

Recently, *physical-layer service integration* (PHY-SI), a technique of combining multicast message and confidential message at PHY for one-time transmission, has received much attention in wireless communications. In comparison with the conventional upper-layer-based approach, PHY-SI enables coexisting services to share the same resources by solely exploiting the physical characteristics of wireless channels, thereby significantly increasing the spectral efficiency (SE). This property makes PHY-SI a prominent approach to satisfy the ever-increasing need for radio spectrum.

There has been much information theory literature on PHY-SI hitherto. Csiszár and Körner's seminar work [1] established the fundamental limitation of PHY-SI in a discrete memoryless broadcast channel (DMBC). Other notable results include the extension to the case with multiple-input multiple-output (MIMO) [2], [3], and to the bidirectional relay networks [4]. These information-theoretic results has thus triggered recent research endeavors on PHY-SI from a signal processing point of view [5]–[8], which aimed to design specific transmit schemes to attain the Pareto boundary of the secrecy capacity regions. However, these works only focused on the multi-input single-output (MISO) channels. To the best of our knowledge, there is no existing papers directly tackling PHY-SI in MIMO channels from a signal processing point of view. We fill this gap in this work .

This work was supported in part by the National Natural Science Foundation of China under Grant 61631004 and 61571089.

Consider a two-user MIMO broadcast channel (BC) with two sorts of messages: a common (multicast) message intended for both receivers, and a confidential message intended for merely one authorized receiver. The confidential message must be kept perfectly secure from the unauthorized receiver. Our interest in this paper lies in the input covariance design of the transmitted messages, such that the secrecy capacity region is maximized. The resulting optimization problem turns out to be a *biobjective* maximization problem. To circumvent the difficulty in solving such problem, a method of scalarization is proposed to convert this problem into a provably equivalent scalar problem, identified as a secrecy rate maximization (SRM) problem with quality of multicast service (QoMS) constraints. This optimization problem is non-convex, but can be transformed into a form of the difference-of-concave (DC) functions. This problem structure motivates us to utilize the classical DC algorithm [9] to solve this problem in an iterative fashion. In each iteration, we approximate the non-convex constraints and objective function via the Taylor series expansion. In addition, a fast power splitting algorithm is put forward to facilitate the efficient implementation of PHY-SI.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider the downlink of a multiuser system in which a multi-antenna transmitter serves two receivers, and each receiver is equipped with multiple antennas. Assume that both receivers have ordered the multicast service and receiver 1 (authorized receiver) further ordered the confidential service.

The received signal at both receivers can be expressed as

$$\mathbf{y}_1 = \mathbf{H}_1\mathbf{x} + \mathbf{z}_1,\ \mathbf{y}_2 = \mathbf{H}_2\mathbf{x} + \mathbf{z}_2, \tag{1}$$

respectively, where $\mathbf{H}_1 \in \mathbb{C}^{N_b \times N_t}$ (resp. $\mathbf{H}_2 \in \mathbb{C}^{N_e \times N_t}$) is the channel matrix from the transmitter to receiver 1 (resp. receiver 2), and N_t, N_b and N_e are the number of transmit antennas employed by the transmitter, receiver 1 and receiver 2, respectively. We assume that $N_t > N_e$, for which the reason will become clear in the proof of Theorem 1. $\mathbf{z}_1$ and $\mathbf{z}_2$ are the additive white Gaussian noise (AWGN) with zero mean and unit variance at receiver 1 and receiver 2, respectively. $\mathbf{x} \in \mathbb{C}^{N_t}$ is the coded information, which consists of two independent components, i.e.,

$$\mathbf{x} = \mathbf{x}_0 + \mathbf{x}_c, \tag{2}$$

where $\mathbf{x}_0$ is the multicast message intended for both receivers, $\mathbf{x}_c$ is the confidential message intended merely for receiver 1. We assume $\mathbf{x}_0 \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_0)$, $\mathbf{x}_c \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_c)$ [2], where $\mathbf{Q}_0$ and $\mathbf{Q}_c$ are the transmit covariance matrices.

