VNU Journal of Science: Com. Science & Com. Eng. Vol. 42, No. xx (2026) xx–xx

VNU Journal of Science:
Computer Science and Communication Engineering

Journal homepage: http://www.jcsce.vnu.edu.vn/index.php/jcsce

Original Article

A Novel LSTM-based OFDM Channel Estimation for Adversarial Attack Defending

Minh Hoang Tran, Thi Thuy Quynh Tran, Trieu Duong Dinh*

VNU University of Engineering and Technology, Hanoi, Vietnam

Received 19th September 2025
Revised 19th April 2026; Accepted 18th May 2026

Abstract: In this paper, we propose a novel Long Short-Term Memory-based channel estimation (LSTM-CE) method which can effectively detect and protect OFDM systems from adversarial attacks. Adversarial attack is a kind of pilot jamming. Generally, this attack is intentionally created to directly attack a neural network, distorting the channel estimation and severely degrading the performance of the OFDM system. Unlike conventional neuron networks based channel estimation, in the proposed LSTM-CE method, we define a novel loss function owning the target to optimize the training process, and to effectively eliminate the effect of adversarial attack. In addition, the effect of perturbations caused by adversarial attack along the time and frequency axes has been carefully analyzed to determine the optimal LSTM model. The experimental results show that the proposed LSTM-CE method can not only detect adversarial attacks well but also effectively exploit the relationship in time and frequency domains to improve the performance of channel estimation as compared to other conventional methods.

Keywords: Channel Estimation, Adversarial Attack, LSTM.

1. Introduction

Orthogonal frequency division multiplexing (OFDM) is among the most important technologies for a modern wireless communication system. Owing to its robust capabilities to frequency-selective fading and its bandwidth efficiency, OFDM has been adopted in both 4G and 5G standards.

In a wireless system, the transmitted signal is typically subjected to distortion, fading, and path loss on account of the characteristics of the propagation channel. The received signal is also corrupted by additive noise jamming or interference, further degrading the quality of the signal. For reliable recovery of the transmitted signal in an OFDM system, the degradation associated with the propagation channel needs to be effectively estimated and compensated. The traditional pilot-based estimation methods, such as Least Square (LS) or Minimum Mean

*Corresponding author.
E-mail address: duongdt@vnu.edu.vn

https://doi.org/10.25073/2588-1086/vnucsce.5818

Square Error (MMSE), find the unknown signal in the propagation channel by using the pilot values in time-frequency domain. LS channel estimation method is widely used since it doesn't require high computational complexity, however, it is more susceptible to noise, which leads to lower performance. MMSE channel estimation method offers more optimal performance than LS method, but it requires prior knowledge of second-order channel statistics [1]. These channel statistics are often difficult to obtain or change continuously in practice. Additionally, its high computational complexity due to large matrix inversions makes MMSE method hard to implement in real-time systems.

In recent years, deep learning (DL) has been widely investigated for physical-layer wireless communications, including signal detection, modulation recognition, decoding, and channel estimation [2], [3]. Unlike conventional estimators that rely heavily on analytical assumptions or prior channel statistics, deep learning-based estimators can learn a direct nonlinear mapping from noisy pilot observations to channel coefficients from data. This data-driven approach allows them to capture complex channel characteristics and noise patterns that traditional methods may fail to model accurately. Several recent studies have applied deep neural networks to channel estimation and reported clear performance improvements over traditional methods. Dong et al. [4] designed a CNN-based channel estimation model that show superior performance compared to traditional methods. Wang et al. [5] introduced a LSTM-based channel estimation model designed for high-frequency Multiple-Input Multiple-Output (MIMO) Single-Carrier Frequency Domain Equalization (SC-FDE) systems. Their work brilliantly addresses the tracking of natural time-varying multipath fading by utilizing an online updating mechanism to prevent accumulation errors. Khichar et al. [6] recently proposed a Fast Super-Resolution CNN (FSRCNN) model (referred to herein as CNN-CE) that achieve great performance compared to standard methods with less computational complexity. However, the performance of these DL-based channel estimation methods can be severely degraded due to the effect of adversarial attacks [7]. Adversarial attack is a kind of pilot jamming and it is intentionally designed to directly attack the neural network-based channel estimation method.

In order to solve the problem caused by the adversarial attack, Park et al. [7] designed an attack training process (ATP) to defend a system from the effect of adversarial attack. Experimental results show that the neural network-based channel estimation using the ATP scheme has better performance compared to those without using the ATP.

