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

Min Jeong Kang[1], Jung Hoon Lee[1]*, and Il-Gu Lee[2]

[1] Department of Electronics Engineering and Applied Communications Research Center,
Hankuk University of Foreign studies
{love_minmin926, tantheta}@hufs.ac.kr

[2] Department of Future Convergence Technology Engineering, Sungshin Women's University
iglee@sungshin.ac.kr

## Abstract

In this paper, we propose machine learning-based nonorthogonal multiple access (NOMA) to enhance the physical layer security in cell-free communication systems. In secure cell-free communication with NOMA, a central processing unit (CPU) finds the optimal access point (AP) that maximizes the sum secrecy rate as well as the decoding order for NOMA. However, when multiple users are involved on the network, finding the optimal decoding order for each AP becomes a computationally intricate challenge. To ameliorate this difficulty, our proposed scheme adopts machine learning to jointly find the optimal user associations and decoding orders for NOMA. This approach enables us to efficiently obtain a combination of AP and decoding order that maximizes the sum secrecy rate with significantly reduced computational complexity. Numerical results show that our proposed scheme achieves near optimal performance with far reduced complexity.

**Keywords**: Machine learning, nonorthogonal multiple access, physical layer security, cell-free communication systems

# 1 Introduction

In wireless communication systems, data transmission exclusively to legitimate users is almost impossible due to the broadcasting nature of wireless channels. There have been many efforts to improve the security of wireless communication systems also with the use of nonorthogonal multiple access (NOMA), which is a promising technology to obtain high spectral efficiency. In NOMA, a transmitter simply transmits a superposed one of multiple users' signals, and each user decodes its own received signals from the received signal using successive interference cancellation (SIC). In this case, the decoding order is a crucial factor to determine the performance of NOMA [1]. The authors of [2] considered physical layer security with NOMA and proposed a suboptimal algorithm that finds decoding order and power allocation for NOMA. Also, the authors of [3] analyzed the security performance of relay selection when several relays are randomly distributed on the network operating with decode-and-forward (DF) or amplify-and-forward (AF) protocol.

Cell-free communication is an emerging technology for next-generation wireless communication systems. It sometimes behaves like a type of distributed antenna systems and is often deployed alongside multi-antenna or NOMA to enhance the system's channel capacity. However, in cell-free communication systems with NOMA, there is no guarantee that NOMA outperforms

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No. 13

*Corresponding author: Department of Electronics Engineering and Applied Communications Research Center, Hankuk University of Foreign studies, Yongin, 17035, Email: tantheta@hufs.ac.kr

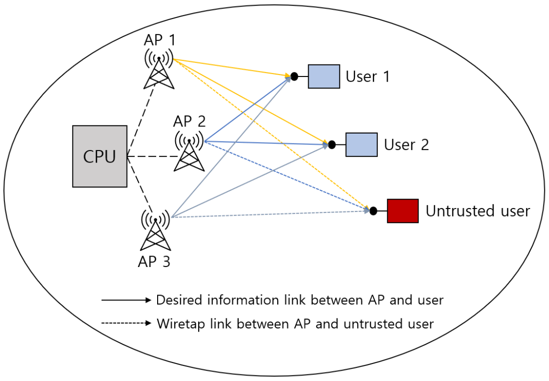
AP 1
AP 2
AP 3
CPU
User 1
User 2
Untrusted user
Desired information link between AP and user
Wiretap link between AP and untrusted user

Figure 1: Our system model.

orthogonal multiple access (OMA) as discussed in [4]. To address this, there have been many studies aimed at optimizing the performance of cell-free communication systems. The authors of [5] considered a cell-free massive multiple-input multiple-output (MIMO) system and proposed an adaptive NOMA/OMA mode switching scheme.