Denote R_0 and R_c as the achievable multicast rate and achievable secrecy rate, respectively. Then the secrecy capacity region

$C_s(\mathbf{H}_1, \mathbf{H}_2, P)$ is given as the set of nonnegative rate pairs (R_0, R_c) satisfying[1] [2]

$$R_0 \le \min_{i=1,2} \log \left| \mathbf{I} + \left(\mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H \right)^{-1} \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right|, \quad (3a)$$

$$R_c \le \log \left| \mathbf{I} + \mathbf{H}_1 \mathbf{Q}_c \mathbf{H}_1^H \right| - \log \left| \mathbf{I} + \mathbf{H}_2 \mathbf{Q}_c \mathbf{H}_2^H \right|, \quad (3b)$$

and $\mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_c) \le P$ with P being total transmit power budget at the transmitter.

With perfect channel state information (CSI) available at the transmitter[2], to find capacity-achieving $\mathbf{Q}_0$ and $\mathbf{Q}_c$, we must first solve the following secrecy capacity region maximization (SCRM) problem, which is a biobjective maximization problem with cone $K = K^* = \mathbb{R}_+^2$:

$$\max_{\mathbf{Q}_0, \mathbf{Q}_c, R_0, R_c} \left(\text{w.r.t. } \mathbb{R}_+^2 \right) \ (R_0, R_c)$$

$$\text{s.t. } \min_{i=1,2} \log \left| \mathbf{I} + \left(\mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H \right)^{-1} \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right| \ge R_0, \quad (4a)$$

$$\log \left| \mathbf{I} + \mathbf{H}_1 \mathbf{Q}_c \mathbf{H}_1^H \right| - \log \left| \mathbf{I} + \mathbf{H}_2 \mathbf{Q}_c \mathbf{H}_2^H \right| \ge R_c, \quad (4b)$$

$$\mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_c) \le P, \quad (4c)$$

$$\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \quad (4d)$$

III. A TRACTABLE APPROACH TO THE SCRM PROBLEM

A standard technique for dealing with biobjective optimization problems is the convex combination of the optimized objectives. However, since problem (4) is a nonconvex biobjective optimization problem, this method might not yield all Pareto optimal points [10]. In view of the limitation of this technique, we next propose an alternative method of scalarization to find all Pareto optimal points of (4).

III-A. An Equivalent Scalarization of (4)

In particular, our strategy is to transform problem (4) into a scalar optimization problem by fixing the variable R_0 as a constant $\tau_{ms} \ge 0$. As a result, the maximization of the vector (R_0, R_c) will be degraded into the maximization of a scalar R_c, which is shown in (5). As it will be proved in Theorem 1, all Pareto optimal solutions of (4) can be found by varying the parameter τ_{ms}.

$$R(\tau_{ms}) = \max_{\mathbf{Q}_0, \mathbf{Q}_c} \log \left| \mathbf{I} + \mathbf{H}_1 \mathbf{Q}_c \mathbf{H}_1^H \right| - \log \left| \mathbf{I} + \mathbf{H}_2 \mathbf{Q}_c \mathbf{H}_2^H \right|$$

$$\text{s.t. } \min_{i=1,2} \log \left| \mathbf{I} + \left(\mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H \right)^{-1} \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right| \ge \tau_{ms}, \quad (5a)$$

$$\mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_c) \le P, \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}. \quad (5b)$$

In (5), the variable R_c is discarded since it can be regarded as a slack variable. $R(\tau_{ms})$ is the optimal objective value of (5), and τ_{ms} can be interpreted as predetermined requirement of the achievable multicast rate. Specially, when we set $\tau_{ms} = 0$, problem (4) becomes a conventional SRM problem in MIMO wiretap channel. On the contrary, the confidential message transmission is terminated when τ_{ms} exceeds a threshold $\tau_{\max}$ given by

$$\tau_{\max} = \max_{\mathbf{Q}_0 \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{Q}_0) \le P} \min_{i=1,2} \log \left| \mathbf{I} + \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right|. \quad (6)$$

[1]In this paper, we only focus on the case where a positive secrecy rate can always be achieved. Otherwise, it is trivial to investigate the secrecy capacity region, since the region would be degraded into a line segment on the axis of multicast rate.

[2]This assumption of perfect CSI is valid in the context of PHY-SI, since all nodes are active in the network for ordering the multicast service so that their channels can be monitored.

