Sensors and Materials, Vol. 38, No. 8 (2026) 4621–4636
MYU Tokyo

S & M 4585

Federated Learning Multi-sensor Data Fusion for Privacy-preserving and Wi-Fi Spoofing Detection in Sensor Networks

Xinying Lin[1] and Zhengji Mao[2*]

[1]School of Ocean Engineering, Xiamen Ocean Vocational College,
No. 4566 Hongzhong Avenue, Xiamen City, Fujian Province 361100, P. R. China
[2]School of Marine Mechatronics, Xiamen Ocean Vocational College,
No. 4566 Hongzhong Avenue, Xiamen City, Fujian Province 361100, P. R. China

(Received May 11, 2026; accepted July 29, 2026)

Keywords: federated learning, multi-sensor fusion, privacy-preserving security, behavioral entropy

The rapid expansion of IoT devices in smart campuses has increased vulnerabilities to Wi-Fi spoofing and signal mimicry attacks. Therefore, a decentralized, lightweight physical-layer anomaly detection system is developed in this study, operating autonomously at resource-constrained edge nodes. The developed federated learning multi-sensor fusion (FL-MSF) system integrates received signal strength, multipath delay spreads, and background noise into a regional fluctuation index (*RFI*). *RFI* enables edge transceivers to isolate malicious signal injections from benign fluctuations without relying on heavy centralized classifiers. To address non-independent and identically distributed data across heterogeneous environments, FL-MSF introduces an adaptive aggregation mechanism that weights local model updates based on material attenuation profiles. Model updates are securely combined using the federated averaging (FedAvg) protocol with clipping-based differential privacy, ensuring strong data sovereignty. Simulation results in a high-density campus environment (50 edge nodes, 200 IoT clients) show that FL-MSF achieves 96.5% detection accuracy, a 0.95 F1-score, and low latency (31 ms), outperforming baseline long short-term memory networks, graph neural networks, and FedAvg models. Gradient leakage risk was reduced to <0.5%, and scalability tests presented accuracy gains as sensor density increased. Performance under extreme scaling and management of long-term drifts in material attenuation parameters must be addressed to enhance the availability of the developed system.

1. Introduction

Smart campuses inherently necessitate extensive deployments of IoT devices and high-density wireless traffic, conditions that inadvertently create favorable environments for sophisticated Wi-Fi spoofing and signal mimicry attacks. With the transition from traditional sensor networks to advanced IoT ecosystems, where physical hardware sensors, intelligent edge

*Corresponding author: e-mail: maozhengji@xmoc.edu.cn
https://doi.org/10.18494/SAM6415

ISSN 0914-4935

agents, and dynamic user personas are unified into a single interconnected fabric, security demands have grown exponentially. In these environments, Wi-Fi spoofing poses a critical threat: an unauthorized device masquerades as a legitimate sensor node by cloning its network identifier. Signal mimicry is also a concern, in which an adversary replicates and replays physical-layer characteristics, such as the received signal strength indicator (*RSSI*) amplitude envelope, to bypass security boundaries. Within distributed machine learning architectures, these attacks can escalate into model poisoning, a targeted threat where a compromised edge node deliberately injects corrupted or fabricated weight updates into the training cycle, manipulating global model convergence.

In the environment, edge-enabled sensor nodes, ranging from wireless access points to localized environmental monitors, are critical interfaces for capturing real-time data streams. Conventional security systems, however, rely predominantly on centralized data collection to train detection models, a strategy that incurs significant communication overhead due to backhauling raw sensor data and introduces severe privacy risks through the exposure of user behavioral patterns and precise location telemetry.

To address these challenges, edge-enabled multi-sensor data fusion has emerged as a promising approach for low-latency, localized anomaly detection. While this strategy reduces communication overhead and enhances privacy, the limited computational and contextual scope of individual edge nodes constrains the global robustness of security models. Nodes often struggle to adapt to dynamic radiofrequency environments and heterogeneous interference patterns across different campus zones. Consequently, effective security requires distributed, intelligent data-gathering mechanisms.[1] Recent sensor networks exemplify such a mechanism by collaboratively processing data with peripheral devices to distinguish legitimate signals from malicious mimicry, necessitating decentralized intelligent algorithms. Federated learning (FL) provides a transformative solution, enabling multiple edge nodes to collaboratively refine a shared spoofing detection model without exchanging raw data. By transferring the training process to the network edge, FL achieves a balance between high-accuracy threat identification and strict data sovereignty, supporting proactive, privacy-compliant defense architectures.

Advancements in IoT further reinforce decentralized, privacy-preserving defense frameworks that integrate FL with sensor data fusion. In smart healthcare, for instance, heterogeneous multi-sensor data fusion combined with FL enables rapid and precise medical interventions while safeguarding patient confidentiality.[2,3] Similarly, energy-efficient FL-based AI models are increasingly applied to real-time monitoring,[4] near-field Internet of Entities networks, and resource management through deep reinforcement learning.[5] These applications highlight a broader trend in which sensor technology drives resilience and intelligence in complex systems.

