

채널 추정 오류가 있는 비직교 다중 접속 시스템을 위한 신경망 기반 보안 빔형성

이진영, 하정석

한국과학기술원

jylee120@kaist.ac.kr, jsha@kaist.edu

Neural Network based Secure Beamforming for NOMA with Channel Estimation Error

Jinyoung Lee, Jeongseok Ha

Korea Advanced Institute of Science and Technology

요약

본 논문에서는 보안 비직교 다중 접속을 위한 빔형성 설계에 관해 연구한다. 보안 비직교 다중 접속 시스템에서의 빔형성 방식을 찾는 문제는 수학적, 수치적으로 풀기 매우 어렵다. 따라서 본 논문에서는 신경망을 이용하여 비직교 다중 접속에서 적합한 보안 빔형성 설계방식을 제안하고, 채널 추정 오류가 있는 상황에서 비직교 다중 접속 시스템의 보안 전송률을 성능에 대해 실험한다.

I. 서 론

비직교 다중 접속은 Toward 6G를 위한 유망 기술 중 하나로써 최근 활발히 연구되고 있는 기술 중 하나이다 [1]. 비직교 다중 접속의 핵심은 기존의 다중화 방식과 손쉽게 결합할 수 있는 전력 계층에서의 다중화 방식으로 기존 직교 다중 접속에 비해 스펙트럼 효율을 증대시킬 수 있다는 것이다. 하지만, 무선 매체를 통해 전달하는 무선 통신의 특성으로 인하여 도청에 취약하다는 약점이 존재한다. 따라서, 비직교 다중 접속 시스템에서의 보안문제에 대해 많은 연구가 진행되고 있는 중이다 [2], [3].

순차적 간섭 제거 방식을 사용하는 비직교 다중 접속 방식에서 보안성 증대를 위한 빔형성 방식을 찾는 것은 수학적, 수치적으로 매우 어렵다. 따라서 본 논문에서는 비직교 다중 접속 방식에서 채널 추정 오류에 강인 보안 빔형성 방식을 찾기 위해 신경망을 이용한 빔형성 설계 방식을 제안하고 채널 추정 오류에 따른 보안 전송률에 대해 실험한다. 시뮬레이션 결과를 통해, 제안하는 빔형성 방식을 사용할 경우 채널 추정 오류에 따른 보안 전송률의 성능을 알 수 있다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서는 시스템 모델을 소개하고 3장에서 비직교 다중 접속 방식에서 신경망 기반의 보안 빔형성 방식을 제안한다. 4장에서 제안하는 빔형성에 따른 채널 추정 오류에 따른 보안 전송률을 실험한 후 마지막으로 5장에서 결론을 맺는다.

II. 시스템 모델

본 논문에서는 단일 셀 네트워크에서 N 개의 안테나를 가진 기지국과 단일 안테나를 가진 2명의 적법 사용자, 1명의 도청자가 존재하는 하향 비직교 다중 접속을 고려한다. 기지국과 사용자를 사이의 채널은 $\mathbf{h}_m = d_m^{-\alpha/2} \mathbf{g}_m$, 기지국과 도청자 사이의 채널은 $\mathbf{h}_e = d_e^{-\alpha/2} \mathbf{g}_e$ 으로 나타낸다. 또한, 사용자의 순서는 채널 이득이 상대적으로 작은 사용자는 1번, 큰 사용자는 2번으로 나타낸다, $0 < \|\mathbf{h}_1\|^2 < \|\mathbf{h}_2\|^2$. 불완전 채널 추정을 모형화하기 위해서, 적법 사용자들이 추정한 채널을 다음과 같이 나타낸다.

$$\hat{\mathbf{h}}_m = \mathbf{h}_m + \mathbf{h}_m^{err}$$

여기서 \mathbf{h}_m^{err} 은 채널 추정 오류를 나타낸다. 따라서, 적법사용자와 도청자에 대한 $N \times N$ 채널 공분산은 각각 \mathbf{R}_m 와 \mathbf{R}_e 로 나타낸다. 본 논문에서는 적법 사용자들은 $\hat{\mathbf{h}}_m$ 을 알고 있고, 기지국은 도청자 채널에 대한 통계적 특성만을 알고 있다고 가정한다.

하향링크에서 기지국이 사용자들에게 전송하는 신호 벡터는 다음과 같다.

$$\mathbf{s} = \mathbf{v}_1 s_1 + \mathbf{v}_2 s_2 + \mathbf{V}_N s_N$$

여기서 \mathbf{v}_m 와 s_m 은 각각 $m \in \{1,2\}$ 번 사용자의 신호에 대한 빔형성 벡터와 전송 메시지를 의미한다. 또한, \mathbf{V}_N 와 s_N 은 각각 인공 잡음 행렬과 인공 잡음 신호를 나타낸다. 위와 같이 기지국이 보낸 신호를 사용자 m 이 수신하는 신호는 다음과 같다.

$$y_m = \mathbf{h}_m \mathbf{s} + n_m = \hat{\mathbf{h}}_m \mathbf{s} - \mathbf{h}_m^{err} \mathbf{s} + n_m$$

