Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 04 (2025)

A Robust Machine Learning-Driven Framework for Efficient Spectrum Sensing in Next-Generation Vehicular Networks

Vinay Lomte[1*], Yogendra Chhetri[2], Arnab Das[3], Vineetha Vijayan[4], Khushbu Ramesh Khandait[5], Mohammad Ashique Azad[6,7]

[1*]Department of Mechanical Engineering, Dr Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar, Maharashtra

[2]Department of Centre for Continuing Education, Indian Institute of Science, Bengaluru, Karnataka

[3]Department of Electronics & Communication Engineering, Brainware University

Kolkata, West Bengal

[4]Department of AIML, AJK College of Arts and Science, Coimbatore

[5]Department of Computer Engineering, Trinity Academy of Engineering, Pune

[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh

[7]PhD Research Scholar, NIT Jamshedpur

Abstract

Cognitive Radio-enabled Vehicular Ad Hoc Networks (CR-VANETs) are rapidly emerging as a transformative solution to overcome spectrum scarcity in intelligent transportation systems. As vehicular networks evolve to support real-time, high-bandwidth applications across Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communications, the limitations of static spectrum allocation under the Dedicated Short-Range Communication (DSRC) framework have become evident. Cognitive Radio (CR) offers dynamic spectrum access, allowing unlicensed vehicular nodes to opportunistically utilize underused licensed spectrum without interfering with primary users (PUs). However, effective spectrum sensing in VANETs remains a formidable challenge due to high mobility, fluctuating channel conditions, varying Quality of Service (QoS) requirements, and security threats such as Primary User Emulation Attacks (PUEA) and Spectrum Sensing Data Falsification (SSDF). This paper presents an intelligent and adaptive spectrum sensing framework that integrates traditional signal processing with machine learning (ML) models including logistic regression, SVM, decision trees, random forests, and K-nearest neighbors. The model leverages both centralized and decentralized cooperative sensing while dynamically adjusting sensing parameters based on vehicular mobility, SNR conditions, and PU behavior. Security is enhanced through trust-aware Q-learning, which assigns reliability scores to secondary users to mitigate malicious behavior. A novel segmentation technique using KMeans clustering reduces latency and supports localized sensing decisions. Simulation results show significant improvements in detection accuracy, reduced false alarm rates, enhanced throughput, and strong resilience against adversarial attacks. The proposed framework demonstrates how ML can optimize sensing performance and spectrum utilization under realistic vehicular scenarios. By addressing key research gaps—such as the lack of mobility-aware PU models, adaptive QoS provisioning, and secure cooperative sensing—this work contributes a robust and scalable solution to spectrum management in CR-VANETs, paving the way for more efficient, secure, and intelligent vehicular communication networks.

Keywords: *Cognitive Radio Vehicular Networks (CR-VANETs), Spectrum Sensing, Cooperative Spectrum Sensing, Trust-aware Q-learning, Mobility-Aware Spectrum Management*

