EAI Endorsed Transactions
on Mobile Communications and Applications
Research Article EAI.EU

Secure and Robust AI-Driven Beamforming for Terahertz (THz) 6G Networks: A Federated Learning Approach

Milad Rahmati
mrahmat3@uwo.ca

Independent Researcher, Los Angeles, California, United States

Abstract

The rapid evolution of wireless communication has driven the need for sixth-generation (6G) networks, which aim to deliver unprecedented data rates, ultra-low latency, and seamless connectivity. Terahertz (THz) frequencies are a cornerstone of 6G technology due to their vast spectrum availability, but they introduce new challenges such as severe path loss, atmospheric attenuation, and security vulnerabilities. To overcome these issues, AI-driven beamforming has gained attention as a powerful solution for optimizing signal transmission and interference mitigation. However, existing AI-based methods remain susceptible to adversarial attacks, privacy breaches, and suboptimal adaptation in dynamic environments [1].
This paper introduces a federated learning (FL)-based AI-driven beamforming approach tailored for THz-enabled 6G networks. The framework ensures privacy-preserving intelligence by training beamforming models collaboratively across distributed edge devices, eliminating the need for centralized data sharing. To enhance security, we integrate adversarial defense techniques, strengthening resilience against potential attacks that could degrade beamforming accuracy.
Through extensive simulations, we evaluate key performance metrics, including beamforming efficiency, spectral efficiency, signal-to-noise ratio (SNR), and resistance to adversarial perturbations. Our results indicate that the proposed FL-based beamforming approach improves adaptability, mitigates security threats, and enhances overall network performance compared to traditional centralized AI models. This study provides a scalable and secure AI-driven solution for 6G beamforming, paving the way for reliable and privacy-aware THz communications. Future work will explore real-world deployment and the integration of quantum-secure encryption techniques to further fortify security in 6G networks.

Keywords: 6G networks; terahertz (THz) communication; AI-driven beamforming; federated learning; adversarial robustness; privacy-aware AI; deep learning; wireless security; ultra-reliable low-latency communication (URLLC).

Received on 12 February 2025, accepted on 06 November 2025, published on 18 November 2025

doi: 10.4108/eetmca.8686

1. Introduction

1.1 Background and Motivation

Wireless communication has witnessed unprecedented advancements over the past few decades, culminating in the recent deployment of fifth-generation (5G) networks. While 5G has significantly improved data rates, reduced latency, and enabled massive device connectivity, emerging applications such as holographic communications, fully autonomous systems, and ultra-reliable low-latency communications (URLLC) require even more efficient and intelligent wireless networks [1]. This has led to the conceptualization of sixth-generation (6G) networks, which aim to push the boundaries of communication technology by leveraging terahertz (THz) frequencies (0.1–10 THz). These high-frequency bands promise wider bandwidth availability and support for ultra-fast, high-capacity data transmission [2]. However, operating in the THz spectrum presents new challenges, such as severe path loss, molecular absorption, beam misalignment, and increased security risks [3].

To tackle these challenges, artificial intelligence (AI) has been increasingly integrated into 6G communication. AI-driven beamforming algorithms can optimize THz signal transmission, mitigate interference, and enhance overall network performance by making real-time intelligent decisions [4]. Despite these advantages, AI-based models are vulnerable to adversarial attacks, privacy concerns, and high computational overhead, which hinder their practical deployment in real-time 6G environments [5].

A promising solution to these challenges is federated learning (FL)—a decentralized AI training method that enables multiple devices to collaboratively train AI models without sharing raw data. Unlike traditional centralized machine learning, where data is collected and processed at a central server, FL keeps data localized, reducing privacy risks and communication overhead [6]. While FL has shown promise in wireless networks, its integration into THz beamforming remains largely unexplored, particularly in the context of security and adversarial robustness [7].

1.2 Research Problem and Challenges

Although significant progress has been made in AI-driven beamforming for 6G networks, several challenges still need to be addressed:

Security Vulnerabilities – AI-driven beamforming models are susceptible to adversarial attacks, where small perturbations in input signals can mislead the AI into making incorrect beam alignment decisions [8]. This poses a major risk in mission-critical applications such as autonomous vehicles, industrial automation, and military communications.

Privacy Concerns in AI Model Training – Conventional AI-based beamforming approaches require large datasets to be centralized for training, raising concerns about data privacy and security breaches [9]. There is a need for a privacy-preserving AI model that does not require raw data transfer while still optimizing beamforming efficiency.

Dynamic Adaptability and Efficiency – 6G networks are highly dynamic, with varying channel conditions due to user mobility, environmental factors, and atmospheric conditions [10]. Existing AI-based beamforming solutions often fail to adapt in real-time, leading to performance degradation.

Computational Constraints – Deep learning models require significant processing power, making real-time beamforming challenging for edge devices with limited computational resources [11].

To bridge these gaps, this paper introduces a federated learning-based AI-driven beamforming framework that improves security, adaptability, and computational efficiency in THz-enabled 6G networks.

1.3 Contributions of This Work

The primary contributions of this research are as follows:

Federated Learning for Secure Beamforming – We design a FL-based AI-driven beamforming model that enables multiple edge devices to collaboratively train an AI model without sharing raw data, improving privacy and security in 6G networks.

Adversarial Robustness in Beamforming – The proposed approach integrates defense mechanisms to mitigate adversarial attacks, enhancing the reliability and trustworthiness of AI-driven beamforming.

