ROBUST ARTIFICIAL-NOISE AIDED TRANSMIT DESIGN FOR MULTI-USER MISO SYSTEMS WITH INTEGRATED SERVICES

Weidong Mei, Zhi Chen, and Chuan Huang

National Key Laboratory of Science and Technology on Communications
University of Electronic Science and Technology of China, Chengdu 611731, China

ABSTRACT

This paper considers an optimal artificial noise (AN)-aided transmit design for multi-user MISO systems in the eyes of service integration. Specifically, two sorts of services are combined and served simultaneously: one multicast message intended for all receivers and one confidential message intended for only one receiver. The confidential message is kept perfectly secure from all the unauthorized receivers. This paper considers a general case of imperfect channel state information (CSI), aiming at a joint and robust design of the input covariances for the multicast message, confidential message and AN, such that the worst-case secrecy rate region is maximized subject to the sum power constraint. To this end, we reveal its hidden convexity and transform the original worst-case robust secrecy rate maximization (SRM) problem into a sequence of semidefinite programming. Numerical results are presented to show the efficacy of our proposed method.

***Index Terms*—** Service integration, artificial noise, broadcast channel, secrecy rate region

1. INTRODUCTION

High spectral efficiency and secure communication are the basic demands for the future 5-Generation (5G) cellular networks; a heuristic way is to merge multiple services, e.g., multicast service and confidential service, into one integral service for one-time transmission. Service integration is in fact not a new concept: traditional service integration techniques rely on upper-layer protocols to allocate different services on different logical channels, which is quite inefficient. On the contrary, service integration in the physical layer enables coexisting services to share the same resources, thereby significantly increasing the spectral efficiency.

The respective investigation on multicast service and confidential service has received significant attention in many literatures. Multicast services can be efficiently offered by transmitting common messages in a way that all receivers can decode it, and confidential services can overcome the inherent difficulties of cryptographic methods, i.e., the distribution and management of secrecy keys. Physical layer multicasting strategies for instantaneous rate maximization have been designed in many literatures, epitomized in [1, 2, 3]. Comparatively, as for the researches on physical layer security, different tactics against eavesdroppers have been proposed with various levels of eavesdropper channel state information (ECSI) available to the transmitter; one can refer to [4, 5, 6] for a detailed review.

Csiszár and Körner's work in [7] established the fundamental limitation of physical-layer service integration, where the optimal integration of multicast service and confidential service was derived in a discrete memoryless broadcast channel (DMBC). In [8, 9, 10], the authors extended the results to the case with multiple-input multiple-output (MIMO). Furthermore, Wyrembelski *et al*. amalgamated broadcast service, multicast service and confidential service in bidirectional relay networks [11]. Nonetheless, the aforementioned works mainly studied the problem from the viewpoint of information theory, which means that they aimed to derive capacity results or characterize coding strategies that result in certain rate regions [12]. As to how to design the input covariance matrices (transmit strategies) to achieve the capacity region, there are few works.

In this paper, we handle the physical layer service integration from the view point of signal processing, i.e., find the optimal input covariance matrices for the transmitted messages. Specifically, we consider the multiuser multiple-input single-output (MISO) broadcast channel (BC) with multiple receivers and two sorts of messages: a common message intended for all receivers, and a confidential message intended for merely one receiver. The confidential message must be kept perfectly secure from all other unauthorized receivers. Moreover, it is assumed that there exist channel mismatches that are norm-bounded by some known constants for links between the transmitter and all the receivers. Different from conventional worst-case robust secrecy rate maximization (SRM) problem [13, 14, 15], our paper further takes into account the guarantee of eavesdroppers' quality of multicast service (QoMS). Additionally, we address a challenging case where artificial noise is employed to degrade the potential eavesdropping of the unauthorized receivers. We focus on obtaining robust transmit covariance matrices of the common message, confidential message and AN. To the best of our knowledge, there is no existing papers tackling the aforemen-

This work was supported in part by the National Natural Science Foundation of China under Grant 61571089, and by the High-Tech Research and Development (863) Program of China under Grant 2015AA011309.

tioned situations simultaneously.