In this paper, we proposed a novel channel estimation method named Long Short-Term Memory-based channel estimation (LSTM-CE) which can effectively defends against adversarial attacks while maintaining superior channel estimation performance. The proposed method integrates an LSTM network with an effective adversarial training technique. Unlike conventional neural network-based channel estimation approaches, our proposed method defines a novel loss function to optimize the training process and effectively eliminate the effect of adversarial attacks. The proposed LSTM-CE model exploits both time and frequency domain correlations in the wireless channel response to enhance channel estimation accuracy. Furthermore, we carefully analyze the effect of perturbations caused by adversarial attacks along both time and frequency axes to determine the optimal LSTM architecture for robust channel estimation. Through extensive simulations, we demonstrate that the proposed LSTM-CE method not only achieves superior channel estimation performance under normal conditions but also maintains remarkable resilience against adversarial attacks compared

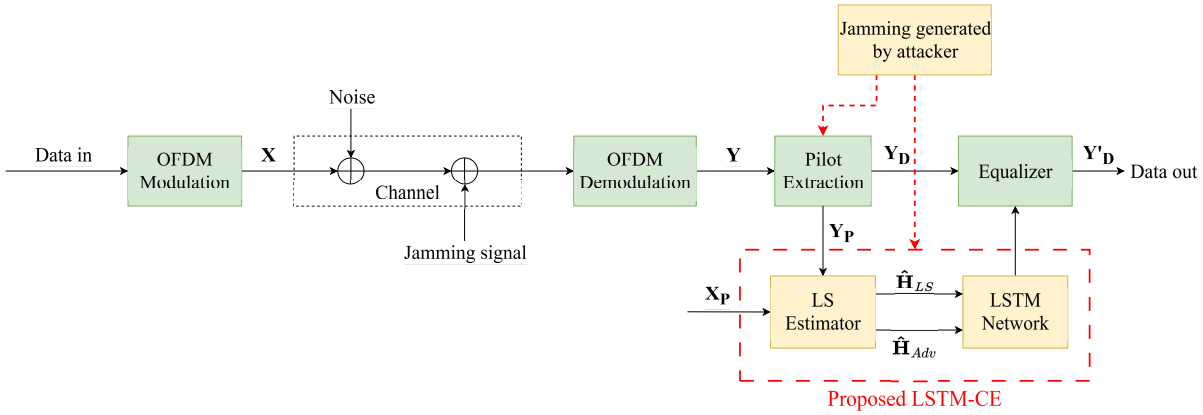

Figure 1. Proposed LSTM–CE framework.

to existing methods.

The rest of this paper is organized as follows. Section 2 presents the LSTM-based channel estimation framework for OFDM transmission, including the system model, adversarial attack analysis, and the proposed LSTM-CE network architecture. Section 3 provides experimental results demonstrating the performance of the proposed method under both normal and adversarial attack conditions. Finally, Section 4 concludes the paper.

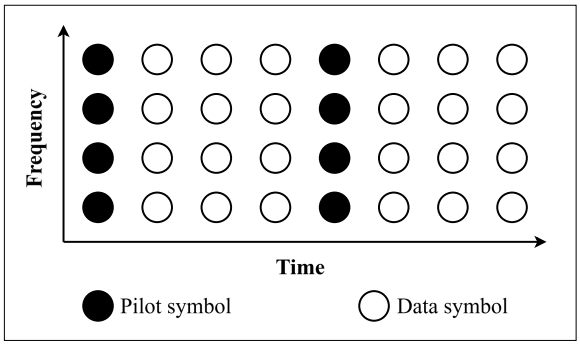

Figure 2. Block-type pilot arrangement pattern.

2. LSTM-based channel estimation (LSTM-CE) for OFDM transmission

2.1. Proposed LSTM–CE framework

Fig. 1 shows the proposed LSTM–CE framework of a downlink OFDM transmission system. In Fig. 1, the modulated OFDM symbol $\mathbf{X}$ is obtained from a typical framework of OFDM modulation system for the PDSCH/5G physical downlink channel [8]. $\mathbf{X}$ is a matrix of dimensions $K \times N_S$, where K and N_S are the number of sub-carriers and OFDM symbols, respectively. Each OFDM symbol, $\mathbf{X}$, composes of OFDM data, $\mathbf{X}_D$, and OFDM pilot, $\mathbf{X}_P$, signals. Several pilot arrangement types have been studied including block-type, comb-type, and scattered-type pilot symbols [9]. This work considers the pilot arrangement type named block-type as shown in Fig. 2.

As shown in Fig. 2, the block-type pilot arrangement includes pilot tones in all subcarriers of OFDM symbols transmitted periodically. This arrangement can deliver highly accurate channel responses across all subcarriers.

Without loss of generality, we assume a single transmitter and a single receiver antenna system are utilized and setup for the proposed framework. Then, at the receiver, the overall transmission at a given OFDM slot can be expressed as:

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}, \tag{1}$$

where $\mathbf{Y}$ and $\mathbf{H}$ are the received OFDM symbol and channel matrices, respectively; $\mathbf{H} \in \mathbb{C}^{K \times N_s}$

and represents the frequency-time response of the wireless communication channel. The additive Gaussian noise at the receiver is given as $\mathbf{N}$ and is assumed to be independent and identically distributed (i.i.d.) with zero mean and variance σ.

