IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 November 2023, accepted 18 December 2023, date of publication 25 December 2023,
date of current version 3 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3347502

RESEARCH ARTICLE

Secure Initial Access and Beam Alignment Using Deep Learning in 5G and Beyond Systems

UTKU OZMAT[1,2], (Member, IEEE), MEHMET AKIF YAZICI[1], AND MEHMET FATIH DEMIRKOL[3], (Senior Member, IEEE)

[1]Information and Communications Research Group, Informatics Institute, Istanbul Technical University, 34469 İstanbul, Turkey
[2]5G Program Management Department, Turk Telekom, 34771 İstanbul, Turkey
[3]Prorize LLC, Marietta, GA 30062, USA

Corresponding author: Utku Ozmat (utkuozmat@itu.edu.tr)

ABSTRACT 5G and beyond networks will require fast, energy efficient, and secure initial access. In this study, a deep learning-based secure initial beam selection method is proposed that ranks the beam pairs between a transmitter and a legitimate user aiming to maximize the signal strength the user receives, while keeping the signal strength that the eavesdropper sees below a threshold. Instead of an exhaustive search, the initial beam selection is performed over a limited number of the top beam pairs, leading to reduced communication overhead and energy consumption. The proposed scheme is evaluated using data obtained from a real-life mobile network topology as well as a synthetic data set based on the same geographical site but with statistical system-level environment variables. Utilizing a multi-layer perceptron model, the neural network takes receiver locations as input and produces a ranked list of beam pairs between transmitter and receiver based on the specified coverage criteria. Numerical results show that the signalling overhead can be reduced by 75% with 99.66% accuracy in terms of the best beam pair, and 99.89% of the achievable signal strength. In terms of security, the proposed method has been shown to improve secure coverage probability by 68.12% compared to the best-coverage beam selection scenario.

INDEX TERMS 5G, physical layer security, beam management, mMIMO, NR SSB beam sweeping, deep learning, DNN.

I. INTRODUCTION

In 5G systems, the use of massive multiple-input-multiple-output (mMIMO) requires directional links. This demands an efficient process for identifying and maintaining a suitable transmit and receive (Tx-Rx) beam pair, known as beam management. This process can be challenging for highly dynamic and dense networks [1]. Initial access is the first step of the beam management process that the first alignment between the Tx and the Rx ends is established. Securing this process, not only in the cryptographic plane, but also in the physical-layer plane is of utmost importance.

The beam management process in 5G new radio (NR) has the following components: (i) beam sweeping, (ii) beam measurement and determination, (iii) beam reporting, (iv) beam recovery, and (v) beam switching [2], [3]. The initial access component of the beam management process is defined by the 3rd Generation Partnership Project (3GPP) as procedure P-1 in standard TR 38.802 [2]. Using synchronization signal blocks (SSB) transmitted as a transmit burst, transmit/receive point (TRP) beam sweeping, and user equipment (UE) beam sweeping are done to establish a beam pair link. To maximize the spectral efficiency between the transmitter and the receiver, the best beam pair in terms of the reference signal received power (RSRP) needs to be discovered. For this purpose, an exhaustive search is performed among all possible transmit and the receive beam pairs. The increasing number of antenna elements, and thus the number of beams, with mMIMO makes initial access a costly process in terms of latency and energy consumption [4]. The accelerated deployment of 5G networks will require fast, energy efficient, and secure initial access.

Recently, machine learning (ML), especially deep learning (DL), has become a prominent technique in a wide range

The associate editor coordinating the review of this manuscript and approving it for publication was Yogendra Kumar Prajapati.

of research areas for mobile and wireless networks. Potential areas of DL include mobility analysis, user localization, wireless sensor networks, network control, network security, signal processing, network-level and application-level mobile data analysis [5]. Specifically, DL has been proposed to be used in the beam management processes. It excels at extracting nonlinear features in angular and time domains, ensuring highly accurate beam pair prediction. Additionally, it has been proposed for predictive beam switching to minimize the overhead in beam tracking [6].

In 5G systems, diverse methods have been explored to improve beam selection and management through learning algorithms. User geolocations are used to select the beam index and the serving gNodeB (gNB) in a 5G-NR millimeter wave (mmWave) system using support vector machines in [7]. A vehicle traffic simulator coupled with a ray-tracing simulator for mmWave channels is used to generate a dataset in a vehicle-to-infrastructure scenario and a number of ML algorithms including a deep neural network (DNN) is employed to find the best beam pair indices in [8].

Beam management is treated as a classification problem, leading to the proposal of various DL methods in many studies. A multi-agent Q-learning algorithm is used to speed up beam alignment in [9], where the states are different Tx-Rx beam pairs, and the actions correspond to the predefined phase rotations applied to the Tx and the Rx beams. The work in [10] provides a DL framework that uses a waveform dataset, which is called DeepBeam, for beam management in mmWave networks. Using the directions and the angles-of-arrival (AoA) of Tx beams, a convolutional neural network learns to identify unique patterns of beams in the in-phase and quadrature representation of the waveform and thus, differentiate from the other beams by each beam's unique signature. Similarly, in [11], a DNN that reduces beam sweep time during initial access is presented. In this work, a framework which is called DeepIA, received signal strength values from beams are used as inputs and the index of the output is selected as the best spatially oriented beam for a mmWave network. A recurrent neural network that uses RSRP and UE orientation information as inputs to predict the best beam index is proposed in [12]. Their results show that including orientation information provides meaningful improvement in the beam prediction accuracy under certain scenarios. It is shown in [13] that sub-6 GHz channel information can be used to directly predict mmWave beams. This is exploited in [14], where a DNN model is proposed to predict the best mmWave beam index using the power delay profile (PDP) of a sub-6 GHz channel for a single cell with both mmWave and sub-6 GHz gNBs. Similarly, sub-6 GHz channel coefficients obtained from a sample ray-tracing environment are used to predict the best mmWave beams in [15]. A self-supervised DL method for channel-beam mapping with sub-6 GHz to predict mmWave beamforming vectors is proposed in [16]. A neural network architecture is designed in [17] to jointly learn site-specific probing beams and the beam predictor. The dataset provided in [18] is used in [13], [15], [16], and [17].

The aforementioned studies formulate the beam selection/management as a classification problem. On the other hand, it is formulated as a regression problem in [19] for a single/multi-cell mmWave network.

ML methods can also be used in the beam management procedures after initial access, procedure P-1, to improve the radio performance using the channel state information reference signal (CSI-RS) [2]. ML-based methods for predicting a narrow Tx-end beam have been proposed in [20] and [21], replacing CSI-RS by the RSRP, AoA, and the timing advance of the Tx-end wide beam as inputs. References [22] and [23] use mobility patterns of users to proactively predict better future beams, whereas [24] proposes a beam recovery scheme for link blockages in highly dynamic mmWave networks.

In the majority of studies focused on ML-aided beam management, DNNs have been the preferred choice. Within the dynamic framework of 5G NR, where optimal beam configurations are contingent upon numerous factors like user location and channel conditions, DNNs are capable of autonomously identifying and leveraging crucial features. This ability significantly reduces the necessity for explicit manual feature engineering. Moreover, the relationships between input parameters and optimal beam configurations often exhibit nonlinear characteristics. Consequently, DNNs excel at representing and learning these intricate relationships, providing a powerful tool for addressing the complexities inherent in beam management tasks [25].

Communications security mainly relies on cryptography techniques and related protocols at the upper layers of the data communication stack. Physical layer security (PLS) has emerged as a new set of techniques employed at the physical layer to either strengthen the high level cryptographic security schemes, or to alleviate their computational overhead [26], [27], [28]. PLS schemes, many of which make use of ML algorithms, can be classified into three domains: channel, signal, and coding-based [29]. A DL-based PLS scheme that predicts the channel coefficients between the legitimate parties is proposed in [30], and a comparison between the proposed scheme and zero forcing based beamforming for mMIMO channels in terms of the secrecy rate and the secrecy outage probability is provided. A trade-off between DL-aided PLS and reliability in terms of the intercept probability and the outage probability is presented in [31]. In our previous work [32], we had presented the maximum probability that a transmission is successfully received at the intended receiver while the most detrimental eavesdropper is denied reception, with varying antenna array size, number of coordinated transmission points, and adaptive transmit power.

In this study, we propose a DNN-based autonomous beam management scheme to predict the most secure beam pair indices between the gNB and the UE during the initial access procedure. A certain level of security against eavesdropping attacks is provided by the intrinsic properties

of mMIMO and beamforming without using any further security mechanisms like artificial noise injection, secure key generation, directional modulation, etc. [33]. The proposed scheme is consistent with 5G NR signaling and does not require any modifications to the standard. It uses only the location of the receivers as input, and no additional channel information parameters including AoA, PDPs, RSRP levels, CSI-RS, etc.

The main goal of the proposed beam management scheme is to improve the beam search/sweeping process in terms of both latency and energy consumption by reducing the search space, while prioritizing communication security. The proposed scheme is evaluated on two different scenarios. In the first one, the data is obtained from a radio network planning software that computes RSRP values using the parameters of a number of currently deployed cells and real 3D terrain information. Since the terrain model in the first scenario belongs to a specific geolocation and environment, we use a second scenario to extend our results to general cases. The second scenario is an artificial one in which the data is generated using a statistical channel model with 5G NR system variables defined in 3GPP procedure P-1. Furthermore, for each scenario, two different experiments are presented: one with an objective of maximizing RSRP, and the other also maximizing RSRP but subject to security constraints.

