Secure Transmission in NOMA Systems: An Efficient Resource Allocation Strategy Using Deep Learning

Miled Alam, Abdul Karim Gizzini, Laurent Clavier

Secure Transmission in NOMA Systems: An Efficient Resource Allocation Strategy Using Deep Learning

Miled Alam*, Abdul Karim Gizzini†, and Laurent Clavier*‡
*IMT Nord Europe, Institut Mines Télécom, Centre for Digital Systems, F-59653 Villeneuve d'Ascq, France
† SogetiLabs Research and Innovation (part of Capgemini), F-92130, Issy Les Moulineaux, France
‡ IEMN, UMR CNRS 8520, University of Lille, France
Email: {miled.alam, laurent.clavier}@imt-nord-europe.fr, abdul.gizzini@sogeti.com

2024 IEEE Conference on Standards for Communications and Networking (CSCN) | 979-8-3315-0742-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSCN63874.2024.10849738

***Abstract*—Deep learning (DL) algorithms have been widely integrated in various aspects of wireless communications research. In this paper, we investigate, in an Internet of Things context, the secrecy energy-efficiency (SEE) of a multi-user downlink non-orthogonal multiple access (NOMA) system in the presence of a passive eavesdropper. Hence, we formulate the convex optimization problem as maximizing the SEE defined as the trade-off between the secrecy sum-rate and the power budget. Notably, this optimization problem has been recently solved in a closed form. The solution can also be utilized to efficiently maximize the ratio between the secrecy sum-rate and power consumption, requiring only a line search. This approach is then used to generate training, validation, and test datasets. Our method relies on a deep neural network designed for resource allocation. The benefits of using a deep neural network include achieving optimal resource allocation results while minimizing complexity and latency. The results presented in this paper highlight the superiority and efficacy of DL optimization compared to traditional iterative search methods.**

***Index Terms*—Deep learning, non-orthogonal multiple access (NOMA), physical layer security (PLS), secrecy energy-efficiency optimization**

I. Introduction

While we are still waiting for the Internet of Things (IoT) to fulfil its promise it becomes crucial to deal efficiently with a massive number of devices, especially in terms of power consumption but also in integrating security considerations [1], [2]. To address the potential massive number of devices, non-orthogonal multiple access (NOMA) is a very promising technique to improve the spectral efficiency, making it particularly adapted to IoT applications. As opposed to the traditional orthogonal multiple access (OMA) currently in use, under NOMA multiple users are served over the same resource block (time or frequency). Hence, managing the incurred interference is crucial, one usual approach being to use superposition coding at the transmitter side and successive interference cancellation (SIC) at the receiver side [3], [4].

A second key issue in IoT networks is the lifetime of the end-devices, meaning that energy efficiency (EE) aspect is a must, without compromising the minimum quality of service (QoS) constraints. Consequently, resource allocation for energy-efficient communications is a significant topic of research, and several works have been proposed for NOMA systems [5], [6].

In this work we consider the downlink in IoT networks. This link is poorly addressed in current Low Power Wide Area Networks (LP-WAN) such as LoRa, mainly because it is energy-intensive to maintain wake-up periods in the end device. This link, however, is shared by many devices and information exchange is likely to be listened by eavesdroppers. Thus, the implementation of security measures is essential to protect the confidentiality and integrity of transmitted data. Physical Layer Security (PLS) techniques have been proposed in Wyner's seminal work [7]. While cryptography-based approaches mainly rely on computational capabilities, PLS exploits instead the dynamic features of wireless communications, such as interference, fading, and noise. In this context, instead of focusing on achievable rates, secrecy achievable rates are considered. They measure the difference between the rate achieved by the legitimate user and by the eavesdropper [7].

The question addressed in this paper is to propose an algorithm to allocate powers in downlink communications based on NOMA in order to minimize the transmitted power while maximizing the secrecy rate. Our contribution consists in an efficient, low complexity, and low latency power allocation algorithm using deep learning (DL) to maximize the ratio between the secrecy sum-rate and energy consumption. Results prove to be very close to the optimal solution.

The remainder of the paper is organized as follows. Section II gives a detailed state of the art. In Section III, we introduce the system model. The optimization problems are defined and solved in section IV. In Section V, the proposed DNN-based power allocation is described. In Section VI, numerical results are presented and show the effectiveness of our proposed DNN approach. Finally, we conclude this article in Section VII.

