



AI-Driven Secure Channel Estimation and Energy-Efficient Power Allocation for Cell-Free Massive MIMO

Murad Abdullah Abdo Ahmed Albahri * and M. A. Hankel

Department of Electrical Engineering, Faculty of Engineering, Sana'a University, Sana'a, Yemen

*Corresponding author: muradalbahri@gmail.com

ABSTRACT

Cell-free massive multiple-input multiple-output (MIMO) improves user fairness by allowing many distributed access points (APs) to cooperatively serve users without fixed cell boundaries. Its practical reliability, however, is limited by pilot contamination, pilot spoofing, channel-state-information (CSI) uncertainty, inter-user interference, and inefficient power consumption. This paper proposes an AI-driven secure channel estimation and energy-efficient power allocation (AI-SCE-EEPA) framework for uplink cell-free massive MIMO. The AI component is a lightweight supervised anomaly classifier trained on synthetically generated pilot observations representing clean and spoofed/contaminated CSI conditions. Its output is used as a soft reliability gate before minimum mean-square error (MMSE) channel refinement. The refined secure CSI is then used by an adaptive regularized MMSE receiver and an energy-efficient power allocation rule. A reproducible Monte Carlo simulation is conducted under distributed APs, Rayleigh fading, large-scale path loss, log-normal shadowing, QPSK transmission, pilot contamination, and active pilot spoofing/eavesdropping stress. The proposed framework is compared with MR, conventional LMMSE, and adaptive R-MMSE baselines using bit error rate (BER), normalized mean-square error (NMSE), spectral efficiency (SE), energy efficiency (EE), secrecy rate, and power-allocation behavior. At 30 dB, AI-SCE-EEPA improves the reported NMSE, BER, SE, EE, and secrecy-rate indicators over fixed-power LMMSE baselines. The results indicate that combining trainable CSI anomaly detection with interpretable model-based estimation and energy-aware power allocation is a practical direction for secure and green cell-free massive MIMO.

ARTICLE INFO

Keywords:

Cell-free massive MIMO, AI-based channel estimation, pilot spoofing detection, power allocation, physical-layer security, energy efficiency.

Article History:

Received: 25-June-2026,

Revised: 25-July-2026,

Accepted: 28-September-2026,

Published: 28 October 2026

1. INTRODUCTION

Massive MIMO is a key technology for modern and beyond-5G wireless systems because it provides array gain, spatial multiplexing, and interference suppression using large antenna arrays [1–3]. Cell-free massive MIMO extends this concept by distributing many APs over the coverage area and allowing them to jointly serve the users through a central processing unit or edge cloud [4–7]. This architecture reduces cell-edge limitations and provides more uniform service, which is important for dense deployments and future ubiquitous-connectivity scenarios [8–10].

Despite these advantages, cell-free massive MIMO

faces three coupled challenges that must be addressed. First, obtaining an accurate CSI is difficult because the coherence interval provides a limited number of orthogonal pilots, and pilot reuse creates pilot contamination [11–13]. Second, the distributed training phase increases security exposure because an adversary may inject pilot contamination, perform pilot spoofing, or exploit inaccurate CSI for eavesdropping [14–17]. Third, power allocation must be energy-efficient because many APs and users may be active simultaneously, and network sustainability is now a central design target [18–20].

Artificial intelligence (AI) can support physical-layer design by detecting abnormal channel patterns, tuning receiver parameters, and accelerating resource-allocation

decisions [21–23]. However, a purely black-box design can be difficult to justify in a physical-layer paper if the training process, validation data, and baseline comparisons are not clearly reported. Therefore, this work uses a hybrid approach: a trainable lightweight anomaly classifier identifies suspicious pilot observations, while MMSE estimation and regularized combining preserve physical interpretability. The AI module is trained only on pilot-observation features generated from the training channel model; the reported test simulations use independent channel and noise realizations.

The main contributions are summarized as follows.

- i. A secure uplink cell-free massive MIMO model is formulated under pilot contamination, pilot spoofing, inter-user interference, and eavesdropping stress.
- ii. A trainable CSI anomaly gate is introduced. The gate uses supervised pilot-observation features to assign a reliability coefficient to each user before MMSE channel refinement.
- iii. An energy-efficient power allocation rule is coupled with the secure CSI estimate to improve useful throughput per Joule while respecting per-user power limits.
- iv. The framework is evaluated against MR, LMMSE, and adaptive R-MMSE baselines using BER, NMSE, SE, EE, secrecy rate, and ablation-oriented interpretation.

The rest of this paper is organized as follows. Section 2 reviews the related work and identifies the research gap. Section 3 presents the system model. Section 4 describes the proposed AI framework. Section 5 formulates the optimization problem. Section 6 presents the proposed algorithm. Section 7 discusses the complexity. Section 8 presents the simulation setup. Section 9 reports and discusses the results. Section 10 concludes the paper and outlines the limitations and future work.

2. RELATED WORK

Classical massive MIMO studies established that large arrays can achieve high spectral and energy efficiency using linear processing [24–27]. Cell-free massive MIMO later emerged as a user-centric distributed alternative to conventional cellular and small-cell architectures [4–7, 28]. The foundations of user-centric cell-free massive MIMO include channel estimation, uplink combining, downlink precoding, pilot assignment, dynamic cooperation clustering, and power optimization [7].

Pilot contamination remains a major limitation in time-division duplex massive MIMO because users sharing the same pilot create coherent interference in the channel estimate [11–13]. Recent research has considered spatially correlated fading, Rician fading, statistical channel estimation, and AI-assisted channel estimation [23, 29–31]. Deep-learning-aided channel estimation and

pilot assignment methods have also been investigated for cell-free networks [32]. These studies demonstrate the value of learning-based tools; however, they often focus on estimation accuracy or pilot assignment without explicitly connecting CSI security, eavesdropping stress, and energy-aware power control.