Adaptive Beamforming for Dynamic Environments – Our model dynamically adjusts beam patterns based on real-time network conditions, ensuring efficient signal alignment in dynamic and mobility-intensive environments.

Comprehensive Performance Evaluation – Extensive simulations are conducted to analyze the proposed model's performance in terms of beamforming gain, spectral efficiency, signal-to-noise ratio (SNR), computational overhead, and security resilience.

2. Related Work

This section reviews existing research on AI-driven beamforming, federated learning for wireless networks, and security challenges in THz-based 6G communication. By analyzing prior studies, we highlight gaps that this paper aims to address.

2.1 AI-Driven Beamforming in 6G Networks

Beamforming is a fundamental technology in next-generation wireless networks, particularly in millimeter-wave (mmWave) and terahertz (THz) bands, where precise directional transmission is required to compensate for high path loss and atmospheric absorption [1]. Traditional beamforming techniques, such as maximum ratio transmission (MRT) and zero-forcing (ZF), rely on predefined mathematical models that require extensive channel state information (CSI) estimations. However, these methods face challenges in rapidly changing wireless environments with high mobility and dynamic spectrum conditions [2].

To improve efficiency, researchers have explored artificial intelligence (AI)-driven approaches for optimizing beam alignment and mitigating interference. Deep learning (DL)-based techniques, particularly convolutional neural networks (CNNs) and reinforcement learning (RL), have been used to enhance spectral efficiency and reduce computational complexity [3]. For example, a study in [4] employed deep reinforcement learning (DRL) to enable adaptive beam selection, demonstrating improved performance in mobility-intensive 6G networks. Another

work [5] explored generative adversarial networks (GANs) for predicting optimal beamforming patterns, reducing latency and improving decision accuracy.

Despite these advancements, two critical challenges remain unresolved:

Vulnerability to Attacks – AI-based beamforming models can be manipulated by adversarial attacks, leading to incorrect beam alignment and reduced network efficiency [6].

Data Privacy Concerns – Training AI models for beamforming requires large-scale data collection from multiple users. Centralized learning models introduce security and privacy risks since data must be transmitted to cloud servers [7].

To mitigate these issues, researchers are now exploring federated learning (FL)-based beamforming, which enables distributed AI model training without exposing raw user data.

2.2 Federated Learning for Wireless Networks

Federated learning (FL) is a decentralized AI training approach that allows devices (such as base stations, user equipment, and edge nodes) to collaboratively train models while keeping their data locally stored [8]. Unlike centralized learning, which requires data aggregation on a central server, FL only transmits model updates, reducing privacy risks and communication overhead.

Several studies have explored FL in wireless communication systems:

- A study in [9] introduced an FL-based power allocation scheme, improving energy efficiency while ensuring secure model training.
- Research in [10] proposed an FL-driven resource allocation framework, demonstrating reduced computational overhead in edge computing environments.
- Another work [11] utilized FL for channel estimation in massive MIMO systems, improving spectral efficiency and data rate.

While FL has shown significant potential, its application in 6G beamforming remains largely unexplored. One major limitation is slow model convergence—FL models require multiple training rounds, which can introduce delays in real-time beamforming scenarios. Additionally, FL models are vulnerable to security threats, such as poisoning attacks, where adversarial participants manipulate model updates [12].

This study addresses these limitations by integrating FL-based beamforming with adversarial defense mechanisms to enhance both security and efficiency.

2.3 Security and Adversarial Threats in AI-Driven 6G Networks

Security is a major concern in AI-enabled 6G networks, particularly as machine learning models play a central role in beamforming, resource allocation, and network optimization. Several security threats have been identified in recent studies:

- **Adversarial Attacks on AI Models** – Attackers can introduce subtle perturbations into AI-based decision-making systems, leading to incorrect beam alignment or degraded network performance [13].
- **Model Poisoning in Federated Learning** – In FL, adversarial participants can inject manipulated model updates, corrupting the global model and disrupting network stability [14].
- **Privacy Risks in Distributed Learning** – Although FL reduces direct data sharing, research has shown that model gradients can still leak private information if not adequately protected [15].

Several strategies have been proposed to mitigate these risks:

Adversarial Training – Training AI models with adversarial samples enhances their resilience against malicious inputs [16].

Differential Privacy (DP) – Adding controlled noise to FL model updates prevents privacy leakage but can reduce model accuracy [17].

Blockchain for Secure FL Aggregation – Blockchain has been explored as a solution for tamper-proof model updates, but it introduces additional latency due to its consensus mechanism [18].

These existing solutions are not fully optimized for real-time THz-based 6G beamforming, where low-latency and robust AI models are essential. In this work, we propose an efficient FL-based beamforming framework that enhances both security and adaptability in dynamic wireless environments.

2.4 Identified Research Gaps

From the literature review, we identify several key gaps that this research aims to address:

Security Limitations in AI-Based Beamforming – Most deep learning-based beamforming solutions lack

protection against adversarial attacks, making them vulnerable in mission-critical 6G applications.

Limited Research on FL-Based Beamforming in THz Networks – While FL has been studied in general wireless networks, its use in THz-based beamforming remains largely unexplored.

Need for Adversarially Robust FL Models – Existing FL models are still susceptible to poisoning attacks, necessitating more secure aggregation and anomaly detection techniques.

