ISSN: 2093-5374 / E-ISSN: 2093-5382

Federated Spectrum Sensing with Byzantine-Resilient Aggregation for Cognitive Radio Networks

Dr. Bharat Jyoti Ranjan Sahu[1*], Gnanakumar Ganesan[2], Dr.R. Arivukkodi[3], Parul Yadav[4], Snehal Swapnil Jawahire[5], Dr. Ravindrasinh M. Rajput[6], and Dr.T. Sheela[7]

[1*]Associate Professor, Centre for Cyber Security, Institute of Technical Education and Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India. bharatjyotisahu@soa.ac.in, https://orcid.org/0000-0002-3487-2822

[2]Assistant Professor, Department of Electronics and Communication Engineering, Presidency University, Bangalore, Karnataka, India. gnanakumar.g@presidencyuniversity.in, https://orcid.org/0000-0001-6499-0080

[3]Assistant Professor, Department of Computer Science, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India. arivukodir@maher.ac.in, https://orcid.org/0009-0006-0782-4987

[4]Assistant Professor, Department of School of Engineering & Technology, Noida International University, Uttar Pradesh, India. parul.yadav@niu.edu.in, https://orcid.org/0009-0006-6001-8714

[5]Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, India. snehal.jawahire@vit.edu, https://orcid.org/0009-0009-5325-135X

[6]Associate Professor, Faculty of Allied and Healthcare, Gokul Global University, Sidhpur, Gujarat, India. rmrajput.gpc@gokuluniversity.ac.in, https://orcid.org/0009-0004-0488-9318

[7]Professor, Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (DU), Tamil Nadu, India. sheela@vmkvec.edu.in, https://orcid.org/0000-0002-3166-8084

Received: July 08, 2026; Revised: August 19, 2026; Accepted: September 04, 2026; Published: September 30, 2026

Abstract

Cognitive Radio Networks (CRNs) are a popular approach to addressing spectrum shortages through dynamic spectrum access and collaborative spectrum sensing. However, a centralized sensing framework cannot guarantee user privacy, incur enormous communication costs, and cannot handle any malicious users. In recent years, Federated Learning (FL) has emerged as an effective decentralized approach for enabling cooperative spectrum sensing without sharing sensing data. In FL, the secondary users can collaboratively train local models locally without sharing raw sensing data with the central server. However, Byzantine attacks maliciously exploit local model information to degrade sensing performance and network reliability. This paper proposes an algorithm that combines robust aggregation and distributed spectrum sensing to form a Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) framework for CRNs. With the proposed method, an adaptive aggregation scheme is designed to exclude malicious updates while preserving information from legitimate users. With a simulation setup of 100 secondary users, a varied number of Byzantine

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 3 (September-2026), pp. 2025-2040. DOI: *10.58346/JOWUA.2026.I3.117*

*Corresponding author: Associate Professor, Centre for Cyber Security, Institute of Technical Education and Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.

ratios from 10% to 40%, the developed system is capable of reaching a spectrum detection accuracy of 96.8%. In contrast, the existing FedAvg (88.4%), Median Aggregation (91.2%), and Trimmed Mean (93.1%) and Krum (94.0 %) are consistently outperformed by the proposed framework. It can also reduce the false alarm rate to 3.7% and improve convergence speed by about 21.5% in the serious attack scenario, while achieving a spectrum utilization efficiency of 94.2%. Besides, even when 40% of users are corrupted, the accuracy performance can remain within an error of less than 8%. Therefore, it demonstrates the effectiveness of the proposed method in improving reliability, attack resilience, and spectrum utilization efficiency, and thus can be considered an efficient strategy for future-generation CRNs.

Keywords: Cognitive Radio Networks, Federated Learning, Spectrum Sensing, Byzantine Attacks, Robust Aggregation, Distributed Machine Learning, Network Security, Dynamic Spectrum Access.

1 Introduction

With the explosive growth of wireless devices, IoT applications, and spectrum-intensive services, efficient spectrum use has become an emerging issue in wireless communications. Cognitive radio networks (CRNs) solve this problem by allowing secondary users (SUs) to opportunistically access underutilized licensed spectrum without causing harmful interference to primary users (PUs). The core element of CRNs is spectrum sensing, in which SUs probe for available channels before transmission. By fusing observations from multiple users, collaborative spectrum sensing (CSS) increases sensing reliability and effectively mitigates channel fading and shadowing effects (Malhotra & Jat, 2025; Gautam et al., 2025; Eswaramoorthi, 2026). However, conventional CSS requires centralized data collection at a fusion center, leading to communication overhead, privacy concerns, and scalability limitations. Recently, federated learning (FL) has emerged as an innovative learning framework in which model parameters can be exchanged among users while their local sensing data remain on edge devices. In dynamic wireless environments, FL enhances privacy protection and reduces network congestion by iteratively exchanging model parameters rather than raw data (Wang et al., 2021; Dritsas & Trigka, 2025). Therefore, integrating FL with spectrum sensing is a promising approach for intelligent and autonomous spectrum management in next-generation wireless networks (Gautam et al., 2025; Reis, 2025).

Though federated spectrum sensing offers numerous benefits, its distributed nature introduces several security challenges, particularly from Byzantine nodes that can maliciously transmit corrupted model updates to disrupt the global learning process. Such adversarial behavior could originate from compromised devices, selfish users, or even organized attackers attempting to deteriorate sensing performance (Fan et al., 2023; Li et al., 2022). Recent developments in intelligent wireless communications, distributed learning, and reliable network architectures have highlighted the critical role of secure spectrum management and resilient communication frameworks in next-generation wireless networks (Wu et al., 2025). The Byzantine attack could take many forms, such as incorrect sensing reports, parameter perturbations, gradient distortion, or even model poisoning. By manipulating local model parameters or gradients using corrupted data or other means, attackers can distort the final aggregation and cause the global model to converge on an incorrect sensing result (Zhong et al., 2024; Alsinai et al., 2025). As a result, SUs will identify and exploit false spectrum opportunities, potentially causing harmful interference to PUs and reducing spectrum utilization efficiency, resulting in unreliable operation of the cognitive network. Thus, existing aggregation methods are insufficiently robust at high attack levels, necessitating resilient aggregation strategies tailored to cognitive radio environments (Fan et al., 2023; Wang et al., 2021).