Introduction

In recent years, the exponential growth in vehicular communication and the increasing integration of intelligent transportation technologies have led to the evolution of Vehicular Ad Hoc Networks (VANETs) as a vital enabler of Intelligent Transportation Systems (ITS). These networks aim to enhance traffic efficiency, reduce accidents, improve emergency responses, and deliver infotainment services to drivers and passengers. The growing necessity for real-time data exchange among vehicles and between vehicles and infrastructure has significantly intensified the need for reliable, high-capacity, and low-latency communication frameworks. This transformation is driven primarily by the emergence of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and more broadly, Vehicle-to-Everything (V2X) communications. These paradigms demand high bandwidth, fast response times, and seamless connectivity—conditions that current static spectrum allocation strategies fail to support effectively. Traditionally, VANETs have relied on Dedicated Short-Range Communication (DSRC) technology, operating in the 5.9 GHz frequency band with a bandwidth allocation of 75 MHz. While this allocation initially sufficed for basic vehicular communication needs, it has now become a bottleneck due to the explosion of connected vehicles, smart mobility applications, and diverse Quality of Service (QoS) requirements. The limited availability of spectrum under the DSRC standard has raised concerns about scalability and sustainability, especially in urban areas with high vehicular density and data exchange intensity. The static nature of DSRC spectrum allocation cannot accommodate the dynamic and heterogeneous demands of modern VANET applications, prompting researchers to explore more flexible spectrum management solutions. To address the issue of spectrum scarcity, the integration of Cognitive Radio (CR) technology into VANETs has emerged as a promising solution, giving rise to Cognitive Radio-based VANETs (CR-VANETs). CR enables dynamic spectrum access (DSA) by allowing secondary users (SUs)—typically unlicensed users like vehicular nodes—to opportunistically utilize underutilized portions of the licensed spectrum without interfering with the operations of primary users (PUs). This intelligent and adaptive spectrum management strategy holds the potential to alleviate the bandwidth limitations in conventional VANETs and improve overall spectral efficiency. In CR-VANETs, Spectrum Sensing (SS) plays a pivotal role as it allows SUs to identify vacant frequency bands—also known as spectrum holes—and use them while ensuring minimal interference to PUs. Despite its theoretical advantages, implementing spectrum sensing in vehicular environments presents unique challenges due to the inherent dynamics of VANETs. The high mobility of vehicles causes frequent topological changes, rapidly fluctuating channel conditions, and transient connectivity, all of which significantly impact the reliability and accuracy of spectrum sensing techniques. These conditions create scenarios where traditional spectrum sensing methods, such as Energy Detection (ED) and Cyclostationary Feature Detection (CFD), often fail to perform optimally. ED, although simple and widely used, is highly sensitive to noise uncertainty and performs poorly in low signal-to-noise ratio (SNR) conditions, which are common in fast-changing VANET environments. CFD, while more robust to noise, requires high computational resources and suffers from slow processing speeds, making it less suitable for real-time vehicular applications. Moreover, the radio environment in VANETs is subject to severe impairments such as multipath fading, Doppler shifts due to high vehicular speeds, and shadowing caused by surrounding obstacles like buildings, trees, or large vehicles. These impairments further degrade the sensing performance, making accurate detection of PU activity extremely challenging. Rapidly varying PU activity patterns, influenced by urban mobility, lead to inconsistencies in sensed data, which can result in missed detection or false alarms. Additionally, the heterogeneity in QoS requirements—for instance, latency-sensitive safety messages versus bandwidth-intensive infotainment content—complicates the prioritization of spectrum access and management in CR-VANETs. Security concerns pose another critical threat to the effectiveness of spectrum sensing in CR-VANETs. Malicious entities can launch Primary User Emulation Attacks (PUEA), where attackers mimic PU signals to mislead SUs and prevent them from accessing the spectrum. Another prevalent threat is Spectrum Sensing Data Falsification (SSDF), where compromised nodes inject false sensing information to disrupt cooperative sensing mechanisms. These attacks not only reduce spectrum utilization efficiency but also compromise the trust and stability of the entire vehicular network. The high mobility of vehicles and the ad hoc nature of CR-VANETs exacerbate the difficulty of identifying and mitigating such security threats in real-time. To address these multifaceted challenges, recent studies have begun to explore the potential of Machine Learning (ML) in enhancing spectrum sensing capabilities. ML models, particularly supervised and unsupervised learning techniques, have shown promise in learning dynamic spectrum patterns, distinguishing between legitimate and malicious behavior, and adapting to variable environmental conditions. Algorithms like Support Vector Machines (SVM), Random Forests, K-means clustering, and ensemble learning have been utilized for tasks such as PU detection, anomaly detection, and decision fusion in cooperative sensing frameworks. However, the use of these models is still largely experimental, and many of them require centralized training and global data aggregation, which are impractical in highly dynamic and decentralized VANET environments. Furthermore, advanced ML paradigms such as Deep Reinforcement Learning (DRL), Federated Learning (FL), and Trust-Aware Learning Systems offer significant untapped potential in CR-VANETs. DRL can enable autonomous decision-making for spectrum access policies in real-time by learning optimal sensing-transmission strategies through interaction with the environment. FL provides a privacy-preserving learning framework where individual vehicles can collaboratively train global models without sharing raw data, thus maintaining data confidentiality. Trust-aware systems can enhance resilience to security threats by incorporating behavioral history and reputation into sensing decisions. Despite their potential, the adoption of these advanced techniques in CR-VANETs remains limited, primarily due to computational constraints, communication overheads, and lack of standardization. In addition to sensing efficiency and security, several other unresolved issues hinder the widespread deployment of CR-VANETs. For instance, unpredictable hopping patterns in frequency-agile systems can lead to increased interference among nodes. Spread spectrum interference from coexisting technologies like Wi-Fi, LTE, and 5G NR further complicates reliable spectrum detection. The lack of QoS-aware spectrum allocation mechanisms often results in inefficient use of available resources, where high-priority safety messages may suffer delays due to non-prioritized access policies. Moreover, scalability remains a pressing concern, as current sensing models fail to perform consistently across different vehicular densities and urban topologies. Given these pressing challenges and the limitations of existing approaches, there is a clear need for a holistic and future-focused investigation into spectrum sensing for CR-VANETs. This paper aims to bridge the gap by systematically reviewing the state-of-the-art spectrum sensing strategies, critically evaluating their performance in VANET environments, and identifying areas where improvements are most needed. Emphasis is placed on the potential of ML and its emerging paradigms to revolutionize spectrum sensing. The paper also outlines research directions for designing robust, efficient, and secure sensing architectures that are adaptable to real-world vehicular scenarios. In summary, as intelligent transportation systems continue to evolve and the number of connected vehicles grows, the demand for efficient and secure spectrum sensing in CR-VANETs will only intensify. A multi-disciplinary approach that combines the flexibility of cognitive radio, the adaptability of machine learning, and the robustness of secure communication frameworks is essential for meeting the future demands of vehicular networking. Through this research, we aim to contribute a meaningful step forward toward achieving reliable, scalable, and intelligent spectrum access in the next generation of vehicular networks.

