IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14611

Federated Trust-Aware Spectrum Sensing For Cognitive Radio Enabled Internet Of Vehicles In 6G Networks

P. Sreesudha[1], Sameera Begum[2]

[1]Assistant Professor, Department of Electronics and Telematics Engineering,

G. Narayanamma Institute of Technology and Science, Shaikpet, Hyderabad[1]

[2]M.Tech Student, Department of Electronics and Telematics Engineering,

G. Narayanamma Institute of Technology and Science, Shaikpet, Hyderabad[2]

Abstract The rapid evolution of sixth-generation (6G) wireless networks has accelerated the development of intelligent communications systems capable of supporting ultra-reliable, low-latency applications.Cognitive Radio-Enabled Internet of Vehicles (CR-IoV) has emerged as a promising solution for efficient spectrum utilization in highly dynamic automotive environment. However, conventional centralized spectrum sensing techniques suffer from high communication overhead, privacy issues, and scalability limitations when deployed in large-scale vehicular networks. To address these challenges, this paper proposes a Federated Trust-Aware Spectrum Sensing framework for CR-IoV networks operating in 6G environments. The proposed approach integrates Federated Learning (FL) with a trust evaluation mechanism to enable decentralized model training while preserving user privacy and improving detection reliabilit. Convolutional Neural Networks (CNN) are used for local spectrum occupancy detection, while support vector machines (SVM) are used for intelligent road unit (RSU) selection and resource allocation. Trust-based aggregation is integrated to mitigate the impact of untrusted and malicious nodes during the global model updating process. MATLAB simulations are performed under different signal-to-noise ratio (SNR) conditions to evaluate the performance of the proposed framework. Simulation results demonstrate significant improvements in detection probability, detection accuracy, throughput, and spectrum utilization compared to centralized and conventional federated learning approaches. The proposed framework provides a scalable, secure and efficient solution for future 6G-enabled intelligent vehicle communication systems.

Keywords: Cognitive Radio, Internet of Vehicles, Federated Learning, Trust Management, Spectrum Sensing, Convolutional Neural Network, Support Vector Machine, 6G Networks.

I. INTRODUCTION

The rapid growth of connected vehicles, autonomous transportation systems and intelligent mobility services has significantly increased the demand for reliable wireless communication networks. Future sixth-generation (6G) communications systems are expected to deliver ultra-low latency, massive connectivity, high data rates, and intelligent resource management to support emerging automotive applications. The Internet of Vehicles (IoV) has become one of the most important components of intelligent transportation infrastructure, enabling seamless communication between vehicles, road units, pedestrians and cloud platforms.

Despite significant advances in wireless communications technologies, spectrum scarcity remains a major challenge due to the ever-increasing number of connected devices. Cognitive Radio (CR) technology provides an effective solution by allowing secondary users to opportunistically access underutilized licensed spectrum bands without causing harmful interference to primary users. Through dynamic spectrum sensing and intelligent spectrum allocation, Cognitive Radio improves spectrum utilization and communication efficiency.

Traditional spectrum sensing techniques, including energy sensing and feature-based sensing methods, often suffer from poor sensing performance in highly dynamic vehicular environments due to channel fading, mobility-induced interference, and noise uncertainty. Recently, machine learning and deep learning approaches have been introduced to improve detection accuracy and spectrum occupancy prediction.. In particular, Convolutional Neural Networks (CNNs) have demonstrated excellent ability to learn spectrum features directly from received signal samples.

Most existing machine learning-based spectrum sensing frameworks rely on centralized training approaches in which sensing data from multiple vehicles is transmitted to a central server. Although these methods provide high

DOI: 10.17148/IJIREEICE.2026.14611

detection accuracy, they introduce significant communication overhead, privacy concerns, and scalability issues. Federated Learning (FL) has recently emerged as a decentralized learning paradigm that enables training of collaborative models without sharing raw sensing data. Vehicles can train local models using their own sensing information and exchange only model parameters with a central aggregator.