The beam search overhead is reduced by searching among the K best beam pairs reported by the DNN, instead of an exhaustive beam search over all the beam pairs. As figures of performance, the prediction accuracy (i.e. the proportion of experiments where the actual best beam pair index is among the best K pairs produced by the DNN) and the achieved RSRP level provided by the best beam pair among these Top-K pairs are obtained. Numerical results show that the proposed scheme can achieve 98% prediction accuracy even with $K = 1$ in certain scenarios. In all experiments, the Top-8 prediction accuracy remains above 90%, corresponding to an 8-fold reduction in beam search overhead when using 64 beam pairs. Furthermore, it is observed that in terms of Top-K accuracy, our proposed DNN model outperforms other ML classifiers, specifically multi-class support vector machines and the K-nearest neighbors algorithm, which serve as benchmarks in this study.

We propose a novel DNN-based secure initial access and beam alignment procedure, which is the first such study in the literature, to the best of the authors' knowledge. The key contributions of this work can be summarized as follows:

- The proposed scheme significantly reduces beam search latency and energy consumption compared to the standard P-1 procedure by limiting the number of beam directions in the search space.
- Instead of selecting the beam pair with the highest RSRP, the pair with the highest RSRP providing secure communications, if possible, is selected during the initial access and beam alignment procedure.

The rest of this paper is organized as follows. The system model that we consider for the proposed method is given in Section II. In Section III, we describe the proposed beam selection method. Performance analysis and numerical evaluation are presented in Section IV. Finally, Section V concludes the paper.

II. SYSTEM MODEL

In this section, we explore channel and antenna configurations, introducing Tx-Rx antenna patterns, steering vectors, and eavesdropper distribution. Subsequently, we detail the baseline beam selection process during initial access, covering aspects such as beam sweeping, measurement, reporting, and the selection criteria based on the standard.

A. CHANNEL AND ANTENNA CONFIGURATIONS

A multi-path propagation channel is adopted in which signals radiated from a transmitting array are reflected from multiple scatterers towards a receiving array. A half-wavelength spaced uniform rectangular array (URA) with $N = N_v \times N_h$ antenna elements is deployed at the gNB, where N_v and N_h are the number of antenna elements in the vertical and the horizontal, respectively. The steering matrix $A(\theta, \phi) \in \mathbb{C}^{N_v \times N_h}$ is the Kronecker product of the steering vectors of a URA in each dimension and given as

$$A(\theta, \phi) = a_v(\theta, \phi) \otimes a_h(\theta, \phi), \tag{1}$$

where (θ, ϕ) stands for the elevation and azimuth angles of the signal, and the steering vectors of the vertical and horizontal axes are respectively defined as

$$a_v(\theta, \phi) = [1, \cdots, e^{j(N_v-1)\pi \sin(\theta)\cos(\phi)}]^T, \tag{2}$$

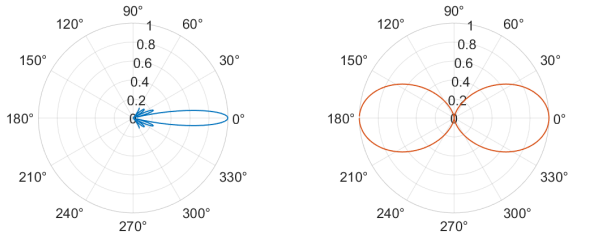
$$a_h(\theta, \phi) = [1, \cdots, e^{j(N_h-1)\pi \sin(\theta)\cos(\phi)}]^T. \tag{3}$$

We assume that the channel is constant over a symbol period and narrowband. The channel for receiver u is given by

$$H^{(u)} = \sum_{l=1}^{L_p} \alpha_l A(\theta_l^T, \phi_l^T) \otimes A^*(\theta_l^R, \phi_l^R) \in \mathbb{C}^{N \times M}, \tag{4}$$

where (θ_l^T, ϕ_l^T) and (θ_l^R, ϕ_l^R) are the angular pairs between the transmitter and the receiver at path l, $l \in \{1, \ldots, L_p\}$, with complex gain α_l and $M = M_v \times M_h$ is the number of antenna elements of the URA at receiver u. UE's antenna array is assumed to be properly oriented with respect to the gNB, i.e. a receiver could achieve the full antenna array gain even if its orientation is changed. The 2D array patterns of both Tx and Rx are shown in Figure 1. Also, an example mMIMO spatial scene that provides a combined view of these Tx and Rx arrays and the respective beams, along with the scatterers is demonstrated in Figure 2.

Legitimate users communicate through the gNB in the presence of eavesdroppers. For a particular legitimate user,



(a) Tx (8×8 antenna elements) (b) Rx (2×2 antenna elements)

FIGURE 1. mMIMO beam patterns of Tx-Rx arrays.

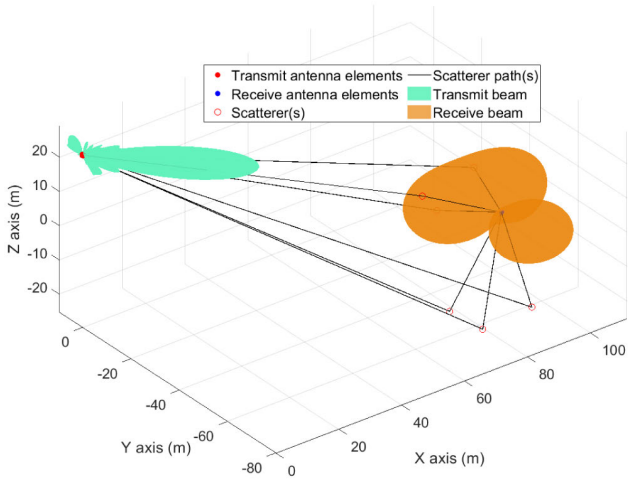


FIGURE 2. An example mMIMO spatial scene with Tx-Rx beams and scatterers.

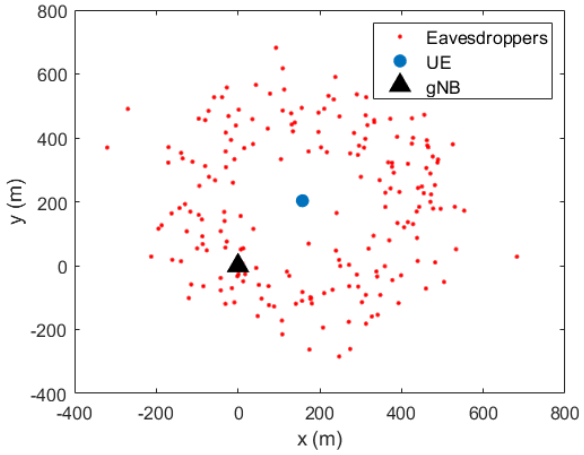


FIGURE 3. The possible eavesdropper locations.

an eavesdropper is randomly placed at a normally distributed random distance with a mean of 300 m and a standard deviation of $\sqrt{5000}$ m, with the angle between the horizontal and the line connecting the user and its eavesdropper uniformly distributed in $[0, 2\pi)$, as illustrated in Figure 3. It is clear that an eavesdropper can be located inside the region between gNB and UE, or outside of it. We assume that eavesdroppers have the same capabilities and antenna configurations (array size, sweep limits, etc.) as the legitimate users.

B. BEAM SELECTION DURING INITIAL ACCESS

A gNB transmits beams sweeping all directions in a burst at regularly defined intervals within the azimuthal and elevation limits. Whenever a UE is synchronizing with the network, it reads the SSB and extracts the primary synchronization signal (PSS), the secondary synchronization signal (SSS), the physical broadcast channel (PBCH), and the demodulation reference signal (DMRS) [34]. A single SSB spans four orthogonal frequency-division multiplexing (OFDM) symbols in time and 240 subcarriers in frequency (20 resource blocks). Each SSB belongs to a specific beam, beamformed in a different direction. A group of SSBs forms one synchronization signal (SS) burst set that spans a 5 ms window. The SS burst is broadcast to different directions in every 20 ms [35]. A group of eight SSBs forms one SS burst set, which corresponds to frequency range-1 (FR-1) from 3 to 7.125 GHz [2]. During the initial acquisition, beam sweeping is used by the UE to select the best beam.

After the initial beam alignment, the same beam pair link can be used for subsequent transmissions. If necessary, the beams can be further refined using CSI-RS for downlink and sounding reference signal (SRS) for uplink. In case of beam failure, these pair links can be re-established.

SS-RSRP Layer 1 measurements are useful for beam management procedures. The mapping between the reported and the measured values for Layer 1 and Layer 3 RSRP is specified in [36]. After applying Layer 1 filtering at the receiver, the RSRP measurement is performed and reported for each beamformed signal $f_{i,j}$ where i and j represent the transmitter and the receiver beam indices, respectively. For simplicity, Tx-Rx powers, gain factors, and large-scale signal-to-noise ratio (SNR) values are aggregated and denoted with a single value γ_u. The measured RSRP with an additive noise power n is obtained as

$$P_{i,j}^{(u)} = \frac{\gamma_u}{N \times M} \left\| \tilde{H}^{(u)} f_{i,j} \right\|_2^2 + n, \tag{5}$$

where $\|\cdot\|_2$ stands for the l_2 norm. Since the value in Eq. (5) is for a specific beamformed signal, the highest RSRP value needs to be found by searching over the entire spatial region, and the best beam pair indices are given as

$$b^{(u)} = \underset{\substack{1 \le i \le K_T \\ 1 \le j \le K_R}}{\arg\max} P_{i,j}^{(u)}, \tag{6}$$

where K_T and K_R are the number of beams at transmit and receive ends, respectively. Since the operating frequency in this study is 3.5 GHz (n78), the SSB transmission pattern is standardized as Case B [34] in which we have eight beams in both Tx and Rx ends ($i, j \in \{1, \ldots, 8\}$). Hence, the best pair is searched over a total of 64 beam pairs, which we enumerate as $(i, j) \mapsto b = 8(i-1) + j$, $b \in \{1, \ldots, 64\}$. This baseline beam selection algorithm to find the highest RSRP among all beam pairs (for general K_T and K_R) is given in Algorithm 1.