여기서 $n_m \sim (0, \sigma_m^2)$ 은 m 번째 사용자의 백색 가우시안 잡음을 나타낸다. 비직교 다중 접속에서 사용자들은 수신 신호를 복호하기 위해 순차적 간섭 제거 방식을 사용한다. 이때 m 번 적법 사용자에서 달성 가능한 데이터 전송률은 아래 수식들과 같다.

$$R_1 = \min \left[\log_2 \left(1 + \frac{|\hat{\mathbf{h}}_1 \mathbf{v}_1|^2}{|\hat{\mathbf{h}}_1 \mathbf{v}_2|^2 + \hat{\mathbf{h}}_1 \mathbf{V}_N (\hat{\mathbf{h}}_1 \mathbf{V}_N)^H + \mathbf{h}_1^{err} (\mathbf{v}_1 \mathbf{v}_1^H + \mathbf{v}_2 \mathbf{v}_2^H + \mathbf{V}_N \mathbf{V}_N^H) \mathbf{h}_1^{errH} + \sigma_1^2} \right), \log_2 \left(1 + \frac{|\hat{\mathbf{h}}_2 \mathbf{v}_1|^2}{|\hat{\mathbf{h}}_2 \mathbf{v}_2|^2 + \hat{\mathbf{h}}_2 \mathbf{V}_N (\hat{\mathbf{h}}_2 \mathbf{V}_N)^H + \mathbf{h}_2^{err} (\mathbf{v}_1 \mathbf{v}_1^H + \mathbf{v}_2 \mathbf{v}_2^H + \mathbf{V}_N \mathbf{V}_N^H) \mathbf{h}_2^{errH} + \sigma_2^2} \right) \right]$$
$$R_2 = \log_2 \left(1 + \frac{|\hat{\mathbf{h}}_2 \mathbf{v}_2|^2}{\hat{\mathbf{h}}_2 \mathbf{V}_N (\hat{\mathbf{h}}_2 \mathbf{V}_N)^H + \mathbf{h}_2^{err} (\mathbf{v}_1 \mathbf{v}_1^H + \mathbf{v}_2 \mathbf{v}_2^H + \mathbf{V}_N \mathbf{V}_N^H) \mathbf{h}_2^{errH} + \sigma_2^2} \right)$$

도청자가 획득하는 m 번 적법 사용자 데이터에 대한 정보량은 다음과 같다.

$$R_{e,1} = \log_2 \left(1 + \frac{|\mathbf{h}_e \mathbf{v}_1|^2}{|\mathbf{h}_e \mathbf{v}_2|^2 + \mathbf{h}_e \mathbf{V}_N (\mathbf{h}_e \mathbf{V}_N)^H + \sigma_e^2} \right)$$
$$R_{e,2} = \log_2 \left(1 + \frac{|\mathbf{h}_e \mathbf{v}_2|^2}{\mathbf{h}_e \mathbf{V}_N (\mathbf{h}_e \mathbf{V}_N)^H + \sigma_e^2} \right)$$

III. 비직교 다중 접속 방식에서 신경망 기반의 범형성 방식

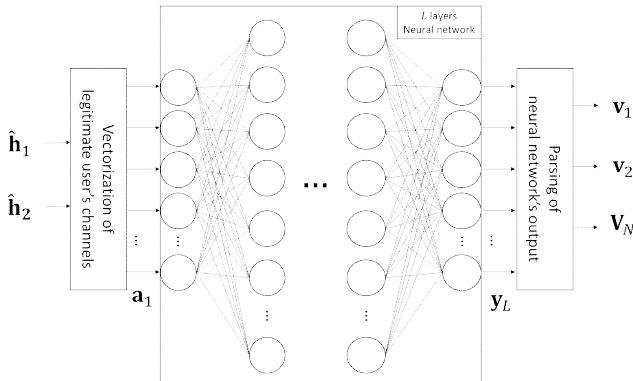


그림 1 제안하는 신경망 기반 범형성 방식의 구조

본 논문에서는 비직교 다중 접속 시스템을 위한 최적의 범형성 방식을 찾기 위해서 그림 1과 같이 완전 연결 신경망 형태의 신경망을 제안한다. 신경망의 입력은 비직교 다중 접속 시스템에서 사용자들의 채널 (\hat{h}_1, \hat{h}_2)이고 출력은 각 사용자에 대한 범형성 벡터 (v_1, v_2, V_N)이다. 전체 L 개의 은닉층으로 구성된 신경망으로 각 l 번째 은닉층의 출력 y_l 은 다음과 같다.

$$y_l = \psi_l(\mathbf{W}_l \mathbf{a}_l + \mathbf{b}_l), l \in \{1, \dots, L\}$$

여기서 \mathbf{a}_l 와 $\psi_l(\cdot)$ 은 각각 l 번째 은닉층의 입력과 활성화 함수를 나타낸다. 마지막으로, 제안하는 신경망의 출력은 다음과 같이 나타낸다.

$$\mathbf{y}_L = \psi_L(\mathbf{W}_L \cdots \psi_1(\mathbf{W}_1 \mathbf{a}_1 + \mathbf{b}_1) + \mathbf{b}_L)$$

