3D Beamforming Based on Deep Learning for Secure Communication in 5G and Beyond Wireless Networks

Helin Yang[1], Kwok-Yan Lam[1,2], Jiangtian Nie[2], Jun Zhao[1,2], Sahil Garg[3], Liang Xiao[4], Zehui Xiong[5], and Mohsen Guizani[6]

[1]Strategic Centre for Research in Privacy-Preserving Technologies and Systems, Nanyang Technological University, Singapore

[2]School of Computer Science and Engineering, Nanyang Technological University, Singapore

[3]Electrical Engineering Department, Ecole de technologie superieure, Universite du Quebec, Montreal, Canada

[4]School of Informatics, Xiamen University, Xiamen, China

[5]Pillar of Information System Technology and Design, Singapore University of Technology and Design, Singapore

[6]Department of Computer Science and Engineering, Qatar University, Doha, Qatar

Email: {hyang013, kwokyan.lam, jnie001, junzhao}@ntu.edu.sg, lxiao@xmu.edu.cn, mguizani@qu.edu.qa

2021 IEEE Globecom Workshops (GC Wkshps) | 978-1-6654-2390-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/GCWkshps52748.2021.9681960

***Abstract*—Three-dimensional (3D) beamforming is a potential technique to enhance communication security of new generation networks such as 5G and beyond. However, it is difficult to achieve optimal beamforming due to the challenges of non-convex optimization problem and imperfect channel state information (CSI). To tackle this problem, this paper proposes a novel deep learning-based 3D beamforming scheme, where a deep neural network (DNN) is trained to optimize the beamforming design for wireless signals in order to guard against eavesdropper under the imperfect CSI. With our approach, the system is capable of training the DNN model offline, and the trained model can then be adopted to instantaneously select the 3D secure beamforming matrix for achieving the maximum secrecy rate of the system, which is measured by the signal received by eavesdroppers outside the path of the beam. Simulation results demonstrate that the proposed solution outperforms the classical deep learning algorithm and 2D beamforming solution in terms of the secrecy rate and robust performance.**

***Index Terms*—3D beamforming, physical layer security, wireless security, deep learning, secrecy rate maximization.**

I. Introduction

Three-dimensional (3D) beamforming is one of the promising techniques to realize communication performance enhancement for fifth generation (5G) and beyond wireless networks [1]-[3]. In communication systems, compared with classical two-dimensional (2D) beamforming towards the ground only, 3D beamforming based on massive multiple-input multiple-output (MIMO) can provide the radiation patterns to desired directions in both vertical and horizontal space, which provides more signal power at the desired receivers and mitigate interference in cellular networks [2], [4]. Recently, 3D beamforming has been applied to improve the secure transmission in the physical layer security perspective [5]-[17]. In detail, due to the 3D nature of wireless channel between MIMO transmitters and receivers, 3D beamforming technique combines both the horizontal and vertical dimensions to enhance desired signal strength at legitimate device locations as well as minimize the information power leakage to nearby eavesdroppers, so that the high average spectral efficiency and secrecy data rate can be achieved.

In [5] and [6], the authors proposed advanced security model-based opportunistic non-orthogonal multiple access (NOMA) methods for 3D secure beamforming design in MIMO systems, and multicast interference reduction was also considered to improve the system throughput and secrecy capacity. Yaacoub *et al.* [7] studied a 3D beamforming approach based on massive MIMO antenna arrays to mitigate eavesdropping by sending a jamming signal under the location estimation error of the eavesdropper. 3D beamforming-based physical layer security in millimeter wave (mmWave) MIMO systems was studied to evaluate the secrecy rate performance [8] [9], and the exact secrecy rate was derived without any approximation. In addition, 3D beamforming based on mmWave was applied in dynamic 5G-based vehicle-to-everything communications to guarantee secure stable communications and quality-of-service (QoS) performance [10]. Liu *et al.* [11] studied the resource management optimization problem of joint power allocation and spectrum selection with the goal to maximize the sum secrecy rate in cellular mmWave networks, while imperfect channel state information (CSI) was considered in the study. Moreover, a location-based 3D beamforming method was presented to improve the secure communication performance for MIMO unmanned