In (1), the channel response information $\mathbf{H}$ associated with each OFDM slot needs to be estimated for all sub-carriers and for all OFDM symbols. Generally, to estimate the channel $\mathbf{H}$, we need to employ the pilot signals $\mathbf{X}_P$ which is priori known at both the transmitter and receiver to estimate the channel response. Specifically, $\mathbf{H}$ can be estimated using LS method [10] as follows:

$$\hat{\mathbf{H}}_{LS} = \arg \min_{\mathbf{H} \in \mathbb{C}^{K \times N_s}} |\mathbf{Y} - \mathbf{H}\mathbf{X}|^2 . \quad (2)$$

At the receiver, though the LS channel estimation method is widely used for its low computational complexity, it is shown that the performance of this method is relatively lower than other conventional channel estimations, especially in cases of noise and adversarial attack effects. To solve the problem, in this work, we propose to use a deep neural network (DNN), namely LSTM-CE to effectively estimate communication channels. In our proposed framework, the effect of noise and adversarial attacks that degrades the performance of the LSTM-CE network is carefully analyzed and maximally reduced. More details on the adversarial attack and LSTM-CE network are described in the next following sub-sections of this paper.

2.2. Adversarial attack at the receiver

Adversarial attack is one kind of pilot jamming attacks that corrupts pilot symbols used for channel estimation, leading to the degradation of system performances [11]. This is the most popular jamming for the practical wireless communications, especially for the OFDM system since the OFDM wireless communication channel is open, however prone to jamming attacks. Unlike other jamming attacks, the adversarial attack is harmful as it is intentionally designed to disrupt the pilot symbol used for channel estimation and equalization, which can seriously degrade the performance of OFDM systems. In addition, adversarial attack also increases the risk for the DNN-based channel estimation methods since neural networks are known to be particularly vulnerable to adversarial jamming [12], which would make neural networks have wrong channel estimation and thus, increase the mismatch between the estimated and actual channels.

There are several types of adversarial attacks in wireless OFDM communication systems, which can be divided into two categories: the conventional jamming attack and the DNN-based jamming attack. In this work, we consider the adversarial attack named FGSM attack, because it is among the simplest and most effective adversarial attacks possible, and also being the most widely used in practical OFDM communication systems [13].

The main concept of the FGSM attack is that the attacker has the capability to compromise the receiver chain, and it can directly perturb the input matrix $\hat{\mathbf{H}}_{LS}$ of the LSTM-CE network to obtain the perturbed version of $\hat{\mathbf{H}}_{LS}$ as follows:

$$\hat{\mathbf{H}}_{Adv} = \hat{\mathbf{H}}_{LS} + \mathbf{v}, \quad (3)$$

where $\mathbf{v}$ is the perturbation matrix, $\mathbf{v} \in \mathbb{C}^{K \times N_s}$. Without loss of generality, the FGSM adversarial attacker is assumed to know the LSTM-CE network architecture, allowing for the training and acquisition all the weights $\boldsymbol{\theta}$ of LSTM-CE network to obtain a minimum perturbation $\mathbf{v}$ so that the mean square error (MSE) between the channel estimated by the LSTM-CE and the actual channel is maximally increased. $\mathbf{v}$ is defined as:

$$\mathbf{v} = \varepsilon \text{sign}(\nabla_{\mathbf{H}} \mathcal{L}(\boldsymbol{\theta}, \mathbf{H}, \mathbf{H}_L)), \quad (4)$$

where $\mathbf{H}_L$ denotes the training label of the

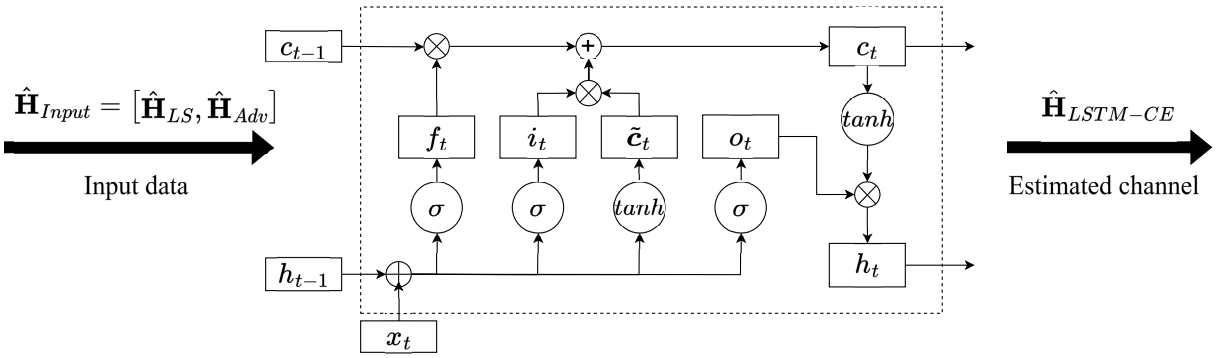

Figure 3. Proposed LSTM–CE model.

channel matrix $\mathbf{H}$, $\text{sign}(\nabla_{\mathbf{H}}\mathcal{L}(\boldsymbol{\theta}, \mathbf{H}, \mathbf{H}_L))$ represents the sign function of the loss gradient with respect to H, and ε is a scalar factor.

