Cell-Free 통신 시스템에서 물리계층보안을 위한 기계학습 기반 비직교 다중 접속

강민정, 이정훈, 이일구*
한국외국어대학교 전자공학과 및 응용통신연구센터, 성신여자대학교 미래융합기술공학과*
{love_minmin926, tantheta}@hufs.ac.kr, *iglee@sungshin.ac.kr

Machine Learning-Based NOMA for Physical Layer Security in Cell-Free Communication Systems

Min Jeong Kang, Jung Hoon Lee, and Il-Gu Lee*
Department of Electronics Engineering and Applied Communications Research Center,
Hankuk University of Foreign studies,
*Department of Future Convergence Technology Engineering, Sungshin Women's University

요 약

본 논문에서는 다수의 액세스 포인트 (access point, AP)로 구성된 cell-free 통신 시스템에서 기계학습 기반 비직교 다중 접속(nonorthogonal multiple access, NOMA) 기법을 활용하여 물리계층보안을 향상시키는 방법에 대해 연구한다. 다수의 액세스 포인트와 다수의 유저가 존재할 경우, 총 보안 전송률을 최대화하는 최적의 액세스 포인트와 복호 순서 조합 찾는 과정은 높은 계산 복잡도가 요구된다. 따라서 본 논문에서는 총 보안 전송률을 최대화하는 최적의 서비스 조합을 구하는 과정에 기계학습 모델을 활용하여 복잡도를 감소시킨 서비스 조합 결정 기법을 제안한다.

Ⅰ. 서론

무선으로 송수신이 이루어지는 무선통신시스템 특성상 무선통신시스템에서는 도청자와 신뢰할 수 없는 유저로 인해 여러가지 보안문제가 발생한다. 이에 따라, 현재 다양한 기법들을 활용하여 보안문제를 해결하기 위한 연구가 활발히 이루어지고 있다. 특히, 높은 주파수 효율을 가져 무선통신시스템에서 주목받고 있는 기술 중 하나인 비직교 다중 접속(nonorthogonal multiple access, NOMA) 기술에서는 총 보안 전송률을 높이기 위해 복호 순서와 전력 할당 기법을 활용하는 연구가 활발히 이루어지고 있다.[1] 그러나 유저수가 증가할수록 총 보안 전송률을 최대화하는 최적의 복호 순서를 찾는 과정의 계산 복잡도가 높아져 찾기 쉽지 않다.

본 논문에서는 다수의 액세스 포인트(access point, AP)로 구성된 cell-free 통신 시스템에서 신뢰할 수 없는 유저가 존재할 때, 기계학습 모델을 활용하여 낮은 복잡도로 총 보안 전송률을 최대화하는 최적의 AP 와 복호 순서 조합을 찾는 기법을 제안한다. 이때 제안하는 기법의 성능은 제안하는 기계학습 모델을 사용하여 구한 최적의 조합으로부터 얻는 총 보안 전송률과 반복적인 계산을 통해 구한 최적의 조합으로부터 얻는 총 보안 전송률을 비교하여 평가한다.

Ⅱ. 본론

① 시스템 모델

본 논문에서 고려하는 시스템 모델은 그림 1 에 나타나 있다. 총 $Q(=3)$ 개의 AP 들이 서로 다른 위치에 존재하며, 각 AP 들은 하나의 중앙처리장치(central processing unit, CPU)에 연결되어 있다. 이때, CPU 는 전체 AP 중 서비스할 AP 를 선택하는 역할을 수행한다. 합법적인 총 $K(=2)$명의 유저와 신뢰할 수 없는 한 명의 유저(Un) 모두 각각 하나의 안테나를 가지며, AP 는 합법적인 유저에게만 서비스한다고 가정한다.