The value of $\tau_{\max}$ can be numerically obtained by solving (6) via the convex optimization solver `CVX` [11].

Currently, the crucial problem lies in whether problem (5) enables us to acquire all Pareto optimal solutions of problem (4). Remarkably, we prove that the answer is yes in the following theorem.

Theorem 1: The rate pair $(\tau_{ms}, R(\tau_{ms}))$ is a Pareto optimal point of (4), and all Pareto optimal points of (4) can be obtained by solving (5) with different τ_{ms}'s lying within the interval $[0, \tau_{\max}]$.

Proof: The proof can be found in Appendix. ■

Remark 1: Theorem 1 bridges the Pareto optimal points of (4) to the boundary points of $C_s(\mathbf{H}_1, \mathbf{H}_2, P)$. When there is no ambiguity, the terms "boundary points" and "Pareto optimal points" will be used interchangeably in the following sections of this paper.

III-B. A DC Approach to the SRM Problem (5)

Problem (5) still remains nonconvex due to its objective function and constraint (5a). Nonetheless, one can notice that the objective function of (5) and constraint (5a) are both in a difference-of-concave form. This property makes problem (4) fall into the context of DC program [9].

In this subsection, our endeavor is to show the DC approach to (5) mathematically. The classical DC programming algorithms have been extensively applied to deal with the nonconvex optimization problems in many research activities, especially those arising in MIMO systems [12]–[14]. Its basic idea is to locally linearize the nonconcave parts in (5) at some feasible point via Taylor series expansion (TSE), and then iteratively solve the linearized problem. To start with, we introduce the TSE via the following lemma.

Lemma 1 ([13]): An affine Taylor series approximation of a function $f(\mathbf{X}) : \mathbb{R}^{M \times N} \to \mathbb{R}$ can be expressed at $\tilde{\mathbf{X}}$ as below.

$$f(\mathbf{X}) = f(\tilde{\mathbf{X}}) + \mathrm{vec}\left(f'(\mathbf{X}) \right)^H \mathrm{vec}(\mathbf{X} - \tilde{\mathbf{X}}). \quad (7)$$

The TSE above enables us to reformulate the primal nonconcave parts of (5) into a linear form. In particular, by applying Lemma 1 and the fact $\partial(\log|\mathbf{X}|) = \mathrm{Tr}\left(\mathbf{X}^{-1} \partial \mathbf{X}\right)$, the second term in the objective function of (5) can be approximated as ($\log(\cdot)$ is natural logarithm.)

$$\begin{aligned}
&\log \left| \mathbf{I} + \mathbf{H}_2 \mathbf{Q}_c \mathbf{H}_2^H \right| \\
&\approx \log \left| \mathbf{I} + \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right| \\
&\quad + \mathrm{vec} \left[\mathbf{H}_2^H \left(\mathbf{I} + \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right)^{-1} \mathbf{H}_2 \right]^H \mathrm{vec} \left(\mathbf{Q}_c - \tilde{\mathbf{Q}}_c \right) \\
&= \log \left| \mathbf{I} + \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right| + \mathrm{Tr} \left[\left(\mathbf{I} + \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right)^{-1} \mathbf{H}_2 \mathbf{Q}_c \mathbf{H}_2^H \right] \\
&\quad - \mathrm{Tr} \left[\left(\mathbf{I} + \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right)^{-1} \mathbf{H}_2 \tilde{\mathbf{Q}}_c \mathbf{H}_2^H \right], \quad (8)
\end{aligned}$$

where $\tilde{\mathbf{Q}}_c$ is a given transmit covariance matrix, and the last equality is due to the fact that $\mathrm{Tr}(\mathbf{A}^H \mathbf{B}) = (\mathrm{vec}(\mathbf{A}))^H \mathrm{vec}(\mathbf{B})$ for appropriate dimensions of $\mathbf{A}$ and $\mathbf{B}$. Likewise, the left hand side (LHS) of constraint (5a) can be approximated as

$$\begin{aligned}
&\log \left| \mathbf{I} + \left(\mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H \right)^{-1} \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right| \\
&= \log \left| \mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H + \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right| - \log \left| \mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H \right| \\
&\approx \log \left| \mathbf{I} + \mathbf{H}_i \mathbf{Q}_c \mathbf{H}_i^H + \mathbf{H}_i \mathbf{Q}_0 \mathbf{H}_i^H \right| - \log \left| \mathbf{I} + \mathbf{H}_i \tilde{\mathbf{Q}}_c \mathbf{H}_i^H \right| \\
&\quad - \mathrm{Tr} \left[\left(\mathbf{I} + \mathbf{H}_i \tilde{\mathbf{Q}}_c \mathbf{H}_i^H \right)^{-1} \mathbf{H}_i (\mathbf{Q}_c - \tilde{\mathbf{Q}}_c) \mathbf{H}_i^H \right]. \quad (9)
\end{aligned}$$