It should be noted that the baseline beam selection algorithm considers neither the minimum RSRP level

Algorithm 1 Baseline Beam Selection Algorithm

Input: Receiver u
Output: Selected beam pair index $b^{(u)}$

$P_{\max} = -\infty$
$b^{(u)} = 1$
for $i = 1$ to K_T **do**
  for $j = 1$ to K_R **do**
    Measure $P_{i,j}^{(u)}$
    if $P_{i,j}^{(u)} > P_{\max}$ **then**
      $P_{\max} = P_{i,j}^{(u)}$
      $b^{(u)} = (i-1)K_R + j$
    end if
  end for
end for

required for reception, nor security in the presence of eavesdroppers.

III. DEEP LEARNING-BASED SECURE BEAM SELECTION

In this section, we describe our proposed beam selection procedure for secure initial access. We assume that an eavesdropper is present in the system, whose location is unknown to the UE. We define a threshold value, β, which represents the minimum RSRP level needed at the receiver side (either legitimate or eavesdropper) to successfully decode the received signal. The expected outcome of the proposed procedure is to maximize the RSRP for the legitimate user, while keeping the RSRP at the eavesdropper below β, if possible. If this is achieved, we say that secure and successful communication has occurred.

We propose a DNN scheme to avoid repeatedly performing an exhaustive search and to reduce the communication overhead. The beam selection problem is posed as a classification task, where the target output is the best Tx-Rx beam pair index and receiver coordinates are used as input to the DNN algorithm. Given this out-of-band information, a trained DNN model recommends a set of K good beam pairs. Instead of an exhaustive search over all the beam pairs, the beam sweeping overhead is reduced by searching only among the selected K beam pairs. Note that, as the number of beams is increased the time overhead while beam sweeping also increases. Current 5G standards for the mmWave bands utilize 64 beams in both the Tx and the Rx ends.

We use two different scenarios to define (and later, evaluate) the proposed DL-based procedure. The data for the first scenario, called *the terrain model*, is obtained from a network planning software that computes RSRP values using the parameters of a number of currently deployed cells and real 3D terrain information. In order to obtain a more general idea about the performance of the proposed method, we also use a second scenario, which we name *the statistical model*. The data for this second model is artificially generated using a statistical channel model with 5G NR system variables defined in 3GPP procedure P-1.

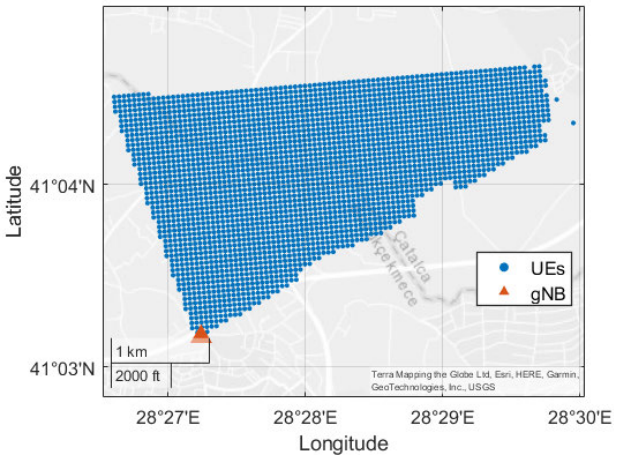


FIGURE 4. User distributions in a real cellular cluster served by a single cell.

For the terrain model, the realistic radio coverage from a base station at İstanbul/Büyükçekmece district in Türkiye, operating at 3.5 GHz is considered. The coverage levels are calculated using a 3D-map-based simulation tool, and validated through a mobile service provider's operational data and drive tests. This site represents a typical urban environment in İstanbul, characterized by high user density and heavy traffic loads. The dataset is built in the following manner:

(i) The RSRP values at 9700 uniformly distributed geographic points, as seen in Figure 4, are computed by a map-based radio network planning software using the parameters of the deployed cells and real 3D terrain information of the region.
(ii) mMIMO antenna gains for all Tx-Rx beam pairs are added to the calculated channel gains as a post-process. Eight beams are assumed on both Tx and Rx ends.
(iii) Finally, the best beam pair for each hypothetical user is determined over all the beam pairs via exhaustive search according to Algorithm 2, where the beam pair that provides the maximum RSRP above β for the UE, among those pairs that lead to RSRP levels below β for the eavesdropper is selected. If no such pair can be found, the pair that provides the maximum RSRP for the UE (even if that pair cannot provide secure communications) is selected. The eavesdropper is randomly generated as explained earlier (see Figure 3). For the training phase, it is assumed that the eavesdropper locations are known, so that the true optimal beam pair can be identified.

In addition to the terrain model, which is based on the radio coverage calculated by a map-based simulation tool from a real base station site, we also use a more general "statistical model," which employs statistically generated multi-path channels, for generalization of our results. Since the terrain model in the first scenario is specific to a particular environment, we aim to broaden the scope of our findings by introducing a second scenario.

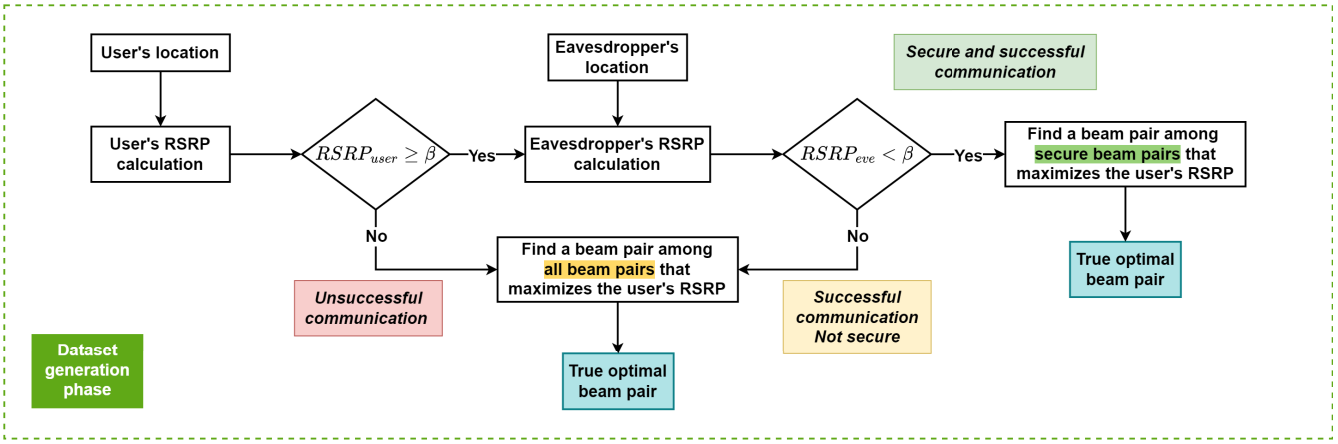


FIGURE 5. The data generation phase of the DNN model.

Algorithm 2 Secure Beam Selection Algorithm

Input: Receiver u, RSRP matrices $P^{(u)}$, $P^{(e)}$
Output: Selected beam pair index $b^{(u)}$, Flags *CommPossible*, *SecureCommPossible*

CommPossible = False
SecureCommPossible = False
$P_{\text{max,all}} = -\infty$
$P_{\text{max,sec}} = -\infty$
for $i = 1$ to K_T **do**
  for $j = 1$ to K_R **do**
    if $P_{i,j}^{(u)} > P_{\text{max,all}}$ **then**
      $P_{\text{max,all}} = P_{i,j}^{(u)}$
      $b_{\text{max,all}} = (i-1)K_R + j$
    end if
    if $P_{i,j}^{(u)} \geq \beta$ **then**
      CommPossible = True
      if $P_{i,j}^{(e)} < \beta$ **then**
        SecureCommPossible = True
        if $P_{\text{max,sec}} < P_{i,j}^{(u)}$ **then**
          SecureCommPossible = True
          $P_{\text{max,sec}} = P_{i,j}^{(u)}$
          $b_{\text{max,sec}} = (i-1)K_R + j$
        end if
      end if
    end if
  end for
end for
if *SecureCommPossible* **then**
  $b^{(u)} = b_{\text{max,sec}}$
else
  $b^{(u)} = b_{\text{max,all}}$
end if

In this artificial setting, we incorporate key variables from a 5G NR system. This approach allows us to explore the generalizability of our results beyond the confines of a specific environment, providing insights into the broader implications and applicability of our study. The same gNB and UE locations are used in this dataset as in the terrain model. We use the 5G toolbox of Matlab [37] to generate the dataset for the statistical model. A spatial scattering MIMO channel is configured with multiple scatterers and both gNB and UEs are equipped with uniform rectangular arrays (URAs) with 8-by-8 and 2-by-2 antenna elements, respectively. To achieve TRP beam sweeping, each of the SSBs is beamformed in the generated burst using analog beamforming. Based on the number of SSBs in the burst and the sweep ranges specified, both the azimuth and elevation directions for the different beams are determined. Then the individual blocks within the burst to each of these directions are beamformed. This beamformed burst waveform is then transmitted over the configured spatially-aware scattering channel. For receive-end beam sweeping, the transmitted beamformed burst waveform is received successively over each receive beam. For K_T transmit beams and K_R receive beams in procedure P-1, each of the K_T beams is transmitted K_R times from gNB so that each transmit beam is received over the M receive beams. In this study, both K_T and K_R are equal to the number of SSBs in the burst and only one burst is generated for simplicity. After the dual-sweep is completed over a time duration of $K_T \times K_R$ time slots for each receive beam, the best beam pair is selected based on the complete set of measurements made. The step-by-step illustration of the data generation phase is given in in Figure 5.