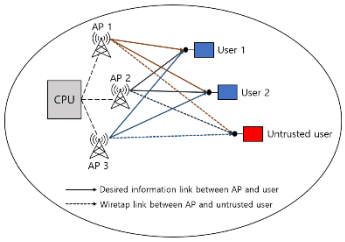

그림 1. 시스템 모델

따라서 q번째 AP 가 NOMA 를 사용하여 서비스할 때, k번째 유저의 수신 신호 $y_{(q,k)}^{\mathrm{NOMA}}$는 다음과 같다.

$$y_{(q,k)}^{\mathrm{NOMA}} = \mathrm{h}_{(q,k)} x_{(q,k)} + \mathrm{n}_{(q,k)}, \quad (1)$$

여기서 $\mathrm{h}_{(q,k)} \in \mathbb{C}^{1\times 1}$는 q번째 AP 와 k번째 유저 사이의 채널을 의미한다. 이때 각 유저들의 채널 이득은 $|\mathrm{h}_{(q,1)}|^2 \geq |\mathrm{h}_{(q,2)}|^2 \geq |\mathrm{h}_{(q,\mathrm{Un})}|^2$ 을 만족한다고 가정한다. 그리고 $n_{(q,k)} \sim \mathcal{CN}(0,1)$ 는 q 번째 AP 와 k 번째 유저 사이에 존재하는 평균이 0 이고 분산이 1 인 백색 가우시안 노이즈를 의미한다. 또한 $x_{(q,k)} \in \mathbb{C}^{1\times 1}$ 는 q번째 AP 가 NOMA 를 사용하여 서비스할 때 k번째 유저의 신호를 의미하며 다음과 같다.

$$x_{(q,k)} = \sum_{i=1}^{K} \sqrt{p_{(q,i)}^{\mathrm{NOMA}}}\, \mathrm{s}_i, \quad (2)$$

여기서 $p_{(q,i)}^{\mathrm{NOMA}}$ 와 s_i 는 각각 q 번째 AP 가 NOMA 로 서비스할 때의 i번째 유저의 전력과 i번째 유저의 신호를 의미한다. 이때 각 AP 의 전체 전력 P가 제한적이라고 가정하므로 $\sum_{i=1}^{K} p_{(q,i)}^{\mathrm{NOMA}} \leq P$를 만족한다.

본 논문에서 고려하는 시스템에서는 CPU 가 하나의 AP 를 선택하고, 해당 AP 로 모든 합법적인 유저에게 NOMA 를 사용하여 동시에 서비스한다고 가정한다. 그러나 고려하는 시스템에서 각 AP 들은 동일한 유저에 대해서 서로 다른 채널 이득을 가지므로 각각의 AP 가 직교 다중 접속(orthogonal multiple access, OMA)를

사용하여 서로 다른 유저에게 동시에 서비스하는 것이 NOMA 로 서비스하는 기존의 방법보다 좋은 성능을 도출해낼 수 있다는 가능성이 있다.[2] 따라서 고려하는 시스템에서는 OMA 로 서비스하는 방법도 함께 고려한다. 그러므로 q번째 AP 가 OMA 를 사용하여 서비스할 때, k번째 유저의 수신 신호 $y_{(q,k)}^{\mathrm{OMA}}$는 다음과 같다.

$$y_{(q,k)}^{\mathrm{OMA}} = \mathrm{h}_{(q,k)} s_i + \mathrm{n}_{(q,k)}. \quad (3)$$

이때, NOMA 또는 OMA 로 서비스하는 AP 는 각 합법적인 유저의 신호 대 간섭 잡음비(signal-to-interference plus-noise power ratio, SINR)가 γ 를 만족하도록 서비스한다고 가정한다. 그러므로 q 번째 AP 를 사용하여 k번째 유저에게 NOMA 로 서비스할 때, 신뢰할 수 없는 유저(Un)의 SINR 은 다음과 같다.