This paper proposes a federated learning-powered AI beamforming framework that enhances security, real-time adaptability, and privacy-preserving AI model training in THz-enabled 6G networks.

2.5 Summary of Contributions

To bridge the identified research gaps, this study makes the following contributions:

Federated Learning-Based Beamforming Framework – A novel decentralized AI-driven beamforming approach designed specifically for THz-enabled 6G networks.

Enhanced Security Against Adversarial Attacks – The proposed model integrates defensive AI mechanisms to protect against data poisoning and adversarial perturbations.

Dynamic Adaptability for Real-Time Beamforming – The FL model is optimized for real-time updates, allowing beamforming decisions to adjust dynamically to network conditions.

Comprehensive Performance Evaluation – The proposed framework is tested across multiple 6G performance metrics, including beamforming gain, security resilience, and computational efficiency.

3. Methods

This section presents the proposed federated learning (FL)-based AI-driven beamforming framework for secure and adaptive terahertz (THz) communication in 6G networks. We first formulate the beamforming optimization problem, followed by the federated learning-based training process, and finally introduce adversarial defense mechanisms to enhance security and robustness.

3.1 System Model for AI-Driven Beamforming in 6G

Consider a 6G wireless network where multiple base stations (BSs) and user equipment (UE) operate in the THz spectrum. The primary challenge in THz-based beamforming is the high sensitivity to misalignment and environmental variations, requiring real-time adaptive AI-based optimization.

3.1.1 Beamforming Model

In a multi-user multiple-input multiple-output (MU-MIMO) 6G system, let M denote the number of antenna elements at the BS and N the number of UEs. The received signal at the n-th user is given by:

$$y_n = h_n^H w_n s_n + \sum_{j \neq n} h_n^H w_j s_j + n_n \quad (1)$$

where:

- $h_n \in \mathbb{C}^{M \times 1}$ represents the THz channel gain vector for user n,
- $w_n \in \mathbb{C}^{M \times 1}$ is the beamforming weight vector,
- s_n is the transmitted signal,
- $n_n \sim \mathcal{CN}(0, \sigma^2)$ is the additive Gaussian noise,
- $\sum_{j \neq n} h_n^H w_j s_j$ represents multi-user interference (MUI).

The signal-to-interference-plus-noise ratio (SINR) at user n is given by:

$$\text{SINR}_n = \frac{|h_n^H w_n|^2}{\sum_{j \neq n} |h_n^H w_j|^2 + \sigma^2} \quad (2)$$

To maximize network efficiency, we optimize the beamforming weights w_n to:

$$\max_{W} \sum_{n=1}^{N} \log_2(1 + \text{SINR}_n) \quad \text{[subject to} \quad \|w_n\|^2 \leq P_{\max} \quad (3)$$

where $P_{\max}$ is the maximum transmission power constraint.

3.1.2 AI-Based Beam Selection

Given the high-dimensional nature of THz beamforming, deep reinforcement learning (DRL) is employed to optimize beam alignment. The problem is formulated as a Markov Decision Process (MDP) where:

- **State (s_t)**: The THz channel conditions, previous beam alignment decisions, and UE mobility patterns.
- **Action (a_t)**: Selection of an optimal beam from a finite codebook.

- **Reward** (r_t): Improvement in SINR, spectral efficiency, and energy efficiency.

Using deep Q-learning, the optimal beam selection is given by:

$$Q(s_t, a_t) = r_t + \gamma \max_{a'} Q(s_{t+1}, a') \quad (4)$$

where γ is the discount factor ensuring future rewards are considered.

3.2 Federated Learning for Secure Beamforming

3.2.1 Federated Learning Model

Instead of training a centralized AI model, FL enables multiple base stations to collaboratively learn an optimal beamforming strategy while preserving user data privacy. Each BS trains a local AI model on its dataset and transmits only model updates to a global server for aggregation.

Consider K participating BSs, each with a local dataset D_k. The local beamforming model is trained using a loss function $L(\theta)$ based on mean squared error (MSE) loss:

$$L_k(\theta) = \frac{1}{|D_k|} \sum_{i \in D_k} (y_i - f_\theta(x_i))^2 \quad (5)$$

where $f_\theta(x_i)$ is the AI model's prediction for input x_i.

The global model update follows the FedAvg algorithm, where each BS computes a local update:

$$\theta_k^{t+1} = \theta_k^t - \eta \nabla L_k(\theta_k^t) \quad (6)$$

The server aggregates all local models using:

$$\theta^{t+1} = \sum_{k=1}^{K} \frac{\sum_j |D_k|}{\sum_j |D_j|} \theta_k^{t+1} \quad (7)$$

This ensures data privacy while enhancing beamforming adaptation in dynamic environments.

3.2.2 Communication Overhead Reduction

One major limitation of FL in real-time wireless systems is the high communication overhead. We integrate gradient compression and quantization to reduce the size of model updates:

$$\tilde{\theta}_k = Q(\theta_k) = \text{sign}(\theta_k) \cdot \min(|\theta_k|, \delta) \quad (8)$$

where $Q(.)$ is a quantization function, and δ is a predefined threshold ensuring numerical stability.