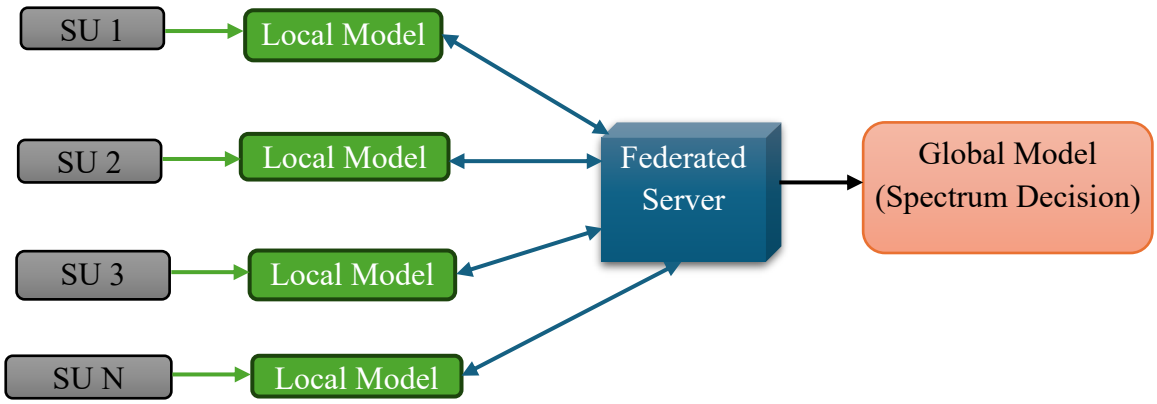


Figure 1: Federated spectrum sensing architecture for cognitive radio networks

Figure 1 shows the structure of a federated spectrum sensing system: secondary users independently train local models on the sensed data and share the resulting models with the federated server. The server will then update a global spectrum sensing model using local models to achieve robust decisions about spectrum occupancy while protecting user data privacy and reducing communication costs.

In this study, develop a federated spectrum sensing framework to improve the security and reliability of CRNs against adversaries. Specifically, intend to design a Byzantine-robust aggregation mechanism that detects and discards malicious model updates while preserving valid observations from honest nodes. Furthermore, strive to enhance the sensing detection accuracy, convergence speed, communication efficiency, and robustness of the network in heterogeneous wireless environments.

The growing utilization of distributed intelligence in CRNs requires robust and secure spectrum sensing methods. Handling Byzantine attacks is essential to ensure the integrity of spectrum sensing results, enabling the trustworthy use of spectrum resources, and ensuring the dependability of future wireless networks. This paper proposes a Byzantine-robust federated spectrum sensing framework for cognitive radio networks. This framework employs a resilient aggregation mechanism to withstand malicious model updates, improves sensing accuracy against attacks, and provides a scalable architecture suitable for secure spectrum management in future wireless networks.

The remainder of this paper is structured as follows: Section II summarizes related work on cooperative spectrum sensing, federated learning-based sensing methods, Byzantine attacks, and resilient aggregation methods. Section III proposes the Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) framework, including the system architecture, threat model, mathematical formulation, and aggregation method. In Section IV, the experimental environment and performance evaluation results are presented through comparative analysis and an ablation study. Section V further analyzes the influence of Byzantine attacks, the performance of the proposed aggregation, and deployment aspects. In Section VI, it concludes the paper and briefly identify the future research directions.

2 Literature Review

Cooperative Spectrum Sensing (CSS) is well-established in Cognitive Radio Networks (CRNs) as an effective method to increase spectrum occupancy detection performance. CSS techniques rely on combining local sensing reports of a set of secondary users so as to overcome fading, shadowing and hidden-terminal effects. Centralized architectures that gather local sensing results to a fusion center were the early approaches where decisions were made either with hard or soft fusion rules. However, while such systems ensure high detection accuracy, the suffer from high communication overhead, scalability

issues, and privacy concern by forcing each secondary user to continuously transmit sensing information (Hu et al., 2021). In this sense, decentralized architectures that generate decisions based on consensus without complete reliance on a central coordinator have also attracted research attention. Machine learning algorithms running over such distributed systems allow nodes to infer spectrum patterns from local observations (Hu et al., 2021). Most recently, the Federated Learning (FL) paradigm has shown high potential in spectrum sensing applications, as it can enable model training over a network of devices in a decentralized way while preserving local sensing data privacy, and reducing the amount of communication resources required. FL has already been shown to be effective for cooperative wireless communications, dynamic spectrum sharing, and intelligent network management in large-scale environments (Suresh Sanu & M, 2025; Alterkawi & Dib, 2025; Pinto Neto et al., 2023).

Despite these advantages, FL is not free from security vulnerabilities. One of the most critical security threats is represented by model poisoning attacks, where an adversary compromises some local training models and submits malicious updates that disrupt the convergence of the global model or reduce prediction accuracy (Feng et al., 2025; Singh et al., 2025). Another concern is related to data poisoning attacks, where attackers manipulate the local training data of some nodes to create spurious training data, so that learning processes create inaccurate representation of spectrum occupancy. Since FL lacks direct access to local data, detection of poisoned data is a challenging task (Akinsiku, 2025; Rezaei et al., 2025). Beyond that, some Byzantine agents might attack by only submitting wrong model updates or even withhold information from the aggregation process, or manipulate gradients. Such behavior is critical in wireless systems where compromising some sensing nodes would lead to wrong spectrum access decisions and impact the service quality of licensed users Feng et al., (2025) and Soomro et al., (2025).