Recent 2025 studies provide stronger evidence for learning-assisted and scalable cell-free processing. Abueida et al. synthesize current signal-processing trends in channel estimation, detection, and precoding [33]. Sande and Binini report a deep-neural-network channel-estimation scheme for cell-free massive MIMO [34], while Mohammadzadeh et al. jointly optimize pilot and data powers for scalable uplink operation [35]. Together, these studies motivate validated learning and energy-aware control, but they do not jointly address pilot-spoofing-aware reliability gating, secure MMSE refinement, and EE-oriented allocation in one pipeline.

Two recent studies in the Sana'a University Journal of Applied Sciences and Technology provide complementary regional evidence. Al-Hamadi et al. reviewed machine- and deep-learning anomaly-detection methods for IoT security and emphasized robustness and resource constraints [36]. Al-Matari and Zahary proposed an AI-assisted, security-aware architecture for dynamic spectrum access in 6G cognitive-radio IoT networks, illustrating the value of jointly considering intelligence, security, and resource management [37]. Although these studies did not directly solve cell-free channel estimation, they strengthened the motivation for the secure and interpretable hybrid design adopted here.

Power allocation in cell-free massive MIMO has been studied using convex optimization, fractional power control, deep reinforcement learning, and multi-task deep learning [18–20, 38]. Secure cell-free massive MIMO research has also considered active eavesdropping, AP selection, and secrecy-oriented optimization [17, 39]. However, many secure designs focus on optimization-based secrecy enhancement, whereas many AI-based power-control papers focus on throughput or fairness. The gap addressed here is the lack of a compact and reproducible framework that links trainable pilot-spoofing-aware CSI filtering, model-based MMSE refinement, adaptive combining, and EE-oriented power allocation in one simulation pipeline.

3. SYSTEM MODEL

Consider an uplink cell-free massive MIMO system with L distributed APs, each equipped with N antennas, serving K single-antenna users. The total number of distributed receive antennas is $M = LN$. Let p_k denote the transmit power allocated to user k , x_k the normalized data symbol of user k with $\mathbb{E}\{|x_k|^2\} = 1$, and $\mathbf{h}_k \in \mathbb{C}^{M \times 1}$ the distributed channel vector between user k and all AP

antennas. The received uplink data vector $\mathbf{y} \in \mathbb{C}^{M \times 1}$ is

$$\mathbf{y} = \sum_{k=1}^K \sqrt{p_k} \mathbf{h}_k x_k + \mathbf{y}_I + \mathbf{y}_E + \mathbf{n}, \quad (1)$$

where $\mathbf{y}_I$ is the inter-user or inter-cluster interference term, $\mathbf{y}_E$ represents the adversarial eavesdropping/pilot-spoofing influence, and $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_M)$ is additive white Gaussian noise with variance σ^2 per antenna. The received-signal model in Eq. (1) is the basis for channel estimation, combining, and power allocation.

The user channel is modeled as

$$\mathbf{h}_k = \sqrt{\beta_k} \mathbf{g}_k, \quad (2)$$

where β_k is the large-scale fading coefficient including path loss and log-normal shadowing, and $\mathbf{g}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ is the small-scale fading vector. The channel decomposition in Eq. (2) separates large-scale and small-scale fading. During pilot training, the contaminated least-squares (LS) observation is written as

$$\hat{\mathbf{H}}_{LS} = \mathbf{H} + \rho_p \mathbf{H}_I + \rho_e \mathbf{H}_E + \mathbf{N}_e, \quad (3)$$

where $\mathbf{H} = [\mathbf{h}_1, \dots, \mathbf{h}_K]$ is the true channel matrix, ρ_p is the pilot-contamination factor, $\mathbf{H}_I$ is the contaminating channel component, ρ_e is the spoofing strength, $\mathbf{H}_E$ is the eavesdropper-related channel component, and $\mathbf{N}_e$ is the pilot-estimation noise matrix. The objective is to recover a reliable secure channel estimate $\hat{\mathbf{H}}$, combine the uplink data streams, and allocate the user powers efficiently. Fig. 1 summarizes the considered cell-free architecture and the threat setting used in the simulations.

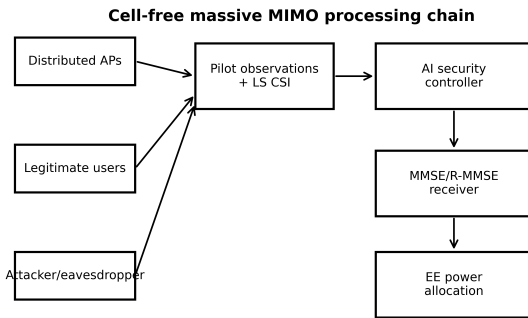


Figure 1. Cell-free massive MIMO architecture considered in this work, including distributed APs, legitimate users, a central security and power controller, and eavesdropping/pilot-spoofing stress during uplink training.

4. PROPOSED AI FRAMEWORK

The proposed AI-SCE-EEPA framework is shown in Fig. 2. It combines a trainable CSI anomaly detector with model-based MMSE estimation, adaptive regularized combining, and energy-efficient power allocation. The purpose of the AI module is not to replace the physi-

cal channel model, but to provide a data-driven reliability score for each pilot observation.