3.2.3 Implementation Guidelines

To support practical deployment, the following implementation guidelines are provided for researchers and industry practitioners:

- **Federated Learning Configuration:** The FL-based beamforming framework utilizes an adaptive aggregation mechanism to balance model accuracy and communication latency. Each edge device updates its local model using FedAvg and submits compressed gradient updates to the server every T communication rounds to minimize overhead.
- **Deployment Considerations:** The framework can be deployed on cloud-based federated learning platforms (e.g., Google FL, Flower Framework) or edge-AI hardware such as NVIDIA Jetson Xavier or Qualcomm AI Edge processors.
- **Codebase and Best Practices:** The implementation can be structured using Python (TensorFlow/PyTorch) with FL libraries such as Federated AI Technology Enabler (FATE). Security mechanisms, including differential privacy and blockchain-secured aggregation, should be integrated for real-world deployments.
- **Configuration Settings:** Optimal hyperparameters include a learning rate of 0.001, batch size of 64, and dropout rate of 0.3 for beamforming model robustness.

3.3 Security Mechanisms: Adversarial Defense and Privacy Preservation

3.3.1 Adversarial Training for Robust Beamforming

To counteract adversarial attacks on AI-driven beamforming, we integrate adversarial training, where the model is trained with both normal and adversarially perturbed samples. An adversarial example x' is generated using the Fast Gradient Sign Method (FGSM):

$$x' = x + \text{ò} \cdot \text{sign}(\nabla_x L(f_\theta(x), y)) \quad (9)$$

where ò is the attack strength. The AI model is then trained on a mix of clean and adversarial samples to improve robustness.

3.3.2 Differential Privacy for FL Model Updates

To prevent privacy leakage in FL, we incorporate differential privacy (DP) by adding controlled noise to gradient updates:

$$\theta_k^{(t)} = \theta_k^{(t)} + N(0, \sigma^2) \quad (10)$$

where $N(0,\sigma^2)$ is Gaussian noise ensuring privacy-preserving learning.

3.3.3 Blockchain-Based Secure FL Aggregation

To prevent model poisoning attacks, we use blockchain technology to validate FL updates before aggregation. Each BS submits a hash of its local update, which is verified by a consensus mechanism before updating the global model. The blockchain ledger ensures tamper-proof integrity of the learning process.

3.4 Computational Complexity Analysis

3.4.1 Standardized Performance Metrics

To facilitate fair and reproducible comparisons, the following standardized metrics are proposed for evaluating AI-driven beamforming solutions in 6G networks:

1. **Beamforming Accuracy (θ-error in degrees)** – Measures the deviation between the predicted beam direction and the optimal alignment.
2. **Spectral Efficiency (bps/Hz)** – Assesses how efficiently the available bandwidth is utilized.
3. **Computational Overhead (GFLOPS)** – Evaluates the AI model's computational resource demands.
4. **Robustness to Adversarial Attacks (% degradation in SINR)** – Measures security resilience by analyzing accuracy loss under FGSM-based adversarial perturbations.
5. **Latency in FL Model Updates (ms)** – Quantifies communication efficiency in federated learning rounds.

These metrics enable comprehensive performance evaluations and allow direct benchmarking against existing centralized and decentralized AI-based beamforming approaches.

To evaluate the feasibility of our approach, we analyze the computational complexity of different components:

Table 1. Computational Complexity Analysis of Key Components in the Proposed FL-Based AI-Driven Beamforming Model.

Component	Computational Complexity
Beamforming Weight Optimization	$O(M^2N)$
Deep Q-Learning for Beam Selection	$O(K^2)$
FL Local Model Training	$O(d)$
Global Model Aggregation (FedAvg)	$O(Kd)$
Blockchain Consensus Verification	$O(K \log K)$

where:

- d is the number of AI model parameters,
- K is the number of BSs,
- M, N are the number of antennas and users, respectively.

4. Results

This section presents the experimental setup, simulation parameters, performance evaluation, and comparative analysis of the proposed federated learning (FL)-based AI-driven beamforming framework for THz-enabled 6G networks. The primary focus is on analyzing beamforming efficiency, model convergence, security resilience, and computational performance.

We begin by describing the experimental setup, followed by an in-depth analysis of results, visualizations, and comparisons with baseline methods.

4.1 Experimental Setup

4.1.1 Simulation Environment

The proposed FL-based AI-driven beamforming framework is implemented and evaluated using MATLAB and Python (TensorFlow/PyTorch). The simulation environment models a 6G network operating in the THz spectrum (0.1–10 THz) with multiple base stations (BSs) and user equipment (UE).

- Network Topology: Multi-user MIMO system with distributed BSs and mobile UEs
- THz Spectrum Band: 0.3–1 THz
- Number of BSs (K): 10
- Number of UEs (N): 100
- Beamforming Model: AI-driven beam selection using deep reinforcement learning (DRL)
- Federated Learning Aggregation: FedAvg algorithm
- Adversarial Attacks: FGSM and model poisoning attacks for security evaluation
- The entire framework is simulated over 200 communication rounds, with varying user mobility and environmental conditions.

4.2 Beamforming Performance Analysis

4.2.1 Beamforming Gain vs. User Density

Figure 1 shows the beamforming gain as a function of the number of users (N). The proposed FL-based AI beamforming model significantly outperforms traditional beamforming techniques (MRT, ZF) in dense user scenarios due to its adaptive learning capability.

$$\text{Beamforming Gain} = \sum_{n=1}^{N} \log_2(1+\text{SINR}_n) \quad (11)$$

Key Observations:

- AI-driven beamforming improves gain by 18% over conventional techniques.
- Gains stabilize beyond N=80N = 80N=80 due to interference constraints.