Our main contribution is that we specify variant target QoMS, and meanwhile maximize the corresponding worst-case secrecy rates with the aided AN. By this means, we obtain the worst-case secrecy rate region for the two sorts of messages.

2. MATHEMATICAL MODEL

We consider the downlink of a multiuser system in which a multi-antenna transmitter serves K receivers, and each receiver has a single antenna. Assume that all receivers have ordered the multicast service and receiver 1 further ordered the confidential service. To enhance the security of the confidential service, the transmitter utilizes a fraction of its transmit power to send artificially generated noise to interfere the unauthorized receivers (eavesdroppers), i.e., receiver 2 to receiver K.

2.1. Signal Model

The received signal at receiver k is modeled as

$$y_k = \mathbf{h}_k\mathbf{x} + z_k, k = 1, 2, \cdots, K \tag{1}$$

respectively, where $\mathbf{h}_k \in \mathbb{C}^{1\times N_t}$ is the channel vector from the transmitter to receiver k, N_t is the number of transmit antennas employed by the transmitter, and z_k is independent identically distributed (i.i.d.) complex Gaussian noise with zero mean and unit variance. The channel state information (CSI) of all receivers is assumed to be available at the transmitter. $\mathbf{x} \in \mathbb{C}^{N_t}$ is the transmitted signal vector which consists of three components, i.e.,

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

where $\mathbf{x}_0$ is the common message intended for all receivers, $\mathbf{x}_c$ is the confidential message intended for receiver 1, and $\mathbf{x}_a$ is the artificial noise. We assume $\mathbf{x}_0 \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_0)$, $\mathbf{x}_c \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_c)$ [8], where $\mathbf{Q}_0$ and $\mathbf{Q}_c$ are the transmit covariance matrices. The AN $\mathbf{x}_a$ follows a distribution $\mathbf{x}_a \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_a)$, where $\mathbf{Q}_a$ is the AN covariance. These three components are assumed to be independent of each other.

Denote R_0 and R_c as the achievable rates related to the common and confidential messages, respectively. Then an achievable secrecy rate region C_s is given by all the rate pairs (R_c, R_0) that satisfy (cf. [8, 16])

$$R_c \le \log \frac{1 + (1 + \mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max\limits_{k\in\mathcal{K}_e} 1 + (1 + \mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}, \tag{3a}$$

$$R_0 \le \min_{k\in\mathcal{K}} \left\{ \log \frac{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a + \mathbf{Q}_0)\mathbf{h}_k^H}{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a)\mathbf{h}_k^H} \right\}, \tag{3b}$$

where $\mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_c + \mathbf{Q}_a) \le P$ with P being total transmission power budget at the transmitter, $\mathcal{K} \triangleq \{1, 2, ..., K\}$, and $\mathcal{K}_e \triangleq \mathcal{K}/\{1\}$ denotes the indices of all unauthorized receivers.

2.2. The Worst-case Robust Problem Formulation

The maximization of (3) with perfect CSI has been solved in our previous work [17]. In the sequel, we consider a more general and realistic assumption that the transmitter has imperfect CSI on links of all receivers. To put into context, let

$$\mathbf{h}_k = \tilde{\mathbf{h}}_k + \mathbf{e}_k, \|\mathbf{e}_k\|_F \le \varepsilon_k, \forall k \in \mathcal{K}, \tag{4}$$

where $\mathbf{h}_k$ is the actual channel vector from the transmitter to the kth receiver as defined before, $\tilde{\mathbf{h}}_k$ is the transmitter's estimation of $\mathbf{h}_k$, and $\mathbf{e}_k$ represents the associated CSI error which is located in a ball whose radius is ε_k [15, 18]. Here, we assume a nontrivial case where ε_k is less than the norm of $\tilde{\mathbf{h}}_k$ for $\forall k \in \mathcal{K}$. The worst-case secrecy rate region is therefore determined by