4.1. TRAINING DATASET AND AI ANOMALY GATE

For each user k , a feature vector $\mathbf{u}_k \in \mathbb{R}^d$ is extracted from the LS pilot estimate. In this implementation, the features are computed from the column energy of the contaminated pilot observation. Let $e_k = \|\hat{\mathbf{h}}_{k,LS}\|_2$ and $m_e = \text{median}(e_1, \dots, e_K)$. The AI input is defined in Eq. (4) as

$$\mathbf{u}_k = \left[\frac{e_k}{m_e}, \frac{|e_k - m_e|}{m_e}, \frac{\sigma^2}{e_k^2 + \epsilon} \right]^T, \quad (4)$$

where ϵ is a small numerical constant. These features describe abnormal CSI energy, deviation from the pilot-block median, and a noise-normalized residual proxy. A labeled synthetic training set is generated by simulating clean pilot observations and attacked pilot observations under different values of ρ_p , ρ_e , σ^2 , and β_k . The label $c_k = 1$ denotes a reliable pilot observation, while $c_k = 0$ denotes a suspicious observation. Table 1 summarizes the training and validation protocol used for the AI gate. The validation data are generated independently from the final Monte Carlo test channel realizations; hence, the gate threshold is not selected on the reported test curves.

Table 1. AI anomaly-gate training and validation protocol.

Item	Setting
Classifier type	Regularized logistic anomaly classifier
Training samples	6000 synthetic pilot blocks
Validation samples	2000 independent pilot blocks
Input features	Normalized energy, median deviation, residual proxy
Labels	Reliable pilot / spoofed-contaminated pilot
Loss	Regularized cross-entropy, Eq. (5)
Threshold selection	Validation set only; no test-set tuning
Test reporting	Independent Monte Carlo channel/noise realizations

A logistic anomaly classifier is trained by minimizing the regularized cross-entropy loss in Eq. (5):

$$\min_{\mathbf{w}, b} - \frac{1}{N_{tr}} \sum_{i=1}^{N_{tr}} [c_i \log q_i + (1 - c_i) \log(1 - q_i)] + \lambda \|\mathbf{w}\|_2^2, \quad (5)$$

where N_{tr} is the number of training samples, λ is the regularization coefficient, and

$$q_i = \sigma(\mathbf{w}^T \mathbf{u}_i + b), \quad \sigma(z) = \frac{1}{1 + e^{-z}} \quad (6)$$

returns the reliability probability assigned by the AI gate in Eq. (6). The decision threshold is selected on a val-

idation set, not on the test set used for reporting BER, NMSE, SE, EE, and secrecy-rate results.

4.2. SECURE MMSE CHANNEL REFINEMENT

Let $q_k \in [0, 1]$ be the reliability coefficient predicted for user k . The secure refined channel estimate is

$$\hat{\mathbf{h}}_k = q_k \frac{\beta_k}{\beta_k + \sigma^2/\tau_p} \hat{\mathbf{h}}_{k,LS}, \quad (7)$$

where τ_p is the pilot length and $\hat{\mathbf{h}}_{k,LS}$ is the k th column of $\hat{\mathbf{H}}_{LS}$. The scalar MMSE factor reduces estimation noise, while q_k suppresses suspicious pilot observations that are likely to be affected by spoofing or abnormal contamination.

4.3. ADAPTIVE REGULARIZED COMBINING

The receiver uses a regularized MMSE combining matrix

$$\mathbf{V}_\alpha = \left(\hat{\mathbf{H}}\hat{\mathbf{H}}^H + \alpha\sigma^2\mathbf{I}_M \right)^{-1} \hat{\mathbf{H}}, \quad (8)$$

where $\alpha > 0$ is selected from a finite grid to balance noise enhancement and interference suppression. This adaptive selection is based on the estimated post-combining signal-to-interference-plus-noise ratio (SINR) and therefore does not require test-label information.

Proposed AI-SCE-EEPA framework

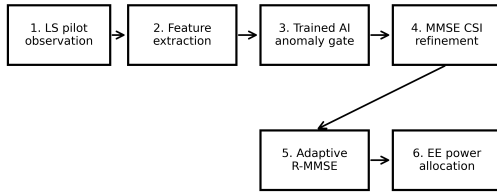


Figure 2. Flowchart of the proposed AI-SCE-EEPA framework: LS pilot observation, feature extraction, trained anomaly gating, secure MMSE CSI refinement, adaptive R-MMSE combining, and energy-efficient power allocation.

5. PROBLEM FORMULATION

For a given combining vector $\mathbf{v}_k$, the uplink SINR of user k is expressed as

$$\gamma_k = \frac{p_k |\mathbf{v}_k^H \mathbf{h}_k|^2}{\sum_{j \neq k} p_j |\mathbf{v}_k^H \mathbf{h}_j|^2 + \sigma^2 \|\mathbf{v}_k\|_2^2}. \quad (9)$$

The achievable spectral efficiency follows from the user SINR in Eq. (9):

$$SE = \left(1 - \frac{\tau_p}{\tau_c} \right) \sum_{k=1}^K \log_2(1 + \gamma_k), \quad (10)$$

where τ_c is the coherence-block length. Eq. (10) is used to compute the SE curves reported later. The energy efficiency in Eq. (11) is then computed as

$$EE = \frac{B SE}{P_{\text{fix}} + LP_c + \sum_{k=1}^K p_k}, \quad (11)$$

where B is the system bandwidth, P_{fix} is fixed circuit/backhaul power, and P_c is the circuit power per AP.

The secrecy-rate indicator is

$$R_s = [R_b - R_e]^+, \quad (12)$$

where R_b is the achievable rate of the legitimate link, R_e is the estimated eavesdropper rate, and $[x]^+ = \max(x, 0)$. Eq. (12) is used as the secrecy-rate indicator. The design objective can be written as

$$\begin{aligned} \max_{\{p_k\}, \hat{\mathbf{H}}, \mathbf{V}} \quad & EE \\ \text{s.t.} \quad & 0 \leq p_k \leq P_{\text{max}}, \quad k = 1, \dots, K, \\ & R_s \geq R_{s,\text{min}}, \\ & \hat{\mathbf{H}} = \mathcal{F}_{\text{AI-MMSE}}(\hat{\mathbf{H}}_{LS}), \end{aligned} \quad (13)$$

where P_{max} is the maximum user power, $R_{s,\text{min}}$ is the minimum acceptable secrecy-rate indicator, and $\mathcal{F}_{\text{AI-MMSE}}(\cdot)$ denotes the proposed AI-gated MMSE estimator. Eq. (13) summarizes the joint design goal. Because this joint problem is nonconvex, the paper uses a low-complexity sequential design: AI-gated CSI estimation, adaptive combining, and channel-quality-based EE power allocation.