After completing the dataset generation for both terrain and statistical models, we initiate the training phase of the DNN by using a multi-layer perceptron (MLP) as a neural network model since MLPs are well-suited for classification prediction problems, leveraging their capacity to capture intricate patterns through hidden layers of neurons. In these tasks, inputs and outputs are assigned specific classes or labels [38]. To this end, in our work, we applied an MLP model that uses receiver locations as the input to the neural network. The output is a ranking of the beam pairs between Tx and Rx according to the selected coverage criteria.

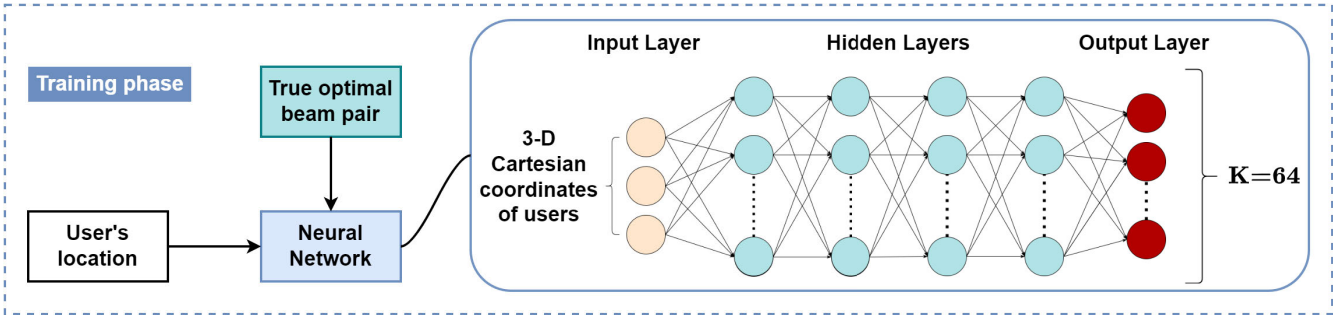


FIGURE 6. The training phase of the DNN model and the model architecture.

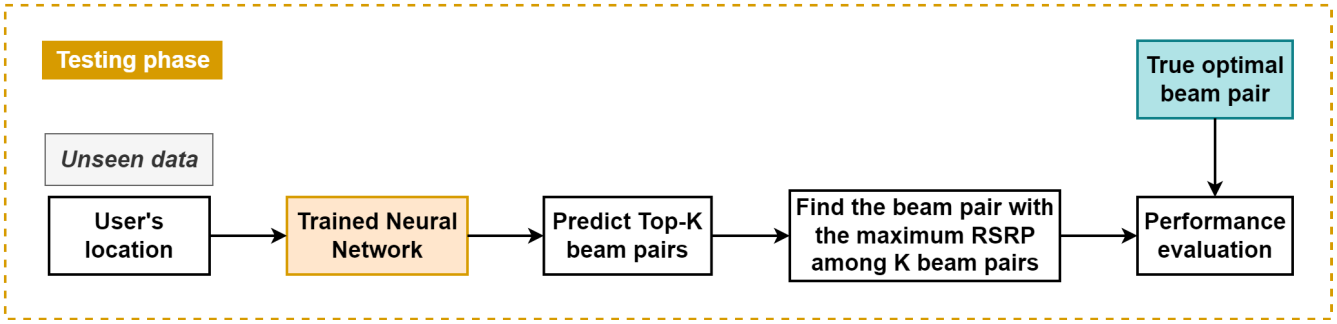


FIGURE 7. The testing phase of the DNN model.

TABLE 1. Results of the varying model hyperparameters.

Hidden layers	Neurons (each layer)	Loss	Accuracy (%)	Recall	Precision
3	24	1.1794	64.90	0.0988	0.0811
	96	0.9467	67.30	0.1179	0.1119
	384	0.9367	69.37	0.1399	0.1373
4	24	1.1074	66.37	0.1008	0.0833
	96	**0.9179**	**69.51**	**0.1318**	**0.1331**
	384	0.9310	69.86	0.1177	0.1170
5	24	1.1867	66.86	0.1011	0.0826
	96	0.9106	69.96	0.1226	0.1521
	384	0.9083	69.91	0.1208	0.1130

DL models have two distinct types of hyperparameters: model hyperparameters, which shape the model's architecture, including the number of hidden layers, and neurons per layer, allowing you to define its complexity, and optimizer hyperparameters, which influence the training process (e.g., learning rate, batch size, and the number of epochs) [39]. We explored various parameter configurations by examining combinations within the model hyperparameters. Table 1 presents the performance results of these experiments in terms of loss, accuracy, recall, and precision metrics to identify the suitable hyperparameters for our DNN model. Note that these results correspond to the terrain model, and the DNN predicts a beam pair by selecting the one with the highest probability under security constraints. Numerical results of the selected hyperparameters, shown in bold, are compared with benchmarks in Section IV-C.

After tuning the hyperparameters, the proposed neural network has four hidden layers with 96 neurons in each layer. As seen in Table 1, adding additional layers beyond four only slightly improves the model's accuracy while maintaining the same number of neurons. Similarly, increasing the number of neurons leads to improved accuracy but comes with a significant increase in computational cost. Once a certain threshold of neurons in each layer is reached (e.g., more than 96), the model's accuracy plateaus, and no significant improvements are observed. Each hidden layer consists of the fully connected layer with leaky rectified linear units as the activation function to ensure that all neurons in the network can contribute to the output, even if their inputs are negative. The 3-dimensional receiver locations based on GPS data are the input to the neural network. Hence, the input layer is of size 3, whereas the output layer's size is equal to the number of beam pairs. The learning rate, which governs the step size at each iteration, is set to 10^{-4}, while the other optimizer hyperparameters, namely the mini-batch size and the number of epochs, are configured as 256 and 1000, respectively. We also used an adaptive moment estimation (Adam) as the solver for training neural network because it can handle noisy problems and is suitable for most problems [40]. Class weighting is also applied such that the classes that occur more frequently in the dataset have smaller weights, and the classes that occur less frequently have larger weights. To quantify the error or discrepancy between the predicted values and the actual target values during the training process, we employ cross-entropy loss function which is a widely adopted and straightforward performance measure for classification tasks [41]. Cross-entropy loss, or log loss, measures the performance of a classification model whose output is a probability value between 0 and 1. It quantifies the

dissimilarity between predicted probabilities and true labels. The goal in using cross-entropy loss is to minimize this loss function during training. When the predicted probabilities are close to the true labels, the cross-entropy loss approaches zero, indicating a better model fit. The cross-entropy loss L_{CE} is calculated as

$$L_{CE} = -\frac{1}{T}\sum_{t=1}^{T}\sum_{k=1}^{K} w_k\, z_{tk}\, \ln y_{tk}, \tag{7}$$

where T is the number of samples, K is the number of classes, w_k is the weight for class k, z_{tk} is the indicator that the t-th sample belongs to the k-th class, and y_{tk} is the output for sample t for class k, which in this case, is the value from the softmax function. In other words, y_{tk} is the probability that the network associates the t-th input with class k. The training phase of the DNN model and its architecture is illustrated in Figure 6.

In the testing phase, the trained network is tested with unseen test data considering the Top-K accuracy metric, which has been widely used in the neural network-based beam selection task [3], [14].

Given a receiver location, K recommended beam pairs are found based on the neural network output. Then, an exhaustive sequential search on these K beam pairs is performed, and the one with the highest average RSRP is selected as the final prediction. The testing phase of the neural network is given in Figure 7. In both datasets, the total data is partitioned as 70% for training, 20% for validation, and 10% for test.

Experiments we performed showed that the complexity of the DNN increases exponentially with the number of layers. Given that we use the same number of neurons in each layer, the complexity converges to n^l, where n and represents the number of neurons in each layer and l is the number of layers. Additionally, adjusting the number of beams at the Tx/Rx ends directly affects the total number of beam pair indices, which serve as the output classes for the DNN, thereby altering the DNN training process. Similarly, incorporating a multi-cell environment introduces new possible beam pairs, leading to new output classes and impacting the DNN training dynamics. Therefore, variations in system parameters create distinct scenarios. As a result, each adjustment necessitates retraining the DNN for adaptation.

IV. PERFORMANCE ANALYSIS

In this section, we present the performance analysis of the proposed DNN scheme for both the terrain model and the statistical model. The main performance metric used is the Top-K accuracy metric, which is defined as the ratio of the number of the test cases where the actual best beam pair (found via exhaustive search) turns out to be among the Top-K values of the softmax distribution of the DNN that classifies the beam pairs, to the total number of test cases.

The performance of the proposed DNN method in terms of Top-K accuracy is compared to four benchmarks. Each of the following schemes produces K recommended beam pairs:

TABLE 2. Simulation parameters.