Based on the approximations above, the original QoMS-constrained SRM problem (5) can be reformulated as

$$\bar{R}(\tau_{ms}) = \max_{\mathbf{Q}_0,\mathbf{Q}_c} \log\left|\mathbf{I}+\mathbf{H}_1\mathbf{Q}_c\mathbf{H}_1^H\right| - \log\left|\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H\right| - \mathrm{Tr}\left[\left(\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H\right)^{-1}\mathbf{H}_2(\mathbf{Q}_c-\tilde{\mathbf{Q}}_c)\mathbf{H}_2^H\right]$$

$$\text{s.t.} \quad \log\left|\mathbf{I}+\mathbf{H}_i\mathbf{Q}_c\mathbf{H}_i^H+\mathbf{H}_i\mathbf{Q}_0\mathbf{H}_i^H\right| - \log\left|\mathbf{I}+\mathbf{H}_i\tilde{\mathbf{Q}}_c\mathbf{H}_i^H\right| - \mathrm{Tr}\left[\left(\mathbf{I}+\mathbf{H}_i\tilde{\mathbf{Q}}_c\mathbf{H}_i^H\right)^{-1}\mathbf{H}_i(\mathbf{Q}_c-\tilde{\mathbf{Q}}_c)\mathbf{H}_i^H\right] \geq \tau_{ms},\ i=1,2 \tag{10a}$$

$$\mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_c) \leq P, \mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}, \tag{10b}$$

where $\bar{R}(\tau_{ms})$ is the optimal objective value of (10), serving as an approximation to $R(\tau_{ms})$.

This approximated problem (10) is convex with regard to (w.r.t.) $(\mathbf{Q}_c, \mathbf{Q}_0)$ and hence $(\mathbf{Q}_c, \mathbf{Q}_0)$ can be iteratively obtained by solving problem (10). We summarize our proposed iterative algorithm for solving (5) in Algorithm 1.

Algorithm 1 Iterative method for solving (5)

1: Initiate $n = 0$ and choose an arbitrary starting point $\tilde{\mathbf{Q}}_{c,n}$ feasible to (10)
2: **Repeat**
3: Solve (10) with $\tilde{\mathbf{Q}}_c = \tilde{\mathbf{Q}}_{c,n}$ and obtain $\mathbf{Q}_c^*$, which is the optimal solution of (10);
4: Update $\tilde{\mathbf{Q}}_{c,n+1} = \mathbf{Q}_c^*$;
5: Update $n = n+1$;
6: **Until the convergence conditions are satisfied.**

In line 3 of Algorithm 1, the convex subproblem (10) can be efficiently solved by CVX. Moreover, by directly applying the DC convergence result [9, Th 10], we immediately have the following conclusion.

Theorem 2: Every limit point of $(\mathbf{Q}_0^*, \mathbf{Q}_c^*)$ is a stationary (Karush-Kuhn-Tucker (KKT)) point of problem (5).

IV. A FAST IMPLEMENTATION FOR PHY-SI

As one may note that each DC iteration in (10) involves solving a convex optimization problem to KKT optimality of (5), which could be time consuming in practice. To mitigate the computational load, we consider a fast and efficient implementation for PHY-SI in this section, rather than seeking a KKT optimal one.

The drawback of solving (5) comes mainly from the coupling of confidential message and multicast message, which renders problem (5) nonconvex. To make (5) easier to handle, it is a natural idea to seek some way to decouple these two sorts of messages in the optimization if possible. To this end, our strategy is to separately maximize the secrecy rate and multicast rate by introducing a power splitting factor α, such that $\mathrm{Tr}(\mathbf{Q}_c) = \alpha P$ and $\mathrm{Tr}(\mathbf{Q}_0) = (1-\alpha)P$. Then we specify a secrecy rate $R_c(\alpha)$ using the power allocated to the confidential message, and find the maximum multicast rate $R_0(\alpha)$ the remaining transmit power can achieve.