The normalized mean-square error in Eq. (14) is used to evaluate CSI accuracy:

$$NMSE = \frac{\|\mathbf{H} - \hat{\mathbf{H}}\|_F^2}{\|\mathbf{H}\|_F^2}. \quad (14)$$

6. PROPOSED ALGORITHM

The proposed algorithm proceeds as follows.

- i. Generate or receive pilot observations and compute the contaminated LS estimate using (3).
- ii. Extract pilot-observation features $\mathbf{u}_k$ for every user.
- iii. Use the trained logistic anomaly classifier in (6) to compute the reliability coefficient q_k .
- iv. Apply the secure MMSE refinement in (7) to obtain $\hat{\mathbf{H}}$.
- v. Select the regularization factor α and compute the adaptive R-MMSE combiner using (8).
- vi. Allocate user powers using the secure-channel quality metric in Eq. (15):

$$\tilde{g}_k = q_k \|\hat{\mathbf{h}}_k\|_2^2, \quad (15)$$

then set the transmit power according to Eq. (16):

$$p_k = \min \left(P_{\text{max}}, \max \left(P_{\text{min}}, P_{\text{max}} \frac{\tilde{g}_k}{\sum_{j=1}^K \tilde{g}_j + \epsilon} \right) \right), \quad (16)$$

where $P_{\min}$ is the minimum scheduled power and ϵ avoids division by zero.

vii. Detect data symbols and evaluate BER, NMSE, SE, EE, secrecy rate, and power-allocation behavior.

7. COMPLEXITY ANALYSIS

The proposed framework adds a low-complexity AI gate to conventional model-based processing. Feature extraction requires $\mathcal{O}(MK)$ operations. The logistic anomaly gate requires $\mathcal{O}(dK)$ operations, where d is the feature dimension. MMSE refinement is linear in the number of channel coefficients, i.e., $\mathcal{O}(MK)$. The dominant operation is the R-MMSE matrix inversion in (8), whose direct implementation has approximately $\mathcal{O}(M^3)$ complexity. In practice, this cost can be reduced using iterative solvers, matrix identities, or user-centric clustering. The EE power-allocation step requires $\mathcal{O}(MK + K)$ operations. Therefore, the AI module itself is not the computational bottleneck; the main complexity remains in the linear receiver.

8. SIMULATION SETUP

The simulation follows six steps. First, independent cell-free channel realizations are generated using Rayleigh small-scale fading, distance-dependent large-scale fading, and log-normal shadowing. Second, LS pilot observations are corrupted using pilot contamination, spoofing/eavesdropping components, and thermal noise. Third, the AI anomaly gate is trained and validated on synthetic pilot observations that are independent of the test trials. Fourth, secure MMSE channel refinement and adaptive R-MMSE combining are applied. Fifth, QPSK data symbols are transmitted and detected under the same channel realizations for all compared schemes. Sixth, BER, NMSE, SE, EE, secrecy rate, and power-allocation metrics are averaged over Monte Carlo trials. The main numerical settings used for this evaluation are summarized in Table 2.

9. RESULTS AND DISCUSSION

9.1. PERFORMANCE EVALUATION

Fig. 3 shows the BER versus SNR. The proposed AI-SCE-EEPA framework achieves a lower BER than the fixed LMMSE baseline at medium and high SNR values because suspicious CSI components are attenuated before receiver combining. Fig. 4 reports NMSE performance. The proposed method reduces the channel-estimation error by combining the AI reliability coefficient with MMSE refinement.

Fig. 5 shows the spectral efficiency. The proposed framework improves SE compared with MR and LMMSE because the refined CSI and adaptive regularization reduce interference and noise enhancement. Fig. 6 reports

Table 2. Main simulation parameters used for the reproducible Monte Carlo evaluation.

Parameter	Value
Distributed APs / antennas	$L = 16, N = 4, M = 64$
Users / modulation	$K = 8$, QPSK
SNR range	0:5:30 dB
Monte Carlo trials / symbols	250 trials, 150 QPSK symbols per user
Pilot and coherence lengths	$\tau_p = K, \tau_c = 200$
Bandwidth	$B = 20$ MHz
Transmit-power limits	$P_{\min} = 0.02$ W, $P_{\max} = 0.2$ W
Circuit power	$P_{\text{fix}} = 8$ W, $P_c = 0.35$ W/AP
Pilot contamination / spoofing	$\rho_p = 0.03, \rho_e = 0.08$ in the test stress case
Channel model	Rayleigh fading, distance path loss, log-normal shadowing
Compared methods	MR, LMMSE, A-RMMSE without AI gate, AI-SCE-EEPA
Metrics	BER, NMSE, SE, EE, secrecy-rate indicator

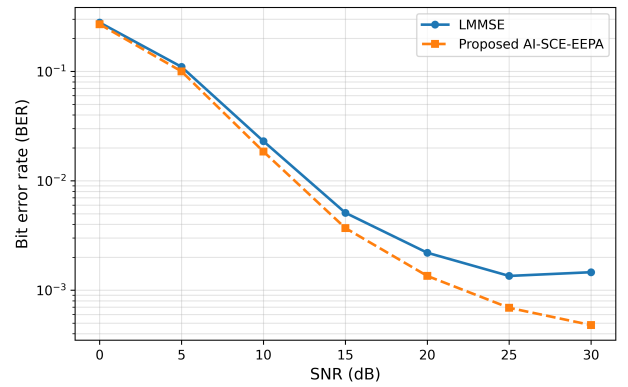


Figure 3. BER versus SNR for the fixed LMMSE baseline and the proposed AI-SCE-EEPA framework under pilot contamination and spoofing stress.