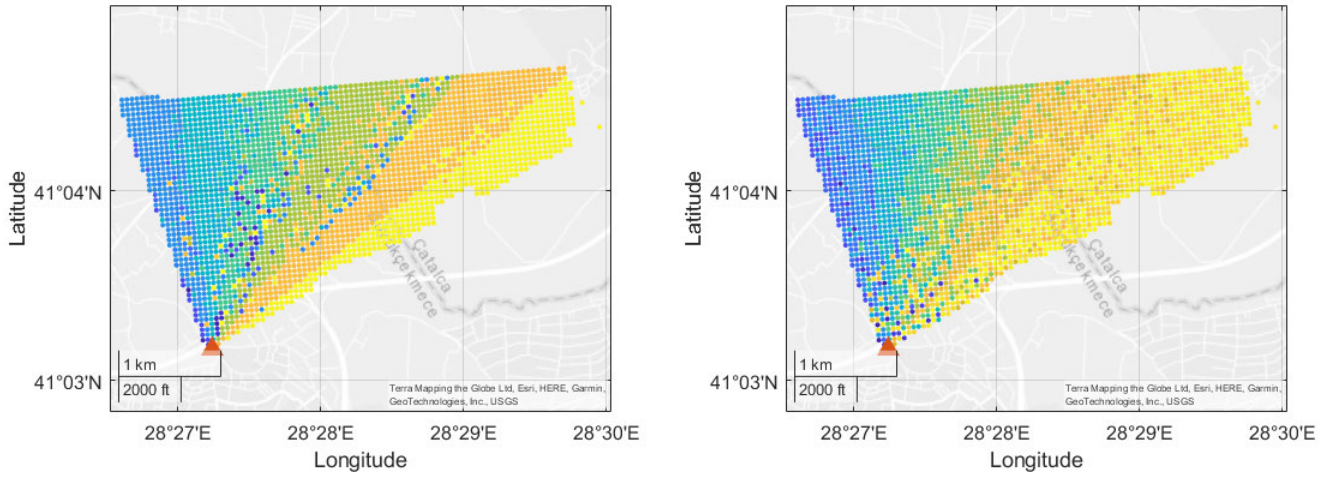
Parameter	Value
Frequency range	FR1 (410 MHz – 7.125 GHz)
Center frequency	3.5 GHz
SSB pattern	Case B
SSB length	8
Transmit array size, [rows cols]	[8 8]
Transmit azimuthal sweep limits	[-60, 60] (in 15° increments)
Transmit elevation sweep limits	[-90, 0]
Transmitter height	25 m
Receive array size, [rows cols]	[2 2]
Receive azimuthal sweep limits	[-180, 180]
Receive elevation sweep limits	[0, 90]
Receiver height	1.5 m
SNR	30 dB
RSRP mode	SSS with DMRS
Number of scatterers for each receiver (for the statistical model)	6
The security threshold β	-60 dBm [42]
Total number of users	9700
Total number of training data	6790
Total number of validation data	2037
Total number of test data	873

- Multi-class support vector machine (SVM) classifier: Since beam pair prediction involves a multi-class classification scenario, we employ a multi-class SVM classifier. We implement an error-correcting output codes (ECOC) scheme, which consists of $K(K-1)/2$ binary SVM models using the one-versus-one coding design. Here, K represents the number of unique class labels, with each class corresponding to a unique beam pair index in our work.
- K-nearest neighbors algorithm (KNN): Classification via KNN takes into account the K nearest training data points to a given test data point, and returns the result of a majority vote as the output. In our study, we take the beam pairs assigned to the K nearest (based on GPS coordinates, i.e. Euclidean distances) training data points for every test data point, which constitutes a list of Top-K beam pairs (some of which might be repeated).
- Statistical Choice: This scheme sorts all the beam pairs according to their relative frequency in the entire training data, and then picks the Top-K beam pairs (for any given test data point).
- Random: This scheme randomly (uniformly) selects K beam pairs.

For both models, we present two different experiments:

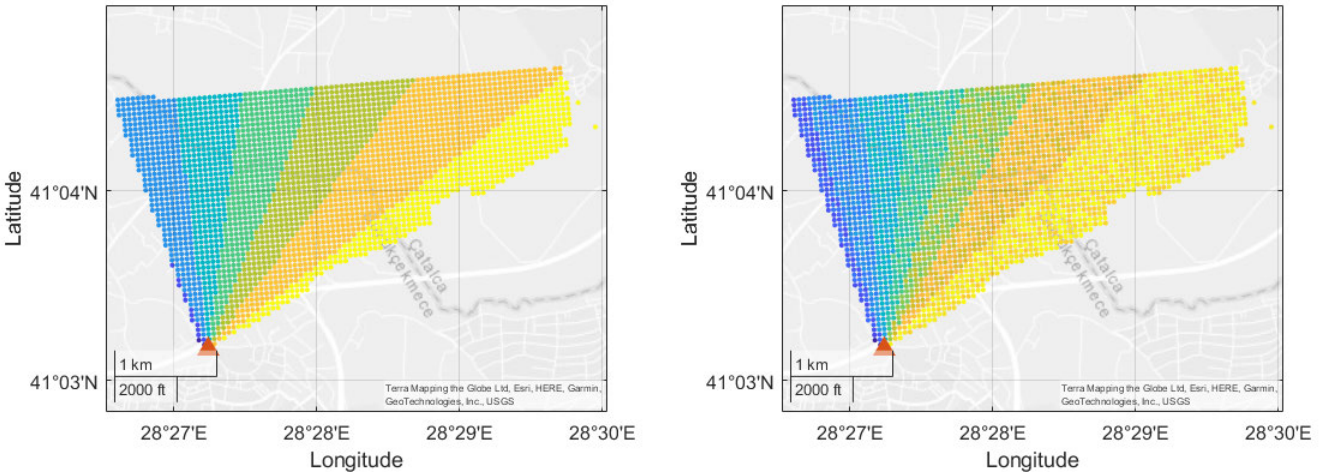
(i) with an objective of maximizing RSRP subject to security constraints,
(ii) with an objective of maximizing RSRP, disregarding security.

The second set of experiments are taken as a baseline that will demonstrate the amount of loss in terms of RSRP when security constraints are imposed. The difference between the performance levels of the two experiments can be seen



(a) for the terrain model (b) for the statistical model

FIGURE 8. The best Tx beams subject to security constraints for each user. Each color represents a different Tx beam.



(a) for the terrain model (b) for the statistical model

FIGURE 9. The best Tx beams disregarding security for each user. Each color represents a different Tx beam.

as the price paid in terms of signal strength for achieving communication security. For both experiments, the structure of the DNNs used (in terms of the number of layers and neurons) are the same. But clearly, as the best beam pairs for each objective can be different, the two systems have their own separate DNNs.

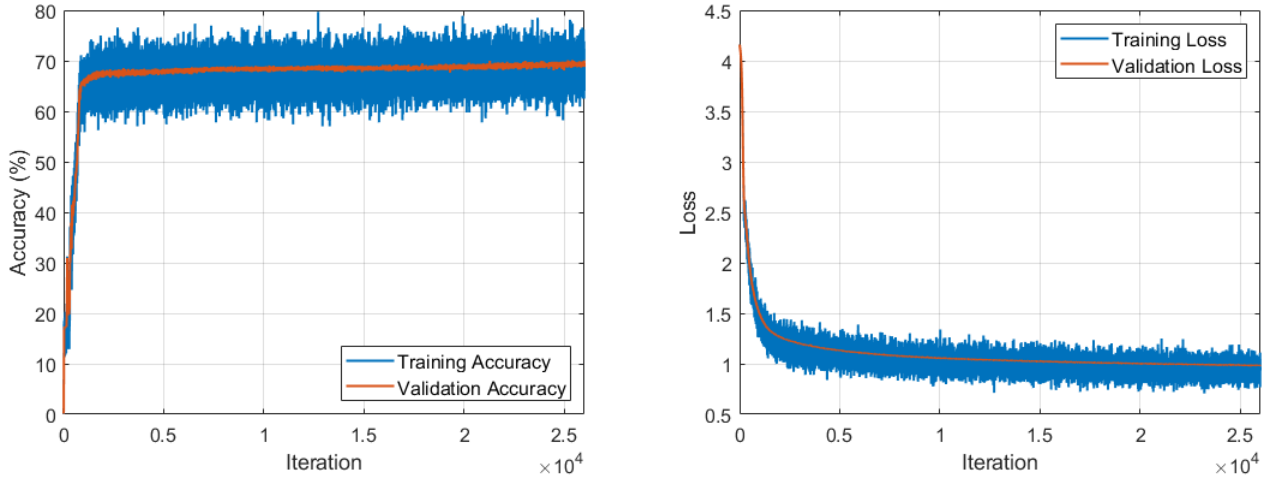
Depending on the locations of the UE and the eavesdropper as well as the value of β, it may or may not be possible to achieve secure communications, or even successful communications in some cases. We define two other metrics to quantify these probabilities. The successful detection (SD) probability, P_{SD}, is defined as the probability that the UE gets an RSRP above β, whereas the secure and successful detection (SSD) probability, P_{SSD}, is defined as the probability that the UE gets an RSRP above β and the eavesdropper gets an RSRP below β. Again, the difference between these two metrics is an indicator of the price paid to achieve a certain level of security.

A. THE TERRAIN MODEL

In this scenario, we use radio coverage levels based on real 3D terrain data obtained for a real cellular cluster in a network of a cell serving Long-Term Evolution (LTE) subscribers. RSRP values are acquired from this cell with a particular sector angle at 9700 uniformly distributed geographic points, as shown in Figure 4. To simulate the effect of mMIMO for the hypothetical users at each of these locations, the existing panel antenna gain is subtracted from the RSRP level, and then mMIMO antenna gains for each Tx-Rx beam pair is added.