In (3), by adding the perturbation $\mathbf{v}$ to the input of LSTM-CE network, the attacker modifies the input towards the direction where the loss function $\mathcal{L}(\boldsymbol{\theta}, \mathbf{H}, \mathbf{H}_L))$ in (4) is increased.

2.3. *Proposed LSTM-CE network for adversarial attack defensing*

In this work, to improve the channel estimation performance in OFDM systems, we propose to utilize the LSTM–CE model to effectively capture the nature time and frequency correlations in wireless channel responses. LSTM is an advanced recurrent neural network (RNN) and has been widely used for the time series sequential data prediction [14]. Utilizing time domain recurrence, long short-term memory (LSTM)-based systems are shown to outperform purely CNN-based systems [15]. Unlike previous researches, in the proposed LSTM–CE model, both the time correlation and the frequency correlation are employed to effectively increase the accuracy of the proposed channel estimation. In addition, the effect of perturbation, which is created in a intentional way to generate $\hat{\mathbf{H}}_{Adv}$, is carefully analyzed and trained in our proposed LSTM–CE model, leading to improve the performance of the LSTM–CE. More details on the architecture of the proposed LSTM–CE model are described as shown in Fig. 3.

As shown in Fig. 3, the proposed LSTM-CE efficiently learns the time and frequency correlations of the channel. The LSTM-CE model achieves this by leveraging its memory cell mechanism, allowing it to consider not only the current input but also the previous output when estimating the current output. The gates of the LSTM-CE model are calculated as follows:

- Forget gate:

$$f_t = \sigma(x_t M_f + y_{t-1} N_f + b_f), \tag{5}$$

- Input gate:

$$i_t = \sigma(x_t M_i + y_{t-1} N_i + b_i), \tag{6}$$

- Output gate:

$$o_t = \sigma(x_t M_o + y_{t-1} N_o + b_o), \tag{7}$$

where σ denotes the activation function; M_k and N_k represent the weight matrices corresponding to the input and recurrent connections with the subscript k which can either be the forget gate (f), input gate (i), or the output gate (o), respectively; y_{t-1} represents the previous hidden state and x_t represents the current input; b_f, b_i, b_o are bias terms. Thus, the behavior of the LSTM-CE model cell is guided by the following steps:

$$c_t = \sigma(f_t \odot c_{t-1} + i_t \odot \tilde{c}_t), \tag{8}$$

and

$$\tilde{c}_t = \tanh\left(x_t M_c + y_{t-1} N_c + b_c\right), \quad (9)$$

where c_t denotes the candidate memory state at time step t, which is calculated based on the current input x_t and the previous hidden state y_{t-1} as in (9); M_c and N_c represent the weight matrices corresponding to the input and recurrent connections, respectively, and b_c is the current bias for candidate memory information.

Then, the hidden state output is updated as

$$h_t = o_t \odot \tanh(c_t) \quad (10)$$

As in (10), h_t is used for predictions or passed to the next time step.

It is worth noticing that in our proposed LSTM-CE, we define a novel loss function as:

$$\min_\theta \frac{1}{|\Lambda|} \sum_{\mathrm{H}\in\Lambda} \max_{\mathrm{v}} \mathcal{L}(\boldsymbol{\theta}, \hat{\mathbf{H}}_{Adv}, \mathbf{H_L}), \quad (11)$$

with $\|\mathbf{v}\| \leq \varepsilon$, where Λ represents the set of training samples; $|\Lambda|$ denotes the total number of samples in this set; $\mathcal{L}(\boldsymbol{\theta}, \hat{\mathbf{H}}_{Adv}, \mathbf{H_L})$ is the loss function of the channel effected by adversarial attack samples; $\mathbf{v}$ is defined using a small perturbation constrained by the scale factor ε.

In (11), the loss function is defined in our proposed LSTM-CE model to effectively remove the perturbation caused by adversarial attack on a neuron network model. The reason lies in the fact that adversarial attack is intentionally created by attackers. This kind of perturbation is harmful and it can directly perturb the network architecture so that maximally increase the error between the estimated channel and the target channel. By utilizing the loss function defined in (11), the proposed LSTM-CE model can keep the error between the channel estimated using $\hat{\mathbf{H}}_{Adv}$ compared with the target channel is barely affected, leading to minimize wrong decision making and thus, improve the overall performance of the proposed LSTM-CE model.