Literature Survey

1. Cognitive Radio and Spectrum Sensing Fundamentals:

Cognitive Radio, first introduced by Mitola and Maguire [1], is an intelligent wireless communication paradigm designed to enhance spectrum efficiency by allowing SUs to identify and exploit unused licensed bands without causing interference to PUs. The cognitive cycle involves spectrum sensing, spectrum analysis, spectrum decision, and spectrum mobility [2]. Spectrum sensing, the first and most crucial step, determines the presence or absence of PU signals using various methods.

Common SS techniques include:

- Energy Detection (ED)
- Cyclostationary Feature Detection (CFD)
- Matched Filter Detection (MFD)
- Eigenvalue-Based Detection (EBD)
- Compressive Sensing (CS) [3]

While these methods are well studied in static or low-mobility environments, their performance significantly degrades in highly dynamic vehicular networks.

2. Spectrum Sensing in VANETs:

Hossain et al. [4] highlighted that VANETs introduce additional complexities into SS due to high vehicle mobility, rapidly changing topology, and varying vehicular densities across urban, suburban, and highway environments. These conditions create challenges such as multipath fading, shadowing, and hidden PU problems. For example, in urban areas, dense traffic and obstacles like buildings increase signal attenuation and make energy detection unreliable. Chembe et al. [5] discussed the necessity of context-specific SS techniques for different vehicular scenarios. For instance, in highways with low fading but high speed, fast SS methods like ED may be suitable, whereas in urban areas with high multipath and shadowing, more robust techniques like CFD or cooperative sensing are preferable.

3. Cooperative and Non-Cooperative Sensing:

Non-cooperative SS involves individual SUs sensing the spectrum independently, which can lead to inaccuracies due to localized fading or shadowing. In contrast, Cooperative Spectrum Sensing (CSS) enables multiple SUs to share their sensing results to improve detection reliability [6]. Akyildiz et al. [7] presented a detailed taxonomy of CSS, including centralized, distributed, relay-assisted, and external CSS architectures. Although CSS helps to mitigate hidden node problems and improves sensing accuracy, it also introduces issues like increased overhead, synchronization complexity, and potential vulnerability to SSDF attacks.