978-1-6654-2390-8/21/$31.00 ©2021 IEEE

aerial vehicle (UAV)-enabled communication systems [12]. Both the two studies [11], [12] divided the optimization problem into two subproblems, and an effective iterative method was used to optimize the secrecy rate performance. However, the above works [5]-[12] mainly used traditional optimization techniques, e.g., Karush–Kuhn–Tucker conditions, Lagrange optimization algorithms to solve the 3D beamforming problem in secure communication systems, which is ineffective in dynamic and complex 5G and beyond wireless networks. In addition, these classical algorithms may converge a suboptimal point and get the greedy-search like performance as they ignore the historical information of wireless networks and the long term benefit.

In this case, machine learning techniques were used to optimize the secure beamforming matrix in MIMO systems [13]-[18]. Our previous work [13], [14] have demonstrated that machine learning based beamforming can significantly improve the commutation performance in dynamic and complex wireless networks. In [15], a multi-agent deep reinforcement learning was presented to optimize the 3D beamforming strategy to improve the UAV-enabled secure communications, and trajectory of UAVs and transmit power were also jointly optimized. Bao $et\ al.$ [16] studied the secrecy outage performance under multiple UAV eavesdroppers, and a deep learning based beamforming model was presented to predict the secrecy rate performance. Considering the partial CSI in practical MIMO systems, a 3D robust beamforming scheme for UAV commutation systems was proposed [17], where a precisely designed deep learning was trained to optimize the beamformer. However, the literature [17] only considered one legitimate user and one eavesdropper, and the inter-used interference is not studied in this work.

In order to better optimize the beamformer for secure communications in large-scale MIMO systems, this paper proposes an advanced deep learning-based 3D beamforming in the physical layer security perspective. In detail, aiming at achieving the maximum secrecy rate of the system against an eavesdropper, a precisely designed deep neural network (DNN) is trained to optimize the beamforming strategy for confidential signal with considering outdated channel information of legitimate mobile devices. This design can train the DNN model offline, and use the trained learning model to select secure beamforming matrix in real-time, which is measured by the signal received by eavesdroppers outside the path of the beam. Simulation results show that the proposed solution outperforms the classical deep learning algorithm and 2D beamforming.

The paper is organized as follows: Section II provides the system model and problem formulation. The deep learning based 3D secure beamforming scheme is presented in Section III. Section IV shows the simulation results and analysis. Conclusion is offered in Section V.

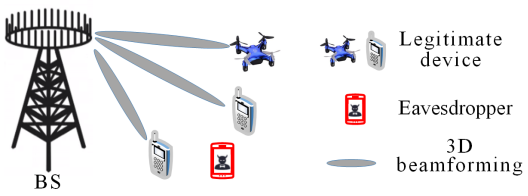

Fig. 1. 3D beamforming for secure communication systems.

II. System Model and Problem Formulation

A. System Model

We consider a downlink MIMO wireless system, as illustrated in Fig. 1, where a base station (BS) is equipped with M_t ($M_t = M_x \times M_y$ uniform planar array (UPA)) directional transmission antennas to server legitimate mobile devices, and each device is equipped with N_r receive antennas. The mobile device set is denoted by $\mathcal{K} = \{1, 2, ..., K\}$. In addition, we assume that one eavesdropper equipped with N_r^{e} receive antennas aims to eavesdrop any of the data streams of the legitimate devices.

According to the aforementioned standard [1], the resultant 3D channel between the BS antenna port s and one mobile device's or eavesdropper's antenna port u at time t is given by

$$\begin{aligned} h_{l,u,s}(t) = &\sum_{n=1}^{N} \begin{bmatrix} \Gamma_{rx,u,\theta_{rx}}(\Phi_{l,n}) \\ \Gamma_{rx,u,\phi_{rx}}(\Phi_{l,n}) \end{bmatrix}^T \\ &\times \begin{bmatrix} a_{l,n,\theta_{rx},\theta_{rx}} & a_{l,n,\theta_{tx},\phi_{rx}} \\ a_{l,n,\phi_{rx},\theta_{tx}} & a_{l,n,\phi_{tx},\phi_{tx}} \end{bmatrix} \begin{bmatrix} \Gamma_{tx,u,\theta_{rx}}(\Omega_{l,n}) \\ \Gamma_{tx,s,\phi_{tx}}(\Omega_{l,n}) \end{bmatrix}, \\ &\times \exp(j2\pi\lambda_0^{-1}(\Phi_{l,n} r_{rx,u})) \exp(j2\pi\lambda_0^{-1}(\Phi_{l,n} r_{tx,u})) \\ &\times \exp(j2\pi\lambda_0^{-1} f_{d,l,n} t) \end{aligned} \tag{1}$$