We can now summarize how the proposed mechanism reacts to a pilot jamming attack in real-time. During an attack, the received pilot signals are intentionally corrupted. This shifts the input data away from its normal distribution. Standard neural networks fail because they cannot recognize this shifted data. However, our proposed LSTM-CE model reacts differently. Thanks to the min-max training process, the model has already adapted to worst-case perturbations. When it receives a jammed pilot, the network acts as an intelligent filter. It learns not to trust the directly corrupted input values. Instead, it relies heavily on the learned time and frequency correlations of the wireless channel. Because these natural correlations are much harder for an attacker to completely distort, the LSTM-CE model successfully suppresses the adversarial noise and reconstructs the true channel response.

3. Experimental Results

3.1. Dataset and Performance Evaluation Metrics

We present our work in a simulation environment established in MATLAB using its Communications Toolbox [16]. The core system parameters were selected as follows: 64 sub-carriers, 16-QAM modulation with unit average power, and a Cyclic Prefix (CP) length of 5. The carrier frequency (fc) was set to 2 GHz, and the sampling frequency (fs) to 20 MHz. The channel environment is modeled using a multipath Rayleigh channel with the standard ITU Pedestrian A (PedA) configuration. This environment uses specific delay spread values and average path gains and accounts for Doppler frequency shift to simulate a user moving at approximately 4 km/h. This setup represents a realistic wireless propagation scenario commonly encountered in urban pedestrian environments.

The dataset generation process iterated over a uniform SNR range from 0 dB to 40 dB to ensure a balanced distribution and prevent model bias. A total of 3,000 OFDM frames

were generated. To process the data for the neural networks, the initial complex-valued LS estimates were normalized and transformed. Because standard neural networks do not natively support complex numbers, the complex vectors of size K (where $K = 64$ subcarriers) were separated and concatenated into real-valued vectors of size $2K$. The true channel responses were processed identically to serve as training labels. The dataset was strictly partitioned into 60% for training, 20% for validation, and 20% for testing. The models were optimized using the Adam optimizer with an MSE loss function.

The performance of our proposed LSTM-CE method is compared with that of other conventional methods, including traditional LS estimator [10], standard-trained Improved Channel Estimator (ICE Std) [12], the Improved Channel Estimator trained against adversarial attacks (ICE Rob) [12] and Khichar et al. [6] with CNN-based estimator (CNN-CE). All of the methods above are implemented based on their proposal and tuned to match with the input dataset considered in this work. We use MSE, channel similarity, an attack-induced degradation ratio (ADR) and computational complexity as the evaluation metrics of the channel estimation performance.

The channel similarity metric is defined as

$$\rho = \mathbb{E}\left[\frac{\hat{\mathbf{H}}^T\mathbf{H}}{||\hat{\mathbf{H}}||_2||\mathbf{H}||_2}\right], \tag{12}$$

where $\hat{\mathbf{H}}$ and $\mathbf{H}$ denote the estimated and true channel vectors, respectively. A larger value of ρ indicates that the estimated channel preserves the structure of the true channel more faithfully.

The ADR is defined as

$$\text{ADR} = \frac{\text{MSE}_{\text{adv}}}{\text{MSE}_{\text{clean}}}, \tag{13}$$

where $\text{MSE}_{\text{clean}}$ and MSE_{adv} denote the MSE under clean and adversarial conditions, respectively. A smaller ADR indicates that the estimator suffers less relative degradation under attack.

To compare the computational complexity of the proposed LSTM-CE model and the CNN-CE model, we calculate the number of trainable parameters, the approximate number of multiply-accumulate operations (MACs) per sample, and the average inference latency per sample for both models. The number of trainable parameters is calculated based on the architecture of each model. The MACs are estimated by counting the number of multiplications and additions required for a single forward pass through the network. The average inference latency is measured by running a batch of samples through each model and recording the time taken for inference, then averaging over the batch.

3.2. Experimental Results

First, we measured the performance of all models under typical random noise conditions, simulating common channel impairments. The results were measured and compared as shown in Fig. 4. In Fig. 4, the LS method consistently shows the worst performance across the entire SNR range with significantly higher MSE compared to DL-based methods. This result underscores the inherent limitation of LS in amplifying noise, especially at lower SNR range. The CNN-CE method shows a notable improvement over LS at medium and high SNR levels. However, its performance at the 0-5 dB SNR range is not substantially better than other DL models, suggesting that the CNN architecture struggles when the input is heavily corrupted by noise. The ICE Std and ICE Rob show better performance than LS and CNN-CE, performing comparably to each other in this scenario. Meanwhile, the proposed method achieves effective performance in this random noise scenario. The proposed LSTM-CE method maintains a very low and stable MSE across the 0-20 dB SNR range and continues to perform excellently as SNR increases. These results

highlight the model's capability to filter noise accurately and reconstruct the channel response, proving its strong generalization and effective handling of random noise.

