보수적인 보안 통신 및 공정 데이터율을 위한 인공 잡음 기반 보안 프리코딩 디자인

김선규, 최은성*, 오민택**, 최진석**
충남대학교, *울산과학기술원, **한국과학기술원

tjsrb724@gmail.com, *eunsungchoi@unist.ac.kr, **{ohmin, jinseok}@kaist.ac.kr

Artificial Noise-aided Secure Precoding Design for Conservative Security and Fairness

Sungyu Kim, Eunsung Choi*, Mintaek Oh**, Jinseok Choi**
Chungnam National University, *UNIST, **KAIST

요 약

본 논문은 다중 안테나 하향 링크 시스템에서 여러 사용자와 공모하는 도청자들이 존재할 때, 최대-최소 공정성(max-min fairness, MMF)을 보장하는 인공 잡음 보안 프리코딩 알고리즘을 제안한다. 부분적인 채널 정보가 존재하는 상황을 가정하고, 인공 잡음과 프리코더를 동시에 디자인하는 MMF 최적화 문제를 다루기 쉬운 형태로 근사한다. 도출된 최적화 조건을 통해서 공정성과 보안을 동시에 유지하는 최적의 프리코더와 인공 잡음을 찾아낸다. 시뮬레이션을 통해서 제안된 알고리즘이 공정성과 보안을 유지할 수 있음을 보여준다.

Ⅰ. 서 론

무선 통신의 발전으로 모바일 기기의 수가 증가하고 다양해지면서, 사용자에게 공정한 서비스를 제공하면서 정보의 보안을 보장하는 것은 매우 중요한 과제가 됐다. 이러한 배경 하에, 모든 사용자가 균일한 서비스를 제공받도록 최대-최소 공정성(Max-Min Fairness, MMF)에 기반한 방법들이 연구되어 왔다 [1]. 또한, 보안의 측면에서는 물리 계층 보안이 기존의 암호학과 달리, 낮은 복잡도로 주목을 받게 되었다. 그중에서, 보안 프리코더와 인공 잡음을 동시에 활용하는 방법들이 있지만, 프리코더와 인공 잡음을 각각 디자인하는 한계가 존재했다. 따라서 공정성과 보안의 문제를 모두 고려하여, 프리코더와 인공 잡음을 동시에 디자인하면서 MMF 문제를 해결하는 알고리즘을 제안한다.

Ⅱ. 본 론

본 논문에서는 하나의 셀에서 N 개의 안테나를 지닌 AP 가 K 명의 단일 안테나 사용자에게 서비스를 제공하는 하향 링크 시스템을 고려하는데, 공모하는 M 명의 단일 안테나 도청자가 함께 존재한다. AP 는 인공 잡음과 함께 프리코딩된 신호 벡터 $\mathbf{x}=\mathbf{Fs}+\mathbf{\Phi z}$를 전송한다. 프리코딩 행렬은 $\mathbf{F}\in\mathbb{C}^{N\times K}$, $\mathbf{s}\sim\mathcal{CN}(\mathbf{0}_K, P\mathbf{I}_K)$는 사용자 심볼 그리고 인공 잡음은 $\mathbf{\Phi z}\sim\ \mathcal{CN}(\mathbf{0}_N, P\mathbf{\Phi\Phi}^{\mathrm{H}})$이다. 여기서, P 는 최대 전송 전력이다. 신호가 전송될 때, $R_k=\log_2\left(1+\frac{|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i=1,\,i\neq k}^{K}|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i|^2+\sum_{j=1}^{J}|\mathbf{h}_k^{\mathrm{H}}\boldsymbol{\phi}_j|^2+\frac{\sigma^2}{P}}\right)$로 k번째 사용자의 전송률을, 도청자들이 k 번째 사용자를 도청할 때 $R_k^{\mathrm{e}}=\log_2\left(1+\sum_{m=1}^{M}\frac{|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i\neq k}^{K}|\mathbf{g}_m^{\mathrm{H}}\mathbf{f}_i|^2+\sum_{j=1}^{J}|\mathbf{g}_m^{\mathrm{H}}\boldsymbol{\phi}_j|^2+\frac{\sigma_{\mathrm{e}}^2}{P}}\right)$로 전송률을 나타낼 수 있다. 여기서, $\mathbf{h}_k$와 $\mathbf{g}_m$은 각각 AP 와 k번째 사용자 사이의 채널 벡터, AP 와 m번째 도청자 사이의 채널 벡터를 의미한다. 이를 위해서 One-ring 모델을 활용하였다 [2]. 우리는 부분적인 채널 정보를 가지는 현실적인 상황을 가정하였으므로, 예측된 사용자의 채널 벡터 $\hat{\mathbf{h}}_k$, 채널 예측 에러 공분산 행렬 $\mathbf{\Psi}_k$, 도청자의 채널 공분산 행렬 $\mathbf{R}_m^{\mathrm{e}}$을 활용하여 새로운 전송률 R_k^{lb}와 $\bar{R}_k^{\mathrm{e,lb}}=\mathbb{E}\left[R_k^{\mathrm{e,lb}}\right]$를 정의한다.