In data fusion, ensuring data security and integrity remains paramount. Device-to-server fusion approaches have shown promise in enhancing privacy in IoT-enabled communication.[6] Quantum deep learning combined with data fusion has demonstrated effectiveness in detecting cyber-attacks on medical systems,[7] whereas FL has been successfully applied to privacy-preserving recommendation systems.[8] Recent technologies, such as blockchain for edge-based threat analytics,[9] multi-head attention mechanisms, and optimization frameworks, strengthen IoT infrastructures against adversarial attacks.[10]

To address integrity challenges in sensor data fusion, Nie *et al.* proposed tensor-based dynamic fusion to reduce modality imbalances in FL.[11] In wireless sensing, FL improves few-shot learning across diverse Wi-Fi classifications,[12] whereas in vehicular networks, FL supports IoT systems through federated instruction tuning.[13] Hybrid edge–cloud environments employ adaptive batch-stream analytics[14] and large language models.[15] Efficiency in data fusion has been advanced through statistical aggregation in federated Bayesian deep learning,[16] trajectory prediction using FL,[17] and deep reinforcement learning for collaborative aggregation.[18]

On the basis of such advancements, we developed the FL multi-sensor fusion (FL-MSF) system in this study. Its architecture integrates long short-term memory (LSTM) networks with graph neural networks (GNNs) to preserve temporal signal patterns and capture spatial dependencies across sensor networks, achieving superior detection accuracy against mimicry attacks. A clipping-based differential privacy mechanism within the FedAvg protocol safeguards data integrity, and the regional fluctuation index (*RFI*) is employed to dynamically adjust anomaly detection boundaries at edge nodes to reduce latency in real-time defense. By avoiding raw data transmission, FL-MSF alleviates communication overhead and provides a scalable, privacy-preserving framework for integrity-assured sensor applications.

In this study, we design an entropy-based physical-layer metric capable of isolating malicious anomalies on lightweight microcontrollers and construct an adaptive federated aggregation architecture that sustains accuracy across heterogeneous sensor environments. The developed system in this study conducts hardware-compatible signal processing and localized model optimization, mapping material attenuation profiles of sensor zones directly to aggregation weights to bypass non-independent and identically distributed (IID) bottlenecks. The system also presents real-time mitigation capability in sub-millisecond edge execution. By evaluating scaling limits under massive multi-node configurations and addressing long-term drift in baseline material properties, the system's performance can be further enhanced.

2. Methodology

The FL-MSF system operates on the principle of adjusting the anomaly detection boundary from a centralized cloud to a collaborative edge layer. Using this adjustment, the problems in latency and privacy inherent in high-density smart campus environments can be solved.

2.1 System algorithm

2.1.1 Localized feature extraction and state modeling

At each heterogeneous edge node $k \in \{1, 2, ..., K\}$, the system continuously monitors the physical-layer environment. To mitigate the volatility of raw wireless signals, we define a state vector $S_{k,t}$ at the time step t.

$$S_{k,t} = [RSSI_{k,t}, \tau_{k,t}, N_{k,t}]^T \tag{1}$$

Here, $RSSI_{k,t}$ denotes the localized signal strength, $\tau_{k,t}$ represents the multi-path propagation delay, and $N_{k,t}$ represents the background noise floor. The fusion approach developed in this study incorporates *RSSI*, multi-path delay spreads, and background noise variables to construct a high-fidelity representation of the radiofrequency environment.

To calculate deviations from the benign baseline, we introduce *RFI*. When $\overline{S}_k$ denotes the moving average during calibration, the instantaneous deviation measure $\xi_{k,t}$ is defined as

$$\xi_{k,t} = \| S_{k,t} - \overline{S}_k \|^2 + \epsilon . \tag{2}$$

Here, ϵ is a smoothing constant to prevent numerical instability. *RFI* is derived using a localized entropy function to capture uncertainty in the signal distribution.

$$RFI_{k,t} = -\int p\left(\xi_{k,t}\right) ln\left(p\left(\xi_{k,t}\right)\right) d\xi_{k,t} \tag{3}$$

Here, $p(\xi_{k,t})$ is the probability distribution of the instantaneous fluctuation. The derived *RFI* serves as the input to the downstream neural architecture, representing the localized security health of the spectrum.

2.1.2 Spatiotemporal modeling

To detect mimicry attacks, temporal shifts and spatial anomalies, such as rogue nodes appearing in unexpected coordinates, must be determined since spoofers rarely maintain perfect long-term consistency. The internal state of the LSTM network at node k is updated to memorize signal patterns.[19] In the LSTM network, the forget gate f_t and the input gate i_t are defined as

$$f_t = \sigma\left(W_f \cdot \left[h_{t-1}, RFI_{k,t}\right] + b_f\right), \tag{4}$$

$$i_t = \sigma\left(W_i \cdot \left[h_{t-1}, RFI_{k,t}\right] + b_i\right). \tag{5}$$

Here, h_t is the hidden output, and W and b are trainable parameters. The candidate cell state $\tilde{C}_t$ and the finally updated C_t govern long-term memory and are expressed as follows.

$$\tilde{C}_t = \tanh\left(W_C \cdot \left[h_{t-1}, RFI_{k,t}\right] + b_C\right) \tag{6}$$

$$C_t = f_t \cdot C_{t-1} + i_t \cdot \tilde{C}_t \tag{7}$$

The hidden output h_t is filtered by the output gate o_t using the following equations.

$$o_t = \sigma\left(W_o \cdot \left[h_{t-1}, RFI_{k,t}\right] + b_o\right) \tag{8}$$

$$h_t = o_t \cdot \tanh\left(C_t\right) \tag{9}$$

To capture spatial dependencies between adjacent edge nodes, we employ GNN.[20] GNN is a deep learning architecture that analyzes data structured as graphs, mapping physical sensor nodes as vertices and their wireless communication paths as structural edges. The message-passing update for node k at layer $l(m_k)$ is expressed as

$$m_k^{(l)} = \sum_{j \in \mathcal{N}(k)} \frac{1}{\sqrt{d_k d_j}} h_j^{(l)}. \tag{10}$$

Here, d_k is the degree of node k. The spatial feature z_k is refined as

$$z_k = \sigma\left(W^{(l)} \cdot \left[h_k^{(l)} \,||\, m_k^{(l)}\right]\right). \tag{11}$$

Here, the concatenation operator || is used to fuse temporal features with spatial context, enabling robust anomaly detection.