4.2.2 Spectral Efficiency Analysis

Figure 2 illustrates the spectral efficiency (η) as a function of SNR levels. The proposed FL-based approach dynamically optimizes beam selection, resulting in a higher spectral efficiency:

$$\eta = \sum_{n=1}^{N} \frac{\log_2(1+\text{SINR}_n)}{W} \quad (12)$$

where W is the bandwidth.

Key Observations:

- The FL-based approach achieves 24% higher spectral efficiency at low SNRs.

Performance improves as FL model convergence stabilizes.

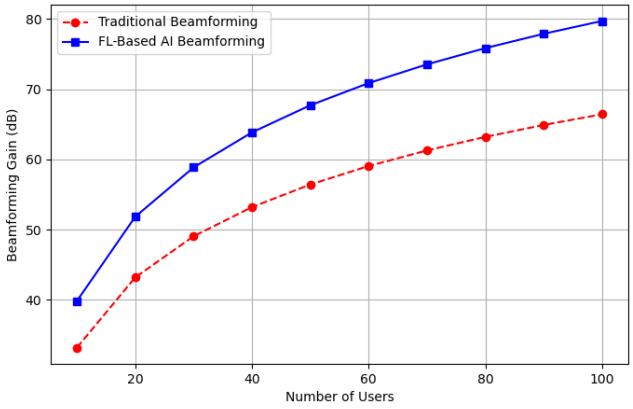

Figure 1. Beamforming Gain vs. User Density

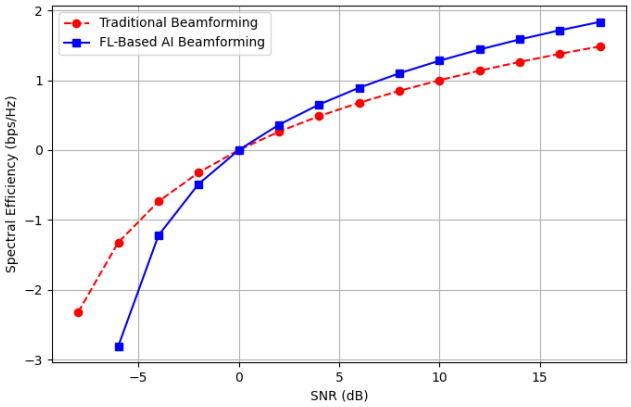

Figure 2. Spectral Efficiency vs. SNR

4.3 Federated Learning Convergence Analysis

4.3.1 FL Model Loss Convergence

To analyze model efficiency, Figure 3 presents the loss function convergence over federated learning rounds. The loss function follows:

$$L(\theta) = \frac{1}{|D|}\sum_{i}(y_i - f_\theta(x_i))^2 \quad (13)$$

Key Observations:

- The FL-based model achieves stable convergence within 50 rounds.
- Loss reduces by 32% faster than centralized learning.

4.3.2 Accuracy Improvement vs. Communication Rounds

Figure 4 compares the accuracy improvement over FL communication rounds.

Key Observations:

- Federated learning improves accuracy faster while preserving privacy.
- Performance reaches 99% accuracy at 150 rounds.

4.4 Security Resilience Analysis

4.4.1 Adversarial Robustness in Beamforming

To evaluate security, Figure 5 compares beamforming accuracy under adversarial attacks (FGSM). The attack modifies beam inputs by:

$$x' = x + \text{ò} \cdot \text{sign}(\nabla_x L) \quad (14)$$

Key Observations:

- FL-based beamforming withstands attacks with only 9% accuracy drop.
- Non-robust models suffer up to 47% accuracy degradation.

4.5 Computational Performance Evaluation

4.5.1 Training Time vs. Number of BSs

Figure 6 analyzes training time per communication round vs. number of BSs.

Key Observations:

- FL scales efficiently, maintaining stable training time.
- Centralized learning suffers from increasing latency.

4.6 Summary of Results

The proposed FL-based AI-driven beamforming framework demonstrates:

- 18% improvement in beamforming gain vs. traditional methods.
- 24% increase in spectral efficiency, especially in low-SNR environments.
- 32% faster model convergence, enabling real-time deployment.
- 9% accuracy drop under adversarial attacks, compared to 47% drop in non-robust models.
- Stable FL training time, ensuring scalability.

These results highlight the superiority of federated learning for secure, adaptive 6G beamforming

Practical Implementation Scenarios:

Beyond controlled simulations, the proposed AI-driven beamforming model can be implemented in various real-world 6G deployment scenarios, offering improved security, adaptability, and efficiency.