where ϕ_{tx} and ϕ_{rx} are the azimuth angle of departure and azimuth angle of arrival , θ_{tx} and θ_{rx} represent the elevation angle of departure and elevation angle of arrival for the each multipath component. The parameter λ_0 denotes the wavelength carrier frequency. Let l and n denote the number of paths and subpaths, respectively. $\Gamma_{rx,u}$ and $\Gamma_{tx,u}$ denote the field pattern of the receive and the transmit antennas. $r_{rx,u}$ is a vector between the $u-\mathrm{th}$ receive antenna and the first antenna. For transmit antenna elements, $r_{tx,u}$ holds the same meaning as $r_{rx,u}$. $f_{d,l,n}$, $\Phi_l = \{\theta_{rx,l}, \phi_{rx,l}\}$ and $\Omega_l = \{\theta_{tx,l}, \phi_{tx,l}\}$ denote the Doppler shift, the angle of departure and the angle of arrival of the (l,n)-th propagation subpath. The polarization matrix of the (l,n)-th subpath from the p_1 polarization component to the p_2 polarization component is defined by a_{l,n,p_1,p_2}.

In the practical situation, due to the transmission and processing latency, it is difficult to achieve the perfect CSI. Thus, the outdated CSI needs to be considered in the system model. The delay between the outdated channel matrix and the accurate channel matrix is denoted by t_{d}. In this case,

the relationship between the outdated matrix $\mathbf{H}(t)$ and the accurate channel matrix $\mathbf{H}(t+t_{\mathrm{d}})$ is given by [14]

$$\mathbf{H}(t+t_{\mathrm{d}}) = \mu\mathbf{H}(t) + \sqrt{1-\mu^2}\widehat{\mathbf{H}}(t+t_{\mathrm{d}}), \tag{2}$$

In (2), $\widehat{\mathbf{H}}(t+t_{\mathrm{d}})$ is independent identically distributed with $\mathbf{H}(t)$ and $\mathbf{H}(t+t_{\mathrm{d}})$, μ denotes the outdated CSI coefficient of the channel matrix $\mathbf{H}(t)$ and $0 \leq \mu \leq 1$. Note that $\mu = 1$ means that the outdated CSI effect is eliminated, while $\mu = 0$ shows that no accurate CSI.

The received signal at the k-th device is expressed as

$$\mathbf{y}_k = \mathbf{H}_k\mathbf{v}_k\mathbf{s}_k + \underbrace{\mathbf{H}_k\sum\nolimits_{i\neq k}^{K}\mathbf{v}_i\mathbf{s}_i}_{\mathrm{inter-userinterference}} + \mathbf{n}_k, \tag{3}$$

where $\mathbf{H}_k$ denotes the channel matrix from the BS to the k-th device, $\mathbf{v}_k$ is the beamforming matrix for the k-th device, and $\mathbf{n}_k$ denotes its additive complex Gaussian noise vector with the with zero mean and variance .

The received signal at the eavesdropper is given by

$$\mathbf{y}^{\mathrm{e}} = \mathbf{H}^{\mathrm{e}}\sum\nolimits_{k=1}^{K}\mathbf{v}_k\mathbf{s}_k + \mathbf{n}^{\mathrm{e}}, \tag{4}$$

where $\mathbf{H}^{\mathrm{e}}$ is the channel matrix from the BS to the eavesdropper.