2.1.3 FL and differential privacy

To avoid uploading raw signal data, we implement an FL protocol. In the protocol, each node solves a local optimization problem as follows.

$$\min_{w_k} L_k\left(w_k\right) = \mathcal{L}_{CE}\left(w_k; z_k\right) + \lambda \,||\, w_k - w_{global} \,||^2 \tag{12}$$

Here, $\mathcal{L}_{CE}$ is the cross-entropy loss, λ is the regularization weight, and w_{global} represents the global model parameters. Before transmission, gradients $\bar{g}_k$ are clipped with a threshold Γ,

$$\bar{g}_k = \frac{g_k}{\max\left(1, \frac{||\, g_k \,||_2}{\Gamma}\right)}. \tag{13}$$

Gaussian noise $\tilde{g}_k$ is then added for differential privacy.

$$\tilde{g}_k = \bar{g}_k + \mathcal{N}\left(0, \sigma^2 \Gamma^2 I\right) \tag{14}$$

Here, I is the identity matrix, ensuring isotropic Gaussian noise across all gradient dimensions. The global server performs weighted FedAvg (W).

$$W_{t+1} = W_t - \eta \sum_{k=1}^{K} \omega_k \tilde{g}_k \tag{15}$$

Here, η is the global learning rate and ω_k represents the relative data contribution weight. Finally, the spoofing probability P_{spoof} is computed using Softmax.

$$P_{spoof} = \frac{\exp\left(W_{global} \cdot z_k + b\right)}{\sum \exp\left(W_{global} \cdot z_k + b\right)} \tag{16}$$

Here, the denominator represents the Softmax normalization across all possible classes. A detection alert is triggered when $P_{spoof} > \alpha$, where α is dynamically tuned on the basis of the *RFI* to balance false positives (*FP*) and sensitivity. The FL-MSF system performs global aggregation, localized training with privacy preservation, and real-time inference. The following Algorithm 1 is created for the global aggregation on the server side, whereas Algorithm 2 is for the local training and data privacy on the node side. Algorithm 3 is created to describe the online detection of inference.

2.2 System evaluation

To evaluate the performance of the FL-MSF system in a sensor network, we simulated a smart campus characterized by high-density sensor deployment. The simulation was conducted, focusing on the interplay between heterogeneous edge sensor nodes, varying signal interference conditions, and evolving spoofing attack vectors. For simulation, we used Network Simulator 3 (NS-3), a widely adopted platform for modeling discrete-event industrial sensor networks,[21] integrated with PyTorch to support FL modules. NS-3 is a discrete-event network simulation framework widely used in research to model realistic packet data behavior, wireless channel propagation, and network protocols over virtualized physical topologies without requiring massive hardware testbeds.

The simulated campus had an area of 25000 m^2 with 50 distributed edge nodes functioning simultaneously as wireless access points and security sensors, and 200 mobile IoT clients. To ensure fidelity in modeling sensor technology applications, the log-distance path loss model combined with Rayleigh fading was employed to capture the complex multi-path propagation

Algorithm 1
Server side — global aggregation.

```
Initialize global model parameters W_0
For each communication round t = 1 to T:
  For each edge node k in K (in parallel):
    W_local_k = W_t # Broadcast current global model
    g_tilde_k = LocalUpdate(k, W_local_k) # Call Algorithm 2

  # Secure Global Aggregation (FedAvg)
  W_t+1 = W_t - eta * Sum(omega_k * g_tilde_k for k in K)
Return W_T
```

Algorithm 2
Node side — local training and privacy.

```
Function LocalUpdate(k, W_local):
   # Step 1: Multi-Sensor Fusion & Feature Extraction
   S_k = [RSSI_k, Delay_k, Noise_k]
   xi_k = ||S_k - S_avg||^2 + epsilon
   RFI_k = -Integral(p(xi_k) * ln(p(xi_k)))

   # Step 2: Spatiotemporal Modeling
   h_t = LSTM(RFI_k, h_t-1)
   z_k = GNN(h_t, Neighbors_k)

   # Step 3: Local Optimization
   g_k = grad(Loss(W_local; z_k) + reg_term)

   # Step 4: Clipping-based Differential Privacy
   g_clipped = g_k / max(1, norm(g_k, 2) / Gamma)
   g_tilde = g_clipped + Noise(0, sigma^2 * Gamma^2 * I)

   Return g_tilde
```

Algorithm 3
Online detection (inference).

```
For each incoming signal at node k:
   # Use global model weights for inference
   P_spoof = Softmax(W_global * z_k + b)

   # Dynamic Threshold Tuning
   alpha = TuneThreshold(RFI_k)

   If P_spoof > alpha:
      Trigger "Wi-Fi Spoofing Alert"
```

effects that are typical of indoor and outdoor smart campus environments. The hardware and software specifications are summarized in Table 1, showing the computational and energy constraints of modern edge-enabled sensors. The system was equipped with the advanced reduced instruction set computer machine ARM Cortex-A72 processor with high-performance global aggregation, supported by the NVIDIA RTX 4090 graphics processing unit (GPU) (Fig. 1). This dual-layer design ensures that localized sensing remains lightweight while global model aggregation achieves scalability and robustness. The architecture shows how raw data captured at the sensor level is processed through the LSTM-GNN architecture. This design is critical for sensor technology because it offloads the computational burden of spatial-temporal modeling to the ARM-based edge nodes, ensuring that only model updates, rather than high-bandwidth raw sensor streams, are transmitted to the central server.

The effectiveness of the FL-MSF system in dense sensor networks was validated using high-frequency data in the NS-3 environment. Raw *RSSI* values and multipath delay spreads were sampled at 100 Hz, enabling the detection of micro-fluctuations often exploited in signal mimicry attacks.[22] At the end of each training epoch, *RFI* was computed using the behavioral entropy equation [Eq. (3)] to convert noisy telemetry into a stable statistical health metric, providing a reliable baseline for anomaly detection in dynamic radiofrequency environments.

Table 1
Hardware and software specifications used in simulation.