II. Previous Works

Recently, there has been a growing focus on research regarding artificial intelligence (AI)-driven methods in wireless communications [8]. AI techniques provide a good performance-

This work has been carried in the context of the project Beyond5G, funded by the French government as part of the economic recovery plan, namely "France Relance" and the investments for the future program.

complexity trade-off by using low-complex architectures to efficiently learn the patterns related to the studied problems [9]. Deep neural networks (DNNs) are one of the most widely adopted AI techniques, that are designed to emulate the functions and structures of the human brain [8]. Intensive work has been carried out in literature where AI-based resource allocation in the NOMA system is considered [10]–[15]. The aim behind these works is to tackle the drawbacks of using traditional convex optimization techniques [16]–[18] in the context of resource allocation. These traditional methods are based on iterative algorithms to find optimal solutions, leading to high computational complexity and time costs. Therefore, conventional resource allocation approaches may be inadequate for emerging Beyond 5G (B5G) and Sixth Generation (6G) systems, since they could struggle to meet the extremely low latency demands of next-generation wireless networks.

Zhang et al. [10] investigated a DL-based approach to resource allocation in a NOMA system involving two users and one eavesdropper. The study demonstrated the ability to optimize allocations with low complexity. The authors used convex optimization techniques to address the basic optimization problem, focusing on maximizing the secrecy rate and facilitating the creation of training, validation and test datasets. Then, a DNN approach was implemented to learn and optimize resource allocation. The results obtained suggest that the proposed DNN can efficiently perform resource allocation with low complexity and latency. Jameel et al. [11] propose a DNN to maximize the secrecy rate of energy harvesting cooperative NOMA users communicating in the presence of an energy harvesting eavesdropper. In their paper, they initially address the optimization problem using a conventional iterative search algorithm. Subsequently, they employ DL to determine the optimal power allocation. The results demonstrate the robustness and superiority of DL-based optimization over conventional iterative search algorithms. Other authors have studied resource allocation problems using DL to maximize energy efficiency (EE) [12] and total system throughput [13]–[15]. In [12], the authors propose the application of DL for power allocation to reduce the impact of imperfect successive interference cancellation (SIC) in an EE context for downlink NOMA systems. In their study, the authors first solve the non-convex EE optimization problem using an exhaustive search method. Then, a DNN is trained to predict the power allocation derived from the optimization process. Simulation results confirm that the proposed scheme offers near-optimal performance with very low computational complexity. In [13], the authors propose a DL-based approach to maximize the throughput of NOMA based Relay-Aided Device-to-Device transmissions. They first derive the optimal solution using a convex optimization paradigm and obtain reliable data for training and testing the DNN. The results show that the DNN provides promising outcomes in both sum rate and computational complexity. Similar to [13], Saetan et al. [14] employ DL to predict optimal power allocation in a multi-user downlink NOMA system. Their results reveal that the proposed scheme can achieve a sum rate performance close to the optimal scheme but with much lower computational complexity. Lin et al. [15] develop a DL-based approach to obtain an efficient resource allocation strategy, which maximizes the transmission rate in simultaneous wireless information and power transfer (SWIPT) NOMA system with power splitting technology. In [19], the authors use DL to minimize the total transmit power in a SWIPT and a multi-carrier NOMA system (MC-NOMA). First, the authors focus on the non-convex nature of the problem, using conventional algorithms based on iterative search. Then, they introduce an efficient DL-based approach and obtain a solution close to the optimal one. Their numerical results indicate that the DL-based approach developed can achieve a level of performance in terms of energy consumption comparable to the exhaustive search method and the genetic algorithm.

If the literature review underlines the potential benefits of machine learning for power allocation, it also shows that research into the secrecy energy-efficiency (SEE) performance of multi-user NOMA systems is very limited.

To advance this promising area of wireless communications, our contribution involves the deployment of deep neural networks to address the challenges associated with non-convex power allocation, aiming to maximize the secrecy energy-efficiency in scenarios where multiple NOMA users communicate in the presence of a single eavesdropper. The latter is defined as the ratio between the secrecy sum-rate (SSR) and energy consumption, as considered in [18]. Our methodology takes into account the individual QoS and power constraints of each user. To the best of our knowledge, the use of machine learning techniques to derive the power allocation policy that maximizes the SEE for NOMA in multi-user downlink has never been explored before. First, we formulate the problem of maximizing the secrecy energy-efficiency defined as the trade-off between the SSR and the total power consumption [20]. Secondly, the derived analytical solution can be utilised to maximize the ratio between SSR and power consumption. To this end, Dinkelbach's iterative procedure is simplified by a linear search [20], generating a complete training dataset. Then, we train the proposed deep neural network using this dataset. Following the training phase, we perform a comparison analysis of the secrecy energy-efficiency and average computation time between our approach and conventional methods. The simulations that follow highlight that the proposed DNN achieves near-optimal secrecy energy-efficiency, accompanied by a significant reduction in average computation time compared to conventional approaches.