$$SINR_{(q,\mathrm{Un})}^{\mathrm{NOMA}} = \frac{p_{(q,k)}^{\mathrm{NOMA}} |\mathrm{h}_{(q,\mathrm{Un})}|^2}{\sum_{i=1}^{k-1} p_{(q,i)}^{\mathrm{NOMA}} |\mathrm{h}_{(q,\mathrm{Un})}|^2 + 1}. \quad (4)$$

또한 $Q[k]$가 k번째 유저에게 OMA 로 서비스한 AP 를 의미할 때, 신뢰할 수 없는 유저(Un)의 SINR 은 다음과 같다.

$$SINR_{(Q[k],\mathrm{Un})}^{\mathrm{OMA}} = \frac{p_{(Q[k],k)}^{\mathrm{OMA}} |\mathrm{h}_{(Q[k],\mathrm{Un})}|^2}{\sum_{i \neq k} p_{(Q[i],i)}^{\mathrm{OMA}} |\mathrm{h}_{(Q[k],\mathrm{Un})}|^2 + 1}, \quad (5)$$

여기서 $p_{(Q[k],k)}^{\mathrm{OMA}}$ 는 $Q[k]$ 가 k 번째 유저에게 OMA 로 서비스할 때, k 번째 유저가 갖는 전력을 의미하며 $p_{(Q[k],k)}^{\mathrm{OMA}} \leq P$ 을 만족한다. 따라서 q번째 AP 가 NOMA 를 사용하여 서비스할 때, k번째 유저가 얻을 수 있는 보안 전송률은 다음과 같다.

$$R_k^{\mathrm{NOMA}} = \begin{cases} [log_2(1+\gamma) - log_2\left(1 + SINR_{(q,\mathrm{Un})}^{\mathrm{NOMA}}\right)]^+, & \sum_{i=1}^{K} p_{(q,i)}^{\mathrm{NOMA}} \leq P \\ 0 & , \sum_{i=1}^{K} p_{(q,i)}^{\mathrm{NOMA}} > P \end{cases}. \quad (6)$$

여기서 $[\Delta]^+ = \max(0, \Delta)$ 를 의미한다. 또한 $Q[k]$ 가 OMA 로 서비스할 때, k번째 유저가 얻을 수 있는 보안 전송률은 다음과 같다.

$$R_k^{\mathrm{OMA}} = \begin{cases} [log_2(1+\gamma) - log_2\left(1 + SINR_{(Q[k],\mathrm{Un})}^{\mathrm{OMA}}\right)]^+, & p_{(Q[k],k)}^{\mathrm{OMA}} \leq P \\ 0 & , p_{(Q[k],k)}^{\mathrm{OMA}} > P \end{cases}. \quad (7)$$

따라서 최대 총 보안 전송률은 다음과 같다.

$$R_{\mathrm{sum}}^{\mathrm{MAX}} = \left[\sum_{i=1}^{K} R_i^{\mathrm{NOMA}}, \sum_{i=1}^{K} R_i^{\mathrm{OMA}}\right]^+. \quad (8)$$

이때 고려하는 시스템에서 NOMA 로 서비스할 때, 가능한 AP 와 복호 순서 조합의 개수와 OMA 로 서비스할 때, 가능한 AP 와 유저 조합의 개수를 합한 총 서비스 조합의 개수 V는 다음과 같다.

$$\mathrm{V} = 3K((K-1)! + 1). \quad (9)$$

따라서 v 번째 서비스 조합으로부터 얻는 총 보안 전송률을 $R_{\mathrm{sum}}^{\mathrm{v}}$ 라고 정의할 때, 총 보안 전송률을 최대화하는 최적의 서비스 조합 V^*은 다음과 같다.

$$\mathrm{V}^* = \underset{1 \leq \mathrm{v} \leq \mathrm{V}}{\mathrm{argmax}}(R_{\mathrm{sum}}^{\mathrm{v}}). \quad (6)$$

그러나 다수의 유저가 존재할 경우, 가능한 총 서비스 조합의 수가 급증하여 총 보안 전송률을 최대화하는 최적의 서비스 조합을 구하는 과정에 높은 계산 복잡도가 요구되므로 구하기 쉽지 않다. 따라서 본 논문에서는 기계학습 모델을 사용하여 낮은 복잡도로 최적의 서비스 조합을 구하고자 한다.