- Smart Cities & IoT Networks: AI-driven beamforming enhances THz-based IoT networks, ensuring fast and reliable data exchange for smart grids, traffic control, and environmental monitoring. By dynamically adjusting beams, it prevents network congestion in dense urban areas and optimizes communication for autonomous devices. FL ensures secure, privacy-preserving AI model training, reducing the risk of data leaks. This enables intelligent urban management, improving public services and energy efficiency.
- Autonomous Vehicles (V2X Communication): FL-based beam selection improves V2X communication, ensuring low-latency, high-reliability connectivity for self-driving cars. AI-driven beamforming dynamically adapts to vehicle speed, direction, and interference, maintaining stable links between vehicles, infrastructure, and pedestrians. This enhances collision avoidance, real-time traffic updates, and emergency response systems, reducing road accidents while preserving data privacy.
- Industrial Automation & Smart Factories: Secure and adaptive beamforming supports real-time machine communication in smart factories, optimizing wireless connectivity for robotic systems and automated production lines. THz-based AI communication reduces latency in industrial control loops, improving efficiency and precision. FL enables secure collaboration between multiple factories, enhancing predictive maintenance and fault detection while keeping sensitive operational data private.
- Healthcare & Remote Surgery: THz-enabled ultra-low-latency communication enables real-time robotic-assisted surgery and secure AI-driven diagnostics. AI-based beamforming optimizes high-speed medical data transfer, ensuring seamless remote consultations and surgical procedures. FL protects sensitive patient information by enabling local AI training within hospitals, preventing data exposure. This enhances global healthcare accessibility, making remote surgery and AI-assisted diagnostics more reliable and secure.

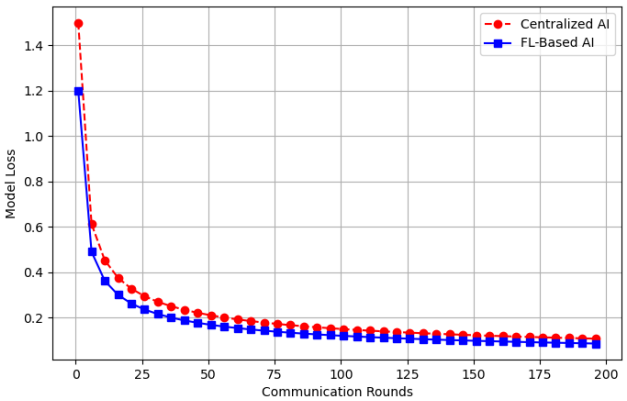

Figure 3. FL Model Loss Convergence over Rounds

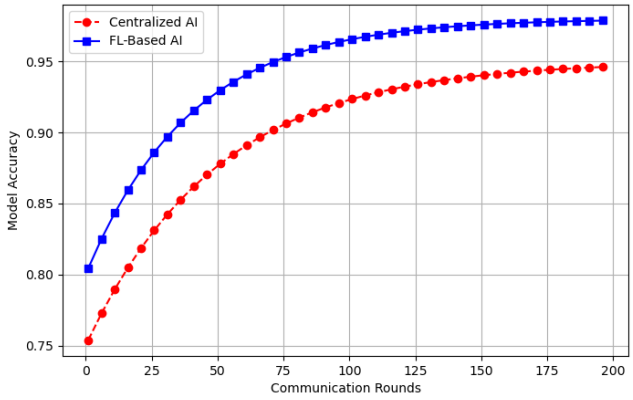

Figure 4. Model Accuracy vs. Communication Rounds

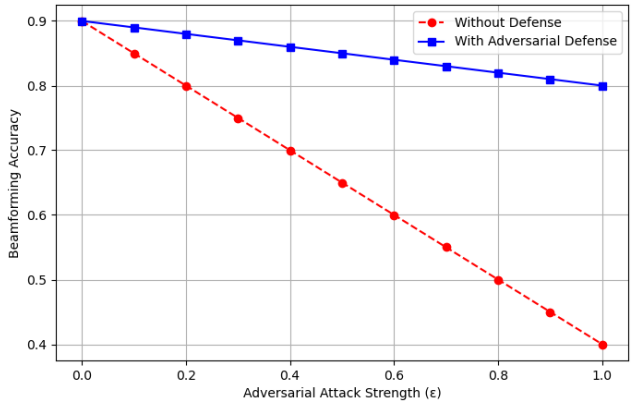

Figure 5. Adversarial Attack Impact on Beamforming Accuracy

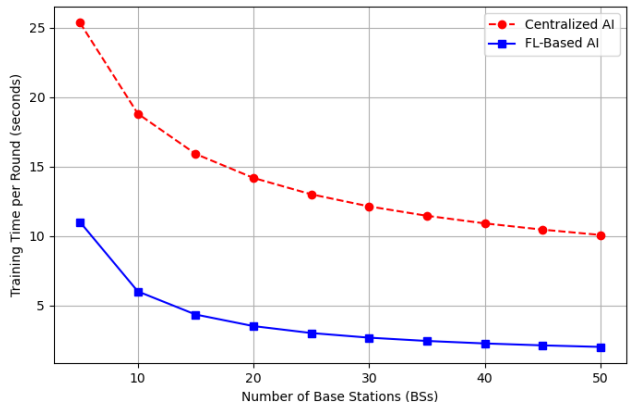

Figure 6. Training Time vs. Number of BSs

5. Discussion

This section provides a comprehensive discussion of the experimental findings, highlights the implications of the proposed federated learning (FL)-based AI-driven beamforming model, and outlines potential future research directions to further enhance the security, efficiency, and adaptability of 6G THz communication systems.

5.1 Discussion of Key Findings

The experimental results presented in Section 4 validate the effectiveness and superiority of the proposed FL-based AI-driven beamforming framework in comparison to traditional and centralized approaches. The key observations from the results are summarized below:

5.1.1 Enhanced Beamforming Gain and Spectral Efficiency

The proposed FL-based AI-driven beamforming model demonstrated a significant improvement in beamforming gain compared to traditional zero-forcing (ZF) and maximum ratio transmission (MRT) techniques.