III. System Model and Problem Formulation

In this work, we consider a network composed of a single transmitter, the base station (BS), K legitimate users and a passive eavesdropper. To cope in a spectral-efficient manner with the arbitrary number of users $K \geq 2$, NOMA is employed. As such, the BS uses superposition coding and broadcasts $X = \sum_{i=1}^{K} \sqrt{p_i} X_i$, where X_i denotes the message intended to user $i \in [\![1, K]\!]$ such that $\mathbb{E}[|X_i|^2] = 1$ and p_i is the allocated power for user i restricted by the power budget of the BS such that $\sum_{i=1}^{K} p_i \leq P_{\max}$. Beside the aforementioned total power constraint, each user i is also required to meet a minimum QoS constraint in terms of its achievable data rate $R_{\min,i}$.

The received signal at the k-th legitimate user and at the eavesdropper are given as

$$Y_k = h_k \sum_{i=1}^{K} \sqrt{p_i} X_i + Z_k, \text{ and } Y_e = h_e \sum_{i=1}^{K} \sqrt{p_i} X_i + Z_e, \quad (1)$$

where h_k and h_e denotes the channel gain between the BS and the k-th user and between the BS and the eavesdropper respectively; $Z_k \sim \mathcal{N}\left(0, \sigma_k^2\right)$ and $Z_e \sim \mathcal{N}\left(0, \sigma_e^2\right)$ are the Additive White Gaussian Noises (AWGN) at the k-th user and eavesdropper respectively. Throughout this paper, we assume that perfect channel state information is available at the BS.

Let us now define $\Gamma_k = h_k^2/\sigma_k^2$ for $k \in [\![1, K]\!]$ and $\Gamma_e = h_e^2/\sigma_e^2$. Without loss of generality, we assume that the channel gains are ordered as

$$\Gamma_1 \leq \cdots \leq \Gamma_{M-1} \leq \Gamma_e < \Gamma_M \leq \cdots \leq \Gamma_{K-1} < \Gamma_K. \quad (2)$$

To deal with the multiple users superposed in the resource blocks, SIC decoding is used by the legitimate receivers to decode the messages. We assume that the eavesdropper also applies SIC to detect all users' messages. Under SIC decoding, a given user first decodes the messages of users with larger allocated powers, while it suffers interference from users with lower allocated powers. The achievable rate R_k to decode the message of user k at the legitimate k-th receiver, and the achievable rate R_k^e to decode the message of user k at the eavesdropper are respectively given as [18], [20]

$$R_k(\mathbf{p}) = \frac{1}{2} \log_2 \left(1 + \frac{h_k^2 p_k}{h_k^2 (p_{k+1} + \cdots + p_K) + \sigma_k^2} \right), \quad (3)$$

$$R_k^e(\mathbf{p}) = \frac{1}{2} \log_2 \left(1 + \frac{h_e^2 p_k}{h_e^2 (p_{k+1} + \cdots + p_K) + \sigma_e^2} \right), \quad (4)$$

where $\mathbf{p} = (p_1, \ldots, p_K)$ denotes the power allocation vector.

In the context of physical layer security, the figure of merit is the secrecy rate, which is defined as the gap between the data rate achieved by the legitimate user and by the eavesdropper to recover the same message. As such, we can define for each user $k \in [\![1, K]\!]$ its achievable secrecy rate as [18], [20]

$$R_k^s(\mathbf{p}) = \left[R_k(\mathbf{p}) - R_k^e(\mathbf{p}) \right]^+, \quad (5)$$

where $[x]^+ = \max\{0; x\}$.

In order to improve the presentation of our results, let us denote by R^s the achievable sum secrecy rate, given as

$$R^s(\mathbf{p}) = \sum_{k=1}^{K} R_k^s(\mathbf{p}) = \sum_{k=M}^{K} \left(R_k(\mathbf{p}) - R_k^e(\mathbf{p}) \right). \quad (6)$$

As in [20], the secrecy energy-efficiency is measured via the scalarized trade-off between secrecy sum-rate and power consumption:

$$\mathrm{SEE}(\mathbf{p}) \coloneqq \sum_{k=1}^{K} R_k^s(\mathbf{p}) - \alpha \left(\sum_{k=1}^{K} p_k + P_c \right), \quad (7)$$

where P_c denotes the circuit power consumption accounting for all blocks implemented at the receiver and transmitter side. The trade-off parameter $\alpha \geq 0$ allows to switch between a secrecy-driven optimization problem and a power-consumption driven one, by respectively setting small or large values of α.