However, federated learning systems remain vulnerable to untrusted or malicious participants who can download inaccurate model updates and negatively affect the overall learning process.Therefore, trust-aware mechanisms are needed to evaluate the reliability of participating vehicles and improve the robustness of aggregation. Motivated by these challenges, this paper proposes a Federated trust-based spectrum sensing framework for radio-enabled Cognitive Internet of Vehicles operating in 6G environments. The proposed framework integrates CNN-based local spectrum sensing, trust-based federated aggregation, and SVM-based intelligent RSU allocation to improve the reliability, scalability, and security of sensing.

The main contributions of this work are summarized as follows:

- Development of a decentralized federated learning framework for spectral sensing in CR-IoV networks:
- Integration of a trust evaluation mechanism to identify reliable detection participants.
- CNN-based local spectrum occupancy detection under various SNR condition.
- Intelligent management of communications and RSU allocation assisted by SVM.
- Performance evaluation using MATLAB simulations in dynamic vehicle environments.

II. LITERATURE REVIEW

The application of machine learning and artificial intelligence techniques for spectrum sensing in Cognitive Radio (CR) networks has received considerable attention in recent years. Traditional spectrum sensing approaches such as energy sensing, matched filtering, and cyclostationary feature detection suffer from reduced sensing performance in low signal-to-noise ratio (SNR) environments and in highly dynamic vehicle scenarios [7], [8]. Therefore, intelligent learning-based approaches have been explored to improve spectrum utilization and detection reliability.

Ahmed et coll. al. proposed a Hybrid machine learning-based spectrum sensing and allocation framework with congestion-aware adaptive modeling in CR-assisted Internet of Vehicles (IoV) networks [1]. The study demonstrated that the combination of supervised and unsupervised learning techniques improves the accuracy of spectrum detection and the efficiency of dynamic spectrum allocation under various traffic conditions.However, the framework relies on a centralized learning architecture, which incurs communication overhead and scalability limitations.

Chen et al. introduced a cooperative spectrum sensing mechanism based on Federated learning for cognitive radio systems [2].Their approach enabled distributed spectrum sensing without sharing raw sensing data among participating users, thereby improving privacy preservation and reducing communication overhead. The results showed improved detection accuracy compared to traditional cooperative detection methods.

Vinita and Vetriselvi proposed SEAFL, a privacy-enhanced federated learning architecture for 6G-enabled vehicular networks [3].Their work demonstrated that decentralized learning can significantly improve privacy while maintaining high model performance.However, the confidence assessment of participating vehicles was not taken into account during model aggregation.

Sirohi et coll. al. presented a comprehensive survey on Federated Learning for 6G-enabled secure communication systems [4]. The authors highlighted the potential of federated learning to support intelligent, privacy-preserving communication architectures, while identifying security threats caused by untrustworthy and malicious participants.

Usha and Prashanth proposed DRLNet, a deep reinforcement learning based framework for hybrid feature extraction and spectrum sensing in cognitive radio networks [5]. Their results showed improved detection performance and adaptability under various channel conditions. However, the framework primarily focused on individual learning rather than distributed collaborative learning.

DOI: 10.17148/IJIREEICE.2026.14611

Ezhilarasi et al. studied blockchain-based machine learning and attack mitigation techniques for cognitive radio networks [6]. The study demonstrated the importance of secure and reliable detection mechanisms to defend against malicious users who attempt to manipulate detection decisions.Recent advances in federated learning have further highlighted its applicability in distributed wireless communication systems, particularly for privacy-preserving spectrum sensing and intelligent resource allocation [9]. Similarly, deep learning-based detection approaches have shown significant improvements in detection accuracy under low SNR conditions compared to conventional detection techniques [16], [17].

Although significant progress has been made in spectral sensing based on machine learning and federated learning, most existing studies address either decentralized learning or trust management independently. Limited research has investigated the integration of Federated Learning, Trust assessment, CNN-based spectrum sensing, and intelligent RSU allocation into cognitive radio-enabled Internet of Vehicles operating in future 6G environments [4], [11], [15].

Evaluation, CNN-based Spectrum Sensing, and Intelligent RSU Allocation within Cognitive Radio-enabled Internet of Vehicles operating in future 6G environments [4], [11], [15]. Motivated by these limitations, the proposed work introduces a reliable Federated spectrum sensing framework that combines CNN-based local sensing, trust-weighted federated aggregation, and SVM-assisted RSU allocation to improve reliability, scalability, security, and spectrum utilization in CR-IoV networks.