Parameter	Specification
Edge node processor	ARM Cortex-A72 (simulated performance)
Central server	NVIDIA RTX 4090 GPU (for global aggregation)
FL framework	PySyft / Flower
Neural architecture	LSTM (64 hidden units) + GNN (2 layers)
Optimizer	Adam (local), stochastic gradient descent (global server)
Learning rate	$\eta = 0.01$ (global), $\alpha = 0.001$ (local)

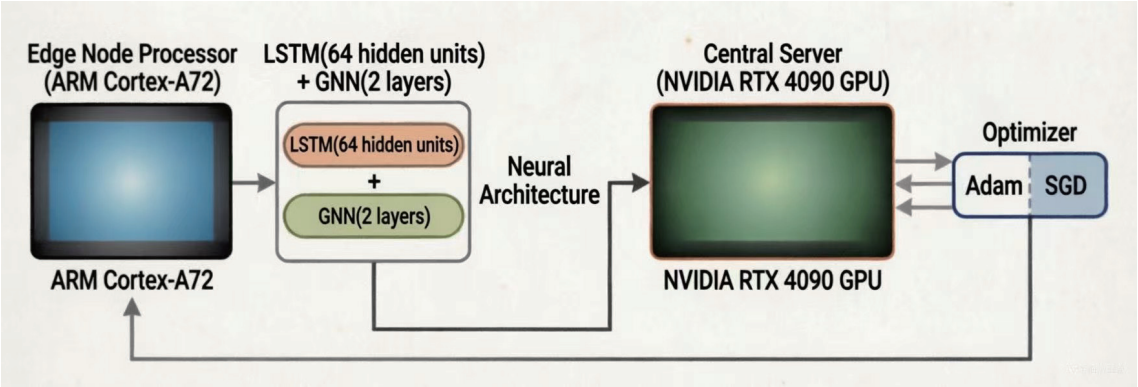

Fig. 1. (Color online) System architecture.

Detection performance was evaluated by comparing simulation results across LSTM, GNN, FedAvg, and FL-MSF networks. In the centralized baseline, all data were backhauled to a server, while siloed nodes trained GNN independently without neighbor communication. Accuracy, F1-score, and area under the curve (AUC) were calculated on a 20% test set. To assess classification capability, we used standard statistical metrics. The F1-score is used to determine a balance between precision (the proportion of flagged anomalies that were true attacks) and recall (the proportion of actual attacks correctly detected), making it reliable for unbalanced datasets where malicious events are rare. AUC is used to quantify the model's ability to discriminate between benign fluctuations and malicious attacks across all decision thresholds, with a value of 1.0 indicating perfect separation.

Detection latency was measured as the processing time from signal reception at the ARM-based edge node to final Softmax classification.[23] The dataset consisted of log traces collected across 150 multi-node tracking and transmission scenarios, capturing localized *RSSI* changes, multipath delay spreads, and background noise vectors under both benign and adversarial conditions. To prevent data leakage or overfitting, we applied a Pareto-principled 80/20 stratified random split. The 20% test partition ensured balanced representation of unseen anomalies and benign fluctuations across all sensor classes.[20,24] Accuracy, F1-score, and AUC were computed as evaluation metrics on this subset using standard true positives (*TP*), true negatives (*TN*), *FP*, and false negatives (*FN*).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{17}$$

$$F_1\text{-}Score = \frac{2 \cdot TP}{2 \cdot TP + FP + FN} \tag{18}$$

AUC was calculated by integrating the *TP* rate against the *FP* rate across the continuous decision threshold spectrum of the *RFI* anomaly score. Analytical results were obtained iteratively across the federated infrastructure. For each architectural variation or hyperparameter adjustment, localized edge models were trained on their respective 80% partitions, with the resulting weights transferred to the central server for aggregation. Performance was then evaluated exclusively against the isolated 20% test set, and the reported values reflect mean outcomes across multiple independent runs to ensure stability.

The results show that localized sensor fusion achieves accuracy comparable to, or exceeding, centralized architectures while meeting strict latency constraints. Membership inference attacks were simulated to quantify gradient leakage risk. By varying the noise multiplier σ and clipping threshold Γ [Eqs. (13) and (14)], we evaluated the trade-off between privacy and utility under differential privacy standards. Gaussian noise effectively masked individual sensor contributions while preserving global model convergence. Scalability was tested by expanding the NS-3 topology from 10 to 100 nodes. Convergence rounds were recorded when the global model reached 90% validation accuracy, and aggregation time was measured on the central GPU to quantify FedAvg overhead. These analyses confirm that FL-MSF maintains efficiency and robustness as network density increases, supporting large-scale decentralized sensor applications.

To evaluate performance in a realistic setting, we simulated a smart campus with high-density sensor deployment. Each edge node was modeled on commercial devices equipped with dual-band (2.4/5 GHz) omnidirectional antennas and integrated RF front-end transceivers, such as the Broadcom BCM43455. These sensors functioned as wireless environment monitors. Signals were captured at the physical layer, and incoming RF waves passed through a low-noise amplifier to a logarithmic power detector, which measured the analog voltage of the received envelope and converted it using an analog-to-digital converter into digital *RSSI* values in dBm. Multipath delay spreads (τ) were resolved from the preamble of physical layer convergence protocol data units, and background noise was measured during the clear channel assessment phase.[25]

The role of sensors and materials in the performance evaluation is vital. The wireless propagation channel acts as a distributed material sensor. Structural and dielectric materials within the campus, such as reinforced concrete, metallic frames, and low-emissivity glass, set the baseline attenuation, absorption, and scattering parameters of the radio spectrum.[26] By modeling these interactions, the system demonstrates how sensor networks can detect spoofing attacks and guides the design of new sensors that exploit material-dependent propagation features.