As such, the considered optimization problem under study writes as

$$\textbf{(SEE)} \quad \max_{\mathbf{p}} \ \mathrm{SEE}(\mathbf{p}),$$

$$\text{such that} \quad \theta_k \geq A_k \theta_{k+1} + \frac{A_k - 1}{\Gamma_k}, \quad k \in [\![1, K]\!], \quad \text{(C1)}$$

$$\theta_1 \leq P_{\max}, \quad \text{(C2)}$$

where we have used the following notations:

$$A_k = 2^{2R_{\min,k}}, \ \theta_k = \sum_{i=k}^{K} p_i, \ k \in [\![1, K]\!], \text{ and } \theta_{K+1} = 0. \quad (8)$$

In the optimization problem **(SEE)**, the constraint (C1) corresponds to the K individual QoS constraints, and is obtained by rewriting $R_k \geq R_{\min,k}$, whereas the constraint (C2) accounts for the total power budget of the BS.

IV. Resource Allocation Scheme with Conventional Approach

In this section, we present the closed-form solution for the convex optimization problem **(SEE)**, as detailed in our previous work [20]. In addition, this solution is used to maximize the SEE metric, as reported in [18].

A. Optimal Power Allocation

The convex problem in **(SEE)** can be efficiently solved by a closed-form solution. To ensure a complete understanding, we formulate the necessary and sufficient feasibility conditions, as well as the closed-form expression for the optimal power allocation policy, denoted by $\mathbf{p}^*$. Interested readers are referred to [20] for proofs and further developments.

Corollary. *[in [20], Proposition 1, Theorem 2] The optimization problem **(SEE)** is feasible if and only if*

$$P_{\max} \geq P_{\min} \coloneqq \sum_{k=1}^{K} \frac{A_k - 1}{\Gamma_k} \prod_{j=1}^{k-1} A_j, \quad (9)$$

*where $P_{\min}$ denotes the total minimum power required for all the K individual QoS constraints to be met with equality. When **(SEE)** is feasible, the optimal power allocation is obtained in closed-form as follows:*

$$p_k^*(\alpha) = (A_k - 1) \left(\frac{1}{\Gamma_k} + p_K^*(\alpha) \prod_{i=k+1}^{K-1} A_i + \sum_{i=k+1}^{K-1} \frac{A_i - 1}{\Gamma_i} \prod_{j=k+1}^{i-1} A_j \right), \quad k \in [\![1, K-1]\!],$$

$$p_K^*(\alpha) = \min\left\{ \max\{\bar{p}_K(\alpha), l\}, u \right\}, \quad (10)$$

where l, u and $\bar{p}_K(\alpha)$ are given by the equations below:

$$l = \frac{A_K - 1}{\Gamma_K}, \tag{11}$$

$$u = \frac{1}{\prod_{i=1}^{K-1} A_i}\left(P_{\max} - P_{\min} + \frac{A_K - 1}{\Gamma_K}\prod_{j=1}^{K-1} A_j\right), \tag{12}$$

$$\bar{p}_K(\alpha) = \frac{-\left(\alpha\gamma_2\Gamma_K\left(1+\gamma_1\Gamma_e\right) + \alpha\gamma_2\Gamma_e\prod_{i=M}^{K-1} A_i\right) + \Delta^{1/2}}{2\left(\alpha\gamma_2\Gamma_K\Gamma_e\prod_{i=M}^{K-1} A_i\right)} \tag{13}$$

with

$$\gamma_1 = \sum_{i=M}^{K-1}\frac{A_i - 1}{\Gamma_i}\prod_{j=M}^{i-1} A_j; \quad \gamma_2 = 2\ln 2\prod_{i=1}^{K-1} A_i;$$
$$\gamma_3 = \Gamma_K\left(1+\gamma_1\Gamma_e\right) - \Gamma_e\prod_{i=M}^{K-1} A_i;$$
$$\Delta = \left(\alpha\gamma_2\gamma_3\right)^2 + 4\alpha\gamma_2\gamma_3\Gamma_e\Gamma_K\prod_{i=M}^{K-1} A_i \tag{14}$$

B. Sum Secrecy Rate vs Power Consumption Ratio

The result from the previous section gives us when varying α the Pareto front of the bi-objective optimization problem, maximizing both SEE and EE. To reduce the solution to a single point, we consider another very relevant secrecy energy-efficiency measure, defined as the ratio between achievable sum secrecy rate and total power consumption [18]:

$$\text{SEE}'(\mathbf{p}) = \frac{\sum_{k=1}^{K} R_k^s(\mathbf{p})}{\sum_{k=1}^{K} p_k + P_c}. \tag{15}$$