The achievable rate at the k-th device is expressed as

$$R_k = \log_2\left(1 + \frac{\left|\mathbf{H}_k\mathbf{v}_k\mathbf{s}_k\right|^2}{\sum_{i\neq k}^{K}\left|\mathbf{H}_k\mathbf{v}_i\mathbf{s}_i\right|^2 + \delta_k^2}\right). \tag{5}$$

If the eavesdropper aims to eavesdrop the legitimate signal of the k-th device, its achievable data rate is given by

$$R_k^{\mathrm{e}} = \log_2\left(1 + \frac{\left|\mathbf{H}^{\mathrm{e}}\mathbf{v}_k\mathbf{s}_k\right|^2}{\sum_{i\neq k}^{K}\left|\mathbf{H}_i\mathbf{v}_i\mathbf{s}_i\right|^2 + \delta_{\mathrm{e}}^2}\right). \tag{6}$$

B. Problem Formulation

In this paper, our objective is to maximize the achievable secrecy rate of each legitimate device by optimizing the beamforming matrix $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_K]$ at the BS while guaranteeing the minimum data rate of each device, then the optimization problem can be formulated by

$$\begin{aligned} \max_{\mathbf{V}} \quad & \min_{k\in\mathcal{K}}\left\{R_k^s \triangleq [R_k - R_k^{\mathrm{e}}]^+\right\} \\ s.t. \quad & \mathrm{Tr}\left(\mathbf{V}\mathbf{V}^H\right) \leq P_{\max}, \end{aligned}, \tag{7}$$

where $P_{\max}$ is the maximum transmit power at the BS, and $R_k^{\min}$ denotes the minimum data rate requirement of the k-th device. Constraint in (7) is used to satisfy the BS's maximum transmit power. It is easy to observe that the optimization problem in (7) is difficult to be solved directly as the objective function is non-convex with respect to $\mathbf{V}$.

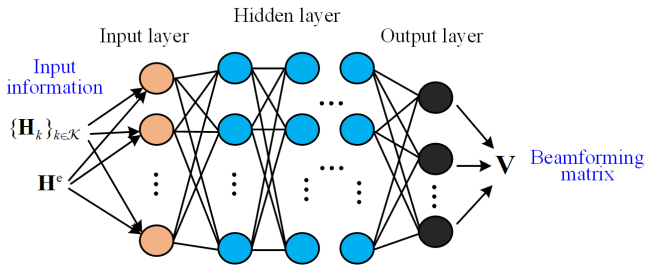

Fig. 2. Architecture of the DNN-based secure beamforming.

III. Proposed Deep Learning Driven 3D Secure Beamforming Design

This section introduces an application of deep learning for the secure beamforming design in downlink multi-user MIMO systems. Although the iterative algorithm can obtain the local optimal solution of the non-convex optimization problem, the iterative algorithm has a relatively high process complexity and the iterative calculation delay is long, and the beamforming matrix cannot be obtained in real time. Therefore, we can apply deep learning technology to address the secure beamforming optimization problem with the objective to maximize the secrecy data rate.

The learning model can be trained on a large number of channel information sets to make the neural network automatically analyze the internal characteristics of the channel, and then generate effective solutions to complex problems with relatively low complexity. Therefore, it is considered to combine the deep learning technology with the 3D beamforming optimization problem for maximum spectrum efficiency, and transfer the complexity of the problem to the stage of offline training of the neural network, so that the complexity of the online training is greatly reduced.

A. Offline Training Phase

The considered DNN architecture is composed of one input layer, multiple hidden layers, and one output layer, as shown in Fig. 2. Three hidden layers are applied to extract channel characteristic from the input channel information, where each hidden layer contains multiple neurons and neural elements between different layers are connected by weights. All hidden layers are fully connected layers, and activation functions are added after the hidden layer nodes, where the function of the activation function is to introduce non-linear transformations.

Input layer: Each input data in DNN is channel matrices ($\mathbf{H}_k$ and $\mathbf{H}^{\mathrm{e}}$) with multiple elements, as DNN currently does not support the use of complex channel coefficients as the input data of the neural network module, and thus each channel matrix should be divided into real-valued vectors without losing the imaginary-part information, and the input vector match has a large number of elements. In this context, the real part and the imaginary part of the channel matrix are

separated and rearranged to obtain a new channel information vector, which is used as the input of the first input layer.