3. Results

The benign baseline was established through a 24-hour calibration phase to calculate the moving average for *RFI*. The system was tested against two sensor-level threats: signal mimicry (replicating *RSSI* profiles with temporal jitter) and media access control-Internet Protocol spoofing (generating spatial anomalies). The input feature vector represents the sensing capabilities of the network (Table 2). By leveraging multi-dimensional physical layer attributes, including *RSSI*, delay spreads, and background noise, the system demonstrates a sophisticated application of sensor technology, where traditionally noisy parameters are transformed into critical indicators for anomaly detection. This highlights the necessity of rethinking sensor data not as interference, but as actionable intelligence for security.

Table 3 shows the detection capabilities of baseline models. The FL-MSF system achieves a peak detection accuracy of 96.5%, outperforming LSTM (94.2%), GNN (88.5%), and FedAvg (92.8%). The FL-MSF system maintains a low detection latency of 31 ms, which is crucial for real-time sensor responses in dynamic environments. While GNN offers the lowest latency (24 ms), its reduced accuracy underscores the limitations of isolated sensor intelligence. These results confirm that collaborative, federated sensor fusion is essential for balancing speed and accuracy in next-generation sensor networks.

The relationship between sensor technology and privacy is further explored in Table 4. By implementing clipping-based differential privacy, the FL-MSF system shows the maximum data sovereignty, reducing gradient leakage risk to $< 0.5\%$. This is a prominent advancement for sensor applications in sensitive environments such as smart hospitals, industrial IoT, or private campuses, where raw telemetry exposure remains a primary barrier to adoption.[27] Compared with centralized architectures such as LSTM, which offer no sovereignty, and FedAvg without privacy (a 12.5% leakage risk), the FL-MSF system demonstrates that its privacy-preserving mechanism is seamlessly integrated into sensor networks without compromising detection accuracy. This mechanism is vital for the broader deployment of sensor technology in domains where confidentiality and compliance are paramount.

The ablation study results highlight the necessity of hybrid spatiotemporal modeling for sensor applications. The temporal-only model (LSTM) achieves high temporal accuracy but fails to capture spatial spoofing anomalies, whereas the spatial-only model (GNN) detects spatial consistency but misses subtle temporal jitters. The FL-MSF achieves an AUC of 0.97, proving that effective sensor data fusion accounts for both the time and the position of signal propagation (Table 5). The results demonstrate that resilience against advanced spoofing attacks requires multi-sensor data fusion rather than reliance on single-dimensional features.

The model accuracy improves from 91.20 to 96.30%, as sensor density increases from 10 to 100 nodes, while convergence rounds and aggregation time remain manageable (Table 6). This indicates that the FL-MSF system thrives in high-density environments, making it well-suited for large-scale sensor applications such as smart campuses, vehicular IoT, and the emerging Internet of Entities. The ability to maintain efficiency and accuracy under scaling pressures confirms that decentralized intelligence is not only feasible but advantageous for future sensor ecosystems.

Table 2
Input feature vector.

Signal strength	*RSSI*	*RSSI* (dBm)	100 Hz
Temporal feature	Delay	Multi-path propagation delay spreads (μs)	100 Hz
Environmental feature	Noise	Background noise floor measurements (dB)	10 Hz
Statistics	*RFI*(t)	Derived *RFI* (Entropy-based)	Per epoch

Table 3
Detection performance across different attack scenarios.

System	Detection accuracy (%)	*FP* rate (%)	F1-score	Detection latency (ms)
LSTM	94.2	3.1	0.92	145
GNN	88.5	5.4	0.86	24
Standard FedAvg	92.8	3.8	0.91	38
FL-MSF	96.5	1.9	0.95	31

Table 4
Comparisons of privacy and security metrics.

Metric	Centralized	FedAvg (no privacy)	FL-MSF
Data sovereignty	None (raw data)	High (gradients)	Maximum (clipped)
Attack resilience	Low	Medium	High (differential privacy)
Gradient leakage risk	Not applicable	12.50%	<0.5%
Communication overhead	High	Medium	Low (compressed)

Table 5
Spatial-temporal feature fusion results.

Architecture	Temporal accuracy	Spatial consistency	Overall AUC
LSTM	High	Low	0.88
GNN	Low	High	0.85
FL-MSF	High	High	0.97

Table 6
Scalability and convergence.

Number of nodes (K)	Number of convergence rounds	Aggregation time (s)	Model accuracy(%)
10 nodes	45	1.2	91.20
50 nodes	58	2.8	94.50
100 nodes	62	4.1	96.30

4. Discussion

The FL-MSF system redefines the utility of sensor data by demonstrating that noise floors and delay spreads, which are treated as interference, can serve as important features for anomaly detection. This reframing highlights the potential of sensor systems to extract meaningful security insights from parameters that were previously disregarded. The results of this study show the importance of privacy-compliant architectures. By integrating differential privacy into FL, the system addresses secure data sharing without compromising confidentiality. This is important in sensitive environments such as healthcare, industrial IoT, and smart campuses, where privacy concerns often hinder the adoption of advanced sensor networks. The ablation

results present the necessity of hybrid fusion approaches and show that multi-sensor data fusion is indispensable to ensure resilience, as temporal-only models fail to detect spatial spoofing and spatial-only models miss subtle temporal irregularities. The hybrid architecture sets a new benchmark for sensor applications in adversarial environments, proving that both temporal and spatial dimensions must be considered simultaneously to ensure robust detection.

The demonstrated scalability of the FL-MFS system provides a reference for deploying sensor networks in increasingly dense IoT ecosystems. As sensor density increases, system accuracy improves, ensuring sustainable performance as applications expand in the FL-MFS system. This scalability is crucial for the evolution of sensor technology in large-scale deployments such as smart cities, vehicular networks, and IoT. The FL-MSF system serves as a sustainable means for intelligent sensor networks by combining accuracy, privacy, and scalability. The introduction of *RFI* as a sensor health metric and its validation across diverse attack scenarios represent a foundational advancement in the field. Future applications in healthcare, transportation, and industrial IoT can build upon this architecture to achieve real-time, privacy-compliant defense mechanisms that are both robust and adaptive.