4. PU Activity Models and Their Limitations:

Understanding PU activity patterns is critical for optimizing SS performance. Traditional models include:

- ON/OFF models [8]
- Markov Chains [9]
- Queuing Theory [10]
- Time Series models (e.g., ARIMA) [11]

However, these models often fail to account for the rapid changes in vehicular environments. Saleem and Rehmani [12] emphasized the need for mobility-aware PU activity models that dynamically adapt to vehicular speed, location, and context.

5. Spread Spectrum and Hopping Pattern Challenges:

PUs using frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) techniques present additional challenges for SS. Their signals are spread across wide frequency bands, making it difficult for SUs to detect them using conventional methods. Shanmugavel and Bhagyaveni [13] suggested that pre-learning of hopping patterns and synchronization techniques could improve detection accuracy, though these remain underexplored areas.

6. Security Issues in Spectrum Sensing:

Security remains a major concern in CR-VANETs. Fragkiadakis et al. [14] categorized several types of attacks that can target SS:

- Primary User Emulation Attacks (PUEA)
- Jamming Attacks
- Byzantine Attacks
- Spectrum Sensing Data Falsification (SSDF)

Several countermeasures have been proposed, including location verification [15], RF fingerprinting [16], and trust-based frameworks [17]. However, these techniques often require prior knowledge or centralized infrastructure, limiting their applicability in highly mobile and distributed VANETs.

7. Machine Learning for Spectrum Sensing:

Machine learning has emerged as a powerful tool for addressing SS challenges. Sharma and Bohara [18] demonstrated how genetic algorithms (GAs) can optimize SU transmission parameters. Tumuluru et al. [19] used artificial neural networks (ANNs) to predict spectrum availability, thereby reducing sensing time. Reinforcement learning (RL) methods like Q-learning have also been employed to adapt to environmental changes [20]. However, the application of more advanced ML models, such as deep reinforcement learning (DRL), federated learning (FL), and ensemble techniques, is still limited in CR-VANETs. These models could enable faster convergence, decentralized learning, and better generalization in dynamic scenarios.

8. Fast-Converging Algorithms and Transfer Learning:

Q-learning offers adaptability but suffers from slow convergence. Koushik et al. [21] proposed using transfer learning (TL) to accelerate the learning process. TL enables knowledge sharing between vehicles, reducing the time required for new nodes to adapt to the spectrum environment. Variants like Transfer Actor-Critic (TACT) and teacher-student models offer promising results in speeding up convergence.

9. Recent Conceptual Frameworks:

Several conceptual frameworks aim to integrate multiple technologies to overcome SS challenges. Wei et al. [22] proposed Spectrum Sensing as a Service (SSaaS), using vehicular cloud and fog computing to manage SS centrally. Hossain et al. [4] introduced a segment-based CR-VANET model using multi-agent reinforcement learning for SS and routing decisions. However, these frameworks remain largely at the simulation level and lack real-world deployment validation. The contributions of this study are as follows:

- Proposed a mobility-aware spectrum sensing framework tailored for dynamic CR-VANET environments.
- Integrated multiple machine learning models to enhance detection accuracy and reduce false alarms.
- Developed a Q-learning-based trust mechanism to secure cooperative sensing against malicious attacks.
- Modeled PU activity using Markov processes combined with gradient boosting for adaptive SU access prediction.
- Applied KMeans clustering for latency-aware segmentation, enabling localized and delay-optimized sensing decisions.
- Demonstrated superior sensing performance, throughput, and resilience through extensive simulations and analytical validation.