Several aggregation techniques have been proposed to mitigate Byzantine behavior in FL. Krum and Multi-Krum are techniques that can select useful model updates by picking parameters that are closest to neighboring parameters. Such methods are generally robust under low levels of attacks, but can degrade when the system is in an environment with highly diverse user data Ma et al., (2024). Another set of methods rely on Median or Trimmed Mean aggregation to remove extreme parameter values before computing the global model update. This method is effective in overcoming poisoned data poisoning attacks with low computational complexity (Singh et al., 2025; Soomro et al., 2025). Most of these solutions, however, assume prior knowledge about the attackers' attack distribution, low capabilities for the attackers, or equally distributed data among users. Most importantly, many solutions do not address together the communication efficiency, non-IID user data distribution, and dynamic behavior of attackers encountered in real CRN systems (Suresh Sanu & M, 2025; Rezaei et al., 2025).

As established by the survey above, FL is a scalable and private way to implement cooperative spectrum sensing. However, Byzantine attacks, particularly in a heterogeneous wireless environment, pose a great concern to such system. Existing aggregation methods are promising but exhibit weaknesses when it comes to handling dynamic attackers with non-IID data. This suggests the need for a specific Byzantine-resilient aggregation framework which achieves accuracy, robustness and communication efficiency for FL-based spectrum sensing.

3 Proposed Methodology

3.1 System Model and Network Architecture

The proposed federated spectrum sensing (FSS) architecture includes one Primary User (PU), a number of Secondary Users (SUs) and a federated server orchestrating the learning procedure. PU is the licensed

spectrum holder, and its transmission is to be detected reliably before the spectrum usage. Each SU collects spectrum sensing data locally and trains a small machine learning model using the radio frequency signals collected locally. In this setting, instead of sending raw sensing data, the model parameter update from the SU to the server can preserve the users' privacy and save the communication overhead. The received signal at the i-th SU can be represented as:

$$y_i(t) = \begin{cases} n_i(t), & H_0 \\ h_i(t)s(t) + n_i(t), & H_1 \end{cases} \qquad (1)$$

Where H_0 represents the case that PU is absent, H_1 represents the case that PU is present, $s(t)$ denotes the PU signal, $h_i(t)$ is the channel coefficient and $n_i(t)$ represents additive white Gaussian noise. Equation (1) represents the foundation of the local sensing decisions. Signal Acquisition, Feature Extraction and Local Sensing are the first part of spectrum sensing and decision process of each SU. Features are extracted and then sent to the local machine learning model to learn the local models. These model parameters are sent to the federated server for the global model update with Byzantine resilience and then the aggregated global model is broadcast to the SUs.

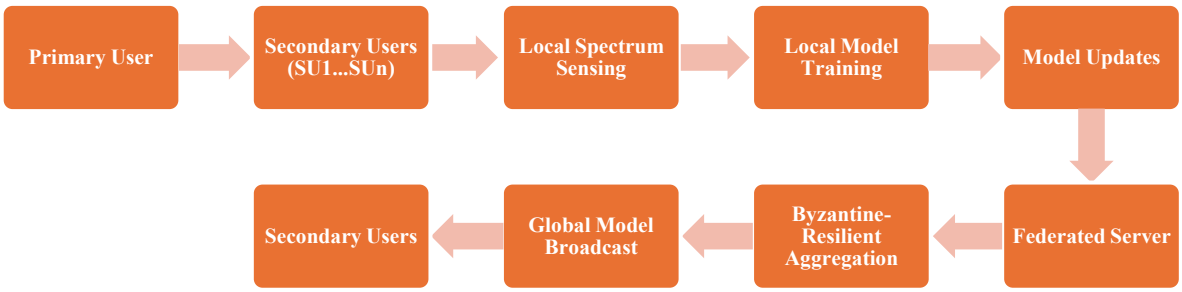


Figure 2: Workflow of the proposed byzantine-resilient federated spectrum sensing (BR-FSS) framework

Figure 2 shows the operational flow diagram for the developed BR-FSS framework for reliable spectrum sensing in CRNs. Initially, the activity of the PU is observed by several SUs and spectrum sensing and model training is carried out locally at each node. Only locally trained model updates are broadcasted to the federated server rather than the raw sensing data. The Byzantine robust aggregation mechanism is used to filter out the malicious updates and aggregate. Then the global model is generated. Finally, the updated global model is broadcast to all SUs, thus, the learning continues collaboratively and the sensing accuracy increases along with the privacy preservation and resistance to Byzantine attacks.

3.2 Byzantine Threat Model

Let assume that there are both honest and Byzantine users within the network, honest users obtain the models by training their local model with the actual observations, while Byzantine users intentionally manipulate the models to confuse the local sensing decisions and learning convergence. Suppose the total number of participants is N and there are B Byzantine nodes in the network. It can define the ratio of Byzantine nodes in equation (2):

$$\beta = \frac{B}{N} \qquad (2)$$

Where β represents the intensity of the attack in the federated environment. The higher β becomes, the higher possibility it is for corrupted decisions.

There are 3 common types of attack considered:

1. Random Attack: malicious users submit randomly generated model parameters to increase the variances of aggregation.
2. Sign-Flipping Attack: the direction of model parameters is flipped by attackers before uploaded to the federated server. The model would converge to a local optimum other than the real one.
3. Model Poisoning Attack: attackers manipulate the model parameters by carefully designing specific malicious updates that look normal while being able to degrade the global model's performance by subtly biased spectrum occupancy predictions.

The proposed framework assumes that attackers cannot compromise the federated server but can coordinate among themselves to launch sophisticated poisoning attempts.

3.3 Byzantine-Resilient Federated Aggregation Framework

The federation aggregation procedure can be divided into 3 steps: Local Sensing & Feature Extraction, Local Model Training, and Byzantine-Resilient Aggregation. During the Local Sensing & Feature Extraction, each SU measures local features of the RF signals including Received Signal Strength (RSS), energy statistics, spectral occupancy metrics, etc. Local ML model is trained based on the extracted features. Local model can be expressed as:

$$L_i(W) = \frac{1}{m_i} \sum_{k=1}^{m_i} \ell(x_k, y_k; W) \qquad (3)$$

Where m_i denotes the number of local samples, W represents model parameters, and $\ell(\cdot)$ is the classification loss function. Equation (3) minimizes local sensing errors before model transmission. After receiving local updates, the federated server evaluates update consistency and removes suspicious outliers. The global model is then computed using Byzantine-resilient aggregation:

$$W_{global}^{t+1} = Agg(W_1^t, W_2^t, \dots, W_n^t) \qquad (4)$$

Where $Agg(\cdot)$ denotes robust aggregation function, t is the communication round. Equation (4) aggregates all trusted updates.