For a particular legitimate user, an eavesdropper is selected from 200 potential eavesdropper locations around the user with 300 m mean distance as shown in Figure 3. Hence, we determine whether a hypothetical eavesdropper can receive the signal with sufficient power at its location. The received power of the legitimate user u in dBm is given by,

$$P_{i,j}^{(u)} = P_T + G_{T_i}^{(u)} + G_{R_j}^{(u)} - P_L^{(u)}, \tag{8}$$



(a) Training and validation accuracy

(b) Training and validation loss

FIGURE 10. The training progress of the proposed DNN in terms of accuracy and loss when $K = 1$.

where P_T is the transmit power in dBm, $G_{T_n}^{(s)}$ and $G_{R_m}^{(s)}$ are the antenna gains in dB for the n^{th} Tx beam and m^{th} Rx beam, respectively, observed by user s (or eavesdropper), and $P_L^{(s)}$ is path loss in dB towards transmitter to user s (or eavesdropper). The same definitions in Eq. (8) are valid for the wiretap links for an eavesdropper like below,

$$P_{i,k}^{(e)} = P_T + G_{T_i}^{(e)} + G_{R_k}^{(e)} - P_L^{(e)}. \tag{9}$$

B. THE STATISTICAL CHANNEL MODEL

Since the data for the terrain model is based on a specific site with a specific channel behavior due to the terrain structure, we chose to produce additional results for a more generic scenario. In this statistical model, we keep the entire scenario the same including the 5G NR system and other parameters as given in Table 2, user and gNB locations, antenna array configurations etc., but instead of the channel behavior for the terrain model, we use a spatial scattering MIMO channel configured with six scatterers for each user, and an eavesdropper placed randomly around them, as the air interface. This channel model applies free space path loss.

After the dual-end sweeping is completed, SS-RSRP is measured for each beam pair by using DMRS in addditon to SSS assuming the SSB information is known at the receiver. Finally, the best beam-pair is determined based on the RSRP measurement for the desired purpose of beam selection, which are explained in Algorithms 1 and 2 for the highest RSRP and security, respectively. The secure and successful detection condition defined earlier with the same threshold value is also applied in this scenario. The eavesdroppers for each user follow the same reception procedures for their ends, but since there will be no coordination between the gNB and the eavesdropper, and an eavesdropper measures its own RSRP based on the Tx beam selected for the legitimate user and can improve its RSRP only by receive-end beam sweeping, this procedure becomes single-end sweeping.

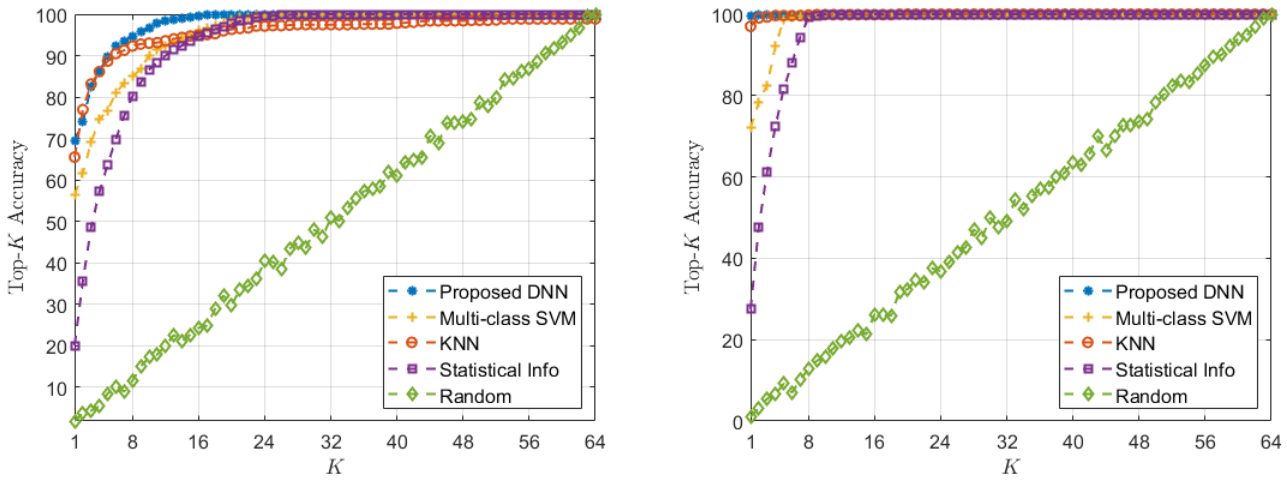
C. SIMULATION RESULTS

The first step of the study is the generation of the dataset. Based on the environmental settings described previously, the inputs and the outputs of the two datasets (the terrain model and the statistical model) are generated and used for training the proposed DNN scheme in both beam selection tasks (RSRP maximization with and without security constraints).

In Figures 8 and 9, the Tx beams that give the highest RSRP with and without security constraints, respectively, are illustrated on the map for all users. These figures are obtained by exhaustive search. We see that the best Tx beams when security constraints are imposed have much more variability, showing that the beam that gives the highest RSRP is not always the best choice when security is taken into account.

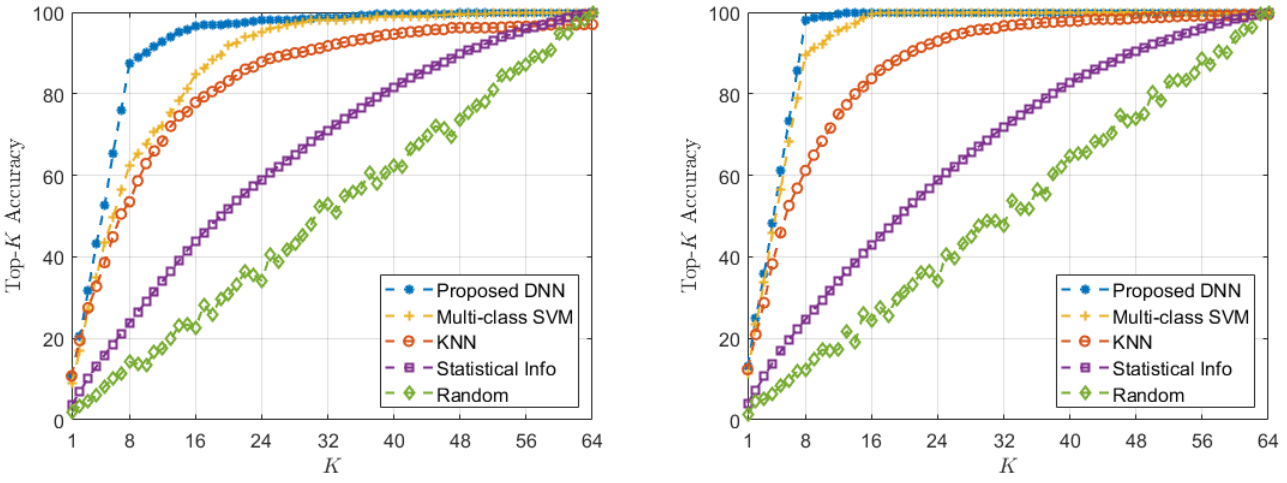
Figure 10 displays the training progress of the proposed DNN in terms of accuracy and loss. To predict the best beam ($K = 1$) under a security constraint for the terrain data, we found that the final validation loss (as given in Eq. 7) and the accuracy of the DNN are 0.92 and 69.5%, respectively. Additionally, in Figure 10b, both the validation and training loss of the proposed model are well-fitted, confirming that our model does not suffer from overfitting or underfitting issues.

The Top-K accuracy of the proposed DNN under the terrain model settings with and without security constraints are given in Figures 11a and 11b, respectively. When security is not an objective, we see that the proposed DNN is highly effective and already achieves more than 98% accuracy even with $K = 1$, whereas the accuracy reaches 90% with $K = 6$ when security constraints are imposed. This demonstrates that finding the best beam pair providing secure communications among all 64 beam pairs is a more difficult task than finding the beam pair which gives the highest RSRP. We can also conclude that, depending on the accuracy requirements, the proposed DNN can significantly improve the beam selection overhead compared to exhaustive search, as sufficiently good performance can be attained with



(a) with security constraints (b) without security constraints

FIGURE 11. The prediction performance comparison of different schemes for the terrain model.



(a) with security constraints (b) without security constraints

FIGURE 12. The prediction performance comparison of different schemes for the statistical model.

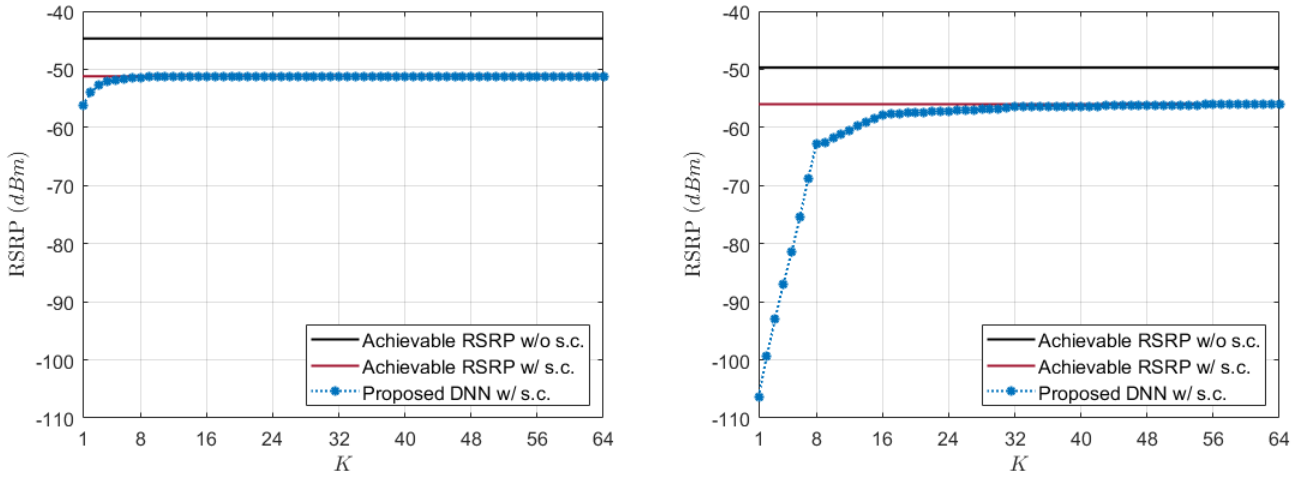
TABLE 3. Classification metrics comparison for learning schemes when $K = 1$ in the terrain model.