Next, we compare the MSE performance of the proposed LSTM-CE method with that of the LS, ICE Std, ICE Rob, and the CNN-CE method, under the adversarial attack condition. This comparison is important since it compares and evaluates the resilience ability of the proposed method with that of other methods to combat the effect of adversarial attacks. As shown in Fig. 5, the LS method's performance remains unchanged compared to the random noise scenario. Since adversarial attack is designed to fool DL models through gradients or DL principles, it typically does not significantly impact traditional algorithms like LS. CNN-CE experiences a considerable performance loss under adversarial attack compared to the random noise scenario. This result indicates the vulnerability of standard CNN architectures to such adversarial perturbations. ICE Std clearly demonstrates the weakness of DL models when it is not trained with adversarial techniques. Under adversarial attack, its MSE surges compared to its performance in random noise. This shows that standard models are highly susceptible to adversarial samples, leading to severe performance loss. The result of ICE Rob under adversarial attack is much lower than that of ICE Std, proving the effectiveness of training against adversarial attacks in making the model more immune to FGSM perturbations. Meanwhile, the proposed method shows resistance to adversarial attacks effectively. This method's result under attack is only negligibly higher than its performance in the random noise scenario. The model maintains a significantly lower MSE than all other methods across the SNR range. These results demonstrate its ability to combat designed perturbations, while maintaining very low estimation error to ensure high reliability for the system.

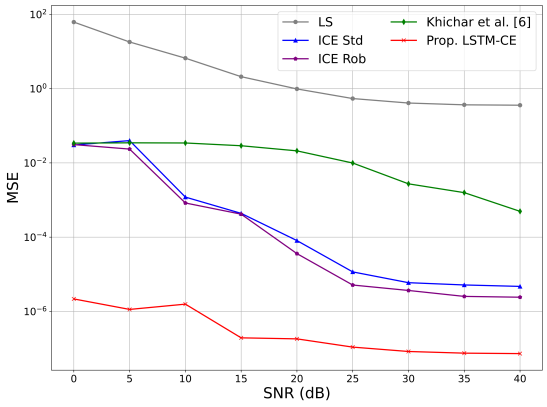

Figure 4. MSE performance comparison between the proposed method with that of the other methods under the typical random noise condition.

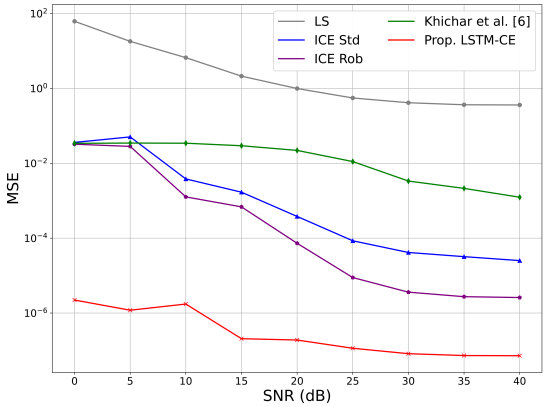

Figure 5. MSE performance comparison between the proposed method with that of the other methods under the adversarial attack condition.

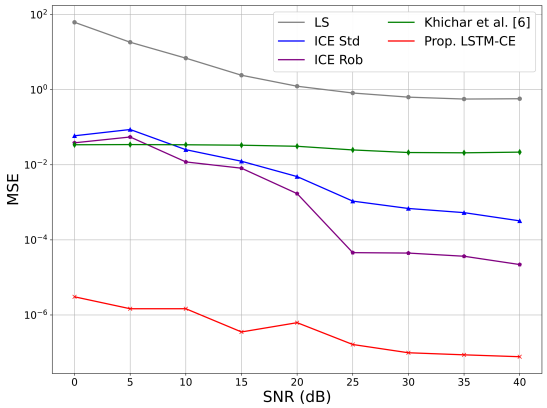

Figure 6. MSE performance comparison between the proposed method with that of the other methods under heavy adversarial attack condition.

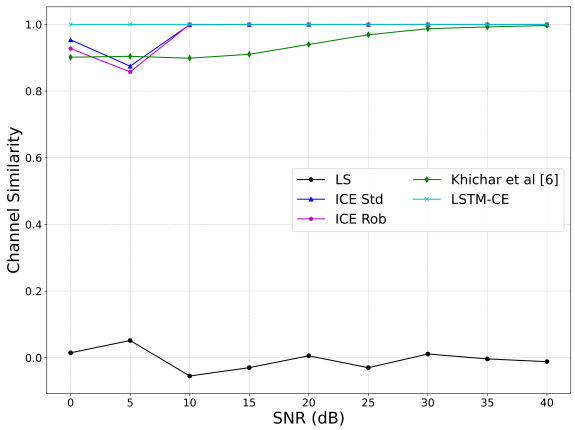

Figure 7. Channel similarity comparison between the proposed method with that of the other methods under heavy adversarial attack condition.