Hidden layer: The DNN hidden layer includes three stages: convolution, nonlinear transformation, and down-sampling. The structure is shown in Fig. 2, the input of a single hidden layer is a feature map composed of a group of vectors, and the input signal of the first convolution stage can be regarded as a high-dimensional feature map with high sparsity. The output part of a single hidden layer is also a feature map composed of a set of vectors, and each output feature map corresponds to a specific feature extracted from the input feature map.

Output layer: The objective of the learning model is to solve the optimization problem (7) to achieve the maximum achievable secrecy rate, thus the model training process tries to minimize a loss function that measures the quality of the model predictions, which is expressed as

$$L\left(\mathbf{V}_i\right) = -\frac{1}{I}\sum_{i=1}^{I}\min_{k\in\mathcal{K}}\left\{R_k^s \triangleq [R_k - R_k^{\mathrm{e}}]^+\right\}_i, \qquad (8)$$

where I denotes the training batch size, $\mathbf{V}_i$ is the beamforming matrix at the BS for the i-th input $\mathbf{H}_k$ and $\mathbf{H}^{\mathrm{e}}$, $\left\{R_k^s \triangleq [R_k - R_k^{\mathrm{e}}]^+\right\}_i$ is the secrecy rate of the i-th input information. The available beamforming matrix $\mathbf{V}$ can be updated during the training process.

B. Online Prediction Phase

After the DNN-based secure beamforming model is trained, it can be applied for beamforming matrix selection. Specifically, once the channel matrices information is received from MIMO systems, it is firstly divided into the real and imaginary parts to get the real-value vector before putting it into the DNN model, and finally the output of the network is the estimation of the beamforming matrix $\mathbf{V}$. However, due to the negative effect of channel information feedback delay, the DNN output and the accurate beamforming matrix still have a certain deviation. Thus, in order to improve the prediction accuracy, we use the output of the DNN model as the initial value of the final beamformer estimation, and then apply the robust learning model to perform an search in a very small set near the initial value to achieve the final prediction, which is shown in **Algorithm 1**.

Algorithm 1 Proposed Deep Learning Based 3D Secure Beamforming

Phase 1: Offline training

1: **Input:** Training data set $\{\mathbf{H}_k, \mathbf{H}^{\mathrm{e}}\}_{k\in\mathcal{K}}$ and DNN architecture.
2: Initialize DNN model.
3: **for** each epoch **do**
4: **for** i=1 to I (batch size) **do**
5: Sample i-th training data (channel matrix information).
6: Calculate loss function by (8) and update DNN parameters.
7: **end for**
8: **end for**
9: **Output:** The trained DNN-based 3D secure beamforming model.

Phase 2: Online prediction

10: Download the trained DNN model.
11: **for** time slot t=1 to T **do**
12: Observe the channel information $\{\mathbf{H}_k(t), \mathbf{H}^{\mathrm{e}}(t)\}_{k\in\mathcal{K}}$ from MIMO system at the t-th slot.
13: Put $\{\mathbf{H}_k(t), \mathbf{H}^{\mathrm{e}}(t)\}_{k\in\mathcal{K}}$ into the trained model, and predict the initial beamforming matrix $\mathbf{V}'(t)$.
14: Interface with dynamic system and estimate the feedback delay by (2).
15: Put the outdated CSI $\widehat{\mathbf{H}}_k(t)$ into the offline training phase.
16: Calculate the secrecy rate $R_k^s(t)$: $R_k^s \triangleq [R_k - R_k^{\mathrm{e}}]^+$.
17: **end for**

C. Computational Complexity Analysis

Here, we provided the computational complexity analysis of both the offline training and online prediction in this section.

Offline training complexity: Let G, X_0 and X_g denote the number of the training layers, the size of the input layer (the channel matrix size), and the number of neurons in the g-th layer, respectively. The computational complexity at the i-th batch is $O(X_0X_1 + \sum_{g=1}^{G-1} X_gX_{g+1})$. Assume that the training process has N^{epi} episodes with each episode being with I batch size, and the DNN model is completed iteratively until convergence. Thus, the total computational complexity in our considered DNN-based 3D beamforming model is $O\left(N^{\mathrm{epi}}I(X_0X_1 + \sum_{g=1}^{G-1} X_gX_{g+1})\right)$ [14]. The computational complexity of deep learning in the training process is generally high, but it can be completed offline at the BS after a finite number of episodes.