III. SYSTEM MODEL

The proposed Cognitive Radio Internet of Vehicles (CR-IoV) framework consists of primary user vehicles (PU), secondary user vehicles (SU), roadside units (RSU), and a hybrid learning spectrum agent (HLSA) operating in a 6G communication environment. The goal of the framework is to improve spectrum sensing reliability, spectrum usage efficiency, and communications security while preserving user privacy through federated learning.

Primary Users represent approved spectrum owners who have priority access rights to specific frequency bands. Secondary User vehicles opportunistically access these spectrum bands whenever they are detected to be inactive. To avoid harmful interference to authorized users, accurate and reliable spectral sensing is necessary before channel access decisions are made.

The considered network consists of several SU vehicles moving under dynamic vehicle conditions.Each vehicle continuously monitors the radio environment and collects local detection samples on nearby channels. Due to mobility, channel fading, shadowing effects, and varying Signal-to-Noise Ratio (SNR) conditions, sensing decisions obtained by individual vehicles may contain uncertainties. Therefore, cooperative detection mechanisms are needed to improve detection reliability.

Each SU vehicle is equipped with a spectrum detection module based on a Convolutional Neural Network (CNN).. . The CNN receives locally detected signal samples and performs spectrum occupancy classification. The output of the CNN indicates whether the observed spectral channel is occupied by a primary user or available for opportunistic access.

Let x(n) represent the signal sample received on the vehicle SU.

$$H_0 : x(n) = w(n) \quad (1)$$

$$H_1 : x(n) = s(n) + w(n) \quad (2)$$

where:

- H_0 represents the absence of a Primary User signal.
- H_1 represents the presence of a Primary User signal.
- s(n) denotes the transmitted PU signal.
- w(n) represents Additive White Gaussian Noise (AWGN).

The locally trained CNN extracts spectral features from the received signal samples and generates a detection decision based on the learned signal features. To preserve privacy and reduce communication overhead, the proposed

DOI: 10.17148/IJIREEICE.2026.14611

framework uses federated learning (FL). Instead of transmitting raw sensing data, each vehicle SU trains the CNN model locally and only shares the model parameters with the nearest roadside unit (RSU).

RSUs serve as intermediate aggregation entities and pass model updates to the Hybrid Learning Spectrum Agent (HLSA).The HLSA performs global model aggregation and generates an updated spectrum detection model. Since malicious or untrustworthy vehicles can submit incorrect updates, a trust mechanism is built into the aggregation process. Each participating vehicle is assigned a trust score based on historical detection performance, update consistency, reporting reliability, and participation behavior.

The trust score of the i-th vehicle is calculated as:

$$T_i = \alpha A_i + \beta C_i + \gamma R_i + \delta E_i \quad (3)$$

where:

• A_i represents detection accuracy.

• C_i represents sensing consistency.

• R_i represents reporting reliability.

• E_i represents energy efficiency.

• α, β, γ and δ are weighting coefficients.

The confidence score is between 0 and 1.Vehicles with higher trust scores contribute more significantly during federated aggregation, while malicious or untrustworthy participants are assigned lower weights. After trust-based aggregation, the global detection model is redistributed to all participating vehicles for subsequent training cycles. This iterative learning process continues until model convergence is achieved.

Additionally, a support vector machine (SVM)-based RSU allocation module is deployed at HLSA. SVM uses channel quality indicators such as SNR, congestion level, confidence score, and channel availability status to determine The most appropriate RSU for each vehicle.

The proposed architecture combines CNN-based local sensing, Federated Learning-based distributed intelligence, trust-based aggregation, and SVM-assisted RSU allocation to achieve reliable spectrum sensing and efficient spectrum utilization in future 6G-enabled CR-IoV networks.

IV. PROPOSED FEDERATED TRUST-AWARE LEARNING METHOD

Traditional spectrum sensing approaches in Cognitive Radio Internet of Vehicles (CR-IoV) primarily rely on centralized processing architectures in which sensing information collected by secondary user (SU) vehicles is transmitted to a central server for analysis and decision-making. Although such approaches can achieve acceptable detection accuracy, they introduce several challenges, including high communication overhead, privacy leaks, scalability limitations, and vulnerability to malicious participants.