$$R_k^{\mathrm{lb}}=\log_2\left(1+\frac{|\hat{\mathbf{h}}_k^{\mathrm{H}}\mathbf{f}_k|^2}{\sum_{i\neq k}^{\mathrm{K}}|\hat{\mathbf{h}}_k^{\mathrm{H}}\mathbf{f}_i|^2+\sum_{i=1}^{\mathrm{K}}\mathbf{f}_i^{\mathrm{H}}\mathbf{\Psi}_k\mathbf{f}_i+\sum_{j=1}^{\mathrm{J}}|\hat{\mathbf{h}}_k^{\mathrm{H}}\boldsymbol{\phi}_j|^2+\sum_{j=1}^{\mathrm{J}}\boldsymbol{\phi}_j^{\mathrm{H}}\mathbf{\Psi}_k\boldsymbol{\phi}_j+\frac{\sigma^2}{\mathrm{P}}}\right)$$

$$\bar{R}_k^{\mathrm{e,lb}}=\frac{1}{M}\sum_{m=1}^{M}\log_2\left(1+\frac{M\mathbf{f}_k^{\mathrm{H}}\mathbf{R}_m^{\mathrm{e}}\mathbf{f}_k}{\sum_{i\neq k}^{\mathrm{K}}\mathbf{f}_i^{\mathrm{H}}\mathbf{R}_m^{\mathrm{e}}\mathbf{f}_i+\sum_{j=1}^{\mathrm{J}}\boldsymbol{\phi}_j^{\mathrm{H}}\mathbf{R}_m^{\mathrm{e}}\boldsymbol{\phi}_j+\frac{\sigma_{\mathrm{e}}^2}{\mathrm{P}}}\right).$$

위의 식은 조건부 평균 전송률, [3]에서의 보조 정리 1, 그리고 Jensen's inequality 를 사용하여 새롭게 정의한 전송률이다. 해당 식을 통해, 부분적인 채널 정보를 활용한 MMF 공정성 문제를 아래와 같이 정의할 수 있다.

$$\underset{\mathbf{F},\mathbf{\Phi}}{maximize}\ \underset{k\,\in\,\mathcal{K}}{min}\left[R_k^{lb}-\bar{R}_k^{\mathrm{e,lb}}\right]^+$$
$$subject\ to\ \sum_{i=1}^{K}\|\mathbf{f}_i\|^2+\sum_{j=1}^{J}\|\boldsymbol{\phi}_j\|^2\leq 1$$