Learning scheme	Accuracy (%)	Recall	Precision
Proposed DNN	69.51	0.1318	0.1331
Multi-class SVM	56.36	0.0309	0.0357
KNN	65.52	0.0931	0.0982

low K values. For instance, Figure 11a shows that, for K values 5, 8, and 16, Top-K accuracy levels are 89.69%, 94.73%, and 99.66%, which lead to 12.8-, 8-, and 4-fold overhead reduction, respectively. Furthermore, the proposed DNN outperforms the other methods, especially for lower K values, highlighting the performance gains of the DNN in terms of overhead reduction. Numeric results in terms of accuracy, precision, and recall metrics to compare the proposed DNN with multi-class SVM and KNN are given in Table 3 when $K = 1$ in the terrain model.

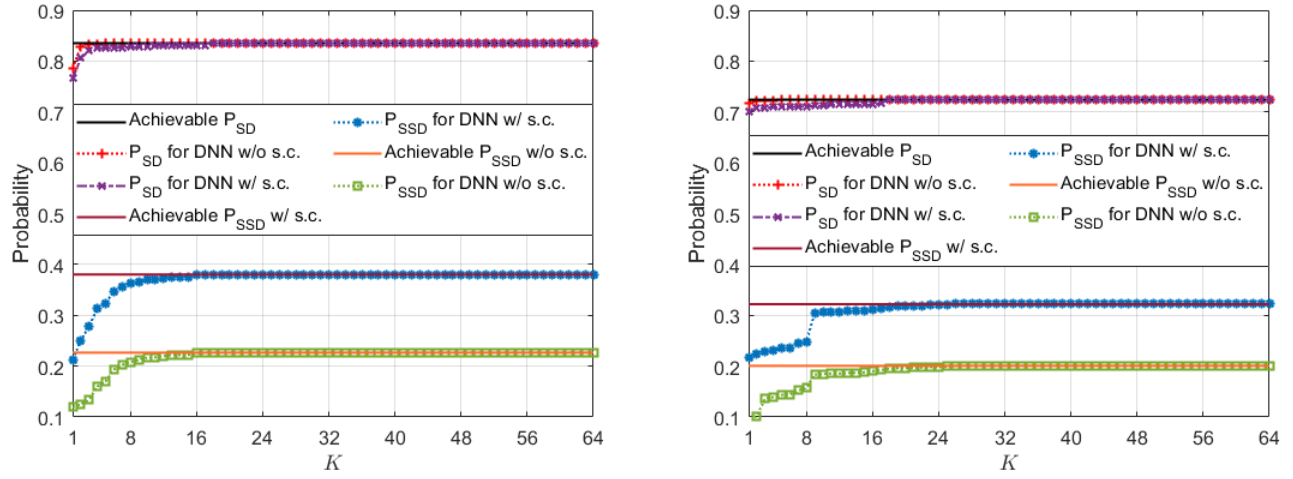
The Top-K accuracy under the statistical model settings with and without security constraints are given in Figures 12a and 12b, respectively. We see a similar pattern here in that the accuracy when security constraints are not considered (Figure 12b), reaches 97.53% when $K = 8$, whereas the accuracy is at 90.10% with $K = 8$, and at 97.87% when $K = 16$, when security is taken into account.

In Figures 13a (for the terrain model) and 13b (for the statistical model), we see the RSRP levels for three cases: (i) the highest achievable RSRP level, where security constraints are disregarded, found from exhaustive search over all possible beam pairs, (ii) the highest achievable RSRP level when security constraints are imposed, found from exhaustive search over all possible beam pairs (see Algorithm 2 on page 6), and (iii) the average RSRP level achieved when the proposed DNN scheme is used and beam selection is performed over the Top-K beam pairs. As observed, there is a 6.51 dB loss in the highest achievable



(a) for the terrain model (b) for the statistical model

FIGURE 13. The achievable RSRP levels with and without security constraints (s.c.), and the RSRP levels the proposed method achieves using the Top-K beam pairs.



(a) for the terrain model (b) for the statistical model

FIGURE 14. The achievable P_{SD} and P_{SSD} probabilities with and without security constraints (s.c.), and the P_{SD} and P_{SSD} probabilities the proposed method achieves using the Top-K beam pairs.

RSRP level when security constraints are imposed in the terrain model, whereas this loss is 6.31 dB for the statistical model. This difference in the highest achievable RSRP level can be regarded as the cost of securing the communication, whenever possible. For the terrain model, the proposed method achieves 96.73% (0.1444 dB difference) and 99.89% (0.0047 dB difference) of the achievable RSRP level with security constraints when the Top-8 and Top-16 beam pairs, respectively, are used for beam selection. On the other hand, these figures are at 20.90% (6.7993 dB difference) and 66.13% (1.7961 dB difference) with the Top-8 and Top-16 beam pairs, respectively, for the statistical model.

We present the SD and SSD probabilities (with and without security constraints) in Figure 14. It should be noted that neither model leads to a P_{SD} value of 1. This means that, due to the placement of the UEs, there are cases where it is not possible for the UE to see an RSRP that exceeds β with none of the beam pairs, and hence, communications will fail. Furthermore, as the achievable P_{SSD} is below P_{SD} (and by extension, below 1), there are cases where security cannot be achieved, no matter which beam pair is used, due to the placement of the eavesdropper, even if successful communication is possible. It can be seen that there is a meaningful difference between the achievable P_{SSD} values obtained from the DNN systems with and without security constraints, showing that the proposed method provides a significant improvement in communication security. For the terrain model, when the Top-8 and Top-16 beam pairs are used for beam selection, P_{SSD} turns out to be 95.19% and 99.71% of the achievable P_{SSD} value, which is 0.3803. This is 1.6812 times the achievable P_{SSD} by the system with no security constraints, 0.2265. Similarly, for the statistical model, Top-8 and Top-16 P_{SSD} values are 77.23% and 96.80% of the achievable P_{SSD} value, which is 0.3219.

This is 1.6055 times the achievable P_{SSD} by the system with no security constraints, 0.2005. We also see that the curves for P_{SD} for both models when security constraints are imposed are almost on top of the P_{SD} curves for the system without security constraints. Therefore, we conclude that the proposed method does not sacrifice communication success to improve security.

V. CONCLUSION

In this paper, we propose a DL-based secure beam selection method that improves the initial beam selection in 5G and beyond systems. The improvement in the initial beam selection process provided by the proposed method is two-folds: (i) Communication security is enhanced by selecting a beam pair that not only maximizes the RSRP of the UE, but also aims to keep the RSRP seen by the eavesdropper below a threshold. (ii) The time incurred, and thus the energy consumed, by the initial beam selection process is significantly reduced by cutting the search space down. The proposed method uses only location information and does not rely on any channel parameters or estimation procedure. Furthermore, no additional PLS method is used, and no modifications on the existing standards is necessary. While our work aligns with 5G NR signaling procedures, variations in system parameters, given in Table 2, introduce unique scenarios, requiring DNN retraining for adaptation with each change. Numerical evaluation results show that up to 92.19% reduction (from 64 down to 5) in the beam pair search space is possible with an accuracy of 89.69%, whereas an accuracy of 99.66% is possible with a reduction of 75% (from 64 down to 16) in the beam pair search space. The secure communication probability is improved by up to 68.12%, compared to the system without security constraints.

Possible future research directions can be into designing a DNN scheme for beam refinement procedures at both Tx and Rx ends. In addition, multi-cell scenarios involving coordinated multi-point will be explored especially for beam switching and beam recovery with a focus on security.

REFERENCES

[1] Y. Heng, J. G. Andrews, J. Mo, V. Va, A. Ali, B. L. Ng, and J. C. Zhang, "Six key challenges for beam management in 5.5G and 6G systems," *IEEE Commun. Mag.*, vol. 59, no. 7, pp. 74–79, Jul. 2021.

[2] *Study on New Radio Access Technology Physical Layer Aspects*, document TR 38.802, version 14.2.0, 3GPP, Sep. 2017. [Online]. Available: https://www.3gpp.org/DynaReport/38802

[3] M. Giordani, M. Polese, A. Roy, D. Castor, and M. Zorzi, "A tutorial on beam management for 3GPP NR at mmWave frequencies," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 173–196, 1st Quart., 2019.

[4] W. Attaoui, K. Bouraqia, and E. Sabir, "Initial access & beam alignment for mmWave and terahertz communications," *IEEE Access*, vol. 10, pp. 35363–35397, 2022.

[5] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2224–2287, 3rd Quart., 2019.

[6] K. Ma, Z. Wang, W. Tian, S. Chen, and L. Hanzo, "Deep learning for beam-management: State-of-the-art, opportunities and challenges," 2021, *arXiv:2111.11177*.