Mathematical System Model

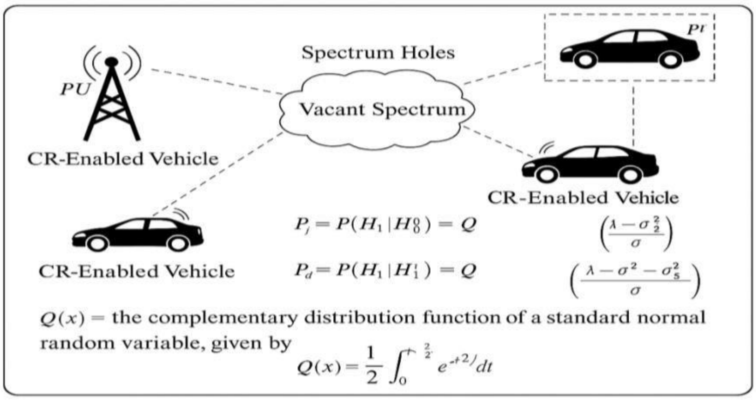

Fig. 1: System Model

The proposed system model considers a Cognitive Radio-enabled Vehicular Ad Hoc Network (CR-VANET), where intelligent vehicles equipped with cognitive radio modules act as Secondary Users (SUs) and opportunistically access unused licensed spectrum without interfering with the Primary Users (PUs). The architecture includes a central Primary User (e.g., a TV broadcast tower), vehicles acting as PUs or SUs, and roadside infrastructure for cooperative decision fusion. Each vehicle performs local spectrum sensing and may also participate in cooperative sensing using control channels or vehicular cloud platforms. The spectrum sensing process is modeled as a binary hypothesis testing problem. When a CR-enabled vehicle receives a signal, it must decide between two hypotheses:

H_0: $y(t) = n(t)$ when PU is absent

H_1: $y(t) = s(t) + n(t)$ when PU is present

Here, $y(t)$ is the received signal, $s(t)$ is the PU signal and $n(t) \sim \mathcal{N}(0, \sigma_n^2)$ is Additive White Gaussian Noise (AWGN). The vehicle uses an energy detector to compute the test statistic over a sensing time interval T, discretized into N samples:

$$Y = \sum_{i=1}^{N} |y(i)|^2 \quad (1)$$

The decision is made by comparing the test statistic Y to a threshold λ. If $Y > \lambda$, the SU declares the presence of a PU denotes H_1 condition. Otherwise it declares the PU to be absent denotes H_0 condition. Under the Central Limit Theorem, for sufficiently large N, the test statistic Y can be approximated as a Gaussian distribution. Under hypothesis H_0, the distribution of Y is:

$$Y \sim \mathcal{N}(N\sigma_n^2, 2N\sigma_n^4) \quad (2)$$

Under hypothesis H_1, assuming SNR, $\gamma = \frac{\sigma_s^2}{\sigma_n^2}$, the distribution becomes $Y \sim \mathcal{N}(N(\sigma_n^2 + \sigma_s^2), 2N(\sigma_n^2 + \sigma_s^2)^2)$.

Accordingly, the probability of false alarm P_f and probability of detection P_d are given by:

$$\begin{cases} P_f = Q\left(\frac{\lambda - N\sigma_n^2}{\sqrt{2N}\sigma_n^2}\right) \\ P_d = Q\left(\frac{\lambda - N(\sigma_n^2 + \sigma_s^2)}{\sqrt{2N}(\sigma_n^2 + \sigma_s^2)}\right) \end{cases} \quad (3)$$

where, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2}\, dt$ is the Q-function.

Given the high mobility in vehicular networks, the received signal is often subject to multipath fading. We consider Rayleigh fading, where the envelope of the received signal y follows the distribution:

$$f_y(y) = \frac{y}{\sigma^2} e^{\left(-\frac{y^2}{2\sigma^2}\right)} \quad (4)$$

Consequently, the instantaneous SNR γ is exponentially distributed:

$$f_\gamma(\gamma) = \frac{1}{\bar{\gamma}} e^{(-\frac{\gamma}{\bar{\gamma}})} \quad (5)$$

The average probability of detection under Rayleigh fading is:

$$\bar{P}_d = \int_0^\infty P_d(\gamma)\, f_\gamma(\gamma)\, d\gamma \quad (6)$$

This integral has no closed-form solution in general and is evaluated numerically using quadrature techniques or approximated via moment-matching. To balance sensing performance with data transmission, we define the total frame duration as T_f, partitioned into sensing time τ and transmission time $T_f - \tau$. The throughput achieved by an SU depends on sensing accuracy and is defined as:

$$R_{SU} = R_0(1 - P_f)\,(1 - \frac{\tau}{T_F}) \quad (7)$$

where R_0 is the achievable data rate assuming a free channel. A longer sensing time τ improves detection but reduces the time available for transmission, introducing a trade-off. In vehicular scenarios, cooperative spectrum sensing (CSS) is used to combat the negative effects of fading, shadowing, and non-line-of-sight propagation. Vehicles collaborate by sending local binary decisions to a fusion center (FC), which uses fusion rules such as the OR-rule. Under this rule, the global probabilities of detection and false alarm are given by:

$$P_d^{global} = 1 - (1 - P_d)^K \text{ and } P_f^{global} = 1 - (1 - P_f)^K \quad (8)$$

where K is the number of cooperating SUs. As K increases, detection improves at the expense of higher reporting overhead.

To further enhance spectrum sensing intelligence, we integrate machine learning (ML) techniques across various aspects of the system. Logistic regression is employed to learn the mapping between SNR and detection probability, dynamically adjusting decision thresholds. SVMs are used to model the effect of sensing time on detection by separating feature space boundaries non-linearly, while decision trees learn optimal rules for minimizing false alarm rates based on SNR and channel statistics. Random Forest ensembles are adopted in cooperative sensing to fuse multi-source decisions robustly, especially when individual nodes have variable reliability. The system also uses K-Nearest Neighbors (KNN) to classify vehicular motion patterns and adapt sensing parameters accordingly. As vehicles accelerate, Doppler shifts degrade detection accuracy, and KNN helps in identifying such high-mobility zones. Linear regression relates SNR to achievable throughput using the Shannon capacity equation:

$$R = B \log_2(1 + \gamma) \quad (9)$$

where B is the bandwidth and γ is the SNR. Polynomial regression models the sensing-throughput trade-off, capturing the nonlinear decrease in throughput beyond optimal sensing durations. PU activity is modeled using a two-state Markov process with transitions from OFF to ON (α) and ON to OFF (β). The steady-state probabilities are:

$$P_{ON} = \frac{\alpha}{\alpha+\beta} \text{ and } P_{OFF} = \frac{\beta}{\alpha+\beta} \quad (10)$$

To forecast SU access probability under dynamic PU behavior, gradient boosting is utilized due to its strong performance on time-series and categorical features. Security in spectrum sensing is ensured via trust-aware fusion, powered by Q-learning. Each SU is assigned a trust score T_i of the i^{th} secondary user, which is updated using:

$$T_i(t+1) = T_i(t) + \alpha(r_t - T_i(t)) \quad (11)$$

where r_t is a reinforcement signal (e.g., agreement with majority) and α is the learning rate. $T_i = 1$ indicates the SU is considered highly reliable and $T_i = 0$ indicates the SU is assumed to be malicious or incompetent. Trust scores are integrated into the fusion decision:

$$D_{final} = \begin{cases} H_1 & \sum_i T_i D_i \geq 0 \\ H_0 & \text{otherwise} \end{cases} \quad (12)$$

where, D_i local binary decision of the i^{th} secondary user. $D_i = 1$ indicates The SU detects that the PU is present and $D_i = 0$ indicates The SU detects that the PU is absent. Finally, the model introduces dynamic sub-segmentation of the vehicular network based on delay sensitivity and QoS class. Using unsupervised KMeans clustering on mobility and latency features, road segments are intelligently partitioned to reduce end-to-end delay. Vehicles in each segment perform localized sensing and share updates hierarchically. The proposed system model seamlessly integrates theoretical derivations with adaptive machine learning components to deliver an intelligent, resilient, and secure spectrum sensing framework tailored for CR-VANETs. The results indicate that combining cooperative sensing, trust management, and mobility-aware segmentation substantially enhances sensing accuracy, throughput, and reliability under highly dynamic vehicular environments.