Online prediction complexity: Similar to the study [17], here we apply the floating point operations to analyze the computational complexity of the proposed DNN-based beamforming model in online perdition state. As the model has been trained with a function, the complexity is mianly related to both the input and output dimensions. Let X_0 and X_G denote the dimensions of the input and output, then the number of computational operations of the DNN model is given by $(2X_0 - 1)X_G$ [17].

IV. Simulation Results and Analysis

This section provides simulation results to evaluate the performance of the proposed deep learning-based 3D secure beamforming scheme and compare it with other existing schemes. We set that the center frequency of carrier wave is 3.5 GHz, and the background noise power at the legitimate mobile devices and eavesdropper is equal to -90 dBm. Both the legitimate devices and the eavesdropper are equipped 4 antennas, and the number of transmit antennas at the BS

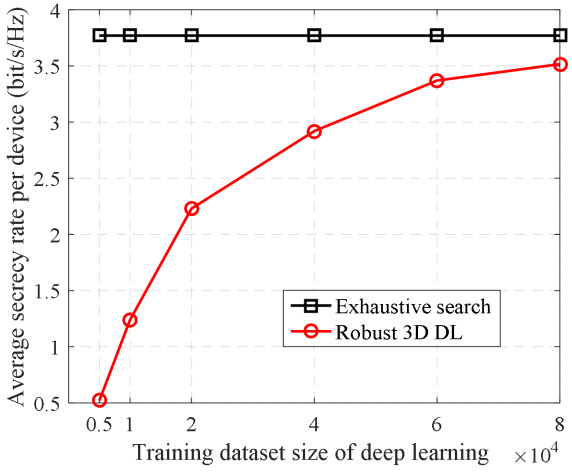

Fig. 3. The achievable secrecy rates of both the proposed deep learning solution and the upper bound (exhaustive search method).

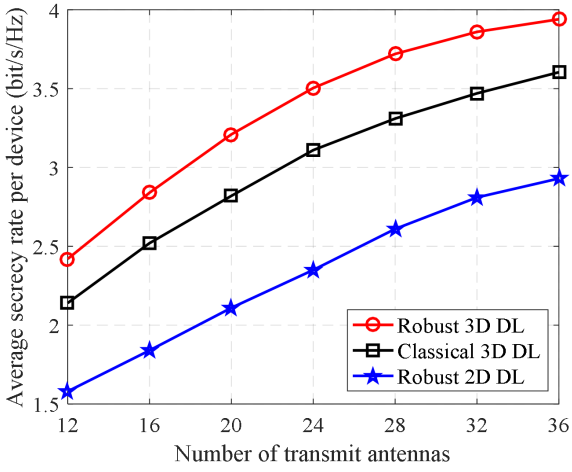

Fig. 4. Secrecy rate comparison with different BS transmit antenna numbers.

uniform planar array varies from 16 to 32 for different simulation settings. The number of legitimate mobile devices K is set to 2. In the MIMO system, 8×10^4 samples are applied for training and 2×10^4 samples are used for the 3D secure beamforming performance evaluation. The neural network architecture consists of there fully-connected hidden layers of 512, 256, and 256 nodes (neurons), respectively, and the learning rate of DNN is 0.0002.

The performance of the following beamforming schemes or algorithms are evaluated in this section: 1) our proposed robust 3D secure beamforming scheme based on deep learning with considering outdated CSI (denoted by Robust 3D DL); 2) the robust 2D secure beamforming scheme based on deep learning with considering outdated CSI (denoted by Robust 2D DL); 3) the 3D secure beamforming scheme based on deep learning without considering outdated CSI (denoted by classical 3D DL).

Fig. 3 shows the average secrecy rate per device of the proposed deep learning algorithm and the exhaustive method when the number of transmit antennas is 4×6. As illustrated, as the increased number of training samples, the secrecy rate performance of the proposed learning algorithm tends to be near the exhaustive search method. We can conclude that the proposed learning algorithm in this study not only is close to the performance of the exhaustive search algorithm, but also significantly reduces the complexity, and it is suitable for different channel scenarios. The above simulation result also shows that the more channel matrix information collected during learning and training process, the better the performance of the 3D secure beamforming based on deep learning.