$$R_c \le \log \frac{\min\limits_{\mathbf{h}_1\in B_1} 1 + (1 + \mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max\limits_{\mathbf{h}_k\in B_k, k\in\mathcal{K}_e} 1 + (1 + \mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H} \tag{5a}$$

$$R_0 \le \min_{k\in\mathcal{K}, \mathbf{h}_k\in B_k} \log \frac{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a + \mathbf{Q}_0)\mathbf{h}_k^H}{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a)\mathbf{h}_k^H}, \tag{5b}$$

where $B_i \triangleq \left\{ \mathbf{h}_k \middle| \mathbf{h}_k = \tilde{\mathbf{h}}_k + \mathbf{e}_k, \|\mathbf{e}_k\|_F \le \varepsilon_k \right\}, \forall k \in \mathcal{K}$ denotes the set of all admissible CSIs. The region in (5) is a safe achievable region when the uncertainties given in (4) exists; the actual secrecy rate pairs with regard to the true channel vectors must not lie within the boundary of (5). Our work focuses on the robust design of $\mathbf{Q}_0$, $\mathbf{Q}_c$ and $\mathbf{Q}_a$, under a worst-case achievable SRM formulation with QoMS constraint, i.e.,

$$\max_{\mathbf{Q}_0, \mathbf{Q}_a, \mathbf{Q}_c} \log \frac{\min\limits_{\mathbf{h}_1\in B_1} 1 + (1 + \mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H)^{-1}\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{\max\limits_{k\in\mathcal{K}_e, \mathbf{h}_k\in B_k} 1 + (1 + \mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H)^{-1}\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}$$

$$\text{s.t.} \min_{\substack{k\in\mathcal{K}, \\ \mathbf{h}_k\in B_k}} \left\{ \log \frac{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a + \mathbf{Q}_0)\mathbf{h}_k^H}{1 + \mathbf{h}_k(\mathbf{Q}_c + \mathbf{Q}_a)\mathbf{h}_k^H} \right\} \ge \tau, \tag{6a}$$

$$\mathrm{Tr}(\mathbf{Q}_0 + \mathbf{Q}_a + \mathbf{Q}_c) \le P, \tag{6b}$$

$$\mathbf{Q}_0 \succeq \mathbf{0}, \mathbf{Q}_a \succeq \mathbf{0}, \mathbf{Q}_c \succeq \mathbf{0}, \tag{6c}$$

where τ is preset requirement of the achievable rate associated with the common message. We should point out that the maximum objective value of problem (6) is obtained when and only when the equality in (6a) holds. The proof can be simply accomplished by contradiction: Assume the maximum value of problem (6) is obtained when the equality in (6a) does not hold, with $\mathbf{Q}_a$ unchanged, we multiply $\mathbf{Q}_c$ and $\mathbf{Q}_0$ by a scaling factor $\eta(\eta > 1)$ and $\xi(0 < \xi < 1)$, respectively, to equalize (6a) while satisfying the total power constraint. Then, we can find a larger objective value for problem (6) in this way, which is contrary to the assumption.

Remark 1 *The preceding proof offers a method to acquire the boundary points of (5). We traverse all possible τ's and*

store the corresponding optimal objective value $g^*(\tau)$, and then the rate pair $(\tau, g^*(\tau))$ is a boundary point of the worst-case secrecy rate region.