In this paper, we propose machine learning-based NOMA for physical layer security in cell-free communication systems, where each user has a target signal-to-interference-plus-noise power ratio (SINR). In secure cell-free communication with NOMA, a central processing unit (CPU) finds the optimal access point (AP) that maximizes the sum secrecy rate as well as the decoding order for NOMA. However, when multiple users are involved on the network, finding the optimal decoding order for each AP requires huge computationally complexity. To resolve this difficulty, our proposed machine learning-based NOMA adopts a machine learning model that jointly finds the optimal user associations and decoding orders for NOMA, where the machine learning model is of a deep neural network (DNN) structure and tries to maximize the sum secrecy rate, equivalently the number of users that fulfills the target SINR. In numerical results, we show that our proposed scheme achieves the performance of the optimal scheme via brute-force manners with far reduced complexity.

The remainder of our paper is organized as follows. In Section II, we explain our system model and formulate the optimization problem. In Section III, we propose ML-based NOMA that solves the optimization problem. In Section IV, we evaluate our proposed ML model, and in Section V, we conclude our paper.

# 2 System model

Our system model is illustrated in Figure. 1. We consider a cell-free communication system that serves multiple users on the network using NOMA, where there is a CPU that controls three APs, and the AP selected from among the APs serves $K(=2)$ single-antenna legitimate users. In our system model, there are two legitimate single-antenna users with a *untrusted* single-antenna user. At the same time, the AP wants to serve only the legitimate users.

Let $M[k]$ denotes the AP that transmits data to the user $k$. Then, the received signal at the user $k$ can be modeled as follows.

$$Y^{\texttt{NOMA}}_{(M[k],k)} = h_{(M[k],k)} X_{M[k]} + n_{(M[k],k)}, \tag{1}$$

where $h_{(M[k],k)}$ represents a channel between the AP $M[k]$ and the user $k$. Without loss of generality, we assume that the users' channel gains satisfies that $|h_{(M[1],1)}|^2 \geq |h_{(M[2],2)}|^2$. Also, $n_{(M[k],k)}$ denotes the circularly symmetric complex Gaussian noise at the user $k$ with zero mean and unit variance, and $X_{M[k]}$ is a transmit signal configured using superposition coding, i.e.,

$$X_{M[k]} = \sum_{i=1}^{K} x_i, \tag{2}$$

where $x_i$ is the transmit signal to the user $i$.

In our system model, we assume that the APs are uniformly distributed within a certain range, resulting in a situation, where each user is located close to a different AP. Note that NOMA does not always achieve the higher performance than OMA in terms of sum secrecy rate. Thus, each AP serves the users with OMA when it outperforms to NOMA. However, when the AP employs OMA to serve users, the AP serves the users one by one. When the AP adopts OMA to serve user $k$, the received signal at the user $k$ can be modeled as follows:

$$Y^{\mathtt{OMA}}_{(M[k],k)} = h_{(M[k],k)} x_k + n_{(M[k],k)}, \tag{3}$$

## 2.1 Power allocation scheme for legitimate users

In this paper, we denote by $\gamma$ target SINR for each user, which is assumed to be same for all users. Also, we assume that the AP only allocates the smallest power to meet the target SINR for each user.

### 2.1.1 Nonorthogonal multiple access (NOMA)

The user $k$'s SINR can be given as follows when the AP adopts NOMA to serve user $k$

$$\mathsf{SINR}^{\mathtt{NOMA}}_{(M[k],k)} = \frac{p^{\mathtt{NOMA}}_{(M[k],k)} |h_{(M[k],k)}|^2}{\sum_{i=1}^{k-1} p^{\mathtt{NOMA}}_{(M[i],i)} |h_{(M[k],k)}|^2 + 1}, \tag{4}$$

where $p^{\mathtt{NOMA}}_{(M[k],k)}$ is the allocated power to the user $k$ when the AP $M[k]$ serves user $k$ using NOMA. In NOMA, successive interference cancellation (SIC) is used to decode the signals of each user. In this process, each user sequentially removes interference signal from users whose decoding order is later than himself, treating the user's signal ahead of him as noise while decoding his signal. Then the user $k$'s power becomes

$$p^{\mathtt{NOMA}}_{(M[k],k)} = \gamma \cdot \frac{\sum_{i=1}^{k-1} p^{\mathtt{NOMA}}_{(M[i],i)} |h_{(M[k],k)}|^2 + 1}{|h_{(M[k],k)}|^2}. \tag{5}$$