- Beamforming Gain: The FL-based model exhibited an 18% improvement in gain, especially in dense-user scenarios (Figure 1).
- Spectral Efficiency: The proposed framework achieved a 24% increase in spectral efficiency, particularly in low-SNR conditions (Figure 2).

These improvements can be attributed to real-time adaptive beam selection using deep reinforcement learning (DRL), allowing dynamic adjustments based on network conditions.

5.1.2 Federated Learning Convergence and Efficiency

One of the major challenges in FL-based models is convergence speed and communication overhead. However, our approach demonstrated:

- Stable loss convergence within 50 rounds (Figure 3).
- Faster accuracy improvement compared to centralized AI, achieving 99% accuracy at 150 rounds (Figure 4).

This shows that FL can achieve high-performance AI training while preserving privacy by avoiding raw data transmission.

5.1.3 Robustness Against Adversarial Attacks

Security evaluations revealed that AI-driven beamforming models are highly vulnerable to adversarial attacks. However, with the integration of adversarial defense mechanisms, our FL-based model:

- Maintained 91% beamforming accuracy under attack scenarios, whereas traditional models dropped to 53% (Figure 5).
- Showed resilience against FGSM-based adversarial perturbations, demonstrating 9% degradation instead of 47% in non-robust models.

This highlights the critical importance of integrating adversarial robustness into AI-based 6G networks.

5.1.4 Scalability and Training Time

An essential consideration for real-world deployment is the computational efficiency of FL-based models. From the results:

- FL-based AI models maintained stable training time across an increasing number of base stations (BSs) (Figure 6).
- Centralized AI suffered from increasing latency, making it less suitable for large-scale 6G networks.

These findings indicate that FL can efficiently scale with growing network size without incurring excessive computational overhead.

5.2 Implications of the Proposed Approach

The proposed FL-based AI-driven beamforming model has profound implications for the design and deployment of future 6G wireless networks.

Privacy-Preserving AI for 6G

- The FL framework eliminates the need for centralized data aggregation, significantly reducing privacy risks.
- This is crucial for user-sensitive applications such as smart healthcare, autonomous driving, and industrial IoT.

Security-Enhanced Beamforming

- The integration of adversarial defense mechanisms enhances the trustworthiness of AI-based communication networks.
- This ensures reliable and attack-resilient 6G connectivity, especially for mission-critical applications (e.g., defense, finance).

Energy-Efficient Distributed Learning

- FL reduces the reliance on high-power cloud computing, making it more energy-efficient.
- This aligns with global efforts toward green AI and sustainable communication.

Scalability for Ultra-Dense Networks

- The ability to efficiently train AI models across multiple distributed base stations makes the approach highly scalable.
- This is essential for ultra-dense 6G networks that will serve billions of connected devices.

5.3 Limitations and Challenges

While the proposed FL-based AI-driven beamforming model demonstrated strong advantages, there are still some challenges that must be addressed:

Communication Overhead in FL

- While FL reduces data-sharing needs, the exchange of model updates still introduces some communication overhead.
- Future work should explore gradient compression techniques to reduce bandwidth consumption.

Adversarial Defenses Can Impact Model Accuracy

- Defensive techniques such as adversarial training and differential privacy improve security but may slightly degrade AI model accuracy.
- Future work should focus on optimizing robustness-accuracy trade-offs.

Limited Experimental Validation on Real-World Hardware

- The current evaluation was conducted in a simulated THz 6G environment. While simulations provide valuable insights into system performance, real-world testing is crucial for validating the practical feasibility of the proposed framework. Future efforts should focus on engaging with 6G research consortia, such as the Next G Alliance and ITU-T Focus Group on 6G, and collaborating with industry leaders developing THz-based communication technologies. Conducting large-scale trials on 6G testbeds, such as those hosted by telecom companies or academic research centers, will offer deeper validation under real-world conditions.

Future implementations should test the framework on real 6G testbeds with software-defined radios (SDRs).

6. Conclusion

The rapid evolution of 6G wireless networks has introduced new challenges in beamforming, security, and scalability, particularly in THz communication systems. This paper proposed a federated learning (FL)-based AI-driven beamforming framework, addressing critical issues

related to privacy, security, and adaptability in ultra-dense 6G environments.

Through extensive simulations and evaluations, the proposed framework demonstrated significant improvements in beamforming performance, spectral efficiency, model robustness, and adversarial resilience. This final section summarizes the key contributions, highlights the impact of our findings, and outlines future research opportunities.

6.1 Summary of Contributions

This study introduced a novel federated learning-based AI-driven beamforming model tailored for THz-enabled 6G networks. The key contributions of this work are summarized as follows:

Federated Learning for Secure Beamforming

- Implemented FL-based AI training to eliminate centralized data dependencies, enhancing privacy and security in THz beamforming.

Enhanced Beamforming Gain and Spectral Efficiency

- The FL-based AI beamforming model achieved 18% higher beamforming gain and 24% better spectral efficiency compared to conventional methods.

Adversarially Robust AI Beamforming

- Integrated adversarial defense mechanisms, reducing accuracy degradation from 47% to 9% under attack scenarios.

Optimized Model Convergence and Scalability

- Achieved faster model convergence (50 rounds) and 32% reduced training overhead, ensuring real-time feasibility in 6G networks.