Remark 2 *A natural question induced by Remark 1 is how to determine an upper bound of τ. Observe that*

$$\begin{aligned} 2^{\tau}-1 &\leq \min_{k\in\mathcal{K},\mathbf{h}_k\in B_k} \frac{\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H} \\ &\leq \min_{k\in\mathcal{K},\mathbf{h}_k\in B_k} \mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H \leq P \min_{k\in\mathcal{K},\mathbf{h}_k\in B_k} \|\mathbf{h}_k\|^2 \quad (7) \\ &= P\min_{k\in\mathcal{K}}(\left\|\tilde{\mathbf{h}}_k\right\|-\varepsilon_k)^2, \end{aligned}$$

where the third inequality follows from the fact that $\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H \leq \mathrm{Tr}(\mathbf{Q}_0)\|\mathbf{h}_k\|^2$ for any $\mathbf{Q}_0 \succeq \mathbf{0}$ and $\mathrm{Tr}(\mathbf{Q}_0) \leq P$, and the last equality is derived by solving a simple quadratically constrained quadratic programming (QCQP) with its Karush-Kuhn-Tucker (KKT) conditions, which leads to one upper bound; an alternative way is to halt the traversal when the primal problem becomes infeasible.

3. ROBUST AN-AIDED TRANSMIT DESIGN WITH SERVICE INTEGRATION

In this section, we derive an SDP-based optimization approach for problem (6). To start with, by introducing the slack variables β and u, we rewrite (6) as

$$\begin{aligned} g^*(\tau') = &\max_{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,\beta,u} \log\left(\frac{u}{\beta}\right) \\ \text{s.t.}\quad & 1+\frac{\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H} \geq u, \forall \mathbf{h}_1\in B_1, && (8a) \\ & \log(1+\frac{\mathbf{h}_k\mathbf{Q}_c\mathbf{h}_k^H}{1+\mathbf{h}_k\mathbf{Q}_a\mathbf{h}_k^H}) \leq \log\beta, \forall k\in\mathcal{K}_e, \mathbf{h}_k\in B_k, && (8b) \\ & \frac{\mathbf{h}_k\mathbf{Q}_0\mathbf{h}_k^H}{1+\mathbf{h}_k(\mathbf{Q}_c+\mathbf{Q}_a)\mathbf{h}_k^H} \geq \tau', \forall k\in\mathcal{K}, \mathbf{h}_k\in B_k, && (8c) \\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c) \leq P, && (8d) \\ & \mathbf{Q}_0\succeq\mathbf{0}, \mathbf{Q}_a\succeq\mathbf{0}, \mathbf{Q}_c\succeq\mathbf{0}, && (8e) \end{aligned}$$

in which $\beta \geq 1$, $\tau' \triangleq 2^{\tau}-1$, and thus constraint (8c) is an equivalent form of constraint (6a). One can notice that β is introduced to simplify the denominator of the logarithm in the objective function of (6), while u is introduced to simplify its numerator, which has been previously used to deal with the QoS-constrained robust beamforming problems arising in wiretap channels with a helper [15, 19]. The obstacle of dealing with (8) lies in the existence of uncertainties in the constraints from (8a) to (8c). Here, we exert $\mathcal{S}$-procedure [20] to turn these constraints into linear matrix inequalities (LMIs) in (9) to (11) at the bottom of this page, where ρ, $\{t_k\}_{k\in\mathcal{K}_e}$ and $\{\delta_k\}_{k\in\mathcal{K}}$ are all nonnegative slack variables.

Next, we show that (8) can be recast as a one-variable optimization problem over β which involves solving a sequence of fractional SDPs. Analogous to Remark 2, to achieve a nonnegative secrecy rate, an upper bound of β can be determined according to

$$\begin{aligned} \beta &\leq 1+\min_{\mathbf{h}_1\in B_1} \frac{\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H} \\ &\leq 1+\min_{\mathbf{h}_1\in B_1} \mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H \leq 1+P\min_{\mathbf{h}_1\in B_1}\|\mathbf{h}_1\|^2. \end{aligned} \quad (12)$$