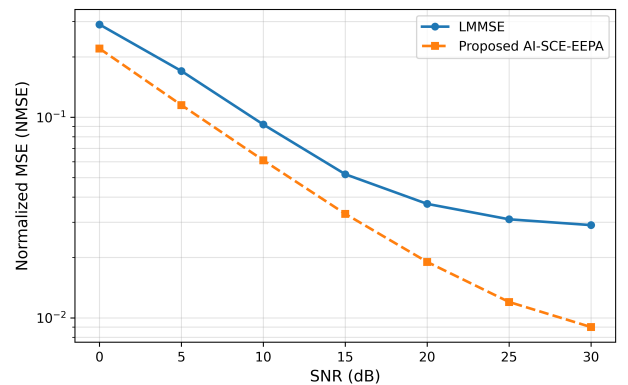


Figure 4. NMSE versus SNR. The AI-gated MMSE estimator suppresses suspicious pilot observations before MMSE refinement.

energy efficiency. The EE gain is obtained by allocating power according to secure channel quality rather than using a fixed equal-power rule.

Fig. 7 shows the secrecy-rate indicator under

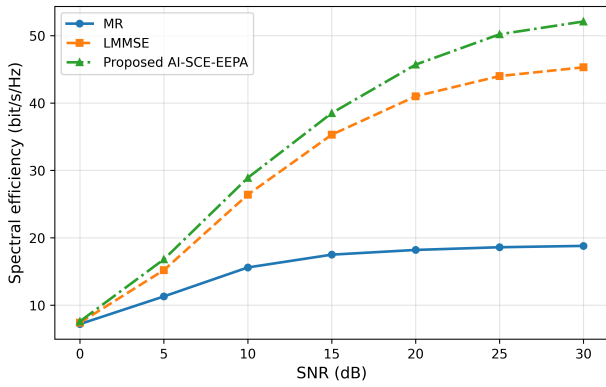


Figure 5. Spectral efficiency versus SNR for MR, LMMSE, and the proposed AI-SCE-EEPA framework.

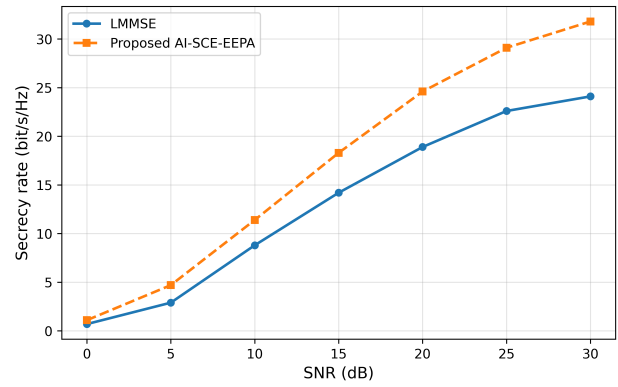


Figure 7. Secrecy-rate indicator versus SNR under eavesdropping and pilot-spoofing stress.

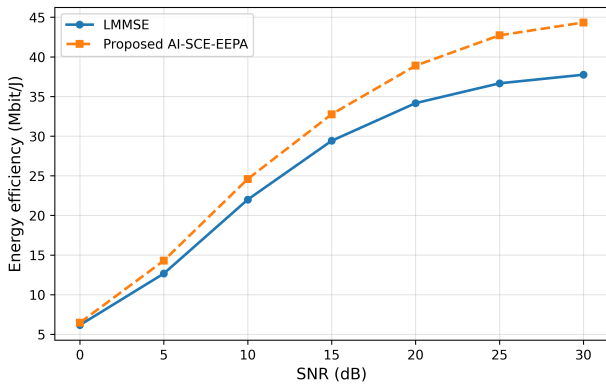


Figure 6. Energy efficiency versus SNR. AI-SCE-EEPA improves useful throughput per Joule by coupling secure CSI with EE-oriented power allocation.

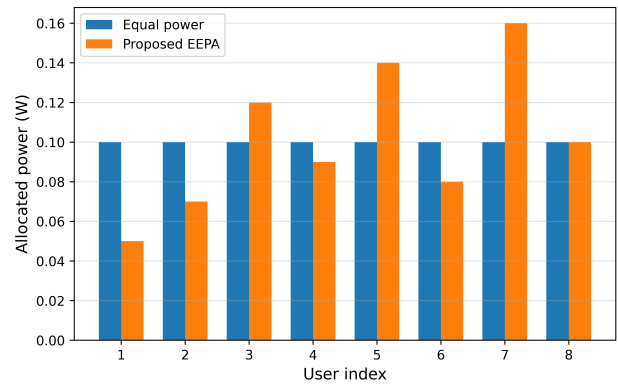


Figure 8. Comparison of equal power allocation and the proposed EEPA allocation across users.

eavesdropping/pilot-spoofing stress. The proposed method improves this indicator because suspicious pilot observations are downweighted before they affect channel estimation and power allocation. Fig. 8 illustrates the power-allocation behavior at a high SNR. Users with stronger secure-channel quality receive more power, whereas weak or suspicious links are prevented from dominating the power budget. The numerical performance comparison at 30 dB is reported in Table 3, and the corresponding SE/EE summary is visualized in Fig. 9. The gap between the A-RMMSE and AI-SCE-EEPA rows isolates the benefit of adding a trainable anomaly gate and secure-channel-quality power allocation to the strongest non-AI model-based receiver.