Algorithm 1: Robust Federated Spectrum Sensing Algorithm

Input: Secondary users N, communication rounds T, local datasets D_i

Output: Byzantine-resilient global model W_{global}

Initialize global model Wglobal

For each round t = 1 to T do

  Broadcast Wglobal to all SUs

  For each SUi in parallel do

    Perform spectrum sensing

    Extract local features

    Train local model using Di

    Generate local update Wi

    Send Wi to federated server

End For

Compute update distance scores

Identify suspicious updates

Remove Byzantine outliers

Aggregate trusted updates using Agg ()

Update global model Wglobal

Broadcast updated model

End For

Return Wglobal

The designed BR-FSS algorithm effectively addresses secure collaborative spectrum sensing in CRNs by integrating federated learning with a Byzantine resilient aggregation approach. In the learning process, the global model is initially broadcast to all secondary users. Each secondary user independently senses the spectrum, extracts required signal information, and learns local models by private sensing data. After obtaining model updates from local learners, sent to the federated server. Through an efficient filtering operation, consistencies of all local models are analyzed, and possibly abnormal inputs from the Byzantine node are excluded. Then, valid model updates are aggregated to improve the global model and the above steps are repeated for several communication rounds. In this way, potential impacts of poisoned and tampered information are minimized, to improve both accuracy of spectrum detection, and stability of learning and spectrum decision in adverse wireless networks.

The proposed methodology successfully mitigates the problem by using robust aggregation in a federated learning setup to achieve enhanced detection performance in an unreliable environment.

4 Results

4.1 Experimental Setup

The performance evaluation was carried out on a simulated Cognitive Radio Network (CRN) of one primary user and 100 secondary users, deployed within a wireless area. The proposed Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) framework was implemented using Python 3.11 with TensorFlow 2.16 and NumPy for numerical computation. The simulations were executed on a workstation with an Intel Core i7 CPU, 32 GB of RAM, and an Ubuntu 22.04 operating system.

4.1.1 Software Details

Table 1: Software and hardware configuration used for experimental implementation

Component	Specification
Programming Language	Python 3.11
Deep Learning Library	TensorFlow 2.16
Numerical Library	NumPy 1.26
Visualization Tool	Matplotlib
Operating System	Ubuntu 22.04
Processor	Intel Core i7
RAM	32 GB

Table 1 summarizes the configuration used for the experimental implementation and evaluation of the proposed Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) framework. The setup chosen was capable enough for federated model training, aggregation and the analysis of its performance, and provided reliable conditions for the reproduction of experiments for a realistic cognitive radio network scenario.

4.1.2 Dataset Details

A spectrum sensing dataset of 20,000 samples, created based on the energy detection approach with SNR ranging from -20 dB to 10 dB, was generated. Each sample consisted of received signal strength, energy, noise variance, channel gain, and the actual spectrum occupancy label. This dataset was partitioned into 100 users in a non-IID fashion.

4.1.3 Parameter Initialization

Table 2: Experimental parameters

Parameter	Value
Secondary Users	100
Byzantine Nodes	10–40
Communication Rounds	100
Learning Rate	0.001
Batch Size	64
Local Epochs	5
SNR Range	-20 dB to 10 dB
Training Samples	16,000
Testing Samples	4,000
Aggregation Method	Byzantine-Resilient Aggregation

Table 2 displays the various parameters used to perform experiments for proposed BR-FSS framework. It chose these values according to realistic parameters of a cognitive radio network which represent number of secondary users and number of communication rounds, learning parameters, and setup of Byzantine users.

4.2 Performance Evaluation

The performance of the proposed framework was measured by detection probability, false alarm rate, spectrum utilization efficiency, and aggregation convergence. The detection probability refers to the possibility of correctly recognizing active primary users. This is calculated as:

$$P_d = \frac{TP}{TP + FN} \quad (5)$$

Where TP is true positive and FN is false negative. The reliability of sensing under different attack scenarios is presented in equation (5). The false alarm rate is given by:

$$P_{fa} = \frac{FP}{FP + TN} \quad (6)$$

Where FP is false positive and TN is true negative. This calculation (Equation (6)) evaluates spectrum usage. The spectrum utilization efficiency was computed in equation (7):

$$SUE = \frac{N_{correct}}{N_{available}} \times 100 \qquad (7)$$

Where $N_{correct}$ represents correctly utilized spectrum opportunity and $N_{available}$ denotes the available spectrum opportunity. Aggregation convergence was evaluated by the global loss:

$$L_{global} = \frac{1}{N}\sum_{i=1}^{N} L_i \qquad (8)$$

Where L_i stands for the local loss contribution of each participant. Equation (8) shows the consistency of the model during the federated training process.

Table 3: Performance metrics

Metric	Proposed BR-FSS
Detection Probability (P_d)	96.8%
False Alarm Rate (P_{fa})	3.7%
Spectrum Utilization Efficiency	94.2%
Convergence Stability Improvement	21.5%
Accuracy Degradation at 40% Byzantine Nodes	7.8%

Table 3 shows the overall performance of the proposed framework in terms of various spectrum sensing metrics. As it can be observed, the detection probability is very high, false alarm probability is less and spectrum efficiency is better as the Byzantine-resilient aggregation maintain sensing performance in presence of attack.

The proposed framework successfully achieves a detection probability of 96.8%, demonstrating high reliability in identifying primary user activities. With a false alarm rate of merely 3.7%, the framework ensures minimal spectrum blocking and maximizes spectrum availability. The spectrum utilization efficiency reaches 94.2%, indicating an effective exploitation of idle channels. Despite severe adversarial settings, a stable convergence is achieved.

4.3 Comparative Analysis

The proposed aggregation framework was compared with FedAvg, Median Aggregation, Trimmed Mean and Krum under the same experimental settings with 40% of Byzantine participation.