Noting that $\log(\cdot)$ function is monotonically increasing, we further rewrite (8) as

$$\begin{aligned} \gamma^*(\tau') = &\max_{\beta}\ \eta(\tau',\beta) \\ &\text{s.t.}\quad 1\leq\beta\leq 1+P\min_{\mathbf{h}_1\in B_1}\|\mathbf{h}_1\|^2, \end{aligned} \quad (13)$$

where $\log\gamma^*(\tau') = g^*(\tau')$, and

$$\begin{aligned} \eta(\tau',\beta) = &\max_{\substack{\mathbf{Q}_0,\mathbf{Q}_a,\mathbf{Q}_c,u \\ \{t_k\}_{k\in\mathcal{K}_e},\{\delta_k\}_{k\in\mathcal{K}},\rho}} \frac{u}{\beta} \\ \text{s.t.}\quad & \mathbf{X}(u,\mathbf{Q}_c,\mathbf{Q}_a,\rho)\succeq\mathbf{0}, \rho\geq 0, && (14a) \\ & \mathbf{T}_k(\beta,\mathbf{Q}_c,\mathbf{Q}_a,t_k)\succeq\mathbf{0}, t_k\geq 0, \forall k\in\mathcal{K}_e, && (14b) \\ & \mathbf{S}_k(\tau',\mathbf{Q}_c,\mathbf{Q}_a,\mathbf{Q}_0,\delta_k)\succeq\mathbf{0}, \delta_k\geq 0, \forall k\in\mathcal{K}, && (14c) \\ & \mathrm{Tr}(\mathbf{Q}_0+\mathbf{Q}_a+\mathbf{Q}_c)\leq P, && (14d) \\ & \mathbf{Q}_0\succeq\mathbf{0}, \mathbf{Q}_a\succeq\mathbf{0}, \mathbf{Q}_c\succeq\mathbf{0}. && (14e) \end{aligned}$$

One can notice that for a fixed value of u, (14) is a convex feasibility problem with LMI constraints. We mention that (14) essentially is an equivalently epigraph reformulation of a quasiconcave problem aiming to maximize $\frac{1}{\beta}(1+\min_{\mathbf{h}_1\in B_1}\frac{\mathbf{h}_1\mathbf{Q}_c\mathbf{h}_1^H}{1+\mathbf{h}_1\mathbf{Q}_a\mathbf{h}_1^H})$ (cf. (8a)). Thus, the inner problem (14) can be efficiently solved by combining a bisection search [20]

$$\mathbf{X}(u,\mathbf{Q}_c,\mathbf{Q}_a,\rho) = \begin{bmatrix} \rho\mathbf{I}+\mathbf{Q}_c+(1-u)\mathbf{Q}_a & (\mathbf{Q}_c+(1-u)\mathbf{Q}_a)\tilde{\mathbf{h}}_1^H \\ \tilde{\mathbf{h}}_1(\mathbf{Q}_c+(1-u)\mathbf{Q}_a) & \tilde{\mathbf{h}}_1(\mathbf{Q}_c+(1-u)\mathbf{Q}_a)\tilde{\mathbf{h}}_1^H-\rho\varepsilon_1^2-u+1 \end{bmatrix} \succeq \mathbf{0}. \quad (9)$$

$$\mathbf{T}_k(\beta,\mathbf{Q}_c,\mathbf{Q}_a,t_k) = \begin{bmatrix} t_k\mathbf{I}+(\beta-1)\mathbf{Q}_a-\mathbf{Q}_c & ((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H \\ \tilde{\mathbf{h}}_k((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c) & \tilde{\mathbf{h}}_k((\beta-1)\mathbf{Q}_a-\mathbf{Q}_c)\tilde{\mathbf{h}}_k^H-t_k\varepsilon_k^2+\beta-1 \end{bmatrix} \succeq \mathbf{0}, \forall k\in\mathcal{K}_e, \quad (10)$$