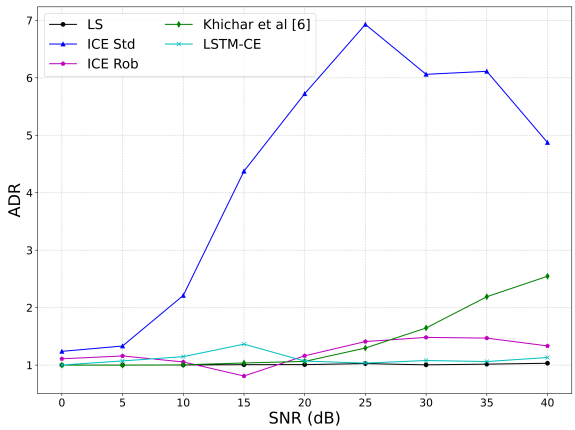

Figure 8. ADR performance comparison between the proposed method with that of the other methods under heavy adversarial attack condition.

Fig. 6 further evaluates the methods under heavy adversarial attack. This comparison represents the limits of all methods and shows how the methods perform when the attack intensity scales up. As shown in Fig. 6, the LS method's performance remains unchanged since the adversarial attack is designed to fool DL-based methods, not traditional methods like LS. CNN-CE experiences higher performance loss at the 20-40 dB SNR range compared to previous comparisons. This result confirms the vulnerability of standard CNN architectures when exposed to strong perturbations. ICE Std collapses under attack, while ICE Rob shows improved resilience due to adversarial training, but its performance is lower than the proposed model. In comparison, the proposed LSTM-CE consistently achieves the lowest MSE across the entire SNR range and remains stable even when the attack strength increases. These results highlight the superior robustness and reliability of the proposed method in scenarios where all other methods fail.

To further explain the superiority of the proposed method under attack, we also evaluate the estimators using channel similarity and ADR. The corresponding curves are shown in Fig. 7 and Fig. 8, and the average values are summarized in Table 1. LSTM-CE achieves the lowest average attacked MSE and the highest average channel similarity. Its ADR is 1.1072, which is the smallest among the DL-based methods. By comparison, ICE Std yields an average attacked MSE of 9.31×10^{-3} and an ADR of 4.3178, indicating strong relative degradation under attack. ICE Rob improves the attacked MSE to 7.90×10^{-3} and reduces the ADR to 1.2213. CNN-CE shows a higher attacked MSE of 1.96×10^{-2}, a lower average channel similarity of 0.9444, and an ADR of 1.4204. Although LS has a numerically small ADR of 1.0108, its average attacked MSE is 10.1739 and its average channel similarity is only -0.0051. LS's low ADR mainly results from poor performance in both clean and attacked conditions rather than true robustness. Therefore, the proposed LSTM-CE offers the best overall adversarial performance. The proposed method simultaneously achieves the lowest absolute estimation error, the highest structural fidelity, and the lowest relative degradation among the channel estimators.

Last, we compare the computational complexity of the proposed LSTM-CE model

Table 1. Additional robustness comparison under FGSM attack.

Model	Avg. MSE under FGSM	Avg. Similarity ρ	ADR
LS	10.1739	-0.0051	1.0108
ICE Std	9.31×10^{-3}	0.9808	4.3178
ICE Rob	7.90×10^{-3}	0.9761	1.2213
CNN-CE	1.96×10^{-2}	0.9444	1.4204
LSTM-CE	5.96×10^{-6}	1.0000	1.1072

Table 2. Complexity comparison between LSTM-CE and CNN-CE.

Model	Trainable parameters	MACs/sample	Latency (ms/sample)
LSTM-CE	39,424	38,912	0.2090
Khichar et al. [6]	4,538	268,288	0.2523

and the CNN-CE model. As summarized in Table 2, the proposed LSTM-CE has 39,424 trainable parameters, which is higher than the 4,538 parameters of CNN-CE. However, the approximate inference cost of LSTM-CE is only 38,912 MACs/sample, which is significantly lower than the 268,288 MACs/sample required by CNN-CE. Moreover, the measured average inference latency is 0.2090 ms/sample for LSTM-CE and 0.2523 ms/sample for CNN-CE. These results indicate that, although LSTM-CE is larger in model size, it is computationally more efficient during inference than the CNN-CE baseline used in our experiments.

Although these results show that the proposed LSTM-CE achieves the best performance under both standard and adversarial conditions, these gains are not obtained for free. The first trade-off is computational complexity. Compared with LS, the proposed method relies on a trained neural model, leading to increased memory usage and inference cost. Compared with the ICE baseline, the proposed model has a more involved architecture. Our method includes an LSTM block rather than simple fully connected layers. The second trade-off is training cost. Our robust training strategy generates FGSM-based adversarial perturbations during training. This process adds an extra gradient computation step before each model update and increases the offline training time. The third trade-off is scope of generalization. The results are obtained for a controlled OFDM setting. Additional retraining or hyperparameter retuning may be required when the simulated environment change substantially.