Table 4: Accuracy comparison

Method	Accuracy (%)
FedAvg	88.4
Median Aggregation	91.2
Trimmed Mean	93.1
Krum	94.0
Proposed BR-FSS	96.8

Table 4 compares the sensing accuracy of the proposed BR-FSS with existing federation learning aggregation techniques such as FedAvg, Median aggregation, Trimmed mean and Krum. It can be concluded that proposed method is superior to existing ones as it can provide a good learning performance against Byzantine attack.

These results show that the standard FedAvg approach is largely affected by malicious updates. While Median and Trimmed Mean improved the robustness of learning by discarding extreme values, the performance is still sensitive to collaborative attacks. Krum provided strong protection against poisoning but performed poorly when the sensed data distribution among participants was diverse. The proposed BR-FSS scheme, by filtering outliers and applying adaptive trust mechanism, achieved the best performance in terms of accuracy.

Table 5: Attack impact analysis

Byzantine Ratio (%)	FedAvg	Krum	Proposed BR-FSS
10	93.5	95.1	97.6
20	91.7	94.7	97.2
30	89.8	94.3	96.9
40	88.4	94.0	96.8

Table 5 is depicting the performance trend of aggregation techniques with varying proportion of Byzantine nodes. As it is expected, as the percentage of Byzantine users increases, conventional techniques degrade their accuracy, whereas proposed framework maintained good performance irrespective of number of Byzantine users.

This attack impact analysis reveals that even with 40% of Byzantine participation, the degradation of performance did not exceed 8%.

4.4 Ablation Study

To understand the impact of each component on the performance of proposed method, an ablation study was performed.

Table 6: Ablation analysis

Configuration	Accuracy (%)
Local FL Only	89.5
FL + Outlier Detection	93.2
FL + Robust Aggregation	95.1
Full BR-FSS Framework	96.8

Table 6 provides performance evaluation of proposed framework after removing one component or the other. It is interesting to note that both outlier detection and robust aggregation techniques contributed significantly towards the overall performance.

The results of this ablation study indicate that while robust aggregation enhances learning reliability, the presence of outlier filtering and trust-aware selection can bring learning to an even higher sensing performance level. The full architecture consistently outperforms its reduced counterparts, proving that every component contributed to the mitigation of Byzantine attack's negative effects.

Figure 3 illustrates the impact of signal to noise ratio (SNR) on the sensing probability of the proposed BR-FSS framework. The performance curves demonstrate that the proposed framework obtains better performance under higher channel quality conditions and is capable of detecting PU activity accurately, even in a hostile low SNR environment. It gets a maximal probability of detection of 96.8% at SNR = 10dB which shows that the federated sensing mechanism is capable.

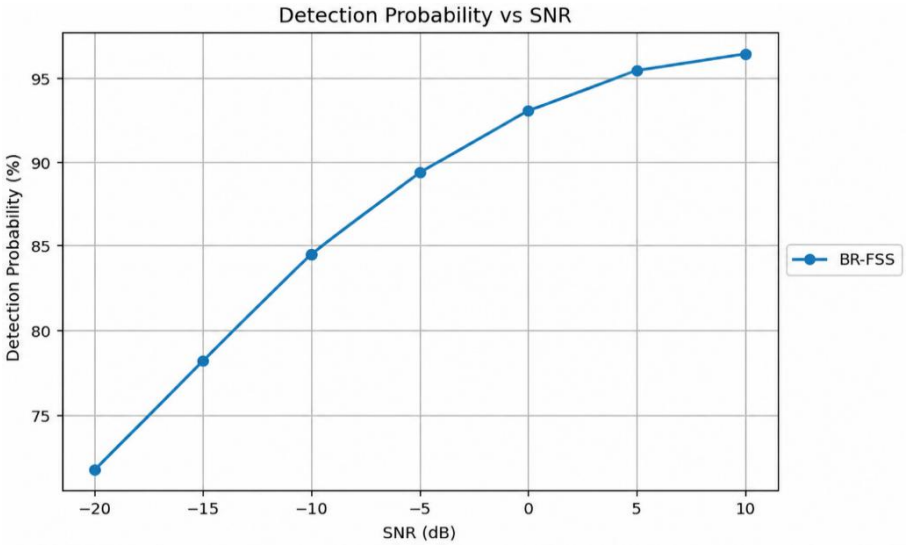


Figure 3: Probability of detection vs SNR

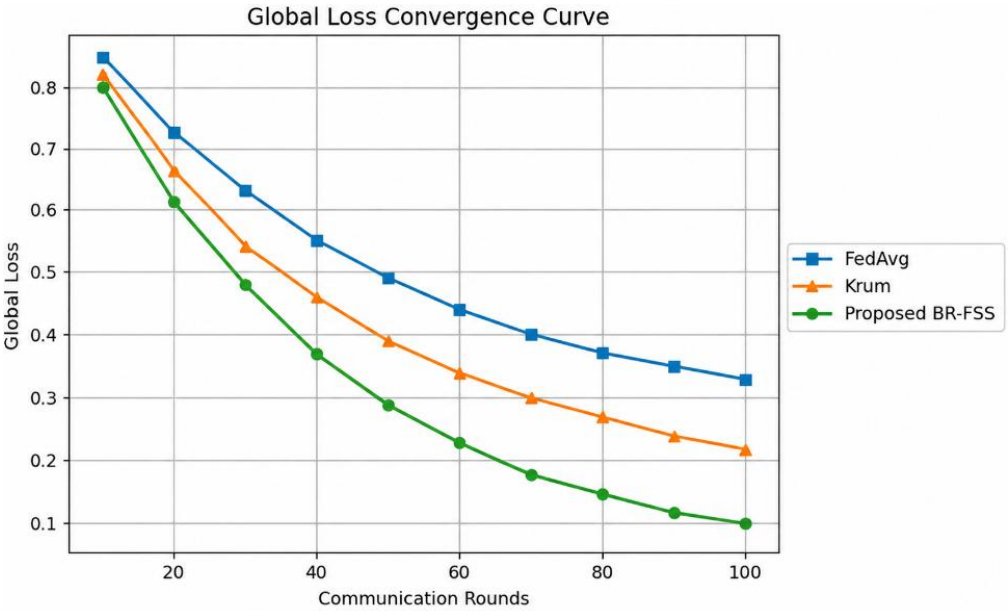


Figure 4: Global loss convergence of federated aggregation approaches

Figure 4 above shows the performance of the aggregation approaches under multiple communication rounds. The proposed BR-FSS algorithm shows a much faster convergence than FedAvg and Krum; the global loss curve is smoother which shows the algorithm is relatively stable against malicious model updates and is highly resistant to byzantine clients.