At this time, the total power $P$ constraint is as follows

$$\sum_{i=1}^{K} p^{\mathtt{NOMA}}_{(M[i],i)} \leq P. \tag{6}$$

Also, the untrusted user (Un)'s SINR can be modeled as follows when the AP adopts NOMA to serve user $k$

$$\mathsf{SINR}^{\mathtt{NOMA}}_{(M[k],Un)} = \frac{p^{\mathtt{NOMA}}_{(M[k],k)} |h_{(M[k],Un)}|^2}{\sum_{i=1}^{k-1} p^{\mathtt{NOMA}}_{(M[i],i)} |h_{(M[k],Un)}|^2 + 1}, \tag{7}$$

where $h_{(M[k],Un)}$ denotes a channel between the AP $M[k]$ and untrusted user, and we assume that untrusted user has the least channel gain compared to all users.

### 2.1.2 Orthogonal multiple access (OMA)

The user $k$'s SINR can be given as follows when the AP adopts OMA to serve user $k$

$$\mathsf{SINR}^{\texttt{OMA}}_{(M[k],k)} = p^{\texttt{OMA}}_{(M[k],k)}|h_{(M[k],k)}|^2, \tag{8}$$

where $p^{\texttt{OMA}}_{(M[k],k)}$ is the allocated power to the user $k$ when the AP $M[k]$ serves user $k$ using OMA. In OMA, the user $k$'s power becomes

$$p^{\texttt{OMA}}_{(M[k],k)} = \gamma \cdot \frac{1}{|h_{(M[k],k)}|^2}. \tag{9}$$

The total power $P$ constraint is given in a similar to NOMA, as follows:

$$\sum_{i=1}^{K} p^{\texttt{OMA}}_{(M[i],i)} \leq P. \tag{10}$$

Also, the untrusted user (Un)'s SINR can be modeled as follows when the AP employs OMA to serve user $k$

$$\mathsf{SINR}^{\texttt{OMA}}_{(M[k],Un)} = \frac{p^{\texttt{OMA}}_{(M[k],k)}|h_{(M[k],Un)}|^2}{\sum_{i\neq k} p^{\texttt{OMA}}_{(M[i],i)}|h_{(M[k],Un)}|^2 + 1}, \tag{11}$$

Each user is served by a different AP, but untrusted user simultaneously receives signals from different APs, causing interference.

## 2.2 Sum secrecy rate of the legitimate users

Based on (7) and (11), the user $k$'s secrecy rate for $A \in \{\texttt{NOMA}, \texttt{OMA}\}$ becomes

$$R^{A}_{(M[k],k)} = \begin{cases} \left[\log_2(1+\gamma) - \log_2\left(1 + \mathsf{SINR}^{A}_{(M[Un],Un)}\right)\right]^+, & \sum_{i=1}^{K} p^{A}_{(M[i],i)} \leq P \\ 0, & \sum_{i=1}^{K} p^{A}_{(M[i],i)} > P, \end{cases}$$

where $[\alpha]^+$ means max $(0,\alpha)$. In this paper, we assume that the total power is limited. Thus, we only provide service if the sum power of all users satisfy the total power constraint. Therefore, the sum secrecy rate can be given by

$$\mathcal{R}^{\mathsf{sum}} = \left[\sum_{i=1}^{K} R^{A}_{(M[k],k)}\right]^+, \ A \in \{\texttt{NOMA}, \texttt{OMA}\}. \tag{12}$$