To overcome these limitations, a trusted Federated learning framework is proposed for robust and scalable spectrum sensing in 6G-enabled CR-IoV networks. The proposed framework combines Convolutional Neural Network (CNN)-based local sensing, Federated Learning (FL)-based distributed training, trust-based aggregation, and support vector machine (SVM)-based RSU allocation. The proposed framework operates through multiple iterative learning cycles in which participating vehicles collaboratively improve a global sensing model without sharing raw sensing data.

A. System Initialisation: The network consists of several secondary user vehicles, roadside units (RSUs), and a hybrid learning spectrum agent (HLSA). Each SU vehicle initializes a local CNN model for spectrum sensing. The HLSA initializes a global model that will be shared among all participating vehicles. First, all vehicles receive the same global model parameters from the HLSA and start local training using their own detection observations.

B. Local Spectrum Data Collection: Each vehicle continuously monitors licensed spectrum bands and collects local signal samples under different channel conditions. The received signal may contain either primary user transmissions or noise components depending on channel occupancy.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14611

The sensing process is represented by:

$H_0 : x(n) = w(n)$

$H_1 : x(n) = s(n) + w(n)$

where x(n) denotes the received signal sample, s(n) represents the main user signal, and w(n) represents additive white Gaussian noise (AWGN). The collected detection samples are stored locally and are never transmitted outside the vehicle, thus preserving user privacy.

C. CNN based local spectrum sensing. The received sensing samples are processed using a convolutional neural network (CNN).The received sensing samples are processed using a Convolutional Neural Network (CNN).

The CNN automatically extracts signal features and learns spectrum occupancy patterns under different Signal-to-Noise Ratio (SNR) conditions. The CNN output layer generates a probability score indicating the presence or absence of primary user activity.

The local sensing decision is represented as:

$D = CNN(x)$

where D denotes the occupancy decision generated by the CNN model.

The CNN enables improved detection performance compared to conventional energy detection methods, especially in low SNR environments.

D. Trust Evaluation Mechanism: Although federated learning improves privacy and scalability, malicious or untrustworthy nodes may submit incorrect model updates. Therefore, a trust evaluation mechanism is integrated into the proposed framework.

The trust score is computed as:

$$T_i = \alpha A_i + \beta C_i + \gamma R_i + \delta E_i$$

where:

A_i = Detection Accuracy

C_i = Historical Consistency

R_i = Reporting Reliability

E_i = Energy Efficiency

$$\alpha + \beta + \gamma + \delta = 1$$

Vehicles with higher trust scores are considered more trustworthy and contribute more significantly during model aggregation.

E. Federated Model Sharing. Instead of transmitting raw sensing data, only the trained model parameters are uploaded to the nearest road unit.

W_i

where W_i denotes the updated CNN weight vector.

.RSUs collect model updates from multiple vehicles and transmit them to the Hybrid Learning Spectrum agent. This process significantly reduces communication costs and preserves data confidentiality.

F. Federated Trust-Based Aggregation: HLSA performs trust-weighted model aggregation to generate an improved overall detection model.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14611

The aggregated model is computed as:

$$W_{global} = \Sigma(T_i W_i) / \Sigma(T_i) \quad (4)$$

where:

W_{global} = Global model parameters

W_i = Local model update

T_i = Trust score of vehicle i

This aggregation strategy ensures that high-reliability vehicles contribute more strongly to the overall model while low-reliability nodes have minimal impact

As a result, the detection framework becomes more resilient to malicious participants and inaccurate detection reporting.

G. SVM-Based RSU Allocation

After obtaining the overall detection model, a support vector machine (SVM) is used to assign the most suitable RSU to each vehicle.The SVM takes into account the following parameters:• Signal-to-noise ratio (SNR)• Confidence score• Channel availability• Network congestion levelThe SVM classifier determines the optimal RSU capable of providing reliable communication and efficient resource utilization.The SVM classifier determines the optimal RSU capable of providing reliable communication and efficient resource utilization.

This intelligent allocation mechanism minimizes communication delay and improves overall network performance.