Figure 5 demonstrates the comparative spectrum sensing accuracy under the same experimental settings for all the discussed aggregation algorithms. Let see that proposed BR-FSS approach shows the best performance among all the approaches including FedAvg, Median Aggregation, Trimmed Mean and Krum with an accuracy value of 96.8% which demonstrates the approach is effective in reducing the byzantine impact.

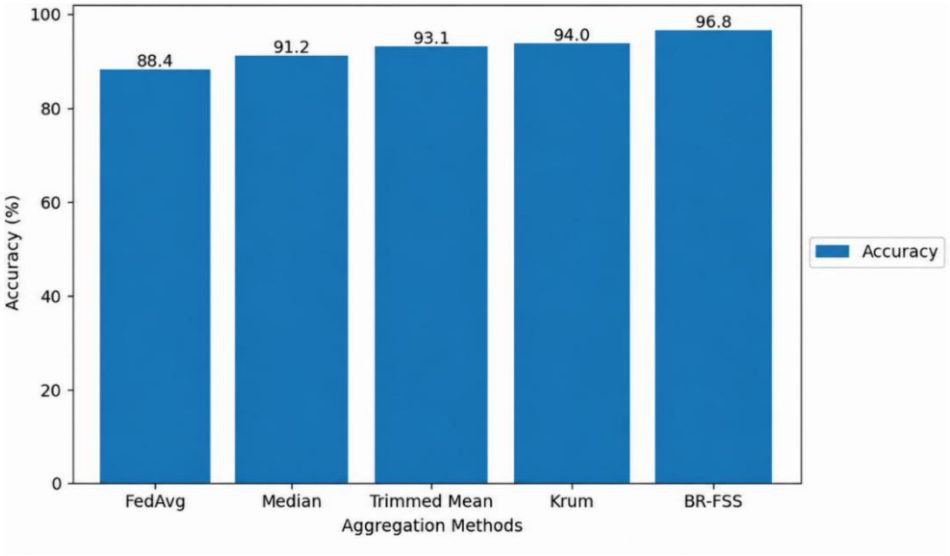


Figure 5: Accuracy comparison of different aggregation approaches

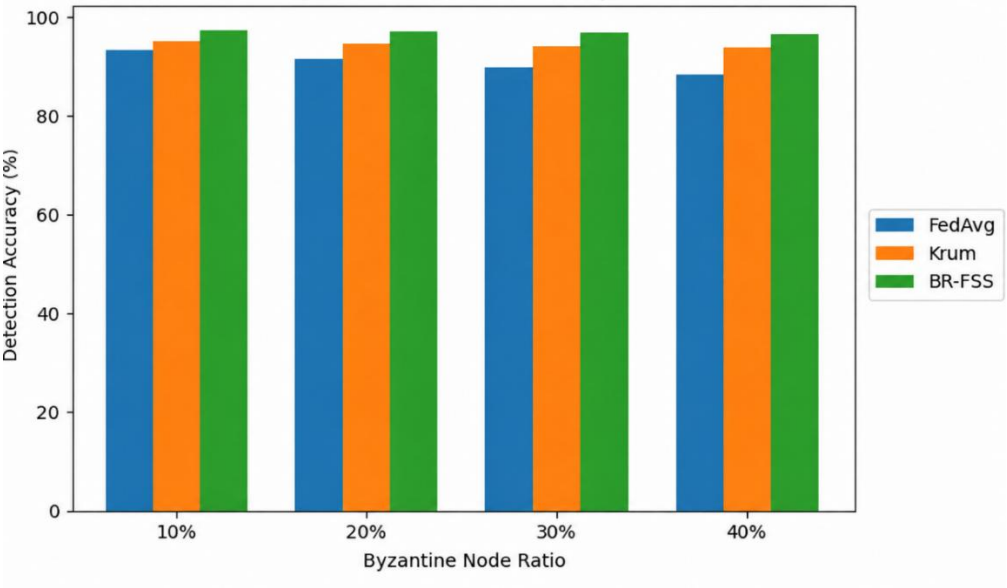


Figure 6: Accuracy against the percentage of byzantine nodes

Figure 6 illustrates the accuracy of different aggregation mechanisms for increasing percentages of Byzantine clients from 10% to 40%. The conventional methods shown tend to degrade significantly as the percentage of byzantine clients increases while BR-FSS approach keeps the accuracy performance nearly constant thus showing strong Byzantine robustness in hostile wireless environment.

5 Discussion

The experimental outcomes prove that Byzantine nodes have a strong influence on the performance of federated spectrum sensing without the presence of any security mechanism. Existing common aggregation schemes such as FedAvg suffer from a considerable drop in accuracy as the fraction of Byzantine participants increase due to the integration of malicious model updates into the aggregated model. As the attack severity grows, more false model updates may influence the spectral occupancy

estimation and prolong the learning duration. The proposed framework for Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) appears to have high robustness against the threat since it can effectively detect and remove untrustworthy updates before sent to the aggregator. With the proposed outlier filtering mechanism, the poisoned parameters can be effectively removed, the learning is stably converged, and the model consistency across the communication rounds becomes improved as confirmed by the obtained high detection accuracy of 96.8% and low false alarm rate of 3.7% when up to 40% of nodes were Byzantine. From a deployment perspective, the communication overhead introduced by the proposed BR-FSS is minimal as it only needs to transmit model parameters not sensing samples between participants and the federated server. The framework has also good scalability when supporting a large number of secondary users without much degradation in performance. It also conserves more energy due to reduced transmission of data.