여기서 $\mathbf{y}_L = [\mathbf{v}_1^T, \mathbf{v}_2^T, \mathbf{V}_N^T]^T$ 는 사용자의 전력 계수로 구성된 신경망의 출력이다. 신경망을 훈련하기 위해서, 손실 함수를 다음과 같이 정의한다.

$$\mathcal{J}(\mathbf{v}_1, \mathbf{v}_2, \mathbf{V}_N; \Omega) = -(E[R_1 - R_{e,1}]) + (E[R_2 - R_{e,2}])$$

여기서 Ω 는 신경망의 가중치, 바이어스들의 집합을 의미한다. 집합 Ω 의 파라미터들은 손실 함수 $\mathcal{J}(\cdot)$ 가 최소화되는 방향으로 갱신한다..

IV. 실험

신경망 기반의 보안 범형성 방식에 대한 실험을 위해 적법 사용자들과 도청자의 페이딩 채널은 랜덤 분포를 따르고 손실계수 $\alpha = 2$ 로 설정한다. 또한, 안테나 수, N , 는 4, 은닉층 수, L , 은 5로 설정한다. 은닉층의 활성화 함수로 eLU (exponential linear unit)를 사용하고 각 은닉층의 크기는 $2N \times (N+2)$ 로 설정하였다. 제안하는 신경망 방식은 0.001의 학습 비율로 10^4 훈련 표본을 사용하여 확률적 경사 하강법 (stochastic gradient descent: SGD) 방식으로 10 epochs 동안 훈련한다. 또한, 10^3 테스트 표본을 이용하여 성능을 측정한다.

그림 2는 채널 추정 오류에 따른 제안하는 딥러닝 기반 보안 범형성 방식과 기존의 직교 다중 접속 방식에서의 보안 전송률을 보여준다. 신호 대 잡음비는 10dB, 기지국과 적법 사용자들과 도청자 사이의 거리는 $d_1 = 1$, $d_2 = 0.5$, $d_e = 0.2$ 로 설정한다. 또한, 채널 추정 오류에 대한 변수를 $\tau \in [0, 1]$ 로 설정하고 $\hat{\mathbf{h}}_m$ 과 \mathbf{h}_e 의 공분산은 각각 $(1 - \tau)\mathbf{R}_m$ 과 \mathbf{R}_e 로 설정한다.

그림 2에서 확인할 수 있듯이 제안한 범형성 방식을 사용할 경우, 채널 추정 오류가 증가함에 따라 성능이 감소함을 알 수 있다. 왜냐하면 \mathbf{v}_1 을

설계하는 경우 R_1 의 정의에 따라 두 사용자 채널의 오류에 모두 영향을 받기 때문에 두 명의 적법 사용자의 채널에 대한 SINR 사이의 최소값으로 정의되는 R_1 이 급감한다. 따라서 채널 추정 오류율에 따라 보안 전송율의 합이 감소한다.

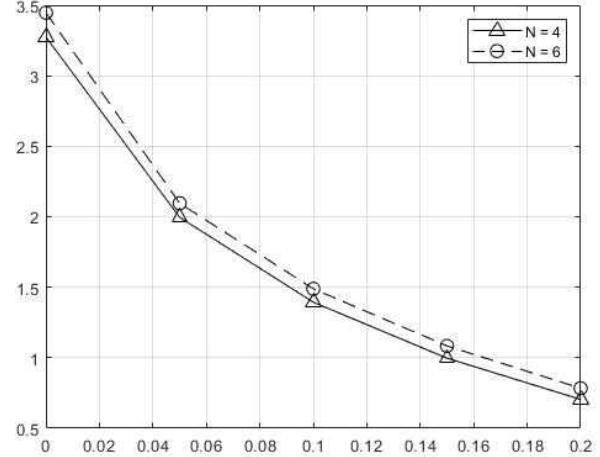


그림 2 채널 추정 오류율에 따른 보안 전송률 합

V. 결론

본 논문에서는 기존의 수학적, 수치적으로 풀기 어려운 비직교 다중 접속 시스템에서의 보안 범형성 설계 문제를 완전 연결 신경망 기반의 딥러닝 방식으로 해결하였다. 신경망 기반의 비직교 다중 접속 시스템을 위한 보안 범형성 설계 방식을 제안하여 채널 추정 오류가 있는 상황에서 보안 전송률의 성능을 실험을 통해 확인하였다. 이후, 직교 시스템에서의 최적의 기법과 기존 비직교 다중 접속 시스템에서의 최신 기법들의 채널 추정 오류에 따른 보안 전송률 성능을 제안하는 기법과 비교할 예정이다.

ACKNOWLEDGEMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업의 연구결과로 수행되었음 (2019-0-01573)

참 고 문 헌

- [1] Z. Ding et al., "Application of Non-Orthogonal Multiple Access in LTE and 5G Networks," in *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185–191, Feb. 2017.
- [2] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao and L. Hanzo, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
- [3] L. Lv, Z. Ding, Q. Ni and J. Chen, "Secure MISO-NOMA Transmission With Artificial Noise," in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6700–6705, Jul. 2018.