프리코딩과 인공 잡음의 공동 디자인 문제로 형성하기 위해, 프리코딩 벡터 $\mathbf{f}_k$와 인공 잡음 공분산 벡터 $\boldsymbol{\phi}_j$를 $\bar{\mathbf{v}}=\left[\mathbf{f}_1^{\mathrm{T}},\,\mathbf{f}_2^{\mathrm{T}},\ldots,\mathbf{f}_{\mathrm{K}}^{\mathrm{T}},\boldsymbol{\phi}_1^{\mathrm{T}},\boldsymbol{\phi}_2^{\mathrm{T}},\,\ldots,\boldsymbol{\phi}_{\mathrm{J}}^{\mathrm{T}}\right]^{\mathrm{T}}$와 같은 하나의 벡터로 만들어준다. 또한 최대 전송 전력 $\|\bar{\mathbf{v}}\|=1$을 사용하여, 사용자와 도청자의 전송률을 새롭게 정의해 준다.

$$R_k^{\mathrm{lb}}=\log_2\left(\frac{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{A}_k\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{B}_k\bar{\mathbf{v}}}\right),\quad \bar{R}_k^{\mathrm{e,lb}}=\frac{1}{M}\sum_{m=1}^{M}\log_2\left(\frac{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{C}_{m,k}\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{D}_{m,k}\bar{\mathbf{v}}}\right)$$

여기서 $\mathbf{A}_k,\mathbf{B}_k,\mathbf{C}_{m,k},\mathbf{D}_{m,k}$는 아래와 같다.

$$\mathbf{A}_k=\mathbf{I}_{(K+J)}\otimes\left(\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^{\mathrm{H}}+\mathbf{\Psi}_k\right)+\mathbf{I}_{(K+J)}\frac{\sigma^2}{P}$$
$$\mathbf{B}_k=\mathbf{A}_k-\mathrm{diag}\left(\mathbf{e}_k^{(K+J)}\right)\otimes\hat{\mathbf{h}}_k\hat{\mathbf{h}}_k^{\mathrm{H}}$$
$$\mathbf{C}_{m,k}=\mathrm{diag}(1,\ldots,M,\ldots,1)\otimes\boldsymbol{R}_m^{\mathrm{e}}+\mathbf{I}_{(K+J)}\frac{\sigma_{\mathrm{e}}^2}{P}$$
$$\mathbf{D}_{m,k}=\mathbf{C}_{m,k}-\mathrm{diag}\left(\mathbf{e}_k^{(K+J)}\right)\otimes M\boldsymbol{R}_m^{\mathrm{e}}$$

하지만 우리가 정의한 최적화 문제는 non-convex 하고 non-smooth 하다는 문제점을 가지고 있다. 따라서, LogSumExp 기법 $\min_{i=1,\dots,N} \approx -\alpha \log\left(\sum_{i=1}^{N} \exp\left(\frac{x_i}{-\alpha}\right)\right)$을 활용하여 non-smoooth 하다는 문제를 해결하며, 목적 함수를 아래와 같이 새롭게 정의해 준다.

$$\underset{\mathbf{F},\boldsymbol{\Phi}}{maximize} \; -\alpha \log\left(\sum_{k=1}^{K}\left\{\left(\frac{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{A}_{\mathrm{k}}\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{B}_{\mathrm{k}}\bar{\mathbf{v}}}\right)^{-\beta}\cdot\left(\prod_{m=1}^{M}\frac{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{C}_{m,\mathrm{k}}\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{D}_{m,\mathrm{k}}\bar{\mathbf{v}}}\right)^{\frac{\beta}{M}}\right\}\right)$$

여기서 $\beta = \frac{1}{\alpha \log 2}$이다. 새롭게 정의한 목적함수는 여전히 non-convex 하므로, 전역 최적해를 찾는 것이 불가능하다. 따라서 generalized power iteration (GPI) 기법 [4]을 적용하여 최상의 국부 최적해를 도출해낸다. 이를 위해서, $\boldsymbol{L}(\bar{\mathbf{v}})$를 $\bar{\mathbf{v}}$에 대해 미분한 뒤 최적화 조건을 구하면 다음과 같은 형태가 된다. $\boldsymbol{L}(\bar{\mathbf{v}}) = \log \boldsymbol{\lambda}(\bar{\mathbf{v}})$이다.