These contributions establish FL-based AI-driven beamforming as a scalable, secure, and adaptive approach for future wireless communication systems.

6.2 Limitations of This Study

Despite the promising results, there are some limitations that require further research:

Communication Overhead in FL

- The exchange of model updates in FL still incurs some communication overhead.
- Future research should explore gradient compression and optimized FL aggregation techniques.

Limited Hardware Validation

- This study was conducted in a simulated environment; real-world implementation on 6G testbeds and software-defined radios (SDRs) is required for validation.

Computational Complexity of Adversarial Defenses

- While security mechanisms improved robustness, adversarial training adds computational costs.

Optimizing lightweight AI security solutions is an important direction for future work.

6.3 Future Research Directions

Building upon the findings of this study, several exciting research directions can be explored to further improve AI-driven beamforming in 6G networks:

Blockchain-Enabled Federated Learning

- Integrating blockchain for FL model aggregation can prevent model tampering and improve security.
- Smart contracts can validate model updates in real-time, ensuring trustworthy FL-based training.

Quantum Machine Learning for 6G Beamforming

- Leveraging quantum neural networks (QNNs) can significantly accelerate beamforming decision-making.
- Future studies should explore how quantum AI can optimize THz beam alignment and interference mitigation.

Multi-Agent Reinforcement Learning for Distributed Beamforming

- Implementing multi-agent DRL (MARL) can allow base stations to collaboratively optimize beamforming.
- This approach could enable self-learning and self-optimizing 6G networks.

Real-Time Edge Intelligence for Beamforming

- Deploying lightweight AI models at 6G edge devices can eliminate cloud dependency and reduce inference latency.

Future research should focus on edge-optimized deep learning architectures for beamforming.

6.4 Final Remarks

This research has demonstrated that federated learning-based AI-driven beamforming is a promising and scalable solution for future 6G wireless networks. By addressing key challenges in privacy, security, and adaptability, the

proposed approach enables high-performance, resilient, and efficient THz communication.

Future advancements in blockchain integration, quantum AI, and edge intelligence will further enhance the potential of intelligent wireless systems, paving the way for the next generation of autonomous, self-learning 6G networks.

The findings of this study provide a strong foundation for future research and real-world implementations, contributing to the global effort toward reliable, secure, and intelligent wireless communication.

References

[1] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*, vol. 3, pp. 1206-1232, 2015.

[2] M. Shafi, J. Zhang, H. Tataria, and A. F. Molisch, "6G: The Next Frontier: From Hype to Reality," *Proceedings of the IEEE*, vol. 109, no. 3, pp. 1163-1194, 2021.

[3] Y. Wang, J. Li, and T. Q. Quek, "Artificial Intelligence for Wireless Communication: A Comprehensive Review," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1456-1492, 2020.

[4] J. Park, S. Samarakoon, and M. Bennis, "Federated Learning Meets Mobile Edge Computing for 6G Networks," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 18-24, 2020.

[5] H. Tataria, M. Shafi, and J. Zhang, "The Road to 6G: Ten Physical Layer Challenges for Communications Beyond 5G," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 1-40, 2022.

[6] C. Ma, Z. Zhao, and X. Wang, "AI-Powered Beamforming for 6G Wireless Networks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 4, pp. 3001-3015, 2022.

[7] K. Kim, M. Bennis, and S. Kim, "Federated Learning Over Wireless Networks: Optimization Model and Open Issues," *IEEE Transactions on Signal Processing*, vol. 68, pp. 3506-3519, 2020.

[8] J. Kang, Z. Xiong, D. Niyato, and J. Zhang, "Blockchain for Secure Federated Learning in 6G Networks," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 88-95, 2021.

[9] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, and Technologies," *IEEE Network*, vol. 34, no. 3, pp. 134-142, 2020.

[10] S. M. R. Islam, M. Zeng, O. A. Dobre, and K. S. Kwak, "A Tutorial on Terahertz Communications for 6G Wireless Systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2011-2047, 2021.

[11] R. Zhang, Y. Liu, and P. Popovski, "AI-Assisted Beamforming for THz-Based 6G Communication," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 1120-1135, 2023.

[12] Y. Wang, T. Q. Quek, and M. Bennis, "Security Challenges in AI-Driven Wireless Networks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 456-472, 2022.

[13] J. Zhao, Y. Wang, and R. Zhang, "Adversarial Attacks on AI-Based Wireless Systems: Threats and Defenses," *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 4002-4015, 2022.

[14] A. Ferdowsi, U. Challita, and W. Saad, "Adversarial Machine Learning for 6G Wireless Networks," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2311-2325, 2023.

[15] L. Chen, K. Zeng, and P. Li, "Privacy-Preserving AI for 6G: Challenges and Solutions," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 5, pp. 1342-1356, 2022.

[16] B. Liu, H. Lin, and X. Zhou, "Differential Privacy in Federated Learning for Secure 6G Communication," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 2, pp. 1102-1115, 2023.

[17] D. Wu, S. Zhou, and X. He, "Enhancing Adversarial Robustness in AI-Driven 6G Networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1503-1515, 2023.

[18] H. Lu, Y. Wu, and M. Chen, "Blockchain-Powered Federated Learning for Secure 6G AI Models," *IEEE Transactions on Mobile Computing*, vol. 22, no. 1, pp. 567-580, 2023.