$$\mathbf{S}_k(\tau',\mathbf{Q}_c,\mathbf{Q}_a,\mathbf{Q}_0,\delta_k) = \begin{bmatrix} \delta_k\mathbf{I}+\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c) & (\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c))\tilde{\mathbf{h}}_k^H \\ \tilde{\mathbf{h}}_k(\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c)) & -\delta_k\varepsilon_k^2-\tau'+\tilde{\mathbf{h}}_k(\mathbf{Q}_0-\tau'(\mathbf{Q}_a+\mathbf{Q}_c))\tilde{\mathbf{h}}_k^H \end{bmatrix} \succeq \mathbf{0}, \forall k\in\mathcal{K}. \quad (11)$$

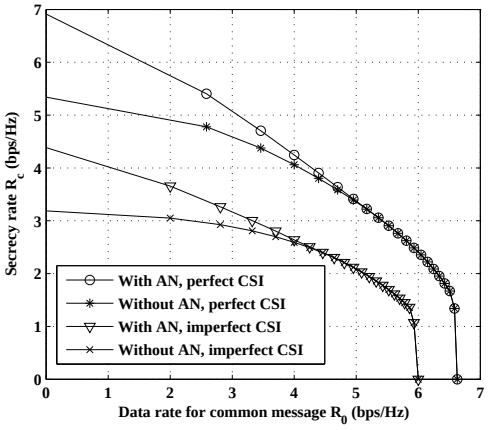

Fig. 1. Secrecy rate regions with and without AN

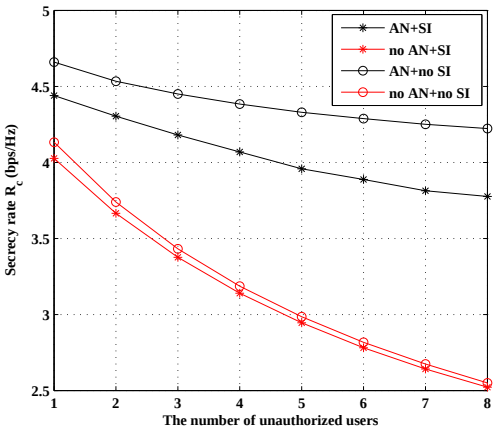

Fig. 2. Secrecy rate versus the number of unauthorized receivers

on u with a convex optimization solver, e.g. `CVX`. The outer problem (13) is a single-variable optimization problem with a bounded interval constraint, which can be handled by performing a proper one-dimensional search algorithm, e.g., the golden section search [21]. The optimal β should be chosen as the one that leads to the maximum $\eta(\tau', \beta)$ in (13).

4. NUMERICAL RESULTS

In this section, we illustrate some numerical results to compare the security performances achieved by different transmit designs. To avoid the large computational load, we generate deterministic real channel vectors to demonstrate the results as [8] did. In our example, we set $N_t = 2$, $K = 5$, $P = 20$dB and $\varepsilon_k = 0.2$ for all k. The channels are given by $\tilde{\mathbf{h}}_1 = [2, 0.4]$ and $\tilde{\mathbf{h}}_k = [0.9 - 0.1k, 0.5 + 0.1k], \forall k \in \mathcal{K}_e$.

Firstly, we plot the worst-case secrecy rate region achieved by AN-aided transmission in Fig. 1, and compare it with that achieved by no-AN transmission where we fix $\mathbf{Q}_a = \mathbf{0}$ when solving (6). Meanwhile, we plot the secrecy capacity region achieved by (3) with perfect CSI as a benchmark. From Fig. 1, we can clearly observe that the existence of channel uncertainty dramatically diminishes the achievable secrecy rate region. Notice that secrecy rates with AN are practically higher than those without AN, the striking gap indicates that AN indeed enhances the security performance without sacrificing the QoMS. Nonetheless, with the increasing demand for QoMS, the gap tends to be reduced, which implies that AN is prohibitive at high QoMS region. This observation demonstrates that the demand of QoMS considerably confines AN's transmission.