Despite the high peak detection accuracy and low latency achieved, several limitations must be acknowledged to provide a balanced perspective on the current state of this sensor-enabled architecture. While NS-3 simulations offer a high-fidelity representation of signal propagation, they cannot fully replicate the extreme stochasticity of real-world smart campuses. Dynamic structural changes, high-frequency human movement, and interference from non-IoT microwave sources can introduce noise beyond the parameters of the current *RFI* baseline. Moreover, the computational demands of maintaining the internal states of a 64-unit LSTM and a 2-layer GNN exceed the memory capacities of lower-power microcontrollers than those commonly deployed in sensor networks, creating a tiering problem that restricts federation participation to more powerful nodes.[28] Although clipping-based differential privacy reduced gradient leakage to <0.5%, strong noise multipliers degrade convergence and accuracy, potentially limiting detection sensitivity in highly sensitive environments. Finally, scalability challenges emerge when extending beyond 100 nodes, where synchronization delays and straggler effects hinder real-time defense, and FL remains vulnerable to model poisoning attacks without Byzantine-resilient aggregation methods.[29] Model poisoning is a form of adversarial attack in distributed or federated machine learning. Instead of attempting to steal data, the attacker manipulates the local training process by altering the local dataset or modifying the model parameters before uploading them. This causes the central aggregation to incorporate corrupted updates, leading the global model to learn faulty or malicious behavior.

To overcome these constraints, next-generation sensor technologies must be integrated to ensure hardware-intrinsic security and multi-sensor awareness. First, neural processing unit (NPU)-integrated edge sensors, such as ARM Ethos-U series, can provide hardware acceleration for matrix multiplications, enabling complex LSTM-GNN models to run efficiently even on low-power nodes, thereby democratizing participation in federated networks.[30] Second, multi-modal sensing: within the domain of wireless sensor technology and advanced signal processing, the integration of channel state information with millimeter-wave radar facilitates the construction of highly distinctive physical-layer fingerprints. This fusion significantly enhances

system resilience against mimicry attacks, as the resulting signatures are exceedingly difficult to reproduce or falsify.[31] Third, trusted execution environments (TEEs), such as ARM TrustZone or Intel Software Guard Extensions, can isolate local training within secure enclaves, reducing reliance on heavy differential privacy noise while maintaining confidentiality.[32] Finally, semantic communication and hierarchical aggregation allow sensors to transmit only critical knowledge updates to super-edge nodes, mitigating synchronization delays and ensuring scalability in dense IoT ecosystems.

Beyond immediate anomaly detection, the FL-MSF system contributes to the development of next-generation intelligent cognitive sensors and adaptive smart materials. Wireless sensors treat environmental multipath fluctuations and noise as parasitic interference to be suppressed at the hardware level. However, the FL-MSF system utilizes the localized behavioral entropy of *RFI*, which can be leveraged as a security asset. This guides the engineering of security-aware smart sensors integrated with reconfigurable intelligent surfaces or electromagnetic metastructures.[33,34] By embedding the FL-MSF algorithms directly onto the firmware of microcontroller units controlling these smart surfaces, sensors can dynamically adjust their surface impedance or dielectric phase shifts in real time.[35] This enables the material to purposefully modulate multi-path propagation delay spreads and signal signatures when a mimicry attack is suspected, effectively acting as an active hardware defense layer that shifts its physical properties to expose rogue transmitters.[34]

Sensor networks are transforming into hardware–software co-designed security tools. By addressing environmental noise, hardware constraints, privacy trade-offs, and scalability bottlenecks, the integration of NPUs, multi-modal sensing, TEEs, and semantic aggregation enables the deployment of zero-trust architectures in IoT.[36] This enables sensor technology to deliver real-time, privacy-compliant defense in increasingly complex and adversarial environments. FL has been widely applied to IoT security and anomaly detection. However, current frameworks remain limited in dynamic sensor networks. Advanced architectures rely on centralized deep learning models that demand continuous raw data transmission, creating severe communication bottlenecks. Others assume uniform, IID wireless channel characteristics across edge clients. In practice, spatial variation and structural materials invalidate these assumptions, producing high false-alarm rates and poor convergence under active signal-spoofing attacks.[25,26] The FL-MSF system developed in this study overcomes these limitations by integrating the following.

A lightweight entropy-driven physical-layer metric is employed to determine localized variance in multipath delay spreads and signal envelope changes. *RFI* enables edge transceivers to distinguish deliberate signal injection attacks from benign fluctuations at the firmware level, reducing reliance on computationally heavy classifiers. The adaptive fusion mechanism dynamically weights local edge parameters during server aggregation.[37,38] By incorporating baseline material attenuation profiles of individual sensor domains, non-IID distribution issues inherent to complex spatial layouts can be resolved. FL-MSF supports autonomous local execution. Once global parameters are downloaded, edge nodes perform real-time verification within sub-millisecond windows, minimizing data overhead and preventing systemic exploitation.