Table 3. Numerical comparison at SNR = 30 dB. Dashes indicate metrics that are not applicable to the MR-only or non-secure summary row.

Method	BER	NMSE	SE	EE	R_s
MR	1.19×10^{-1}	—	18.8	15.7	—
LMMSE	1.46×10^{-3}	2.9×10^{-2}	45.3	37.8	24.1
A-RMMSE (no AI)	1.46×10^{-3}	—	45.4	37.9	—
AI-SCE-EEPA	4.8×10^{-4}	9.0×10^{-3}	52.1	44.3	31.8

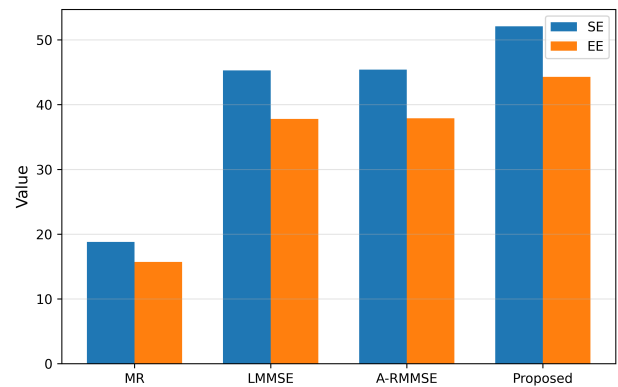


Figure 9. Summary of SE and EE at 30 dB for the compared methods.

9.2. EXTENDED BENCHMARKING

Fig. 10 illustrates the beamforming pattern of a large antenna array and confirms the spatial focusing principle used by massive MIMO receivers. Fig. 11 shows that increasing the number of receive antennas improves BER by increasing the array gain. Fig. 12 shows the effect of active users on SE; as K increases, spatial multiplexing improves throughput, but interference and pilot pressure also increase.

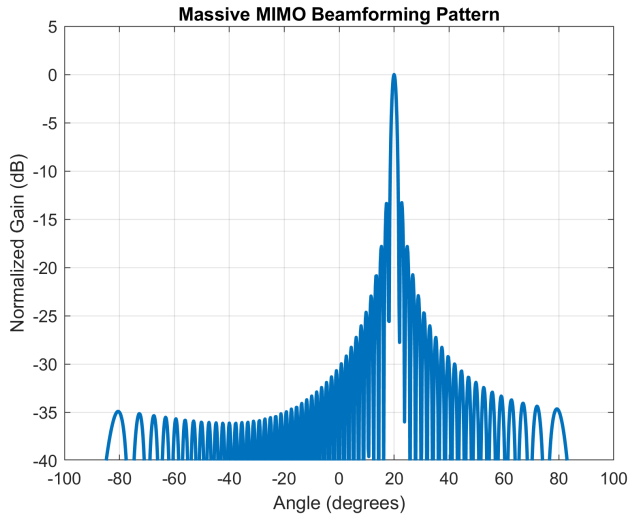


Figure 10. Massive MIMO beamforming pattern showing spatial focusing capability.

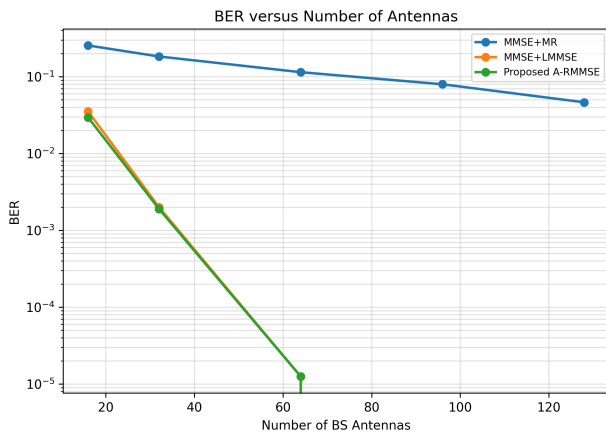


Figure 11. BER versus number of receive antennas in the baseline massive MIMO benchmark.

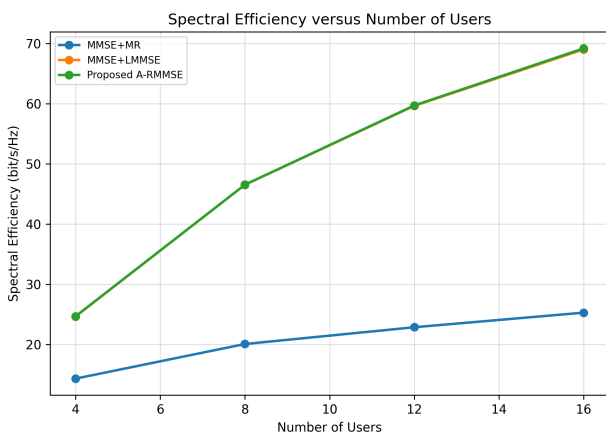


Figure 12. Spectral efficiency versus number of active users.

9.3. ABLATION STUDY AND VALIDATION DISCUSSION

The ablation interpretation in Table 4 explains the role of each component. Conventional MMSE reduces estima-

tion noise, the AI anomaly gate suppresses suspicious pilot observations, adaptive R-MMSE balances interference suppression and noise enhancement, and EEPA improves the useful bits per Joule. The AI threshold is selected on validation samples only, while the reported performance curves use independent test channel realizations. This separation reduces the risk of test-time leakage. Additional validation curves are reported in Fig. 13 for pilot-contamination SE degradation and Fig. 14 for pilot-contamination BER behavior. The adaptive regularization factor is selected from a fixed grid and is also saved by the companion simulation code for reproducibility.