Observe that this metric can also be maximized using our closed-form optimal power allocation policy provided in the above Corollary. Indeed, since the numerator of SEE$'$ is a concave function of the power allocation vector, and since the denominator is linear in the power allocation vector, using fractional programming [21], maximizing SEE$'$ is equivalent to finding the fixed point of the function

$$F(\alpha) = \sum_{k=1}^{K} R_k^s\left(\mathbf{p}^*(\alpha)\right) - \alpha\left(\sum_{k=1}^{K} p_k^*(\alpha) + P_c\right).$$

It can be achieved using Dinkelbach's algorithm (see Algorithm 1).

Algorithm 1 Dinkelbach Algorithm Maximizing SEE'

1: **Initialization:** $\varepsilon > 0$, $\alpha = 0$
2: **while** $F(\alpha) \le \varepsilon$ **do**
3: Compute optimal power allocation $\mathbf{p}^*(\alpha)$ using (10)
4: Update $F(\alpha) = \sum_{k=1}^{K} R_k^s\left(\mathbf{p}^*(\alpha)\right) - \alpha\left(\sum_{k=1}^{K} p_k^*(\alpha) + P_c\right)$
5: Update $\alpha = \text{SEE'}(\mathbf{p}^*(\alpha))$
6: **end while**

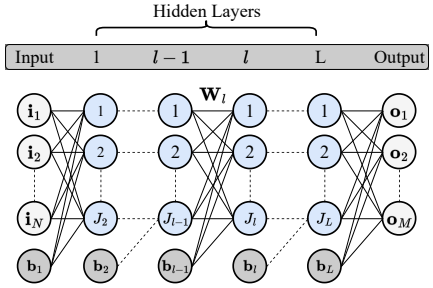

Fig. 1. DNN architecture showing the input, output, and hidden layers.

TABLE I
PROPOSED DNN PARAMETERS.

(Hidden layers; Neurons per layer)	(2;200-200)
Activation function	ReLU ($y = \max(0, x)$)
Number of epochs	200
Training samples	80000
Testing samples	20000
Batch size	256
Optimizer	ADAM
Loss function	MSE
Learning rate	0.001

V. Resource Allocation Scheme with DNN Approach

A. DNN Overview

DNN network functionality lies in the input-output mapping performed by learning their correlation during the training phase. The general DNN architecture consists of an input layer followed by L hidden layers and an output layer as shown in Figure 1. The output of the l-th hidden layer denoted as $\boldsymbol{o}_l$ can be expressed as follows:

$$\boldsymbol{o}_l = \boldsymbol{f}_l\left(\boldsymbol{b}_l + \boldsymbol{W}_l\boldsymbol{i}_l\right), \ \boldsymbol{i}_{l+1} = \boldsymbol{o}_l. \tag{16}$$

where $\boldsymbol{W}_l \in \mathbb{R}^{J_l \times J_{l-1}}$, and $\boldsymbol{b}_l \in \mathbb{R}^{J_l \times 1}$ refer to the weight matrix and the bias vector of the l-th hidden layer consisting of J_l neurons, respectively. $\boldsymbol{f}_l$ is a vector resulting from the stacking of the activation functions of the J_l neurons within the l-th hidden layer. We note that the DNN input and output are represented by $\boldsymbol{i} = [i_1, i_2, ..., i_N] \in \mathbb{R}^{N\times 1}$ and $\boldsymbol{o} = [o_1, o_2, ..., o_M] \in \mathbb{R}^{M\times 1}$, where N and M refer to the number of DNN inputs and outputs, respectively.

The main DNN trainable parameters can be described as $\beta = (\boldsymbol{W}, \boldsymbol{B})$, where the objective of the DNN training is to select β that minimizes the defined loss function $\text{Loss}(\beta)$ defined as follows:

$$\text{Loss}(\beta) = \arg\min_{\beta}(\boldsymbol{o}_{(L)}^{(\text{P})} - \boldsymbol{o}_{(L)}^{(\text{T})}). \tag{17}$$