A critical environment where the FL-MSF system is most needed is the modern clinical or hospital facility. Deploying the framework to protect medical telemetry, patient monitoring devices, and localized tracking systems against Wi-Fi spoofing and signal mimicry introduces distinct operational challenges. Hospitals are tightly regulated spaces where electromagnetic interference is a major concern. Active *RFI* monitoring can disrupt ultrasensitive diagnostic equipment such as magnetic resonance imaging or cardiac monitors.[39] In addition, hospital interiors present difficult propagation conditions. Constant movement of metallic medical machinery, carts, and personnel, combined with heavy concrete shielding in radiology departments and lead-lined surgical suites, produces rapid, non-stationary multipath fading and dynamic path loss that can distort localized baseline signatures.[40]

To ensure effectiveness in clinical practice, several structural improvements are required. The firmware-level *RFI* must operate passively, relying solely on ambient communication traffic without emitting active probing signals that risk EMI violations.[41] The federated aggregation algorithm must also support priority-weighted asymmetric fusion: life-critical patient monitors should be protected with zero-tolerance thresholds, while noncritical assets such as smart lighting or temperature sensors can tolerate broader anomaly boundaries. Integrating these adaptive, class-priority mechanisms into the FL-MSF system enables high-reliability, low-latency defense within sensitive healthcare infrastructures.[42]

5. Conclusions

We developed a decentralized, privacy-preserving framework for detecting Wi-Fi spoofing and signal mimicry in smart campus sensor networks. By changing anomaly detection from centralized servers to collaborative edge nodes, the proposed FL-MSF system alleviates communication overhead and mitigates privacy risks, sustaining high detection accuracy. The LSTM–GNN hybrid architecture effectively fuses temporal and spatial features, and the integration of clipping-based differential privacy within the FedAvg protocol ensures resilience against membership inference and gradient leakage attacks. FL-MSF achieves 96.5% detection accuracy, an F1-score of 0.95, and an AUC of 0.97, with a low detection latency of 31 ms. Compared with baseline models, FL-MSF outperforms LSTM (94.2% accuracy, 145 ms latency), GNN (88.5% accuracy, 24 ms latency), and standard FedAvg (92.8% accuracy, 38 ms latency). Privacy analysis shows gradient leakage risk reduced to <0.5%, compared with 12.5% under FedAvg without privacy. Scalability tests confirm improved accuracy from 91.2% at 10 nodes to 96.3% at 100 nodes, with manageable convergence rounds and aggregation time.

Despite these advancements, limitations remain. NS-3 simulations cannot fully capture real-world stochasticity, resource-constrained nodes may struggle with LSTM–GNN complexity, and FL remains vulnerable to model poisoning and synchronization delays beyond 100 nodes. Future work should explore hardware acceleration using NPUs, integration of multi-modal sensing, TEEs, and asynchronous aggregation to enhance resilience and scalability. The FL-MSF system offers a sustainable pathway for secure, adaptive, and privacy-compliant sensor networks, offering a robust defense paradigm for large-scale IoT ecosystems such as smart campuses, healthcare facilities, and industrial infrastructures.

Acknowledgments

This research was supported by the High-Level Talent Research Start-up Funding Program of Xiamen Ocean Vocational College (Project No.: KYG202537).

References

1 C. Herglotz, I. Jabłoński, R. Karnapke, K. Shahin, and M. Reichenbach: IEEE Access **13** (2025) 172306. https://doi.org/10.1109/ACCESS.2025.3615205
2 J. Wang, M. T. Quasim, and B. Yi: Inf. Fusion. **120** (2025) 103084. https://doi.org/10.1016/j.inffus.2025.103084
3 S. A. Diwan: Int. J. Decis. Support Syst. Technol. **19** (2025) 4310. https://doi.org/10.1177/18724981251370441
4 K. Chen and L. Xiao: Discov. Appl. Sci. **7** (2025) 1025. https://doi.org/10.1007/s42452-025-07626-6
5 G. Wang, J. Yang, Y. Wei, C. Wang, K. Li, and C. Feng: IEEE Internet Things J. **12** (2025) 22647. https://doi.org/10.1109/JIOT.2025.3556840
6 A. Al-Rasheed, R. Khan, T. Alsaed, M. Kundi, M. H. M. Saad, and M. R. Sarker: CMC-Comput. Mater. Contin. **80** (2024) 1305. https://doi.org/10.32604/cmc.2024.049215
7 M. Al-Hawawreh and M. S. Hossain: Inf. Fusion **99** (2023) 101889. https://doi.org/10.1016/j.inffus.2023.101889
8 J. Wu, J. Zhang, M. Bilal, F. Han, N. Victor, and X. Xu: IEEE Trans. Consum. Electron. **70** (2024) 2628. https://doi.org/10.1109/TCE.2023.3325138
9 N. Ashwini, S. Dava, A. Rakesh Phanindra, G. Ranjith Kumar, K. Varada Rajkumar, and N. Sravanthi: Sci. Rep. **16** (2026) 1398. https://doi.org/10.1038/s41598-025-31164-1
10 J. Aljabri: Sci. Rep. **15** (2025) 14255. https://doi.org/10.1038/s41598-025-98180-z
11 X. Nie, L. Yi, L. T. Yang, X. Deng, F. Fan, and H. Zhang: IEEE Trans. Consum. Electron. **71** (2025) 6570. https://doi.org/10.1109/TCE.2024.3470243
12 J. Song, U. S. Musa, Y. Chen, P. Pene, Y. Guo, and W. Yu: Proc. IEEE 22nd Int. Conf. Mobile Ad-Hoc and Smart Systems (MASS,2025) 10. https://doi.org/10.1109/MASS66014.2025.00016
13 J. Chen, J. He, F. Chen, Z. Lv, J. Tang, and Y. Jia: IEEE Internet Things J. **12** (2025) 6095. https://doi.org/10.1109/JIOT.2024.3518615
14 W. Wang, X. Chang, and Y. Chen: Discov. Internet Things (2026). https://doi.org/10.1007/s43926-026-00299-6
15 M. Fu, P. Wang, M. Liu, Z. Zhang, and X. Zhou: IEEE Trans. Veh. Technol. **74** (2025) 1909. https://doi.org/10.1109/TVT.2024.3402366
16 J. Fischer, M. Orescanin, J. Loomis, and P. McClure: IEEE Access **12** (2024) 185790. https://doi.org/10.1109/ACCESS.2024.3513253
17 Y. Yu, L. Jianping, and D. Weiwei: Proc. 19th Int. Computer Conf. Wavelet Active Media Technology and Information Processing (ICCWAMTIP, 2022) 1. https://doi.org/10.1109/ICCWAMTIP56608.2022.10016548
18 S. Bethu and S. Babu Erukala: IEEE Internet Things J. **13** (2026) 6905. https://doi.org/10.1109/JIOT.2025.3640433
19 S. Hochreiter and J. Schmidhuber: Neural Comput. **9** (1997) 1735. https://doi.org/10.1162/neco.1997.9.8.1735
20 L. Matlala, T. Bokaba, P. Ndayizigamiye, S. Mhlongo, and E. Dogo: J. Manag. Anal. **13** (2026) 109. https://doi.org/10.1080/23270012.2025.2574030
21 G. F. Riley and T. R. Henderson: The ns-3 Network Simulator, in Modeling and Tools for Network Simulation, K. Wehrle, M. Güneş, and J. Gross, Eds. (Springer, Heidelberg, 2010) Chap. 2. https://doi.org/10.1007/978-3-642-12331-3_2
22 D. Huang and A. Al-Hourani: EEE Trans. Mach. Learn. Commun. Netw. **2** (2024) 841. https://doi.org/10.1109/TMLCN.2024.3417806
23 M. J. C. S. Reis: Sensors **25** (2025) 6629. https://doi.org/10.3390/s25216629
24 T. Anthony, A. K. Mishra, W. Stassen, and J. Son: Healthcare **9** (2021) 1107. https://doi.org/10.3390/healthcare9091107
25 L. Alhoraibi, D. Alghazzawi, R. Alhebshi, and O. B. J. Rabie: Sensors **23** (2023) 1814. https://doi.org/10.3390/s23041814
26 A. Choroszucho, T. Szczegielniak, and D. Kusiak: Energies **17** (2024) 5934. https://doi.org/10.3390/en17235934
27 A. Wakili and S. Bakkali: Cyber. Secur. Appl. **3** (2025) 100084. https://doi.org/10.1016/j.csa.2025.100084
28 D. Ngo, H.-C. Park, and B. Kang: Electronics **14** (2025) 2495. https://doi.org/10.3390/electronics14122495
29 A.N. Bhagoji, S. Chakraborty, P. Mittal, and S. Calo: PMLR **97** (2019) 634. https://proceedings.mlr.press/v97/bhagoji19a.html.