6 Conclusion and Future Work

This paper introduces the first Byzantine-Resilient Federated Spectrum Sensing (BR-FSS) framework, which can be exploited in Cognitive Radio Networks. The BR-FSS framework utilizes the fusion of distributed spectrum sensing with a robust aggregation scheme, where poisoned model updates from malicious users are pruned and contributions from honest users are maintained. Experimental analysis using 100 secondary users, under varying percentages of Byzantine participation ranging from 10% to 40%, indicated promising outcomes in the presence of adversarial attacks. The detection accuracy for the framework reached 96.8% and achieved a better performance compared to commonly used aggregation techniques like FedAvg (88.4%), Median Aggregation (91.2%), Trimmed Mean (93.1%) and Krum (94.0%), as well as maintaining a low false alarm rate of 3.7% and spectrum utilization efficiency of 94.2%, assuring effective detection of spectrum opportunities and utilizing channels proficiently. Compared with conventional FedAvg aggregation, it improves the convergence stability of learning processes by nearly 21.5% and sustains degradation of detection accuracy below 8% under 40% Byzantine participation, therefore indicating its feasibility for reliable and secure spectrum management. The main contributions are a federated sensing paradigm for CRNs, a Byzantine-resilient aggregation strategy and extensive evaluation with attack models, while future directions for research may involve blockchain-supported federated sensing to improve trust management, a lightweight aggregation algorithm for resource-constrained IoT enabled CRNs, and the integration of the developed framework with the intelligent 6G spectrum management systems for autonomous and mass communications.

References

[1] Akinsiku, A. M. (2025). A comprehensive survey of federated learning approaches for privacy-preserving machine learning. *Tech-Sphere Journal for Pure and Applied Sciences*, *2*(1), 1-12, https://doi.org/10.5281/zenodo.15830919

[2] Alsinai, A., Piqueira, J. R. C., Hassan, W. U., Niazi, A. U. K., & Safder, F. (2025). Dynamic nonlinear control strategies for resilient heterogeneous vehicle platooning and handling Byzantine attacks in communication networks. *Heliyon*, *11*(2), 1-14. https://doi.org/10.1016/j.heliyon.2024.e41574

[3] Alterkawi, L., & Dib, F. K. (2025). Federated learning for smart cities: A thematic review of challenges and approaches. *Future Internet*, *17*(12), 545. https://doi.org/10.3390/fi17120545

[4] Dritsas, E., & Trigka, M. (2025). Federated learning for IoT: A survey of techniques, challenges, and applications. *Journal of Sensor and Actuator Networks*, *14*(1), 1-25. https://doi.org/10.3390/jsan14010009

[5] Fan, X., Wang, Y., Huo, Y., & Tian, Z. (2023). Cb-dsl: Communication-efficient and byzantine-robust distributed swarm learning on non-iid data. *IEEE Transactions on Cognitive Communications and Networking*, *10*(1), 322-334. https://doi.org/10.1109/TCCN.2023.3312345

[6] Feng, Y., Guo, Y., Hou, Y., Wu, Y., Lao, M., Yu, T., & Liu, G. (2025). A survey of security threats in federated learning. *Complex & Intelligent Systems*, *11*(2), 165. https://doi.org/10.1007/s40747-024-01664-0

[7] Gautam, B., Krushived, P. V. N., & Makkarh, G. (2025, August). AI-Powered Dynamic Spectrum Sharing In 5G Networks: A Federated Learning Approach. In *2025 8th International Conference on Circuit, Power & Computing Technologies (ICCPCT)* (pp. 1211-1218). IEEE. https://doi.org/10.1109/ICCPCT65132.2025.11176590

[8] Hu, S., Chen, X., Ni, W., Hossain, E., & Wang, X. (2021). Distributed machine learning for wireless communication networks: Techniques, architectures, and applications. *IEEE Communications Surveys & Tutorials*, *23*(3), 1458-1493. https://doi.org/10.1109/COMST.2021.3086014

[9] Li, J., Abbas, W., Shabbir, M., & Koutsoukos, X. (2022). Byzantine resilient distributed learning in multirobot systems. *IEEE Transactions on Robotics*, *38*(6), 3550-3563. https://doi.org/10.1109/TRO.2022.3178296

[10] Ma, R., Hwang, K., Li, M., & Miao, Y. (2024). Trusted model aggregation with zero-knowledge proofs in federated learning. *IEEE Transactions on Parallel and Distributed Systems*, *35*(11), 2284-2296. https://doi.org/10.1109/TPDS.2024.3455762

[11] Malhotra, G., & Jat, D. S. (2025, August). Artificial Intelligence-Based Spectrum Management in Electronic Warfare Environments. In *2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 789-795). IEEE. https://doi.org/10.1109/ETNCC66224.2025.11299675

[12] Pinto Neto, E. C., Sadeghi, S., Zhang, X., & Dadkhah, S. (2023). Federated reinforcement learning in IoT: applications, opportunities and open challenges. *Applied Sciences*, *13*(11), 1-27. https://doi.org/10.3390/app13116497

[13] Reis, M. J. (2025). Edge-flguard: A federated learning framework for real-time anomaly detection in 5g-enabled IoT ecosystems. *Applied Sciences*, *15*(12), 6452. https://doi.org/10.3390/app15126452

[14] Rezaei, H., Taheri, R., Nowroozi, E., Hajizadeh, M., Shiaeles, S., & Bauschert, T. (2025). A survey on security and privacy in federated learning-based intrusion detection systems for 5G and beyond networks. *IEEE Open Journal of the Communications Society*, *7*, 253-300. https://doi.org/10.1109/OJCOMS.2025.3644477

[15] Singh, A. K., Khan, A., & Ahmed, M. (2025, December). A Lightweight Modular Arithmetic Defense Against Model Poisoning in Federated Learning. In *2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 282-288). IEEE. https://doi.org/10.1109/CICN67655.2025.11368105