To gain more insights in our robust transmit design, now we turn our attention to the relation between the secrecy rate and the number of unauthorized receivers. To expose it, we plot the worst-case secrecy rates versus the number of unauthorized receivers with setting $\tau = 1$ bps/Hz in Fig. 2. In addition, we also give the results of a no-SI ("SI" is the abbreviation for "service integration") scenario where only the confidential service is employed, i.e., τ is specified as zero. Our purpose of including the no-SI scenario is merely to provide a reference to see how the service integration will influence the security performance. From Fig. 2, we have the following observations: First, the worst secrecy rates drops with the number of unauthorized receivers, especially rapid in the cases without AN; meanwhile, incorporating AN can offer an increasing secrecy gain as the number of unauthorized receivers increases. Second, adversely, incorporating SI restrains the maximum worst-case security rates in that the guarantee of QoMS will occupy the resources originally assigned to the confidential service.

5. CONCLUSION

In this paper, we consider the optimal robust AN-aided transmit design for multiuser MISO broadcast channel with amalgamating confidential service and multicast service. Our goal is to maximize the worst-case secrecy rate with constrained QoMS, and then obtain the boundary points of the worst-case secrecy rate region for the two services. This worst-case SRM problem is challenging to solve due to its intrinsically complex problem structures. By resorting to an SDP-based optimization approach, we show that it can be handled by solving a sequence of SDPs. The numerical results reveal that the existence of channel uncertainty has an adverse effect on the security performance, and that AN can effectively fortify the transmission security, but high demand for QoMS will confine its use in turn.

To obtain the optimal solutions to our worst-case SRM formulation, we employ the golden section search which involves solving a sequence of factional SDPs, which is computationally expensive albeit tractable. As a future work, it would be interesting to find efficient methods for dealing with this problem.

6. REFERENCES

[1] H. Kim, D. J. Love, and S. Y. Park, "Optimal and successive approaches to signal design for multiple antenna physical layer multicasting," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2316–2327, Aug. 2011.

[2] H. Zhu, N. Prasad, and S. Rangarajan, "Precoder design for physical layer multicasting," *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 5932–5947, Nov. 2012.

[3] S. X. Wu, W.-K. Ma, and A. M.-C. So, "Physical-layer multicasting by stochastic transmit beamforming and Alamouti space-time coding," *IEEE Trans. Signal Process.*, vol. 61, no. 17, pp. 4230–4245, Sep. 2013.

[4] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Berlin, Germany: Springer Publishing Company, Incorporated, 2013.

[5] A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[6] B. He, X. Zhou, and T. D. Abhayapala. (2013, Jun.) Wireless physical layer security with imperfect channel state information: A survey. [Online]. Available: http://arxiv.org/abs/1307.4146

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

[8] 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.

[9] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2010)*, Austin, TX, Jun. 2010, pp. 2583–2587.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2010)*, Austin, TX, Jun. 2010, pp. 2578–2582.

[11] 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.

[12] 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.

[13] 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.

[14] J. Li and A. P. Petropulu, "Explicit solution of worst-case secrecy rate for MISO wiretap channels with spherical uncertainty," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3892–3895, Jul. 2012.

[15] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Dec. 2012.

[16] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 5:1–5:12, Mar. 2009.

[17] W. Mei, L. Li, Z. Chen, and C. Huang, "Artificial-noise aided transmit design for multi-user MISO systems with integrated services," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP 2015)*, Orlando, FL, Dec. 2015, pp. 1–5.

[18] 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.

[19] J. Huang and A. L. Swindlehurst, "QoS-constrained robust beamforming in MISO wiretap channels with a helper," in *45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR'2011)*, Pacific Grove, CA, Nov. 2011, pp. 188–192.

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

[21] D. Bertsekas, *Nonlinear Programming*, 2nd ed. Belmont, MA, USA: Athena Scientific, 1999.