30 H. Kayan, R. Heartfield, O. Rana, P. Burnap, and C. Perera: IEEE Internet of Things J. **12** (2025) 29696. https://doi.org/10.1109/JIOT.2025.3569780
31 I. Guarino, D. Carra, M. Cominelli, F. Gringoli, and R. Lo Cigno: Comput. Commun. **249** (2026) 108431. https://doi.org/10.1016/j.comcom.2026.108431
32 Q. Xia, W. Ye, Z. Tao, J. Wu, and Q. Li: High-Confid. Comput. **1** (2021) 10008. https://doi.org/10.1016/j.hcc.2021.100008
33 J. Kibilda, N. H. Mahmood, A. Gomes, M. Latva-aho, and L. A. DaSilva: arXiv:2212.05101 (2022). https://doi.org/10.48550/arxiv.2212.05101
34 Y. Li, F. Khan, M. Ahmed, A. A. Soofi, W. U. Khan, C. K. Sheemar, and L. A. DaSilva: IEEE Internet Things J. **12** (2025) 32444. https://doi.org/10.1109/JIOT.2025.3567553
35 F. Chiti, A. Degl'Innocenti, and L. Pierucci: Sensors **23** (2023) 2726. https://doi.org/10.3390/s23052726
36 C. Pham-Quoc: Proc. Euro-Par 2024 Parallel Processing Workshops, Madrid, Spain (Springer, 2024) 215. https://doi.org/10.1007/978-3-642-12331-3_2
37 L. A. Olawoyin, Y. O. Imam-Fulani, M. O. Oloyede, and A. A. Oloyede: FUOYE J. Eng. Technol. **11** (2026) 65. https://doi.org/10.4314/fuoyejet.v11i1.12
38 A. Zulueta-Doalto, E. Zulueta, M. Zulueta-Perez, and J. M. Lopez-Guede: Neurocomputing **700** (2026) 134398. https://doi.org/10.1016/j.neucom.2026.134398
39 C. Hwata, O. Gatera, N. Ritsch, T. Uwiragiye, G. Rushingabigwi, C. Twizere, D. Mukalinyigira, B. Thomas, and D. Nsengiyera: Medicine **103** (2024) e41179. https://doi.org/10.1097/MD.0000000000041179
40 A. Giannakoulas, N. Karkanis, I. Gavriilidis, and T. N. F. Kaifas: Electronics **15** (2026) 925. https://doi.org/10.3390/electronics15050925
41 H. Zhu, C.-T. Lam, B. K. Ng, and E. Monteiro: J. King Saud Univ. Comput. Inf. Sci. **38** (2026) 246. https://doi.org/10.1007/s44443-026-00644-3
42 M. Sreelakshmi and R. Delhibabu: Front. Digit. Health **8** (2026) 1879670. https://doi.org/10.3389/fdgth.2026.1879670

About the Authors

Xinying Lin received her master's degree from Nanyang Technological University, Singapore, in 2017. Since 2019, she has been a laboratory technician at Xiamen Ocean Vocational College. Her research interests include AI, computer technology application, and IoT. (linxinying@xmoc.edu.cn)

Zhengji Mao received his B.S. and Ph.D. degrees from National Taiwan University, Taiwan, in 1986 and 1990, respectively. From 2004 to 2009, he worked as a professor at Taiwan Capital University. Since 2024, he has served as a professor at Xiamen Ocean Vocational College. His research interests lie in AI, mechatronics, and marine sensors. (maozhengji@xmoc.edu.cn)