H. Iterative Learning Process;The entire process is repeated over several communication cycles.

The iterative learning procedure includes

Step 1: Initialize the CNN detection models.

Step 2: Collect local spectrum sensing data.

Step 3: Train CNN locally.

Step 4: Calculate confidence scores.

Step 5: Share local model settings.

Step 6: Perform trust-based aggregation.

Step 7: Update and distribute the global model.

Step 8: Run SVM-based RSU allocation.

The learning process continues until the detection accuracy converges or the desired performance level is achieved. The integration of CNN-based sensing, Federated Learning, trust-based aggregation, and SVM-assisted resource allocation enables the proposed framework to achieve reliable spectrum sensing, enhanced security, improved scalability, and efficient spectrum utilization in future 6G-enabled vehicular cognitive radio Internet networks.

V. RESULTS AND DISCUSSION

Monte Carlo simulations are performed to evaluate the performance of the proposed federated trust-aware spectrum sensing framework in cognitive radio-enabled vehicular Internet (CR-IoV) environments.The simulations are performed under Rayleigh fading channel conditions using BPSK (Binary Phase Shift Keying) modulation. A network composed of several secondary user vehicles, roadside units (RSUs) and primary users is considered. The Signal-to-Noise Ratio (SNR) varies from -30 dB to 10 dB to analyze detection performance under different channel conditions. The Probability of Detection (Pd), Receiver Operating Characteristics (ROC), and detection accuracy during malicious

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14611

node attacks are used as the main performance metrics to compare the proposed trust-based federated learning framework with conventional centralized detection and traditional federated learning approaches.

Fig. 1 shows the Probability of Detection (Pd) performance of centralized detection, conventional federated learning and the proposed confidence-aware federated learning framework under various SNR conditions. At low SNR values, all detection schemes exhibit relatively poor detection performance because noise dominates the received signal and makes it difficult to distinguish the user's main activity. As the SNR increases, the detection probability gradually improves for all approaches due to the increased intensity of the received signal. However, the centralized sensing approach demonstrates the lowest sensing performance across the entire considered SNR range, as sensing decisions are based on limited information and are very sensitive to channel degradations.

The conventional federated learning framework achieves better detection performance by enabling collaborative learning between multiple vehicles.Through distributed model training, detection information from different vehicles contributes to the overall model, thereby improving detection accuracy. Nevertheless, unreliable participants may still upload inaccurate model updates, which may negatively affect the quality of the aggregated model.

The proposed trust-based federated learning framework consistently achieves the highest detection probability over the entire SNR range. Incorporating trust-based aggregation allows The system to assign higher weights to trusted sensing participants while removing the influence of malicious or untrustworthy nodes. As a result, the overall detection model becomes more robust and accurate. The improvement achieved by the proposed framework becomes increasingly significant at higher SNR values, where the detection model can effectively exploit the improved signal quality. These results demonstrate that trust-based federated learning provides reliable spectral sensing even under challenging wireless channel conditions.

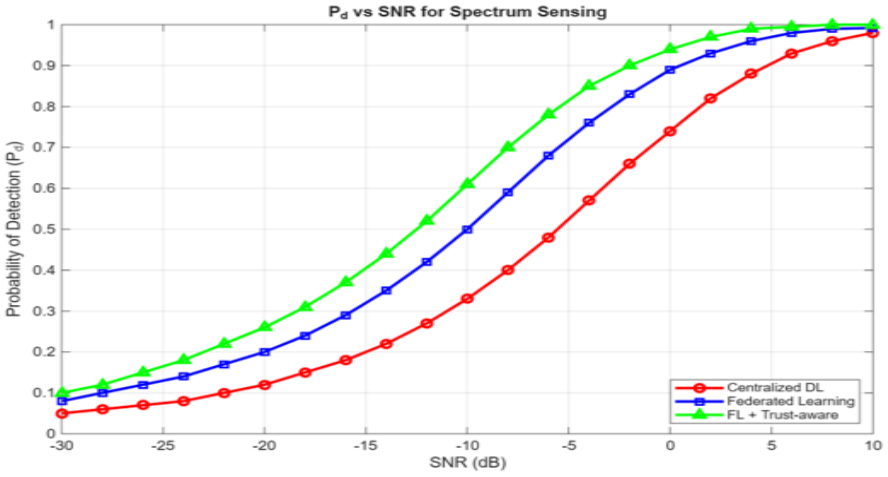

Fig. 1 Probability of Detection versus SNR

Fig. 2 presents the Receiver Operating characteristic (ROC) curves of the considered detection approaches at an SNR value of -15 dB. The ROC curve illustrates the trade-off between detection probability (Pd) and false alarm probability (Pf), providing a comprehensive measure of detection performance. An ideal spectrum detection system should achieve high detection probability while maintaining a low false alarm rate.

