Max-Min Fairness Precoding for Enhanced Security with Partial Channel Knowledge

Sangmin Lee
Dept. of Electrical Engineering
Ulsan National Institute of Science and Technology (UNIST)
Ulsan, South Korea
sangminlee@unist.ac.kr

Eunsung Choi
Dept. of Electrical Engineering
Ulsan National Institute of Science and Technology (UNIST)
Ulsan, South Korea
eunsungchoi@unist.ac.kr

Jinseok Choi
School of Electrical Engineering
Korea Advanced Institute of Science and Technology (KAIST)
Daejeon, South Korea
jinseok@kaist.ac.kr

Abstract— This study introduces a novel approach for achieving secure max-min fairness (MMF) precoding in a downlink multi-antenna system catering to multiple users and eavesdroppers. The challenges posed by the non-convex and non-smooth nature of the optimization problem, along with partial channel knowledge, are considerable. To address these, we reformulate the problem using conditional average rates and approximate it using the LogSumExp approach. By translating the primary optimality condition into a generalized eigenvalue problem, solved through a power iteration technique, we obtain a local optimal solution. Simulations confirm the effectiveness of our proposed secure-MMF precoding method.

Keywords— Physical layer security, secure precoding, max-min fairness, generalized power iteration, imperfect CSIT.

I. Introduction

The growth of smart devices has led to a rapid increase in the density of devices per access point (AP), underscoring the heightened significance of delivering consistently high data rates to these devices

II. System Model

We consider a single-cell downlink multi-user MIMO system where an AP equipped with N antennas serves K users with a single antenna. There exist M eavesdroppers with a single antenna. The AP transmits a precoded signal vector $\mathbf{x} = \mathbf{F}\mathbf{s}$, where $\mathbf{F}$ is the precoding matrix and $\mathbf{s}$ is the user symbols vector. Then, user k and eavesdropper m receive signals

$$y_k = \mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k s_k + \sum_{i=1,i\neq k}^{K} \mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i s_i + n_k, \qquad y_m^{\mathrm{e}} = \sum_{i=1}^{K} \mathbf{g}_m^{\mathrm{H}}\mathbf{f}_i s_i + n_m^{\mathrm{e}},$$

respectively. Here, $\mathbf{h}_k$ is the channel vector between user k and the AP and $\mathbf{g}_m$ is the channel vector between eavesdropper m and the AP. For the spatial channel covariance matrix, we adopt the one ring model for the channel covariance matrix [1].

To ensure the prevention of any unauthorized eavesdropping on user messages, the concept of secrecy spectral efficiency (SE) necessitates an assessment based on the maximum achievable wiretap SE for the specific message in question. We formulate the secure max-min fairness (MMF) optimization problem

$$\underset{\mathbf{f}_1,\ldots,\mathbf{f}_K}{\text{maximize}} \ \min_{k\in\mathcal{K}} \left(\left[R_k - \max_{m\in\mathcal{M}} R_{k,m}^{\mathrm{e}} \right]^{+} \right) \text{ subject to } \sum_{k=1}^{K} \|\mathbf{f}_k\|^2 \leq 1,$$

where $R_k = \log_2\left(1 + \frac{|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i=1,i\neq k}^{K}|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i|^2+\sigma^2/P}\right)$, $R_{k,m}^{\mathrm{e}} = \log_2\left(1 + \frac{|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i=1,i\neq k}^{K}|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_i|^2+\sigma_{\mathrm{e}}^2/P}\right)$.

III. Proposed Algorithm

Given that the AP has access solely to the estimated legitimate channel and other enduring channel statistics, we employ a strategy based on conditional averaged secrecy SE. This approach serves to reframe the problem, thereby leveraging the available long-term channel information. Therefore, we set $\bar{R}_k = \mathbb{E}[R_k]$, $\bar{R}^{\mathrm{e}}{}_{k,m} = \mathbb{E}[R_{k,m}^{\mathrm{e}}]$. With Jensen's inequality and Lemma 1 in [2], we derive the lower bound of the optimization problem. Subsequently, we proceed to represent the expression for SE in a Rayleigh quotient form. Finally, we solve the problem by identifying the best stationary point.

IV. Numerical Results

Fig.1 illustrates the minimum secrecy SE as a function of the signal-to-noise ratio (SNR). Notably, the proposed method demonstrates the highest minimum secrecy SE, closely followed by MMF-GPI. This discernible performance gap between the proposed method and MMF-GPI underscores the significance of integrating wiretap channel SE into the optimization process.

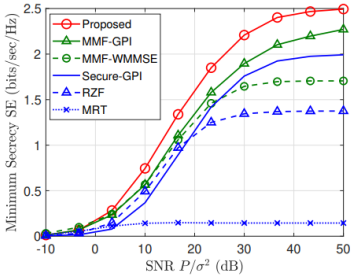

Fig. 1. The minimum spectral efficiency versus SNR for $N = 6$ AP antennas, $K = 4$ users, and $E = 2$ eavesdroppers.

V. Concolusion

This paper introduced a novel precoding algorithm that addresses the dual concerns of fairness and security within the framework of partial CSIT. By leveraging conditional average SE with lower bounding and subsequent approximations, the challenge posed by partial CSIT was effectively managed.

Reference

[1] A. Adhikary, J. Nam, J.-Y. Ahn, and G. Caire, "Joint spatial division and multiplexing—The large-scale array regime," *IEEE Trans. Inform. Theory*, vol. 59, no. 10, pp. 6441–6463, Jun. 2013.

[2] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, "Power scaling of uplink massive MIMO systems with arbitrary-rank channel means," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 966–981, May 2014.