4. Conclusions

In this paper, we proposed a method for OFDM channel estimation called LSTM-CE. This method is based on LSTM and is trained to detect and protect OFDM systems from adversarial attacks effectively. In this method, a novel loss function is introduced to optimize the training process and improve the resistance from adversarial attacks. Through experimental results, the proposed method achieves a remarkable performance advantage and significant better resistance against adversarial attacks compared to other methods. However, these gains are accompanied by increased model and training complexity, as well as dependence on the considered training scenario, which should be taken into account in practical deployment.

References

[1] M. Soltani, V. Pourahmadi, A. Mirzaei, H. Sheikhzadeh, Deep Learning-Based Channel Estimation, IEEE Communications Letters, Vol. 23, No. 4, 2019, pp. 652–655. https://doi.org/10.1109/LCOMM.2019.2898944.

[2] T. O'Shea, J. Hoydis, An Introduction to Deep Learning for the Physical Layer, IEEE Transactions on Cognitive Communications and Networking, Vol. 3, No. 4, 2017, pp. 563–575. https://doi.org/10.1109/TCCN.2017.2758370.

[3] Z. Qin, H. Ye, G. Y. Li, B.-H. F. Juang, Deep Learning in Physical Layer Communications, IEEE Wireless Communications, Vol. 26, No. 2, 2019, pp. 93–99. https://doi.org/10.1109/MWC.2019.1800601.

[4] P. Dong, H. Zhang, G. Y. Li, N. NaderiAlizadeh, I. S. Gaspar, Deep CNN for Wideband mmWave Massive MIMO Channel Estimation Using Frequency Correlation, in: ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 4529–4533. https://doi.org/10.1109/ICASSP.2019.8682819.

[5] Z. Wang, F. Pu, X. Yang, N. Chen, Y. Shuai, R. Yang, Online LSTM-Based Channel Estimation for HF MIMO SC-FDE System, IEEE Access, Vol. 8, 2020, pp. 131005–131020. https://doi.org/10.1109/ACCESS.2020.3010359.

[6] S. Khichar, W. Santipach, L. Wuttisittikulkij, A. Parnianifard, S. Chaudhary, Efficient Channel Estimation in OFDM Systems Using a Fast Super-Resolution CNN Model, Journal of Sensor and Actuator Networks, Vol. 13, No. 5, (2024). https://doi.org/10.3390/jsan13050055.

[7] S. Park, J. So, On the Effectiveness of Adversarial Training in Defending against Adversarial Example Attacks for Image Classification, Applied Sciences, Vol. 10, No. 22, (2020). https://doi.org/10.3390/app10228079.

[8] 3GPP, NR; Physical Channels and Modulation, Technical Specification (TS) 38.211, 3rd Generation Partnership Project (3GPP), version 18.6.0 (03 2025).

[9] Y. S. Cho, J. Kim, W. Y. Yang, C. G. Kang, MIMO-OFDM Wireless Communications with MATLAB®, John Wiley & Sons, Ltd, 2010. https://doi.org/10.1002/9780470825631.

[10] S. Coleri, M. Ergen, A. Puri, A. Bahai, Channel Estimation Techniques Based on Pilot Arrangement in OFDM Systems, IEEE Transactions on Broadcasting, Vol. 48, No. 3, 2002, pp. 223–229. https://doi.org/10.1109/TBC.2002.804034.

[11] E. Habler, R. Bitton, D. Avraham, D. Mimran, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, A. Shabtai, Adversarial Machine Learning Threat Analysis and Remediation in Open Radio Access Network (O-RAN) (2025). https://doi.org/10.1016/j.jnca.2024.104090.

[12] M. O. K. Mendonça, P. S. R. Diniz, J. M. Morales, P. Frossard, Adversarial Training for Jamming-Robust Channel Estimation in OFDM Systems, IEEE Open Journal of Signal Processing, Vol. 5, 2024, pp. 1031–1041. https://doi.org/10.1109/OJSP.2024.3453176.

[13] I. J. Goodfellow, J. Shlens, C. Szegedy, Explaining and Harnessing Adversarial Examples (2015). arXiv:1412.6572, https://doi.org/10.48550/arXiv.1412.6572.

[14] H. Verma, S. Kumar, An Accurate Missing Data Prediction Method Using LSTM-Based Deep Learning for Health Care, in: Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19, Association for Computing Machinery, New York, NY, USA, 2019, p. 371–376. https://doi.org/10.1145/3288599.3295580.

[15] N. Farsad, A. Goldsmith, Neural Network Detection of Data Sequences in Communication Systems, IEEE Transactions on Signal Processing, Vol. 66, No. 21, 2018, pp. 5663–5678. https://doi.org/10.1109/TSP.2018.2868322.

[16] The MathWorks Inc., Communications Toolbox Version: 8.0 (R2023a) (2023).