The centralized detection approach has the least favorable ROC performance because detection decisions rely heavily on local observations sensitive to fading and noise uncertainty. Although conventional federated learning improves detection performance through collaborative training, its effectiveness is still limited by inaccurate updates provided by unreliable participants.

The proposed trust-based federated learning framework achieves the most desirable ROC characteristics among all compared approaches. The trust-based aggregation process improves the quality of the overall model by reducing the impact of incorrect detection reports. Therefore, the framework achieves higher detection probabilities with lower false alarm rates. The superior ROC performance confirms the effectiveness of integrating trust assessment with federated learning for robust spectral sensing in CR-IoV environments.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026

DOI: 10.17148/IJIREEICE.2026.14611

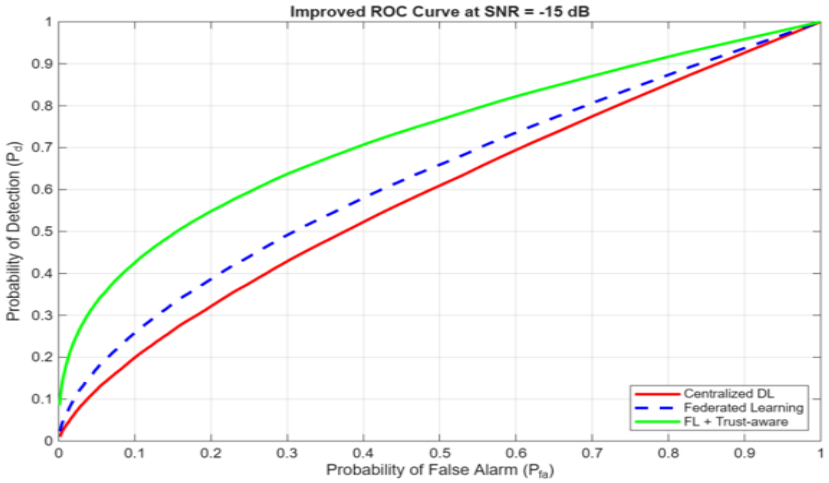

Fig.2 Receiver Operating Characteristics (ROC) Analysis at −15 dB

Fig. 3 illustrates the impact of malicious participants on the detection accuracy of learning-based federated spectrum sensing systems. Initially, conventional federated learning and trust-based federated learning achieve high detection accuracy when no malicious nodes are present. However, as the proportion of malicious participants increases, the detection accuracy gradually decreases because misleading model updates are introduced into the aggregation process.

The conventional federated learning framework experiences a significant reduction in detection accuracy as the percentage of malicious nodes increases. Since all participating vehicles contribute equally during model aggregation, inaccurate updates generated by malicious users harm the quality of the overall detection model. As a result, the overall detection performance deteriorates rapidly.

In contrast, the proposed trust-based federated learning framework demonstrates significantly higher resilience against malicious behaviour. Vehicles with low trust scores contribute less to the aggregation process, thereby minimizing the influence of malicious updates. Even when a high percentage of participants behave maliciously, the proposed framework maintains significantly higher detection accuracy than conventional federated learning. This demonstrates the effectiveness of trust-based aggregation in improving the security, robustness, and reliability of distributed spectrum sensing systems.

