전송률분할 기반 다중접속 네트워크의 물리계층 보안을 위한 프레임워크

이상민, 최진석
울산과학기술원 전기전자공학과

sangminlee@unist.ac.kr, jinseokchoi@unist.ac.kr

A Framework of Physical Layer Security for Rate-Splitting Multiple Access Networks

Sangmin Lee, Jinseok Choi
Dept. of Electrical Engineering, UNIST

요 약

본 논문은 하향링크 통신 시스템에서 물리계층 보안을 위해 타 유저 및 도청자들로부터 발생하는 손실을 예방하고, 에르고딕 스펙트럼 효율(ergodic spectral efficiency, ergodic SE)을 극대화하는 전송률분할(Rate-Splitting, RS) 프리코딩 알고리즘을 제안한다. 해당 알고리즘은 앞으로의 무선통신에서 필수적일 보안을 신경 씀과 동시에, 높은 효율을 보여주는 고신뢰, 고효율 알고리즘이라는 점에 의의가 있다.

Ⅰ. 서 론

전송률분할 방법은 무선통신 다중안테나(MIMO) 시스템에서 sum SE 에 대한 상당한 이득과 공간적 자유도를 얻을 수 있는 전망있는 물리계층 방법이다[1]. 그렇지만 5G, 더욱이 6G 가 주목받고 있는 상황에서, 저지연, 고효율, 고신뢰 등 고려해야만하는 영역은 더욱 커지고 있다. 따라서 앞으로의 무선통신 분야 발전을 위해서는 해당 영역들을 긴밀하게 고려하는 방법을 구현하는 것이 필수적이며, 추후 우리가 해결해야하는 과제이다.

기존 프리코딩 기법들 즉 maximum ratio transmission (MRT), zero forcing (ZF) 등에 국한되어 있는 이전 연구들과는 다르게, 본 논문에서는 sum SE 를 극대화하는 동시에 도청을 고려하여 보안에까지 강인한 새로운 고효율 및 고신뢰 프리코딩 기법을 제안한다.

Ⅱ. 본 론

본 논문에서는 하향링크 통신 시스템을 고려하며, 전체 K명 유저는 도청을 고려해야하는 S명의 '보안 유저'와, 도청을 신경 쓰지 않는 M명의 '일반 유저'로 이루어진다. 이와 별개로 보안 유저의 메시지를 들으려는 E명의 도청자가 존재하며, 보안 유저들은 자신을 제외한 모든 사람들($K-1+E$ 명)에게 도청을 당하면 안된다고 가정한다. 여기서 각 유저들은 하나의 안테나를, Access Point (AP)는 N개의 안테나를 가지고 있다.

프리코딩된 전송 신호벡터 $\mathbf{x}=\mathbf{f}_{\mathrm{c}}s_{\mathrm{c}}+\sum_{i=1}^{K}\mathbf{f}_i s_i$ 이며, 여기서 $s_{\mathrm{c}}\in\mathbb{C}^N$와 $s_i\in\mathbb{C}^N$는 각각 공통 부분과 개인 부분에 해당하는 심볼을 의미하고, $\mathbf{f}_{\mathrm{c}}\in\mathbb{C}^N$와 $\mathbf{f}_i\in\mathbb{C}^N$는 각 심볼에 해당하는 프리코더를 의미하고, 한다. 공통 메시지는 모든 유저들에게 해독가능해야 하기 때문에 전체 K명 유저가 해독가능하게 설정되어야 하고, 모든 유저는 공통 메시지를 해독한 이후에 각 유저의 개인 메시지를 해독한다. AP 와 유저들간 채널 매트릭스를 $\mathbf{H}\in\mathbb{C}^{N\times K}$라 정의하고 송신 단자에서 해당 채널을 완벽하게 알고 있다고 가정한다(perfect Channel State Information at Transmitter, perfect CSIT). $\mathbf{h}_k$를 매트릭스 $\mathbf{H}$ 의 k번째 열이라고 할 때, k번째 유저가 받는 Baseband 신호는 다음과 같다:

$$y_k=\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_{\mathrm{c}}s_{\mathrm{c}}+\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k s_k+\sum_{l=1,l\neq k}^{K}\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_l s_l+z_k$$

여기서 $z_k\sim\mathcal{CN}(0,\sigma^2)$는 AWGN 이다.