## 2.3 Problem description

In this paper, our objective is to maximize the sum secrecy rate when the AP selected from among the APs adopts NOMA or OMA to serve users. To achieve this, we need to determine the sum secrecy rate when employing NOMA and OMA, respectively. To begin with, in NOMA, SIC plays a crucial role in the decoding process, and its effectiveness depends on the decoding order. Therefore, our challenge is to identify the optimal decoding order that maximizes the sum secrecy rate among all possible decoding orders in each AP. Next, in the case of OMA, where each AP serves only one user, a critical task is to find the optimal pairing of APs and users to maximize the sum secrecy rate. Hence, the number of total possible combinations becomes

$$S = 3K((K-1)! + 1). \tag{13}$$

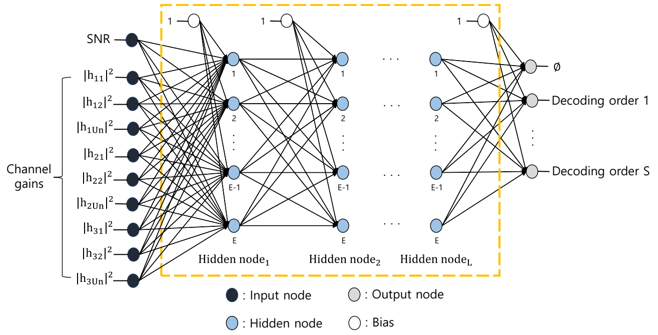

Figure 2: The structure of our proposed machine learning model.

Therefore, when the secrecy rate that the $j$th user can obtain when it is part of the $s$th combination is as follows

$$R_{\left(M\left[O_{(s,j)}\right],O_{(s,j)}\right)} = \begin{cases} \left[\log_2(1+\gamma) - \log_2\left(1+\mathsf{SINR}_{\left(M\left[O_{(s,j)}\right],Un\right)}\right)\right]^+, & \sum_{i=1}^{K} p_{\left(M\left[O_{(s,i)}\right],O_{(s,i)}\right)} \leq P \\ 0, & \sum_{i=1}^{K} p_{\left(M\left[O_{(s,i)}\right],O_{(s,i)}\right)} > P, \end{cases}$$

where $O_{(s,i)}$ is the $j$th user at the $s$th combination. Thus, the sum secrecy rate of the $s$th combination can be represented by

$$\mathcal{R}_s^{\texttt{sum}} = \sum_{i=1}^{K} R_{\left(M\left[O_{(s,i)}\right],O_{(s,i)}\right)}. \tag{14}$$

Also, the maximum sum secrecy rate becomes

$$\mathcal{R}^{\texttt{max}} = \underset{1\leq s\leq S}{\text{maximize}}\, \mathcal{R}_s^{\texttt{sum}}. \tag{15}$$

As a result, when the number of total possible combinations is $S$, the optimal combination becomes

$$s^\star = \underset{1\leq s\leq S}{\text{argmax}} \left( \mathcal{R}_s^{\texttt{sum}} \mid \sum_{i=1}^{K} p_{\left(M\left[O_{(s,i)}\right],O_{(s,i)}\right)} \leq P \right). \tag{16}$$

# 3 Proposed machine learning-based NOMA for physical layer security

In this section, we propose machine learning-based NOMA for physical layer security. Initially, we outline the procedure for identifying the optimal combination using machine learning and subsequently explain details regarding the structure of our proposed machine learning model.

## 3.1 Basic idea

In this paper, our objective is to determine the optimal combination that maximizes the sum secrecy rate among the total possible combinations, denoted as $S$, within the considered system model. However, manually comparing all possible combinations is challenging due to the complexity of the calculations involved. Therefore, our scheme uses the machine learning model

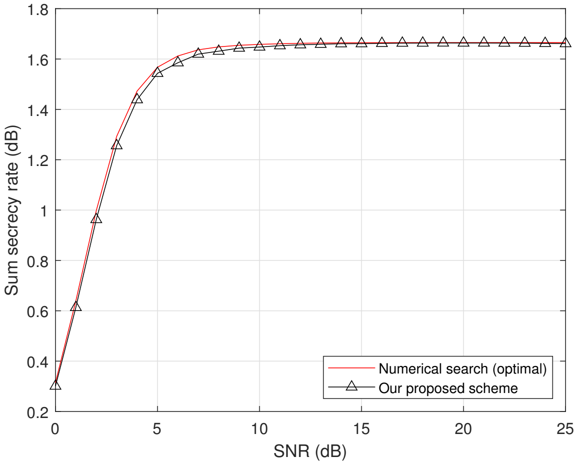

Figure 3: The sum secrecy rate of various schemes.

to efficiently identify the optimal combination among the total possible combinations, utilizing the channel gains between each AP and each user, as well as the channel gains between each AP and untrusted user.