$$\mathbf{B}_{\mathrm{KKT}}^{-1}(\bar{\mathbf{v}})\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{v}})\bar{\mathbf{v}} = \boldsymbol{\lambda}(\bar{\mathbf{v}})\bar{\mathbf{v}}$$

여기서, $\boldsymbol{\lambda}(\bar{\mathbf{v}}) = \boldsymbol{\lambda}_{\mathrm{num}}(\bar{\mathbf{v}})/\boldsymbol{\lambda}_{\mathrm{den}}(\bar{\mathbf{v}}) = \left(\sum_{k=1}^{K} w_k(\bar{\mathbf{v}})\right)^{-\alpha}$

$$\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{v}}) = \boldsymbol{\lambda}_{\mathrm{num}}(\bar{\mathbf{v}}) \times$$
$$= \sum_{k=1}^{K}\left\{\beta w_k(\bar{\mathbf{v}})\left(\frac{\mathbf{B}_{\mathrm{k}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{B}_{\mathrm{k}}\bar{\mathbf{v}}} + \frac{\sum_{m=1}^{M}\left(w_{m,k}^{e}(\bar{\mathbf{v}})\frac{\mathbf{C}_{m,\mathrm{k}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{C}_{m,\mathrm{k}}\bar{\mathbf{v}}}\left(\prod_{l\neq m}^{M} w_{m,k}^{e}(\bar{\mathbf{v}})\right)\right)}{M\prod_{m=1}^{M} w_{m,k}^{e}(\bar{\mathbf{v}})}\right)\right\}$$

$$\mathbf{B}_{\mathrm{KKT}}(\bar{\mathbf{v}}) = \boldsymbol{\lambda}_{\mathrm{den}}(\bar{\mathbf{v}}) \times$$
$$= \sum_{k=1}^{K}\left\{\beta w_k(\bar{\mathbf{v}})\left(\frac{\mathbf{A}_{\mathrm{k}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{A}_{\mathrm{k}}\bar{\mathbf{v}}} + \frac{\sum_{m=1}^{M}\left(w_{m,k}^{e}(\bar{\mathbf{v}})\frac{\mathbf{D}_{m,\mathrm{k}}}{\bar{\mathbf{v}}^{\mathrm{H}}\mathbf{D}_{m,\mathrm{k}}\bar{\mathbf{v}}}\left(\prod_{l\neq m}^{M} w_{m,k}^{e}(\bar{\mathbf{v}})\right)\right)}{M\prod_{m=1}^{M} w_{m,k}^{e}(\bar{\mathbf{v}})}\right)\right\}$$

위에서 구한 최적화 조건을 고유 벡터 의존 비선형 고유값 문제로 해석하면, $\bar{\mathbf{v}}$와 $\boldsymbol{\lambda}(\bar{\mathbf{v}})$는 각각 고유벡터와 고유값으로 볼 수 있다. 따라서 우리는 GPI 를 사용하여 문제를 해결하도록 아래의 알고리즘을 제안한다:

1) $\bar{\mathbf{v}}_0$를 초기화해준다.
2) t번째 단계에서 $\bar{\mathbf{v}}_t$로, $\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{v}}_t)$와 $\mathbf{B}_{\mathrm{KKT}}(\bar{\mathbf{v}}_t)$를 계산한다.
3) $\bar{\mathbf{v}}_{t+1}$을 $\frac{\mathbf{B}_{\mathrm{KKT}}^{-1}(\bar{\mathbf{v}}_t)\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{v}}_t)\bar{\mathbf{v}}_t}{\left\|\mathbf{B}_{\mathrm{KKT}}^{-1}(\bar{\mathbf{v}}_t)\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{v}}_t)\bar{\mathbf{v}}_t\right\|}$로 업데이트해준다.
4) 2, 3 단계를 $\|\bar{\mathbf{v}}_{t+1} - \bar{\mathbf{v}}_t\| \leq \tau$ 또는 $t > t_{max}$를 만족할 때까지 반복해준다.