우리는 에르고딕 스펙트럼 효율에 관심이 있고, 기댓값은 다중 채널 페이딩 블록에 대해 이루어진다. 받은 신호 y_k를 기반으로 공통 메시지 SE와 k번째 유저에 대한 SE는 각각 다음과 같이 정의된다.

$$R_{\mathrm{c}}=\min_{k\in\mathcal{K}}\left\{\mathbb{E}\left[\log_2\left(1+\frac{\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_{\mathrm{c}}\right|^2}{\sum_{i=1}^{K}\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i\right|^2+\frac{\sigma^2}{P}}\right)\right]\right\}$$

$$R_k=\mathbb{E}\left[\log_2\left(1+\frac{\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k\right|^2}{\sum_{i=1,i\neq k}^{K}\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i\right|^2+\frac{\sigma^2}{P}}\right)\right]$$

추가적으로, 보안을 고려하기위해 보안 유저에 대한 손실 $R_l^{(s)}$를 정의할 필요가 있으며, 손실은 보안 유저 본인을 제외한 $K-1$명의 유저로부터 발생한 $R_u^{(s)}$와 E명의 도청자로부터 발생한 $R_{\mathrm{e}}^{(s)}$로 나누어진다.

$$R_u^{(s)}=\mathbb{E}\left[\log_2\left(1+\frac{\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_k\right|^2}{\sum_{i=1,i\neq k}^{K}\left|\mathbf{h}_k^{\mathrm{H}}\mathbf{f}_i\right|^2+\frac{\sigma^2}{P}}\right)\right]$$

$$R_e^{(s)}=\mathbb{E}\left[\log_2\left(1+\frac{\left|\mathbf{g}_{\mathrm{e}}^{\mathrm{H}}\mathbf{f}_s\right|^2}{\left|\mathbf{g}_{\mathrm{e}}^{\mathrm{H}}\mathbf{f}_{\mathrm{c}}\right|^2+\sum_{i=1,i\neq s}^{K}\left|\mathbf{g}_{\mathrm{e}}^{\mathrm{H}}\mathbf{f}_i\right|^2+\frac{\sigma^2}{P}}\right)\right]$$

위 식에서 $\mathbf{g}_{\mathrm{e}}$ 는 도청자 e 의 채널을 의미한다. 정의한 $R_l^{(s)}$의 여러 값 중 최대값을 고려할 때, 효과적으로 보안을 고려한 알고리즘이 되기 때문에 최종 손실에 해당하는 값 $R^{(s)}=\max_{l\in\mathcal{L}}R_l^{(s)}$이다.

최종적으로, 정의된 SE 와 파워 제약조건을 기반으로 최적화 문제를 다음과 같이 수식화 할 수 있다.

$$\underset{\mathbf{f}_{\mathrm{c}},\mathbf{f}_1,\ldots,\mathbf{f}_K}{\text{maximize}}\ R_c+\sum_{s\in\mathcal{S}}\left[R_s-R^{(s)}\right]^{+}+\sum_{m\in\mathcal{M}}R_m$$

$$\text{subject to}\ \|\mathbf{f}_{\mathrm{c}}\|^2+\sum_{k=1}^{K}\|\mathbf{f}_k\|^2\leq 1.$$

알고리즘 1: Proposed Sum SE Maximization Algorithm

1. **initialize**: $\bar{\mathbf{f}}_0$
2. Set the iteration count $t = 0$
3. **while** $\|\bar{\mathbf{f}}_{t+1} - \bar{\mathbf{f}}_t\| > \epsilon \,\&\, t \le t_{\max}$ **do**
4. Build $\mathbf{A}_{\mathrm{KKT}}$ and $\mathbf{B}_{\mathrm{KKT}}$
5. Compute $\bar{\mathbf{f}}_{t+1} = \mathbf{B}_{\mathrm{KKT}}(\bar{\mathbf{f}}_t)^{-1}\mathbf{A}_{\mathrm{KKT}}(\bar{\mathbf{f}}_t)\bar{\mathbf{f}}_t$
6. Normalize $\bar{\mathbf{f}}^{(t)} = \bar{\mathbf{f}}^{(t)} / \|\bar{\mathbf{f}}^{(t)}\|$
7. Update $t = t + 1$
8. **return** $\bar{\mathbf{f}}_t$