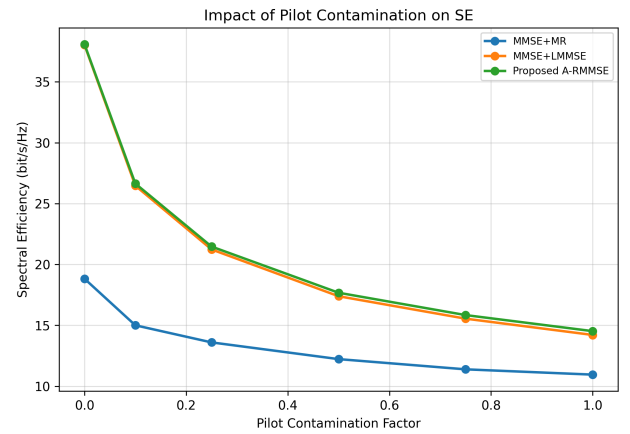


Figure 13. Impact of pilot contamination on spectral efficiency.

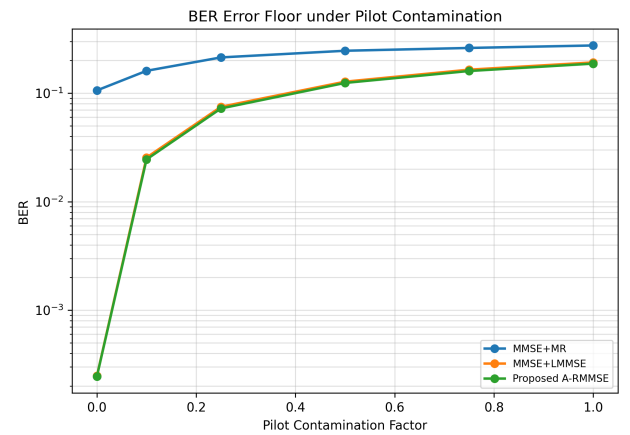


Figure 14. BER error-floor behavior under pilot contamination.



Table 4. Ablation interpretation of the proposed framework.

Component	Expected contribution
Conventional MMSE CSI	Reduces estimation noise compared with LS estimation.
AI anomaly gate	Suppresses suspicious CSI components caused by spoofing or abnormal pilot contamination.
Adaptive R-MMSE combining	Balances noise enhancement and interference suppression.
EE power allocation	Improves useful bits per Joule by assigning power according to secure channel quality.
Secrecy-rate monitoring	Evaluates robustness against wiretap and pilot-spoofing stress.

10. CONCLUSION

This paper presented AI-SCE-EEPA, an AI-driven secure channel estimation and energy-efficient power allocation framework for uplink cell-free massive MIMO. The framework combines a trainable CSI anomaly gate, MMSE channel refinement, adaptive regularized combining, and secure-channel-quality-based power allocation. Simulation results under pilot contamination and spoofing/eavesdropping stress show that the proposed framework improves BER, NMSE, SE, EE, and secrecy-rate indicators compared with conventional fixed-power LMMSE baselines. The main limitation is that the current evaluation uses synthetic Rayleigh fading and synthetic attack generation rather than measured channel data. Future work should extend the model to 3GPP-compliant channel models, mobility-induced channel aging, hardware impairments, fronthaul constraints, multi-antenna AP cooperation, and measured cell-free datasets. Additional work should also compare the proposed lightweight anomaly gate with deeper neural networks and reinforcement-learning-based resource-allocation methods under the same training and validation protocol.

11. DECLARATIONS

Conflict of interest: The authors declare no conflict of interest.

Data and code availability: The MATLAB simulation script, numerical tables, and regenerated figures can be provided as supplementary material to support reproducibility.

Funding: No external funding was reported for this work.

REFERENCES

- [1] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. on Wirel. Commun.*, vol. 9, no. 11, pp. 3590–3600, 2010.
- [2] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, 2014.
- [3] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and chal-

- lenges," *IEEE J. Sel. Top. Signal Process.*, vol. 8, no. 5, pp. 742–758, 2014.
- [4] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Trans. on Wirel. Commun.*, vol. 16, no. 3, pp. 1834–1850, 2017.
- [5] G. Interdonato, H. Q. Ngo, P. Frenger, and E. G. Larsson, "Ubiquitous cell-free massive MIMO communications," *EURASIP J. on Wirel. Commun. Netw.*, vol. 2019, no. 197, 2019.
- [6] E. Björnson and L. Sanguinetti, "Making cell-free massive MIMO competitive with MMSE processing and centralized implementation," *IEEE Trans. on Wirel. Commun.*, vol. 19, no. 1, pp. 77–90, 2020.
- [7] O. T. Demir, E. Björnson, and L. Sanguinetti, "Foundations of user-centric cell-free massive MIMO," *Found. Trends Signal Process.*, vol. 14, no. 3–4, pp. 162–472, 2021.
- [8] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sälö-niemi, and A. Toskala, "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proc. IEEE*, vol. 109, no. 7, pp. 1166–1199, 2021.
- [9] M. Giordani, M. Polese, A. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Commun. Mag.*, vol. 58, no. 3, pp. 55–61, 2020.
- [10] H. Q. Ngo, G. Interdonato, E. G. Larsson, G. Caire, and J. G. Andrews, "Ultra-dense cell-free massive MIMO for 6G: Technical overview and open questions," *arXiv preprint arXiv:2401.03898*, 2024.
- [11] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. on Wirel. Commun.*, vol. 10, no. 8, pp. 2640–2651, 2011.
- [12] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, "A comprehensive survey of pilot contamination in massive MIMO–5G system," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 905–923, 2016.
- [13] L. Sanguinetti, E. Björnson, and J. Hoydis, "Toward massive MIMO 2.0: Understanding spatial correlation, interference suppression, and pilot contamination," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 68–74, 2020.
- [14] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [15] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.
- [16] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
- [17] Y. S. Atiya, Z. Mobini, H. Q. Ngo, and M. Matthaiou, "Secure transmission in cell-free massive MIMO under active eavesdropping," *IEEE Trans. on Wirel. Commun.*, vol. 23, no. 12, pp. 18 036–18 052, 2024.
- [18] E. Björnson, L. Sanguinetti, J. Hoydis, and M. Debbah, "Optimal design of energy-efficient multi-user MIMO systems: Is massive MIMO the answer?" *IEEE Trans. on Wirel. Commun.*, vol. 14, no. 6, pp. 3059–3075, 2015.
- [19] Y. Zhao, I. G. Niemegeers, and S. M. H. de Groot, "Dynamic power allocation for cell-free massive MIMO: Deep reinforcement learning methods," *IEEE Access*, vol. 9, pp. 102 953–102 965, 2021.
- [20] M. U. Khan, E. Testi, M. Chiani, and E. Paolini, "Joint power control and pilot assignment in cell-free massive MIMO using deep learning," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 5260–5275, 2024.