Specifically, $R_c(\alpha)$ is chosen as the maximum secrecy rate with $\mathrm{Tr}(\mathbf{Q}_c) = \alpha P$, i.e.,

$$R_c(\alpha) = \max_{\mathbf{Q}_c \succeq \mathbf{0}, \mathrm{Tr}(\mathbf{Q}_c) \leq \alpha P} \log \frac{\left|\mathbf{I}+\mathbf{H}_1\mathbf{Q}_c\mathbf{H}_1^H\right|}{\left|\mathbf{I}+\mathbf{H}_2\mathbf{Q}_c\mathbf{H}_2^H\right|}. \tag{11}$$

Problem (11) is a standard SRM problem in MIMO systems; different methods have been proposed to find the stationary points or near-optimal solutions to this problem, such as the GSVD method [15], the alternating optimization (AO) method [16] and the TSE method [12]. Among the existing methods, we choose the GSVD method to solve (11) due to its efficient implementation and approximate optimality in the high SNR regime [17]. The optimal $\mathbf{Q}_c$ generated from GSVD, denoted by $\mathbf{Q}_c(\alpha)$, could be obtained by following the procedures in [15].

With $\mathbf{Q}_c(\alpha)$ returned by solving (11), next we will determine the maximum multicast rate with $\mathrm{Tr}(\mathbf{Q}_0) = (1-\alpha)P$, which can be obtained by solving the following optimization problem,

$$R_0(\alpha) = \max_{\substack{\mathrm{Tr}(\mathbf{Q}_0) \leq (1-\alpha)P,\ \\ \mathbf{Q}_0 \succeq \mathbf{0}}} \min_{k\in\{1,2\}} \log\left|\mathbf{I}+\mathbf{A}(\mathbf{Q}_0)\right|. \tag{12}$$

in which $\mathbf{A}(\mathbf{Q}_0) = \left(\mathbf{I}+\mathbf{H}_i\mathbf{Q}_c(\alpha)\mathbf{H}_i^H\right)^{-1}\mathbf{H}_i\mathbf{Q}_0\mathbf{H}_i^H$. Clearly, problem (12) is a convex optimization problem after recasting it as an epigraph form. Thus, the optimal solution of problem (12), $\mathbf{Q}_0(\alpha)$, can be obtained by CVX. Finally, traversing all α lying within the interval $[0, 1]$ will give rise to the secrecy rate region achieved by this power spliting scheme.

V. NUMERICAL RESULTS

In this section, we provide numerical results to illustrate the secrecy rate region derived from our proposed DC approach. We compare our results with the traditional service integration strategies, which assign the confidential message and multicast message to two different logic channels, for instance, two orthogonal time slots. For the fairness of comparison, the secrecy rate and multicast rate achieved by the time division multiple address (TDMA)-based method should be **halved** [4].

In the simulation, unless specified, we assume $N_t = 5$, $N_r = 4$, $N_e = 4$, $P = 11.8$ dB. As [2] did, we investigate the secrecy rate regions achieved by deterministic channels. All channels are generated from i.i.d. complex Gaussian distribution with zero mean and unit variance.

First, we evaluate the convergence of our proposed DC algorithm. Especially, we are concerned about whether the primal QoMS constraint (5a) is violated by our approximation. Setting τ_{ms} as 2 bps/Hz, Fig. 1 shows the convergence of the multicast rate in the iteration with two different initializations. As seen, the multicast rates ultimately converge to our predefined multicast rate with a limited number of iterations in both initialization. This observation indicates the efficacy of TSE in approximating the multicast rate. Then we also plot the achieved secrecy rates and the approximated secrecy rates in Fig. 2. The result shows that they are coincident at the convergence of our proposed algorithm.