The loss function in (17) quantifies how far apart the predicted DNN outputs $\boldsymbol{o}_{(L)}^{(\text{P})}$ from the true outputs $\boldsymbol{o}_{(L)}^{(\text{T})}$. Hence the overall DNN training procedure can be summarized in two main steps: (i) Calculate the loss and (ii) update β. This training procedure is carried over N_{train} training samples for

sufficient training epochs to guarantee the DNN convergence, i.e., the loss is minimized. This iterative process updates β as follows:

$$\beta_{\text{new}} = \beta - \rho \frac{\partial \text{Loss}(\beta)}{\partial \beta}. \quad (18)$$

ρ denotes the learning rate of the DNN that controls how quickly β is updated. Small ρ leads to a smaller updated β in each iteration, where it requires more training time. Whereas large ρ result in rapid β updates where less training time is required. It is worth mentioning that this minimization problem can be tackled by various optimization algorithms including stochastic gradient descent, root mean square prop, and adaptive moment estimation (ADAM) [22]. After training the DNN network, its performance is evaluated in the testing phase where unseen data are given to the employed DNN network.

B. Proposed DNN-based Power Allocation Scheme

We propose a DNN-based approach that is a DL-based alternative since DL can solve more efficiently the optimization problem than classical solutions by automatically detecting their heuristics based on training data. Our objective is to maximize the secrecy energy-efficiency ratio, where the channel gains of the users and eavesdropper are given as input to the employed DNN network that predicts the power allocation coefficients. Hence the DNN input and output vectors will be $\boldsymbol{i} = [h_1, h_2, ..., h_K, h_e] \in \mathbb{R}^{(K+1)\times 1}$ and $\boldsymbol{o} = [\hat{p}_1^*, \hat{p}_2^*, ..., \hat{p}_K^*] \in \mathbb{R}^{K\times 1}$, respectively. Table I shows the employed DNN hyper parameters where a 2 hidden layers architecture is employed with 200 neurons per layer. We recall that the perfect channel is used in this approach, where the objective of using the DNN is to predict the power allocation coefficients. However, using an imperfect channel is kept as a future work. Finally, the DNN predicted power allocation coefficients are substituted in (15) to calculate the DNN-based secrecy energy-efficiency ratio.

VI. Simulation Results

In this section, we present numerical results to evaluate the performance of our proposed DL-based joint resource allocation approach. This evaluation is based on a comparison of predicted results with those obtained using the Dinkelbach optimal algorithm, for maximizing the secrecy energy-efficiency ratio of the multi-user downlink network considered in the presence of a eavesdropper. Additionally, we compare NOMA with its counterpart based on OMA, as discussed in [20]. We set the noise variance for all users and the eavesdropper to $\sigma_k^2 = \sigma_e^2 = -60$ dBm, $P_c = 30$ dBm. The channel gains are $h_k = \frac{g_k}{\sqrt{1+d_k^a}}$ $(g_k \sim \mathcal{N}(0,1))$, $h_e = \frac{g_e}{\sqrt{1+d_e^a}}$ $(g_e \sim \mathcal{N}(0,1))$, where d_k and d_e are distances between the devices and the BS, whose locations are drawn from a uniform distribution in a square of 1km^2. The path loss exponent is $a = 3$. Unless otherwise specified, all users are required to respect a minimum data rate of $R_{\min,k} = R_{\min} = 0.05$ bit/s/Hz. We note that the training is performed once for each K users configuration and the considered datasets are obtained using the Dinkelbach algorithm. The curves are averaged over 10^5 independent channel realizations.

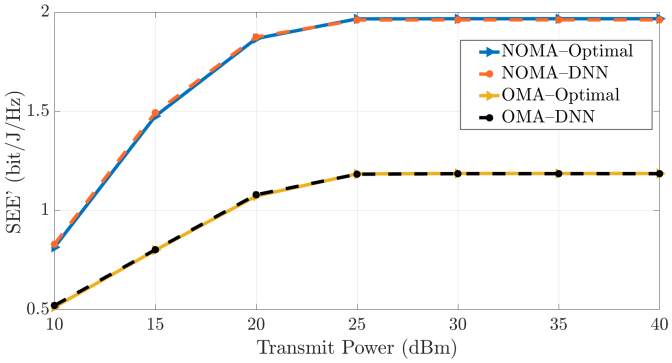

Fig. 2. Secrecy Energy-Efficiency (SEE') versus the total transmit power available at BS obtained by iterative and DNN approaches for $K = 3$ users.