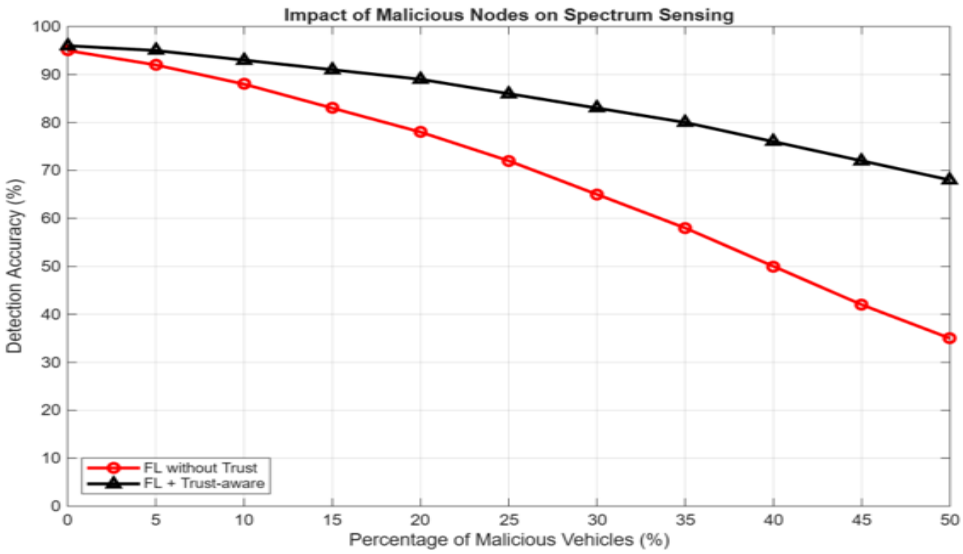

Fig. 3 Impact of Malicious Nodes on Spectrum Sensing

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 6, June 2026
DOI: 10.17148/IJIREEICE.2026.14611

Key Observations

The simulation results clearly demonstrate that integrating Trust Management with Federated Learning significantly improves spectrum sensing performance in Cognitive Radio-enabled vehicular Internet networks. Compared to conventional centralized detection and traditional federated learning approaches, the proposed framework offers:

- Higher probability of detection (Pd)
- Improved ROC performance
- Better spectrum usage efficiency
- Improved resistance against malicious participants
- Reduced communication overhead
- Improved privacy preservation
- Superior scalability in large-scale vehicular networks
- Reliable operation under low SNR conditions

The results further indicate that conventional federated learning systems remain vulnerable to untrustworthy and malicious participants, while trust-based aggregation effectively mitigates these threats.Overall, the proposed Federated Trust-Aware Spectrum Sensing framework provides a practical, secure and efficient solution for intelligent spectrum management in future 6G-enabled vehicular communication networks.

VI. CONCLUSION

In this paper, a Federated trust-based spectrum sensing framework for cognitive radio-enabled Internet of Vehicles (CR-IoV) operating in 6G communication environments was proposed. Unlike conventional centralized spectrum sensing approaches, the proposed framework uses federated learning to enable collaborative model training between secondary user (SU) vehicles without sharing raw sensing data. This decentralized learning mechanism significantly reduces communication overhead, improves privacy preservation, and improves the scalability of large-scale vehicular networks. Furthermore, the framework integrates Convolutional Neural Network (CNN)-based local spectrum sensing and Support Vector Machine (SVM)-assisted road unit (RSU) allocation to improve sensing accuracy and communication efficiency.

A trust-based aggregation mechanism has also been integrated to address the challenges posed by untrusted and malicious participants in federated learning environments. By assigning trust scores based on detection accuracy, reporting consistency, reliability, and participation behavior, the framework effectively minimizes the influence of malicious nodes during overall model aggregation. MATLAB simulation results demonstrate that the proposed approach achieves higher Probability of Detection (Pd), superior Receiver Operating characteristic (ROC) performance, improved spectrum utilization, and improved resilience against malicious attacks compared to traditional centralized and conventional federated learning methods. The results confirm that decentralized trust-driven learning is a practical and effective solution for intelligent spectrum sensing in future 6G-enabled vehicular communication systems.

Overall, the proposed framework successfully combines Federated Learning, Trust Management, CNN-based sensing, and SVM-assisted resource allocation to achieve reliable, secure, and scalable spectrum management in Cognitive Radio-enabled vehicular Internet networks. The study highlights the importance of integrating intelligent distributed learning techniques with trust assessment mechanisms to address the challenges of dynamic vehicle-to-vehicle communication environments.