② 제안하는 기계학습 모델

본 논문에서 제안하는 기계학습 모델은 심층 신경망(deep neural network, DNN) 구조를 갖는다. 이때, 입력 노드에는 신호 대 잡음비(signal to noise ratio, SNR)와 각 AP 와 각 합법적인 유저 사이의 채널 이득, 각 AP 와 신뢰할 수 없는 유저 사이의 채널 이득 정보가 입력된다. 따라서 제안하는 기계학습 모델은 총 $QK+1$개의 입력 노드와 총 V개의 출력 노드를 갖는다. 또한 은닉층과 은닉 노드의 수는 각각 H_L 개와 H_N 개이다. 이때, 은닉 노드의 활성함수로는 rectified linear unit (ReLU) 함수를 사용하며, 출력 노드의 활성함수로는 softmax 함수를 사용한다. 또한 손실 함수와 최적화 알고리즘으로는 각각 범주형 교차 엔트로피(categorical cross-entropy) 함수와 adaptive momentum (Adam) 최적화 알고리즘을 사용하였다. 이때 과적합으로 인해 발생하는 성능저하를 감소시키기 위해 손실 값이 일정할 경우에는 학습을 조기에 종료하도록 설정하였다.

③ 성능평가

본 논문에서는 각 합법적인 유저의 SINR 이 $\gamma = 1$인 시스템에서 기계학습 모델로 구한 서비스 조합으로부터 얻는 총 보안 전송률과 반복적인 계산을 통해 구한 조합으로부터 얻는 총 보안 전송률을 비교하여 제안하는 기계학습 모델의 성능을 평가하였다. 이때, 두 가지 방법으로 구한 총 보안 전송률은 그림 2 에 나타나 있다.

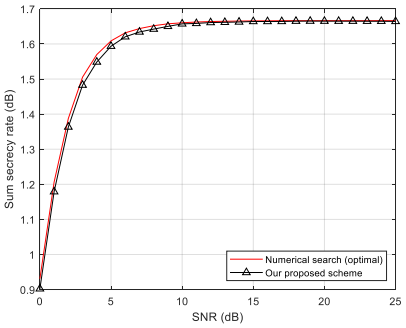

그림 2. 총 보안 전송률

Ⅲ. 결론

본 논문에서는 3 개의 AP 와 1 명의 신뢰할 수 없는 유저, 2 명의 합법적인 유저가 존재하는 cell-free 통신 시스템에서 기계학습 모델을 활용하여 낮은 복잡도로 총 보안 전송률을 최대화하는 최적의 서비스 조합을 구하는 기법을 제안하였다. 제안하는 기법의 성능은 제안하는 기법과 기계학습 모델을 사용하지 않는 최적의 기법으로 각각 구한 총 보안 전송률을 비교하여 평가하였으며, 두 기법으로 구한 총 보안 전송률이 유사함을 확인하였다.

ACKNOWLEDGMENT

본 연구는 2023 년도 과학기술정보통신부 및 정보통신기획평가원의 ICT 혁신인재 4.0 사업의 연구결과로 수행되었음 (IITP-2022-RS-2022-00156310).

참 고 문 헌

[1] S. Thapar, D. Mishra, and R. Saini, "Decoding orders and power allocation for untrusted NOMA: A secrecy perspective, " in Proc. IEEE WCNC, Seoul, South Korea, pp. 1-6, May 2020.

[2] M. Bashar, K. Cumanan, A. G. Burr, H. Q. Ngo, L. Hanzo, and P. Xiao, "On the performance of cell-free massive MIMO relying on adaptive NOMA/OMA mode-switching," IEEE Trans. Commun., vol. 68, no. 2, pp. 792-810, Feb. 2020.