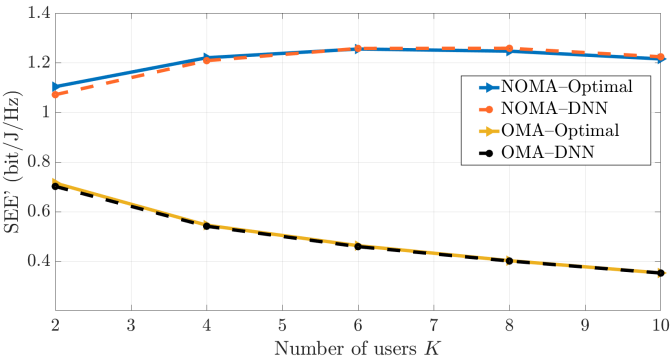

Fig. 3. Secrecy Energy-Efficiency (SEE') versus number of users K under NOMA and OMA obtained by iterative and DNN approaches for $P_{\max} = 40$ dBm.

Figure 2 illustrates the secrecy energy-efficiency under NOMA and OMA obtained by conventional and DNN approaches versus transmit power. It can be noticed that NOMA always outperforms OMA in terms of SEE' when the transmit power increases. Moreover, the proposed DNN approach is capable of achieving a similar secrecy energy-efficiency performance as the optimal solution.

Figure 3 shows the SEE' under NOMA and OMA as a function of the number of users K. We can clearly notice that the performance of the benchmarked approaches is better in NOMA regardless of K. Moreover, as K increases, the SEE' decreases for OMA with both approaches. On the other hand, in the case of NOMA, this metric achieves its maximum value when the network includes $K = 6$ users, and then gradually decreases. In addition, the proposed DNN-based approach demonstrates the capability to achieve a comparable secrecy energy-efficiency performance to the Dinkelbach optimal solution.

Figure 4 depicts the impact of the number of hidden layers on the secrecy energy-efficiency (left axis) and the average computational time of the test dataset (right axis), for $K = 3$ users and $P_{\max} = 40$ dBm. It can be seen that the influence of increasing the number of hidden layers on the SEE' is marginal. However, the average time for testing

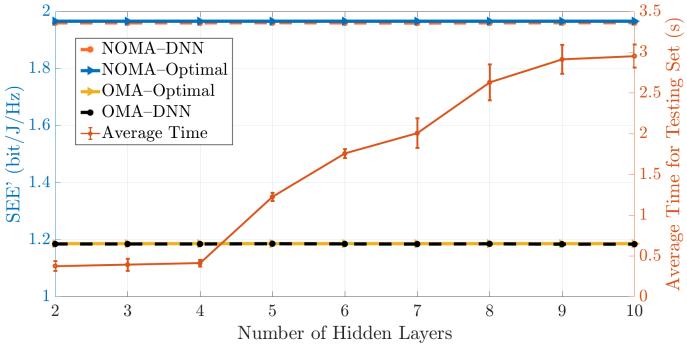

Fig. 4. Secrecy Energy-Efficiency ratio (left axis) and average time (right axis) as a function of the number of hidden layers for $K = 3$ users.

TABLE II
AVERAGE EXECUTION TIME.

	Optimal	DNN, 2 Hidden Layers	Ratio (%)
Avg. time	3.48×10^5 s	0.4 s	0.000011

set increases as the number of hidden layers increases. In other words, adding more hidden layers does not significantly improve performance, but it does increase the computational complexity of the neural network.

Table II shows the average time for both approaches. The time is calculated as $\bar{\zeta} = \frac{\sum_{n=1}^{N_t} \overline{\Theta_n}}{N_t}$, where $\overline{\Theta_n}$ represents the time taken by the DNN to calculate the solution for the n-th sample. The total number of testing samples, denoted as N_t and specified in Table I as 20000, is used in the calculation. The ratio is determined by dividing the average time of the DNN by the average time for the iterative approach. The table shows that the DNN approach does not require more than 0.000011% average time compared to the Dinkelbach optimization approach.

To sum up, we show that the DNN approach takes 0.000011% computing average time to achieve no less than 97% (cf. Figure 3, for $K = 2$) secrecy energy-efficiency performance compared to the Dinkelbach optimization approach.

VII. Conclusion

In this paper, we proposed a DNN-based resource allocation approach that aims to maximize the secrecy energy-efficiency in a multi-user downlink NOMA system in the presence of a passive eavesdropper. The formulated trade-off between the secrecy sum-rate and the power consumption is first introduced. After that, a closed-form solution is presented and used to maximize the ratio between the secrecy sum-rate and power consumption. To further reduce the computational complexity as well as the latency, a DNN-based approach is proposed where the channel gains of the users and the eavesdropper are fed as an input to the employed DNN that predicts the power allocation coefficients. Simulation results demonstrate that the proposed DNN-based approach provides a secrecy energy-efficiency performance close to that of the optimal scheme but with much lower complexity and latency. As a future perspective, the efficiency of the proposed approach will be tested and finetuned taking into consideration imperfect channel estimates.