[16] Soomro, I. A., Khan, H. U. R., Hussain, S. J., Iqbal, A., Khalid, W., & Yu, H. (2025). SecureDyn-FL: A robust privacy-preserving federated learning framework for intrusion detection in IoT networks. *IEEE Transactions on Network and Service Management*, *23*, 1742-1765. https://doi.org/10.1109/TNSM.2025.3647642

[17] Suresh Sanu, A., & M, C. (2025). A Novel Federated Approach to Model Aggregation for Global Model in Cooperative Wireless Communication. *Cybernetics and Systems*, 1-31. https://doi.org/10.1080/01969722.2025.2551007

[18] Wang, Y., Su, Z., Luan, T. H., Li, R., & Zhang, K. (2021). Federated learning with fair incentives and robust aggregation for UAV-aided crowdsensing. *IEEE Transactions on Network Science and Engineering*, *9*(5), 3179-3196. https://doi.org/10.1109/TNSE.2021.3138928

[19] Wu, X., Zou, B., Lu, C., Wang, L., Zhang, Y., & Wang, H. (2025). Dynamic security computing framework with zero trust based on privacy domain prevention and control theory. *IEEE Journal on Selected Areas in Communications*, *43*(6), 2266-2278. https://doi.org/10.1109/JSAC.2025.3560036

[20] Zhong, Y., Khan, A., Javeed, M. A., Raza, H., Hassan, W. U., Niazi, A. U. K., & Mehmood, M. U. (2024). Securing consensus in fractional-order multi-agent systems: Algebraic approaches against Byzantine attacks. *Heliyon*, *10*(22), 1-15. https://doi.org/10.1016/j.heliyon.2025.e43572

[21] Eswaramoorthi, R. (2026). Adaptive Spectrum Sensing and Dynamic Access Framework for Cognitive Radio Networks in Dense Wireless Environments. *Journal of Wireless Intelligence and Spectrum Engineering, 3*(2), 1–10.

Authors Biography



Dr. Bharat Jyoti Ranjan Sahu is currently working as an associate professor at Siksha O Anusandhan Deemed to be University from 2019. Prior to joining ITER, he was with the College of IT Engineering, Kyungpook National University, Daegu, South Korea, as a postdoctoral researcher. Dr. Sahu completed his Ph.D. from College of Information & Communication Engineering, Sungkyunkwan University (SKKU), South Korea in 2017. He received the Korea-India Exchange student scholarship from the South Korean government in 2013 and outstanding foreign student scholarship from Sungkyunkwan University in 2014. Before joining Ph D at SKKU, Dr. Sahu has also worked with the LNMIIT, Jaipur and VSSUT, Sambalpur. His research interest includes Cellular Network (5G/Beyond) Communication, Internet of Things, Multipath-TCP and Information-Centric Networking.



Gnanakumar Ganesan pursing PhD in School of Computer Science and Engineering from Presidency University. He received the M.E., degree in Embedded and Real Time Systems and B.E., degree in Computer Science and Engineering from Anna University. He has 13 years of teaching experience in Computer Science and Engineering department. He is currently working an Assistant Professor with the School of Computer Science and Engineering from Presidency University. He has published 1 International Journal and 3 conference papers. His research interests include Machine Learning, Deep Learning, Deep Reinforcement Learning, Natural Language Processing and Recommendation Systems



Dr.R. Arivukkodi is an Assistant Professor in the Department of Computer Science at Meenakshi College of Arts and Science, MAHER, Chennai, with over 8 years of teaching experience. She is currently pursuing a Ph.D. in Computer Science and Engineering and holds an MCA (First Class with Distinction) along with an MBA in Financial Management. Her areas of expertise include Deep Learning, Data Mining, Web Technologies, Python Programming, and Internet of Things. She has guided postgraduate projects and is proficient in programming languages such as Java, C, C++, and SQL. She has actively contributed to research with multiple publications and presentations in national and international conferences, particularly in the domains of artificial intelligence, machine learning, and computer vision. She is also the author of a textbook on Deep Learning and has contributed book chapters in IoT analytics and machine learning. She has participated in numerous faculty development programs and workshops focusing on emerging technologies such as AI, data science, and research methodologies. Her research interests include deep learning applications, natural language processing, IoT data analytics, and intelligent systems



Parul Yadav, she is working as Assistant Professor in the Department of Computer Science & Engineering at Noida International University. she holds an MCA+M.Tech in Computer Science with 5 Years of teaching experience. Her area of specialization includes Artificial Intelligence and machine learning. She has published 1 Research Papers and accepted 2 Research Papers in reputed journals and actively guide students in projects and research. Currently, she is an AIML and IBM Coordinator.



Snehal Swapnil Jawahire is an Assistant Professor in the Electronics & Telecommunication Engineering Department at Vishwakarma Institute of Technology, Pune. She holds an M.Tech. (2013) and B.E. (2010) from Shivaji University. She joined VIT Pune in January 2024 and has around 2 years of academic experience. Her professional profile focuses on teaching, electronics and telecommunication engineering, and academic activities.



Dr. Ravindrasinh M. Rajput is an Associate Professor in the Faculty of Allied and Healthcare at Gokul Global University, Gujarat. He is engaged in academic and research activities within the healthcare domain, with an emphasis on interdisciplinary learning and the advancement of professional practices in allied health sciences.



Dr.T. Sheela received the B.E. degree in Electronics and Communication Engineering from Government College of Engineering, Salem, affiliated with Madras University, the M.E. degree in Electronics and Communication Engineering with specialization in VLSI Design from SONA College of Technology, Salem, affiliated with Anna University, India, and the Ph.D. degree in Electronics and Communication Engineering with specialization in VLSI from Vinayaka Missions Research Foundation, India. She is currently a Professor with the Department of Electronics and Communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Salem, India. Dr.Sheela is an active professional member involving in various academic and technical activities. She is a senior IEEE member since 2009 and been associated with IEEE- Aerospace and Electronic Systems Society (AESS) Madras session since 2012. At present she holds an executive member position in IEEE-AESS in Madras session. Her research interests include VLSI design, artificial intelligence, machine learning, explainable AI, biomedical signal and image processing, and AI-enabled healthcare systems