Fig. 4 illustrates the average secrecy rate per device varying with the number of transmit antennas. The simulation result shows that as the number of transmit antennas increases, the performance of all algorithms monotonically enhances, with the benefit being brought by multiple antennas, and our

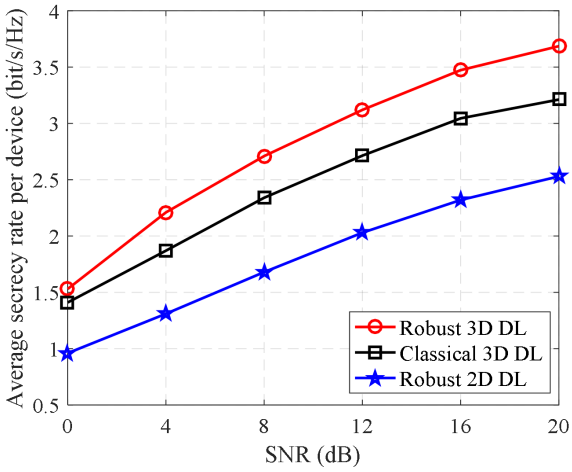

Fig. 5. Secrecy rate comparison with different SNR values.

proposed learning scheme achieves the highest secrecy rate. When the number of antennas at the BS is small, the performance difference among the three algorithms is small, but the advantage between our proposed scheme and other two schemes becomes more obviously during this process. It is important to note that the performance of the 3D secure beamforming scheme is significantly higher than that of the 2D secure beamforming. For example, when the number of transmit antennas is 24, the average secrecy rate of 3D and 2D beamforming schemes are 3.504 and 2.387 bit/s/Hz respectively, having 46.80% enhancement.

Fig. 5 represents the comparisons of the average secrecy rate per device among the three solutions with different signal-to-noise ratio (SNR) values. It can be seen that when the SNR is low, the performance of the three solutions cannot achieve considerable satisfaction. However, as the increase of SNR level, the performance gap between each other becomes more obviously, and the performance advantage of our proposed solution becomes more significant.

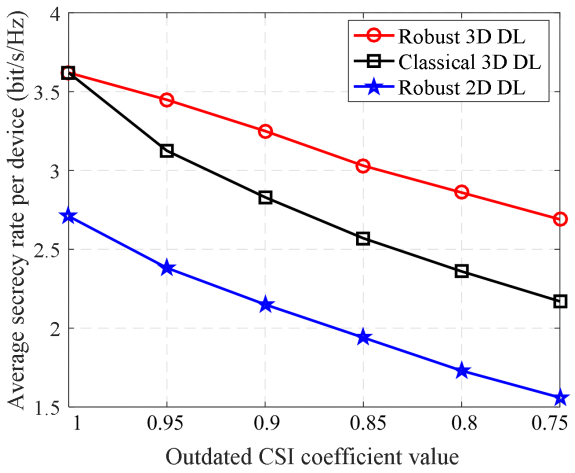

Fig. 6. Secrecy rate comparison versus outdated CSI coefficient.

We further analyze the effect of the outdated CSI coefficient μ on the system secrecy rate, when the number of transmit antennas is 4×6. As the illustrated from Fig. 6, the performance of all scheme declines as the decrease of the outdated CSI coefficient (CSI becomes more outdated), as the feedback delay increases and channel estimation error becomes more serious. However, we can observe that the classical DL algorithm without considering outdated CSI is more sensitive to the coefficient μ, and its secrecy rate drops more faster than that of our proposed leaning algorithm. The result also indicates that our presented learning algorithm obtains the best secure communication performance among three schemes against imperfect CSI in mobile wireless communication networks.

V. Conclusion

In this paper, in order to better optimize the beamforming matrix in large-scale 3D MIMO systems, we have proposed a 3D secure beamforming scheme based on deep learning. The custom Lamda layer and loss function are designed to deal with the MIMO system design with outdated CSI challenges. The proposed robust 3D secure beamforming achieved the better security performance than that of 2D secure beamforming. The simulation results indicated that, compared with existing deep learning algorithm, the proposed solution achieves high secrecy data rate, especially in the large number of transmit antennas and high SNR domain. In addition, the proposed learning model is more robust against the outdated CSI in dynamic scenarios.