Fig. 3 plots the secrecy rate regions achieved by our proposed DC and power splitting approaches. Meanwhile, we plot the TDMA secrecy rate region as a benchmark. As expected, our proposed methods achieves significantly larger secrecy rate regions compared with the TDMA-based one, which implies the inherent advantage of PHY-SI over traditional service integration. Additionally, one can observe that there is small rate performance loss between the power splitting approach and the DC approach, especially at low QoMS region. This observation indicates that the power splitting method may serve as a good approximation to the KKT optimal transmit solution, with significant computational time saving.

To verify the computational complexity saving, we tabulated the averaged running times of the two proposed methods in getting one boundary point in Table I. One can see that the power splitting method is much faster than the TSE-based one, especially for large powers. In particular, the running time of the power splitting method keeps almost invariant to the increase of power, whereas

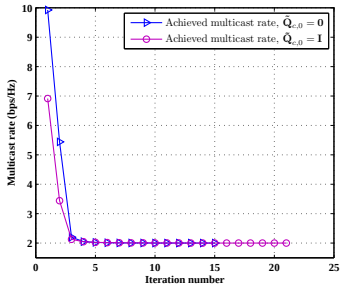

Fig. 1. Convergence of the multicast rate

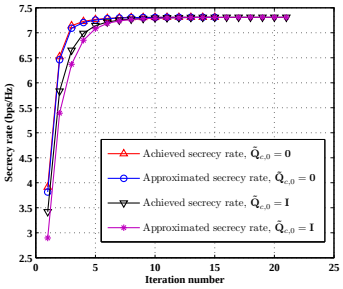

Fig. 2. Convergence of the secrecy rate

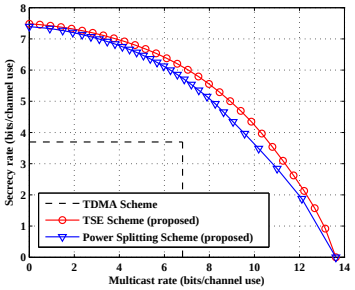

Fig. 3. Secrecy rate regions

Table I. Averaged running times (in secs.)

Method	Power (dB) 4	8	12	16	20
Power splitting	0.65	0.65	0.58	0.64	0.7
TSE	6.05	8.16	10.77	16.12	25.2

that of the TSE-based method scales nearly exponentially with the power.

VI. CONCLUSION

In this paper, we consider the transmit design for two-user MIMO broadcast channel with integrated confidential service and multicast service. The transmit covariances of the confidential message and multicast message are designed to maximize the secrecy capacity region. Since the SCRM problem is a biobjective optimization problem, a method of scalarization is proposed to convert it into a standard scalar optimization problem, which can be iteratively solved by DC algorithm. Next, we put forward a heuristic power splitting scheme to facilitate the fast implementation of PHY-SI. Numerical results show that, our proposed methods significantly outperform the traditional TDMA-based one, and that there is only a small performance gap between the power splitting method and the TSE-based one.

VII. APPENDIX

First, we claim that problem (5) has some interesting properties shown as below.

Property 1: The maximum objective value of problem (5), $R(\tau_{ms})$, is obtained only when the equality in (5a) holds.

Property 2: The optimal objective value of (5), denoted as $R(\tau_{ms})$, is monotonically decreasing w.r.t. τ_{ms}.

VII-A. Proof of Property 1

The proof of Property 1 can be accomplished by contradiction. Assume that the maximum value of problem (5) is obtained at the solution $(\hat{\mathbf{Q}}_0, \hat{\mathbf{Q}}_c)$ and the equality in (5a) does not hold, i.e., $\min\limits_{i=1,2} \log|\mathbf{I}+(\mathbf{I}+\mathbf{H}_i\hat{\mathbf{Q}}_c\mathbf{H}_i^H)^{-1}\mathbf{H}_k\hat{\mathbf{Q}}_0\mathbf{H}_k^H| > \tau_{ms}$.