[7] M. Arvinte, M. Tavares, and D. Samardzija, "Beam management in 5G NR using geolocation side information," in *Proc. 53rd Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2019, pp. 1–6.

[8] A. Klautau, P. Batista, N. González-Prelcic, Y. Wang, and R. W. Heath, "5G MIMO data for machine learning: Application to beam-selection using deep learning," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2018, pp. 1–9.

[9] D. C. Araujo and A. L. F. de Almeida, "Beam management solution using Q-learning framework," in *Proc. IEEE 8th Int. Workshop Comput. Adv. Multi-Sensor Adapt. Process. (CAMSAP)*, Dec. 2019, pp. 594–598.

[10] M. Polese, F. Restuccia, and T. Melodia, "DeepBeam: Deep waveform learning for coordination-free beam management in mmWave networks," in *Proc. 22nd Int. Symp. Theory, Algorithmic Found., Protocol Design Mobile Netw. Mobile Comput.* New York, NY, USA: Association for Computing Machinery, Jul. 2021, pp. 61–70, doi: 10.1145/3466772.3467035.

[11] T. S. Cousik, V. K. Shah, J. H. Reed, T. Erpek, and Y. E. Sagduyu, "Fast initial access with deep learning for beam prediction in 5G mmWave networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2021, pp. 664–669.

[12] K. N. Nguyen, A. Ali, J. Mo, B. L. Ng, V. Va, and J. C. Zhang, "Beam management with orientation and RSRP using deep learning for beyond 5G systems," 2022, *arXiv:2202.02247*.

[13] M. Alrabeiah and A. Alkhateeb, "Deep learning for mmWave beam and blockage prediction using sub-6 GHz channels," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5504–5518, Sep. 2020.

[14] M. S. Sim, Y.-G. Lim, S. H. Park, L. Dai, and C.-B. Chae, "Deep learning-based mmWave beam selection for 5G NR/6G with sub-6 GHz channel information: Algorithms and prototype validation," *IEEE Access*, vol. 8, pp. 51634–51646, 2020.

[15] D. Jagyasi and M. Coupechoux, "DNN based beam selection in mmW heterogeneous networks," in *Network Games, Control and Optimization*, S. Lasaulce, P. Mertikopoulos, and A. Orda, Eds. Cham, Switzerland: Springer, 2021, pp. 172–184.

[16] I. Chafaa, R. Negrel, E. V. Belmega, and M. Debbah, "Self-supervised deep learning for mmWave beam steering exploiting sub-6 GHz channels," *IEEE Trans. Wireless Commun.*, vol. 21, no. 10, pp. 8803–8816, Oct. 2022.

[17] Y. Heng, J. Mo, and J. G. Andrews, "Learning site-specific probing beams for fast mmWave beam alignment," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 5785–5800, Aug. 2022.

[18] A. Alkhateeb, "DeepMIMO: A generic deep learning dataset for millimeter wave and massive MIMO applications," in *Proc. Inf. Theory Appl. Workshop (ITA)*, San Diego, CA, USA, Feb. 2019, pp. 1–8.

[19] X. Li, B. Gao, Y. Wang, Q. Luo, S. Shao, X. Yang, W. Yan, H. Wu, and B. Han, "Compressed beam selection for single/multi-cell beam management," in *Proc. IEEE 95th Veh. Technol. Conf.*, Jun. 2022, pp. 1–5.

[20] H. Patel, "Beam refinement and beam tracking using machine learning techniques in 5G NR RAN," M.S. thesis, Faculty Comput., Blekinge Inst. Technol., Lund, Sweden, 2021.

[21] B. Wang, "Adaptive beam management in 5G-NR: A machine learning perspective," M.S. thesis, Dept. Elect. Inf. Technol., Lund Univ., Lund, Sweden, 2021.

[22] A. Ö. Kaya and H. Viswanathan, "Deep learning-based predictive beam management for 5G mmWave systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2021, pp. 1–7.

[23] W. Na, B. Bae, S. Cho, and N. Kim, "Deep-learning based adaptive beam management technique for mobile high-speed 5G mmWave networks," in *Proc. IEEE 9th Int. Conf. Consum. Electron. (ICCE-Berlin)*, Sep. 2019, pp. 149–151.

[24] A. Aldalbahi, F. Shahabi, and M. Jasim, "Instantaneous beam prediction scheme against link blockage in mmWave communications," *Appl. Sci.*, vol. 11, no. 12, p. 5601, Jun. 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/12/5601

[25] D. D. S. Brilhante, J. C. Manjarres, R. Moreira, L. D. O. Veiga, J. F. de Rezende, F. Müller, A. Klautau, L. L. Mendes, and F. A. P. de Figueiredo, "A literature survey on AI-aided beamforming and beam management for 5G and 6G systems," *Sensors*, vol. 23, no. 9, p. 4359, Apr. 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/9/4359

[26] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[27] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[28] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.
[29] A. K. Kamboj, P. Jindal, and P. Verma, "Machine learning-based physical layer security: Techniques, open challenges, and applications," *Wireless Netw.*, vol. 27, no. 8, pp. 5351–5383, Nov. 2021.
[30] C. I. Siyad and S. Tamilselvan, "Deep learning enabled physical layer security to combat eavesdropping in massive MIMO networks," in *Proc. 2nd Int. Conf. Comput. Netw. Commun. Technol.*, S. Smys, T. Senjyu, and P. Lafata, Eds. Cham, Switzerland: Springer, 2020, pp. 643–650.
[31] T. M. Hoang, D. Liu, T. V. Luong, J. Zhang, and L. Hanzo, "Deep learning aided physical-layer security: The security versus reliability trade-off," *IEEE Trans. Cognit. Commun. Netw.*, vol. 8, no. 2, pp. 442–453, Jun. 2022.
[32] U. Ozmat, M. F. Demirkol, and M. A. Yazici, "Service-based coverage for physical layer security with multi-point coordinated beamforming," in *Proc. IEEE 25th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Sep. 2020, pp. 1–6.
[33] W. Shi, X. Jiang, J. Hu, A. M. S. Abdelgader, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu, and J. Wang, "Physical layer security techniques for data transmission for future wireless networks," *Secur. Saf.*, vol. 1, 2022, Art. no. 2022007.
[34] *NR; Physical Channels and Modulation*, document TS 38.211, version 17.3.0, 3GPP, Sep. 2022. [Online]. Available: https://www.3gpp.org/DynaReport/38211
[35] *NR; Physical Layer Measurements*, document TS, 38.215, version 17.2.0, Sep. 2022. [Online]. Available: https://www.3gpp.org/DynaReport/38215
[36] *NR; Requirements for Support of Radio Resource Management*, document TS 38.133, version 17.7.0, 3GPP, Oct. 2022. [Online]. Available: https://www.3gpp.org/DynaReport/38133
[37] (2023). *5G Toolbox Version: 2.6 (R2023a)*, The MathWorks, Natick, MS, USA. [Online]. Available: https://www.mathworks.com/help/5g/
[38] P. Gupta and N. K. Sinha, "Chapter 14—Neural networks for identification of nonlinear systems: An overview," in *Soft Computing and Intelligent Systems* (Academic Series in Engineering), N. K. Sinha and M. M. Gupta, Eds. San Diego, CA, USA: Academic Press, 2000, pp. 337–356. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780126464900500172
[39] L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," *Neurocomputing*, vol. 415, pp. 295–316, Nov. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231220311693
[40] D. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proc. Int. Conf. Learn. Represent.*, Dec. 2014, pp. 1–15.
[41] C. Robert, "Machine learning, a probabilistic perspective," *CHANCE*, vol. 27, no. 2, pp. 62–63, Apr. 2014.
[42] R. Rudd and S. Kirtay, "Coverage thresholds for 5G services" Plum Consulting London LLP, London, U.K., Commission Commun. Regulation Consultants Rep. 21/118a, Nov. 2021. [Online]. Available: https://www.comreg.ie/media/2021/11/ComReg-21118a.pdf

UTKU OZMAT (Member, IEEE) received the B.S. degree in electrical and electronics engineering from Istanbul University, Turkey, in 2012, and the M.S. degree in telecommunication engineering from Istanbul Technical University, Turkey, in 2016, where he is currently pursuing the Ph.D. degree in cybersecurity engineering and cryptography. He was a Senior Research and Development Engineer with NETAS, Huawei Technologies, and Ulak Communication Inc., from 2015 to 2021. Since 2021, he has been a 5G Program Management Expert with Turk Telekom. His research interests include deep learning-driven physical layer operations, advanced antenna systems, spectrum and power planning, and physical layer security for 5G and beyond networks.

MEHMET AKIF YAZICI received the B.Sc. and M.Sc. degrees in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, and the Ph.D. degree from Bilkent University, Ankara. He was with the Department of Computer Science, University of Antwerp, Belgium, as a Postdoctoral Researcher, from 2014 to 2015. Since 2016, he has been with the Informatics Institute, Istanbul Technical University, Turkey, where he is currently an Assistant Professor. His research interests include computer and communication networks, performance evaluation, stochastic modeling, and queueing theory.

MEHMET FATIH DEMIRKOL (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Southern California, in 1998, and the M.Sc. and Ph.D. degrees from the Georgia Institute of Technology, in 2000 and 2003, respectively. Between 2003 and 2007, he was an Assistant Professor with the Hawaii Center for Advanced Communications, University of Hawaii. Between 2007 and 2020, he held various positions in the mobile communications industry with Turkcell, Avea, Huawei Technologies, and Ulak Communications. Since 2020, he has been a Data Scientist with Prorize LLC. His research interests include wireless communications and signal processing for communications.