References

[1] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1759–1799, 2021.
[2] Y. Zhao, W. Zhai, J. Zhao, T. Zhang, S. Sun, D. Niyato, and K.-Y. Lam, "A comprehensive survey of 6g wireless communications," *arXiv preprint arXiv:2101.03889*, 2020.
[3] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, 2015.
[4] M. Vaezi, Z. Ding, and H. V. Poor, *Multiple access techniques for 5G wireless networks and beyond*. Springer, 2019.
[5] Y. Zhang, H.-M. Wang, T.-X. Zheng, and Q. Yang, "Energy-efficient transmission design in non-orthogonal multiple access," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2852–2857, 2016.
[6] H. El Hassani, A. Savard, and E. V. Belmega, "A closed-form solution for energy-efficiency optimization in multi-user downlink NOMA," in *IEEE PIMRC*, 2020.
[7] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[8] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, 2019.
[9] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.
[10] M. Zhang, Y. Zhang, Q. Cen, and S. Wu, "Deep learning–based resource allocation for secure transmission in a non-orthogonal multiple access network," *International Journal of Distributed Sensor Networks*, vol. 18, no. 6, p. 15501329221104330, 2022.
[11] F. Jameel, W. U. Khan, Z. Chang, T. Ristaniemi, and J. Liu, "Secrecy analysis and learning-based optimization of cooperative NOMA SWIPT systems," in *IEEE Int. Conf. on Commun. Workshops (ICC Workshops)*, 2019, pp. 1–6.
[12] W. Saetan and S. Thipchaksurat, "Application of deep learning to energy-efficient power allocation scheme for 5G SC-NOMA system with imperfect SIC," in *Proc. 16th Int. Conf. Elect. Eng. Electron. Comput. Telecommun. Inf. Technol. (ECTI-CON)*, 2019, pp. 661–664.
[13] Z. Ali, G. A. S. Sidhu, F. Gao, J. Jiang, and X. Wang, "Deep learning based power optimizing for NOMA based relay aided D2D transmissions," *IEEE Trans. on Cognitive Commun. and Network*, vol. 7, no. 3, pp. 917–928, 2021.
[14] W. Saetan and S. Thipchaksurat, "Power allocation for sum rate maximization in 5G NOMA system with imperfect SIC: A deep learning approach," in *Proc. 4th Int. Conf. Inf. Technol. (InCIT)*, 2019, pp. 195–198.
[15] R. Lin, Y. Zhao, L. Tian, M. Liu, B. Chen, Y. Zhu, and J. Tang, "Deep learning based resource allocation in NOMA wireless power transfer networks," in *Proc. IEEE Int. Elect. Energy Conf. (CIEEC)*, 2019, pp. 2098–2103.
[16] C. E. Garcia, M. R. Camana, and I. Koo, "Secrecy energy efficiency maximization in an underlying cognitive radio–NOMA system with a cooperative relay and an energy-harvesting user," *Applied Sciences*, vol. 10, no. 10, p. 3630, 2020.
[17] C. E. Garcia, M. R. Camana, I. Koo, and M. A. Rahman, "Particle swarm optimization-based power allocation scheme for secrecy sum rate maximization in NOMA with cooperative relaying," in *Lect. Notes Comput. Sci.*, 2019, pp. 1–12.
[18] R. Yao, L. Yao, X. Zuo, N. Qi, Y. Liu, and J. Xu, "Secrecy energy efficiency maximization in a NOMA system," in *IEEE ICCSN*, 2019.
[19] J. Luo, J. Tang, D. K. So, G. Chen, K. Cumanan, and J. A. Chambers, "A deep learning-based approach to power minimization in multi-carrier NOMA with SWIPT," *IEEE Access*, vol. 7, pp. 17 450–17 460, 2019.
[20] A. Savard, G. Cervia, M. Alam, and A. Louchart, "Secrecy energy-efficient multi-user NOMA: closed-form solution to bi-criterion formulation," in *IEEE Joint European Conf. on Networks and Commun. & 6G Summit (EuCNC/6G Summit)*, 2024, pp. 487–492.
[21] C. Isheden, Z. Chong, E. Jorswieck, and G. Fettweis, "Framework for link-level energy efficiency optimization with informed transmitter," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 2946–2957, 2012.
[22] S. De, A. Mukherjee, and E. Ullah, "Convergence Guarantees for RMSProp and ADAM in Non-Convex Optimization and An Empirical Comparison to Nesterov Acceleration," 2018.