Our next step is to construct a new solution $(\bar{\mathbf{Q}}_0, \bar{\mathbf{Q}}_c)$ from $(\hat{\mathbf{Q}}_0, \hat{\mathbf{Q}}_c)$, which achieves a larger objective value and satisfies the QoMS constraint (5a) with equality. Specifically, we multiply $\hat{\mathbf{Q}}_0$ by a scaling factor ξ $(0<\xi<1)$ and add a positive semidefinite (PSD) matrix $\mathbf{E}=\rho\mathbf{I}-\rho\mathbf{H}_2^H(\mathbf{H}_2\mathbf{H}_2^H)^{-1}\mathbf{H}_2$ to $\hat{\mathbf{Q}}_c$, i.e., $\bar{\mathbf{Q}}_0=\xi\hat{\mathbf{Q}}_0$ and $\bar{\mathbf{Q}}_c=\hat{\mathbf{Q}}_c+\mathbf{E}$, where the coefficient ρ controls the power of $\mathbf{E}$. Note that $\mathbf{E}$ is the orthogonal complement projector of $\mathbf{H}_2^H$, and its existence is guaranteed by the condition $\mathrm{rank}(\mathbf{H}_2)=N_e<N_t$. To keep the total transmit power constant, the coefficient ρ should be chosen to satisfy $(1-\xi)\mathrm{Tr}(\hat{\mathbf{Q}}_0)=\mathrm{Tr}(\mathbf{E})=\rho(N_t-N_e)$, that is, $\rho=\frac{(1-\xi)\mathrm{Tr}(\hat{\mathbf{Q}}_0)}{N_t-N_e}$. To proceed, we need the following lemma.

Lemma 2 ([18]): For matrices $\mathbf{A},\mathbf{\Delta}\succeq\mathbf{0}$ and $\mathbf{B}\succ\mathbf{0}$, the following inequality hold:

$$\frac{|\mathbf{A}+\mathbf{B}|}{|\mathbf{B}|}\geq\frac{|\mathbf{A}+\mathbf{B}+\mathbf{\Delta}|}{|\mathbf{B}+\mathbf{\Delta}|}. \tag{13}$$

Then, by applying Lemma 2, one can obtain

$$\begin{aligned}&\log|\mathbf{I}+(\mathbf{I}+\mathbf{H}_i\hat{\mathbf{Q}}_c\mathbf{H}_i^H)^{-1}\mathbf{H}_i\hat{\mathbf{Q}}_0\mathbf{H}_i^H|\\ \geq&\log|\mathbf{I}+(\mathbf{I}+\mathbf{H}_i(\hat{\mathbf{Q}}_c+\mathbf{E})\mathbf{H}_i^H)^{-1}\mathbf{H}_i\hat{\mathbf{Q}}_0\mathbf{H}_i^H|\\ >&\log|\mathbf{I}+(\mathbf{I}+\mathbf{H}_i\bar{\mathbf{Q}}_c\mathbf{H}_i^H)^{-1}\mathbf{H}_i\bar{\mathbf{Q}}_0\mathbf{H}_i^H|\end{aligned} \tag{14}$$

for any $i\in\{1,2\}$. Thus, by adjusting the value of ξ, the equality in (5a) could be achieved.

Next, we will show a larger objective value could always be achieved by $(\bar{\mathbf{Q}}_0, \bar{\mathbf{Q}}_c)$. To this end, we apply the Weyl theorem [19] to get $\lambda_k(\mathbf{I}+\mathbf{H}_1\tilde{\mathbf{Q}}_c\mathbf{H}_1^H+\mathbf{H}_1\mathbf{E}\mathbf{H}_1^H)>\lambda_k(\mathbf{I}+\mathbf{H}_1\tilde{\mathbf{Q}}_c\mathbf{H}_1^H),\forall k$. Meanwhile, due to the equality $\mathbf{H}_2\mathbf{E}\mathbf{H}_2^H=\mathbf{0}$, it is easy to see $\lambda_k(\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H+\mathbf{H}_2\mathbf{E}\mathbf{H}_2^H)=\lambda_k(\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H),\forall k$. By applying the property $\det(\mathbf{A})=\prod_i\lambda_i(\mathbf{A})$, we immediately obtain $\log|\mathbf{I}+\mathbf{H}_1\bar{\mathbf{Q}}_c\mathbf{H}_1^H|>\log|\mathbf{I}+\mathbf{H}_1\tilde{\mathbf{Q}}_c\mathbf{H}_1^H|$ and $\log|\mathbf{I}+\mathbf{H}_2\bar{\mathbf{Q}}_c\mathbf{H}_2^H|=\log|\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H|$, which yields $\log|\mathbf{I}+\mathbf{H}_1\bar{\mathbf{Q}}_c\mathbf{H}_1^H|-\log|\mathbf{I}+\mathbf{H}_2\bar{\mathbf{Q}}_c\mathbf{H}_2^H|>\log|\mathbf{I}+\mathbf{H}_1\tilde{\mathbf{Q}}_c\mathbf{H}_1^H|-\log|\mathbf{I}+\mathbf{H}_2\tilde{\mathbf{Q}}_c\mathbf{H}_2^H|$, i.e., a larger objective value can be found with $(\bar{\mathbf{Q}}_0, \bar{\mathbf{Q}}_c)$. This fact is contrary to the primal assumption, which completes the proof of Property 1.