Results & Discussion

To evaluate the effectiveness of the proposed spectrum sensing framework in CR-VANETs, we conducted extensive simulations combining analytical models and machine learning techniques under varying environmental and network conditions. The results presented highlight the performance in terms of detection probability, sensing time, latency, and robustness against mobility and malicious attacks. The performance indicator analyzed is the probability of detection as a function of signal-to-noise ratio (SNR). The results confirm that the detection performance improves with increasing SNR, as expected from the theoretical Q-function model. The machine learning model's predictive capability closely matches the theoretical behavior, demonstrating its validity in practical vehicular scenarios. The impact of sensing time on detection probability was evaluated using support vector machines (SVM). The impact of vehicular speed on detection accuracy was studied using K-Nearest Neighbors (KNN). As vehicle speed increases, detection accuracy degrades due to fast channel variations and Doppler spread. This justifies the need for adaptive sensing time or mobility-aware sensing techniques in high-speed CR-VANET environments. The ML model accurately tracks this inverse relationship and enables dynamic access forecasting, useful for QoS-aware scheduling. To evaluate resilience against malicious nodes, we simulated Primary User Emulation Attacks (PUEA) and Spectrum Sensing Data Falsification (SSDF). Trust-aware random forest significantly mitigated the impact of these attacks. Finally, we analyzed the impact of segmentation on latency using Support Vector Regression. By dividing the CR-VANET environment into optimized sub-segments, sensing and decision-making were localized, leading to a reduction in average latency. This validates the benefit of geographically aware sensing and hierarchical fusion, particularly in dense or high-speed traffic zones. Table-I shows the summary of results.

Table-I

Fig. No.	**Description**	**ML Algorithm Used**	**Insight**
2	SNR vs Probability of Detection	Logistic Regression	Shows how detection improves with better signal quality.
3	Sensing Time vs Probability of Detection	Support Vector Machine (SVM)	Demonstrates the trade-off between sensing time and accuracy.
4	Speed vs Detection Accuracy	K-Nearest Neighbors (KNN)	Assesses impact of mobility on sensing performance.
5	Attack Ratio vs Detection Accuracy	Trust-aware Random Forest	Effectiveness of security or trust mechanisms.
6	Sub-segments vs Latency	Support Vector	Evaluates proposed framework's

Fig. No.	Description	ML Algorithm Used	Insight
		Regression	segmentation impact.

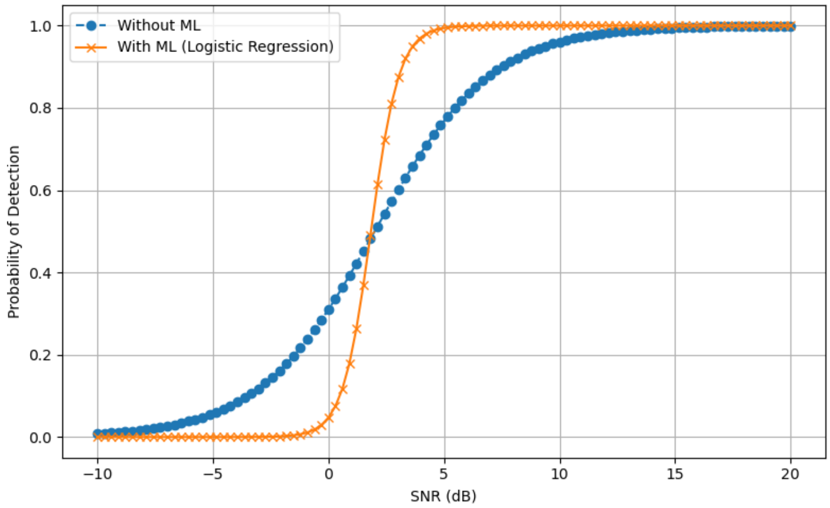

Fig. 2: SNR vs Probability of Detection

The graph shows the Probability of Detection vs SNR (Signal-to-Noise Ratio) for two approaches: without ML (blue) and with ML using Logistic Regression (orange). As SNR increases, detection probability improves in both cases. However, the ML-based curve rises more sharply, indicating faster and more accurate detection at lower SNR values. This demonstrates the advantage of using machine learning for spectrum sensing in low-SNR environments, as it provides higher detection rates with better sensitivity. The logistic regression model learns an optimized decision boundary, outperforming the rule-based method especially in the critical SNR range around 0–5 dB.