VI. Acknowledgements

This research is supported by the National Research Foundation, Singapore under its Strategic Capability Research Centres Funding Initiative, Nanyang Technological University (NTU) Startup Grant, and SUTD SRG-ISTD-2021-165. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

References

[1] U. Karabulut, A. Awada, I. Viering, M. Simsek, and G. P. Fettweis, "Spatial and temporal channel characteristics of 5G 3D channel model with beamforming for user mobility investigations," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 38-45, Dec. 2018.

[2] Y. Huang, Q. Wu, R. Lu, X. Peng, and R. Zhang, "Massive MIMO for cellular-Connected UAV: Challenges and promising solutions," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 84-90, Feb. 2021.

[3] X. Li, S. Jin, H. A. Suraweera, J. Hou, and X. Gao, "Statistical 3-D beamforming for large-scale MIMO downlink systems over rician Fading channels," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1529-1543, Apr. 2016.

[4] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106-112, Jan. 2020.

[5] K. Xiao, L. Gong, and M. Kadoch, "Opportunistic multicast NOMA with security concerns in a 5G massive MIMO system," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 91-95, Mar 2018.

[6] X. Su, P. Nkurunziza, J. Gu, A. Castiglione, and C. Choi, "Inter-beam interference cancellation and physical layer security constraints by 3D polarized beamforming in power domain NOMA systems," *IEEE Trans. Sustainable Comp.*, vol. 5, no. 2, pp. 291-303, Apr. 2020.

[7] E. Yaacoub, M. Al-Husseini, A. Chehab, K. Abualsaud, T. Khattab, and M. Guizani, "3D beamforming with massive cylindrical arrays for physical layer secure data transmission," *IEEE Commun. Lett.*, vol. 23, no. 5, pp. 830-833, May 2019.

[8] H. Nguyen, D. Maurais-Galejs, T. Anderson, J. Krieger, W. Moulder, and J. Muldavin, "Scalable prototyping testbed for MMW imager system," in *Proc. IEEE International Symposium on Phased Array Systems and Technology (PAST)*, 2016, pp. 1-6

[9] B. You, I. -H. Lee, and H. Jung, "Optimal subset Size analysis of randomized analog beamforming using uniform planar arrays in mmWave networks," Appear in *IEEE Wireless Commun. Lett.*

[10] I. Rasheed, F. Hu, Y. -K. Hong and B. Balasubramanian, "Intelligent vehicle network routing with adaptive 3D beam alignment for mmWave 5G-Based V2X communications," *IEEE Trans. Intelligent Transportation Syst.*, vol. 22, no. 5, pp. 2706-2718, May 2021.

[11] Y. Liu, X. Fang, and M. Xiao, "Resource management for maximizing the secure sum rate in dense millimeter-wave networks," *IEEE Access*, vol. 8, pp. 158416-158431, 2020.

[12] Q. Yuan, Y. Hu, C. Wang, and Y. Li, "Joint 3D beamforming and trajectory design for UAV-enabled mobile relaying system," *IEEE Access*, vol. 7, pp. 26488-26496, 2019.

[13] H. Yang *et al.*, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1963-1974, Mar. 2021

[14] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 375-388, Jan. 2021.

[15] Y. Zhang, Z. Mou, F. Gao, J. Jiang, R. Ding, and Z. Han, "UAV-enabled secure communications by multi-agent deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11599-11611, Oct. 2020.

[16] T. Bao, J. Zhu, H. -C. Yang, and M. O. Hasna, "Secrecy outage performance of ground-to-air communications with multiple aerial eavesdroppers and its deep learning evaluation," *IEEE Wireless Commun. Lett.*, vol. 9, no. 9, pp. 1351-1355, Sept. 2020,

[17] R. Dong, B. Wang, and K. Cao, "Deep learning driven 3D robust beamforming for secure communication of UAV systems," Appear in *IEEE Wireless Commun. Lett.*

[18] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep reinforcement learning-enabled secure visible light communication against eavesdropping," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6994-7005, Oct. 2019.