VII-B. Proof of Property 2

As for Property 2, we only need to note that increasing r_{ms} would shrink the feasible region of problem (5). Hence, $R(\tau_{ms})$ must be monotonically nonincreasing w.r.t τ_{ms}. Furthermore, we claim that any two distinct τ_{ms} cannot generate an identical objective value of (5), since it will contradict Property 1. This completes the proof of Property 2.

Back to Theorem 1, let us denote the set of objective values (1-by-2 vectors) of feasible points of (4) as $\mathcal{O}$. Suppose that $(r_1,r_2),(r_3,r_4)$ are two arbitrary rate pairs in $\mathcal{O}$, for which $r_1\neq r_3$. From our problem formation of (5) and Property 1, it is immediate to get $(r_1,R(r_1))\succeq_{\mathbb{R}_+^2}(r_1,r_2),(r_3,R(r_3))\succeq_{\mathbb{R}_+^2}(r_3,r_4)$. According to Property 2, if $r_1\gtrless r_3$, then we will have $R(r_1)\lessgtr R(r_3)$. Consequently, $(r_1,R(r_1))$ and $(r_3,R(r_3))$ are both Pareto optimal points of (5), since it is impossible to increase any one element of $(r_1,R(r_1))$ (or $(r_3,R(r_3))$) without decreasing the other one element of it. Substituting r_1 (or r_3) by τ_{ms}, we then complete the proof of Theorem 1.

VIII. REFERENCES

[1] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[2] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Oct. 2010.

[3] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[4] R. Wyrembelski and H. Boche, "Physical layer integration of private, common, and confidential messages in bidirectional relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.

[5] R. Schaefer and H. Boche, "Physical layer service integration in wireless networks: Signal processing challenges," *IEEE Signal Process. Mag.*, vol. 31, no. 3, pp. 147–156, Apr. 2014.

[6] W. Mei, Z. Chen, and J. Fang, "Secrecy capacity region maximization in Gaussian MISO channels with integrated services," *IEEE Signal Process. Lett.*, vol. 23, no. 8, pp. 1146–1150, Jul. 2016.

[7] W. Mei, L. Li, Z. Chen, and C. Huang, "Artificial-noise aided transmit design for multi-user MISO systems with integrated services," in *Proc. IEEE Global Conf. Signal Info. Process. (GlobalSIP)*, Orlando, FL, Dec. 2015, pp. 1382–1386.

[8] W. Mei, Z. Chen, and C. Huang, "Robust artificial-noise aided transmit design for multi-user MISO systems with integrated services," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Shanghai, Mar. 2016, pp. 3856–3860.

[9] G. R. Lanckriet and B. K. Sriperumbudur, "On the convergence of the concave-convex procedure," in *Proc. Advances Neural Inf. Process. Syst.*, 2009, pp. 1759–1767.

[10] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, UK: Cambridge university press, 2009.

[11] M. Grant and S. Boyd. (2011, Apr.) CVX: Matlab software for disciplined convex programming. [Online]. Available: http://cvxr.com/cvx

[12] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678–1690, May 2014.

[13] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[14] B. Fang, Z. Qian, W. Shao, and W. Zhong, "Precoding and artificial noise design for cognitive MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6753–6758, Aug. 2016.

[15] S. A. A. Fakoorian *et al.*, "Optimal power allocation for GSVD-based beamforming in the MIMO gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2012)*, Cambridge, MA, Jul. 2012, pp. 2321–2325.

[16] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[18] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "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.

[19] G. H. Golub and C. F. V. Loan, *Matrix computations*. Baltimore, Md: The Johns Hopkins University Press, 2012.