In future work, the proposed framework can be extended by incorporating advanced deep learning architectures such as Long Short-Term Memory networks (LSTM), graph neural networks (GNN), and transformer-based learning models to improve spectrum prediction and decision making. Blockchain-assisted trust management can also be integrated to further improve security and transparency in distributed vehicle networks. Furthermore, the framework can be evaluated in real-world vehicular environments with varying traffic densities and mobility conditions to validate its practical applicability in future large-scale 6G communication systems.

DOI: 10.17148/IJIREEICE.2026.14611

REFERENCES

[1] R. Ahmed, Y. Chen, B. Hassan, L. Du, T. Hassan and J. Dias, "Hybrid Machine-Learning-Based Spectrum Sensing and Allocation With Adaptive Congestion-Aware Modeling in CR-Assisted IoV Networks," IEEE Internet of Things Journal, vol. 9, no. 24, pp. 25100–25116, Dec. 2022.

[2] Z. Chen, Y. Q. Xu, H. Wang and D. Guo, "Federated Learning-Based Cooperative Spectrum Sensing in Cognitive Radio," IEEE Communications Letters, vol. 26, no. 2, pp. 330–334, Feb. 2022.

[3] L. J. Vinita and V. Vetriselvi, "SEAFL: Transforming Federated Learning for Enhanced Privacy in 6G-Enabled Vehicles," International Conference on Intelligent Systems, pp. 1–8, 2023.

[4] D. Sirohi, N. Kumar, P. Rana, S. Tanwar, R. Iqbal and M. Hijji, "Federated Learning for 6G-Enabled Secure Communication Systems: A Comprehensive Survey," Artificial Intelligence Review, 2023.

[5] A. Usha and R. Prashanth, "DRLNet: A Deep Reinforcement Learning Network for Hybrid Feature Extraction and Spectrum Sensing in Cognitive Radio Networks," Journal of Advances in Information Technology, 2023.

[6] Ezhilarasi, I. E., Clement, J. C. and Arul, J. M., "A Survey on Cognitive Radio Network Attack Mitigation Using Machine Learning and Blockchain," Journal of Wireless Communications and Networking, 2023.

[7] Y. Zeng and Y. C. Liang, "Eigenvalue-Based Spectrum Sensing Algorithms for Cognitive Radio," IEEE Transactions on Communications, vol. 57, no. 6, pp. 1784–1793, 2009.

[8] T. Yucek and H. Arslan, "A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications," IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 116–130, 2009.

[9] Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, 2019.

[10] I. F. Akyildiz, W. Y. Lee, M. C. Vuran and S. Mohanty, "Next Generation Dynamic Spectrum Access Cognitive Radio Wireless Networks: A Survey," Computer Networks, vol. 50, pp. 2127–2159, 2006.

[11] O. U. Akgul et al., "Discussion on 6G Architecture Evolution: Challenges and Emerging Technology Trends," EuCNC/6G Summit, pp. 664–669, 2024.

[12] A. M. Ahmed and S. A. Majeed, "A Survey of 6G Mobile Systems, Enabling Technologies, and Challenges," International Journal of Electrical and Electronic Engineering & Telecommunications, vol. 12, no. 1, pp. 1–21, 2023.

[13] K. Takeuchi, S. Kaneko and S. Nomoto, "Radio Environment Prediction for Cognitive Radio," CrownCom, pp. 1–6, 2008.

[14] P. Sridhar, S. D. Arivan, R. Akshay and R. Farhathullah, "Anomaly Detection Using CNN with SVM," ICSSS, pp. 1–4, 2022.

[15] W. Chen et al., "5G-Advanced Toward 6G: Past, Present and Future," IEEE Journal on Selected Areas in Communications, vol. 41, no. 6, pp. 1592–1619, 2023.

[16] M. Chen, U. Challita, W. Saad, C. Yin and M. Debbah, "Artificial Neural Networks-Based Machine Learning for Wireless Networks," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3039–3071, 2019.

[17] H. Ye, G. Y. Li and B. H. Juang, "Power of Deep Learning for Channel Estimation and Signal Detection in OFDM Systems," IEEE Wireless Communications Letters, vol. 7, no. 1, pp. 114–117, 2018.