해당 최적화 문제는 max function 과 min function 내부에 기댓값이 존재하기 때문에 문제를 풀기 쉽지 않다. 따라서 $\min\{\mathbb{E}[R]\} \ge \mathbb{E}[\min\{R\}]$와 $\max\{\mathbb{E}[R]\} \le \mathbb{E}[\max\{R\}]$ 성질을 이용하여 lower-bound 값을 취해준다. 최종적으로 해당 문제는 다음과 같은 형태가 된다.

$$\underset{\mathbf{f}_c,\mathbf{f}_1,\ldots,\mathbf{f}_K}{\text{maximize}}\ \mathbb{E}\left[\bar{R}_c + \sum_{s\in\mathcal{S}}\left[\bar{R}_s - \bar{R}^{(s)}\right]^+ + \sum_{m\in\mathcal{M}}\bar{R}_m\right]$$

$$\text{subject to } \|\mathbf{f}_c\|^2 + \sum_{k=1}^{K}\|\mathbf{f}_k\|^2 \le 1.$$

따라서 우리는 기댓값 안에 있는 항을 최대화하는 문제로 치환이 가능하다.

새롭게 정의한 최적화 문제를 풀 수 있는 형태로 바꾸기 위해, 우리는 generalized power iteration (GPI) 방법을 쓴다[2]. 우선 프리코딩 벡터들을 쌓아서 높은 차원의 프리코딩 벡터 $\bar{\mathbf{f}}$를 다음과 같이 만든다.

$$\bar{\mathbf{f}} = \left[\mathbf{f}_C^{\mathsf{T}}, \mathbf{f}_1^{\mathsf{T}}, \ldots, \mathbf{f}_k^{\mathsf{T}}\right]^{\mathsf{T}} \in \mathbb{C}^{N(K+1)\times 1}$$

해당 벡터를 이용하면 앞에서 정의한 각 전송률을 $\log_2\left(\frac{\bar{\mathbf{f}}^{\mathrm{H}}\mathbf{A}\bar{\mathbf{f}}}{\bar{\mathbf{f}}^{\mathrm{H}}\mathbf{B}\bar{\mathbf{f}}}\right)$ 형태로 표현이 가능하며, max function 과 min function 의 non-smooth 성질로 인한 어려움을 해결하기 위해 logsumexp method 를 적용하여 각각의 근사값을 다음과 같이 구할 수 있다[3].

$$\min_{i=1,\ldots,N}\{x_i\} \approx -\alpha\log\left(\sum_{i=1}^{N}\exp\left(\frac{x_i}{-\alpha}\right)\right)$$

$$\max_{i=1,\ldots,N}\{x_i\} \approx \alpha\log\left(\sum_{i=1}^{N}\exp\left(\frac{x_i}{\alpha}\right)\right)$$

목적함수를 $\mathcal{L} = \log_2\lambda(\bar{\mathbf{f}})$라 새롭게 정의하고, 해당 목적함수는 비볼록(non-convex)하기에 전역 최적해를 찾을 수 없다. 따라서 우리는 GPI 기법을 통해 국부적 최적해(sub-optimal solution)를 찾는 것을 목적으로 한다.

목적함수를 $\bar{\mathbf{f}}$에 대해 일계 편미분하여 최적화 조건을 구하면 다음 수식이 유도된다.

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

이 수식은 위의 조건을 만족하는 $\bar{\mathbf{f}}$에 대해 $\mathbf{B}_{\mathrm{KKT}}^{-1}\mathbf{A}_{\mathrm{KKT}}$ 행렬의 고유값 문제로 볼 수 있으며, $\bar{\mathbf{f}}$와 $\lambda(\bar{\mathbf{f}})$는 각각 고유벡터와 고유값으로 해석될 수 있다. 따라서 GPI 를 기반으로 $\lambda(\bar{\mathbf{f}})$를 최대화하는 $\bar{\mathbf{f}}$를 반복적으로 찾는다. 해당 알고리즘은 $\bar{\mathbf{f}}_{t+1}$와 $\bar{\mathbf{f}}_t$의 차가 ϵ보다 크거나, 사전에 할당한 iteration 횟수보다 작을 때 계속 반복된다.