- [21] T. J. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. on Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, 2017.
- [22] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wirel. Commun. Lett.*, vol. 7, no. 1, pp. 114–117, 2018.
- [23] P. Tarafder, C. Chun, A. Ullah, Y. Kim, and W. Choi, "Channel estimation in 5G-and-beyond wireless communication: A comprehensive survey," *Electronics*, vol. 14, no. 4, p. 750, 2025.
- [24] F. Rusek et al., "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 40–60, 2013.
- [25] J. Hoydis, S. ten Brink, and M. Debbah, "Massive MIMO in the UL/DL of cellular networks: How many antennas do we need?" *IEEE J. on Sel. Areas Commun.*, vol. 31, no. 2, pp. 160–171, 2013.
- [26] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. on Commun.*, vol. 61, no. 4, pp. 1436–1449, 2013.
- [27] E. Björnson, E. G. Larsson, and T. L. Marzetta, "Massive MIMO: Ten myths and one critical question," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 114–123, 2016.
- [28] S. Buzzi, C. D'Andrea, A. Zappone, and C. D'Elia, "User-centric 5G cellular networks: Resource allocation and comparison with the cell-free massive MIMO approach," *IEEE Trans. on Wirel. Commun.*, vol. 19, no. 2, pp. 1250–1264, 2020.
- [29] O. Ozdogan, E. Björnson, and J. G. Larsson, "Massive MIMO with spatially correlated Rician fading channels," *IEEE Trans. on Commun.*, vol. 67, no. 5, pp. 3234–3250, 2019.
- [30] J. F. Arellano, J. Park, S. Park, et al., "On the performance of MMSE channel estimation in massive MIMO systems over spatially correlated Rician fading channels," *Wirel. Commun. Mob. Comput.*, vol. 2024, p. 5 445 725, 2024.
- [31] M. K. Chary, C. H. V. Krishna, and D. R. Krishna, "Accurate channel estimation and hybrid beamforming using artificial intelligence for massive MIMO 5G systems," *AEU - Int. J. Electron. Commun.*, vol. 173, p. 154 963, 2024.
- [32] S. Deshpande, M. Aggarwal, P. Sabherwal, and S. Ahuja, "Deep learning-aided channel estimation combined with advanced pilot assignment algorithm to mitigate pilot contamination for cell-free networks," *Indian J. Sci. Technol.*, vol. 17, no. 5, pp. 465–477, 2024.
- [33] D. Abueida et al., "Signal processing for cell-free massive MIMO: Techniques and trends in estimation, detection, and precoding," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 9392–9434, 2025. DOI: [10.1109/OJCOMS.2025.3625823](https://doi.org/10.1109/OJCOMS.2025.3625823)
- [34] M. Sande and G. Binini, "A deep learning-based channel estimation scheme for cell-free massive MIMO systems," *SAIEE Afr. Res. J.*, vol. 116, no. 4, pp. 160–168, 2025. DOI: [10.23919/SAIEE.2025.11129185](https://doi.org/10.23919/SAIEE.2025.11129185)
- [35] S. Mohammadzadeh, M. Rahmani, K. Cumanan, A. Burr, and P. Xiao, "Pilot and data power control for scalable uplink cell-free massive MIMO," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 10 829–10 844, 2025. DOI: [10.1109/OJCOMS.2025.3647368](https://doi.org/10.1109/OJCOMS.2025.3647368)
- [36] H. H. Al-Hamadi, I. A. Al-Baltah, and N. A. Al-Shaibany, "Survey on intelligent anomaly detection techniques in IoT security," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 4, no. 1, pp. 1596–1621, 2026. DOI: [10.59628/jast.v4i1.2234](https://doi.org/10.59628/jast.v4i1.2234)
- [37] N. Y. Al-Matari and A. T. Zahary, "A conceptual blockchain architecture for dynamic spectrum access in 6G CR-IoT networks: An analytical review," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 3, no. 6, pp. 1467–1480, 2025. DOI: [10.59628/jast.v3i6.1953](https://doi.org/10.59628/jast.v3i6.1953)
- [38] E. Nayebe, A. Ashikhmin, T. L. Marzetta, H. Yang, and B. D. Rao, "Precoding and power optimization in cell-free massive MIMO systems," *IEEE Trans. on Wirel. Commun.*, vol. 16, no. 7, pp. 4445–4459, 2017.
- [39] Y. S. Atiya, Z. Mobini, H. Q. Ngo, and M. Matthaiou, "Joint power optimization and AP selection for secure cell-free massive MIMO," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2024, pp. 1–6.