시뮬레이션을 통해서, 1) 인공 잡음 없이 공정성을 고려한 GPI 기반 보안 프리코딩 알고리즘 (Secure-MMF), 2) regularized zero-forcing (RZF)와 같은 알고리즘과 최소 보안 전송률을 비교한다.

그림 1 은 안테나 4 개, 도청자 4 명, 사용자는 2 명, 3 명을 각각 가정하였을 때의 결과를 나타낸 것이다. 제안된 알고리즘이 가장 높은 성능을 보이며, 고정된 안테나 수에 따른 고정된 공간 자유도에 의해 유저 수가 적을수록 인공 잡음과 프리코더에 의해 높은 보안 성능을 보이는 것을 알 수 있다.

그림 2 는 안테나 4 개, 사용자 2 명, 신호-대-잡음비 (SNR) 30dB 에 대해 도청자 수를 1 명에서 8 명까지 늘리면서 시뮬레이션을 진행한 결과이다. 공모하는 도청자의 수가 늘어날수록, 다른 알고리즘과 상대적인 차이가 점점 더 커짐을 볼 수 있다.

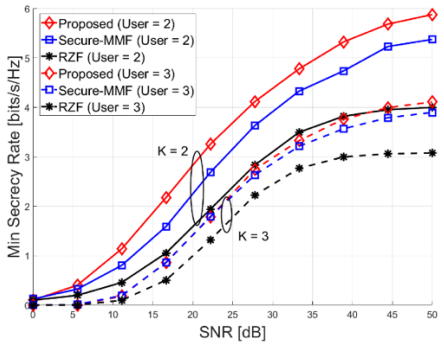

그림 1. 신호-대-잡음비에 대한 최소 보안 전송률

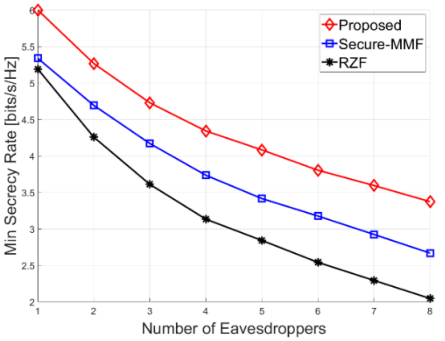

그림 2. 도청자 수에 대한 최소 보안 전송률

Ⅲ. 결 론

본 논문에서는 부분적 채널 정보 하에서 공모하는 도청자들이 존재할 때, 최대-최소 공정성과 보안을 동시에 고려하는 인공 잡음 프리코딩 알고리즘을 제안하였다. 해당 문제 해결을 위해, 조건부 평균 전송률을 사용하여 문제를 접근하고, 비선형 고유값 문제로서 최적화 조건을 도출한 후, GPI 방법을 사용하여 국부 최적해를 찾았다. 시뮬레이션을 통해 제안한 알고리즘이 공정성과 보안을 지키며, 우수한 성능을 보임을 확인하였다. 따라서, 제안한 알고리즘을 통해 무선 통신에서 공정한 통신과 강화된 정보 보안을 제공할 수 있다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단(No. 2021R1C1C1004438)의 지원과, 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업(IITP-2023-RS-2023-00259991)의 지원을 받아 수행된 연구임.

참 고 문 헌

[1] H. Shi, R. V. Prasad, E. Onur, and I. Niemegeers, "Fairness in wireless networks:Issues, measures and challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 5–24, May 2014

[2] 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.

[3] 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.

[4] C. Shen and H. Li, "On the dual formulation of boosting algorithms," *IEEE Trans. on Pattern Anal. and Mach. Intell.*, vol. 32, no. 12, pp. 2216–2231, Mar. 2010.