### 3.2 Structure of our proposed machine learning model

Figure. 2 illustrates the structure of our proposed machine learning (ML) model, which is based on a deep neural network (DNN) structure. Our ML model consists of a total of three layers: input layer, output layer and hidden layer. The input node consists of the signal-to-noise ratio (SNR) and the channel gains between each AP and user, as well as channels between untrusted user and APs. Consequently, the input layer of the model comprises a total of $3(K+1)+1$ input nodes. In the output node, $\emptyset$ represents the case where the AP does not serve any user. Therefore, the output layer of the ML model comprises $S+1$ nodes, with $\emptyset$ indicating no combination. Furthermore, our ML model includes $L$ hidden layers with each hidden layer containing $E$ hidden nodes. We adopt the rectified linear unit (ReLU) activation function at each hidden node and the softmax function at each output node. For training, we utilize the categorical cross-entropy loss function, computed as the discrepancy between the labels and the output data. Thus, the loss function becomes

$$\xi = -\sum_{i=1}^{S+1} \varphi_i log2(c_i), \tag{17}$$

where $\varphi_i$ takes values in the range of 0 and 1, and $c_i$ represents the $i$th label and the output value of $i$th output node, respectively. Additionally, we employ the adaptive moment (Adam) algorithm and implement an early stopping regulation.

## 4 Numerical results

In this section, we evaluate our proposed scheme for determining the optimal combination. First, we consider an environment where the target SINR for each user is set to one, i.e.,

$\gamma = 1$. In our system, there are three APs, two legitimate users and one untrusted user. Thus, our machine learning model consists of a total 10 input nodes and total 13 output nodes. Furthermore, we consider that our model has three hidden layers, each comprising 100 hidden nodes. The samples used in the training and test process of the proposed ML model are obtained using MATLAB. Figure. 3 represents the accuracy of our proposed ML model, where the number of training samples as $26 \times 10^5$ and the number of test samples as $26 \times 10^4$. As shown in Figure. 3, our proposed scheme has similar performance to that of manually comparing all possible combinations without using ML.

## 5 Conclusions

In this paper, we proposed machine learning-based NOMA for physical layer security in cell-free communication systems, where our machine learning (ML) model is employed to identify the optimal combination that maximizes the sum secrecy rate among all possible combinations, utilizing the channel gains between each AP and each user, as well as the channel gains between each AP and untrusted user. In our system, the optimal combination can be determined through repetitive calculations without utilizing machine learning model, but this approach is hindered by high computational complexity. Therefore, obtaining an optimal combination through repetitive calculations in a system with rapidly changing channel state information and low latency requirements is challenging. However, our proposed scheme utilizes machine learning with channel gains to obtain the optimal combination with low complexity. Hence, it can be effectively applied in systems characterized by fast channel state information changes and tight delay constraints.

## Acknowledgments

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ICAN(ICT Challenge and Advanced Network of HRD) program(No. IITP-2022-RS-2022-00156310) supervised by the IITP(Institute of Information & Communications Technology Planning & Evaluation).

## References

[1] M. K. Hasan, M. Shahjalal, M. M. Islam, M. M. Alam, M. F. Ahmed, and Y. M. Jang, "The role of deep learning in NOMA for 5G and beyond communications," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Fukuoka, Japan, pp. 303–307, 2020.

[2] 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.

[3] Z. Wang and Z. Peng, "Secrecy performance analysis of relay selection in cooperative NOMA systems," *IEEE Access*, vol. 7, pp. 86274–86287, July. 2019.

[4] Y. Li and G. A. A. Baduge, "NOMA-aided cell-free massive MIMO systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 950–953, Dec. 2018.

[5] 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.