$\mathbf{h}_k$는 k유저의 공간 공분산 행렬 $\mathbf{R}_k = \mathbb{E}[\mathbf{h}_k\mathbf{h}_k^{\mathrm{H}}]$에 의해 계산되고, 우리는 시뮬레이션에서 $\mathbf{R}_k$를 생성하기 위해 one-ring channel model 을 채택한다[4], [5]. AP 는 6 개의 안테나를 가지고 보안 유저 2 명과 일반 유저 2 명으로 이루어진 총 4 명의 유저들에게 프리코딩 된 신호를 보내며, 그와는 별개로 2 명의 도청자가 존재한다. $\sigma = 1$, $\epsilon = 0.01, t_{\max} = 100$으로 세팅했고, 100 회 시행하여 편차를 줄였다. 성능 평가를 위해 다음의 알고리즘들과 함께 시뮬레이션 한다: (1) 제안된 알고리즘, (2) 기존 GPI 알고리즘, (3) RZF, (4) ZF, (5) MRT.

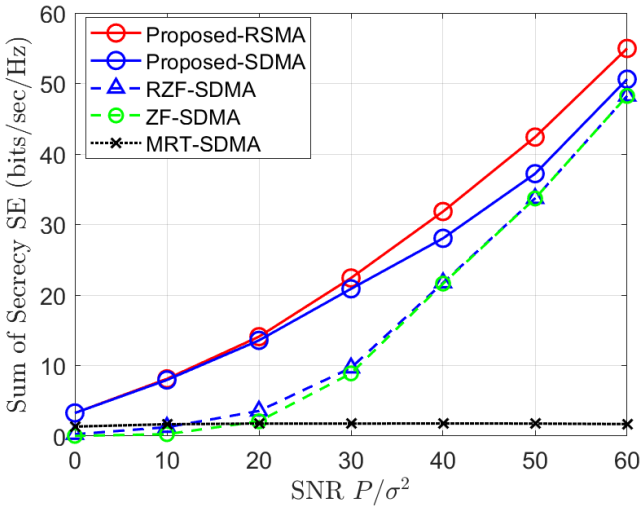

그림 1. Sum SE 대 SNR(P/σ^2)

그림 1 은 파워 제약 P가 변함에 따라 변화하는 Sum SE 에 대한 성능을 보여주며, 기존에 제시되었던 기존방법보다 본 논문에서 제안된 알고리즘이 모든 구간에서 우수한 성능을 지니고 있음을 시사한다.

Ⅲ. 결 론

본 논문에서는 하향링크 통신 시스템에서 보안과 스펙트럼 효율을 극대화하는 고효율, 고신뢰 프리코딩 기법을 제안하였다. 구체적으로, 기존의 최적화 문제를 풀 수 있는 형태로 만들기 위해 logsumexp 을 통해 근사하였고, GPI 기법을 통해 해당 문제를 풀었다. 제안된 알고리즘은 모든 SNR 구간에서 기존에 존재하던 다른 알고리즘보다 Sum SE 성능이 우수함을 보여준다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단(No. 2021R1C1C1004438)의 지원을 받아 수행된 연구임.

참 고 문 헌

[1] Clerckx, Bruno, et al. "Rate splitting for MIMO wireless networks: A promising PHY-layer strategy for LTE evolution," *IEEE Commun. Mag.* 54.5 (2016): 98-105.

[2] Choi, Jiwook, et al. "Joint user selection, power allocation, and precoding design with imperfect CSIT for multi-cell MU-MIMO downlink systems." *IEEE Trans. on Wireless Commun.* 19.1 (2019): 162-176.

[3] Shen, Chunhua, and Hanxi Li. "On the dual formulation of boosting algorithms." *IEEE Trans. on Pattern Analysis and Machine Intelligence* 32.12 (2010): 2216-2231.

[4] Adhikary, Ansuman, et al. "Joint spatial division and multiplexing—The large-scale array regime." *IEEE Trans. on Inform. Theory* 59.10 (2013): 6441-6463.

[5] J. Choi, J. Park, and N. Lee. "Energy Efficiency Maximization Precoding for Quantized Massive MIMO Systems." *IEEE Trans. on Wireless Commun.*, vol. 21, no. 9, pp. 6803 - 6817, Sep. 2022