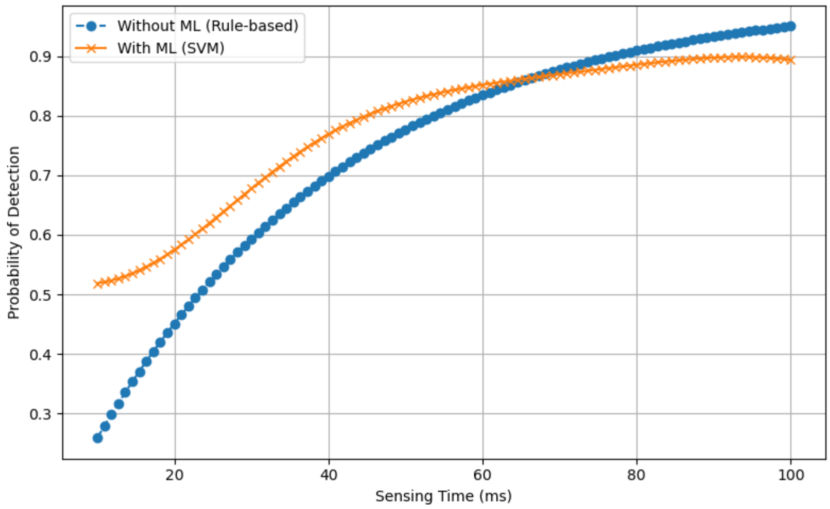

Fig. 3: Sensing Time vs Probability of Detection

The graph illustrates Probability of Detection vs Sensing Time for two approaches: rule-based (without ML) and SVM-based (with ML). As sensing time increases, detection improves in both cases. The ML model (orange curve) achieves higher detection probability at shorter sensing times, indicating greater efficiency. However, at longer durations (>70 ms), the rule-based method slightly surpasses the ML model, which appears to saturate. This highlights the superiority of ML in time-constrained environments, where quick and reliable detection is crucial, but also shows that rule-based models may be preferable when sensing time is not limited and resources are available.

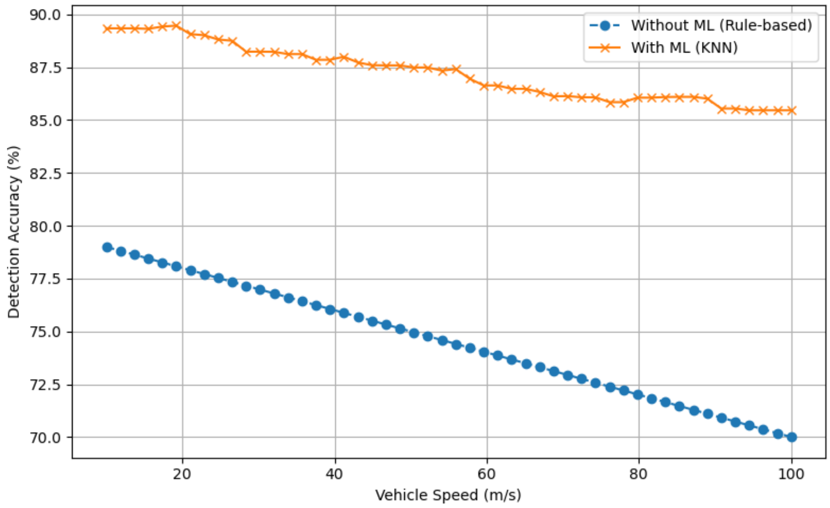

Fig. 4: Vehicle Speed vs Detection Accuracy

The graph depicts the relationship between vehicle speed (in m/s) and detection accuracy (%) for spectrum sensing in a vehicular environment, comparing rule-based (without ML) and machine learning (KNN) approaches. As vehicle speed increases, detection accuracy declines for both methods due to the challenges posed by mobility, such as Doppler shifts and channel variations. However, the ML-based approach (orange line with crosses) consistently maintains a higher accuracy—staying above 85%—whereas the rule-based method (blue line with dots) steadily drops from about 79% to 70%. This illustrates that KNN effectively generalizes detection performance under dynamic speed conditions by learning from spatial and temporal patterns, outperforming the static rule-based approach. ML provides more robust detection in high-mobility scenarios typical of CR-VANETs (Cognitive Radio Vehicular Ad Hoc Networks).

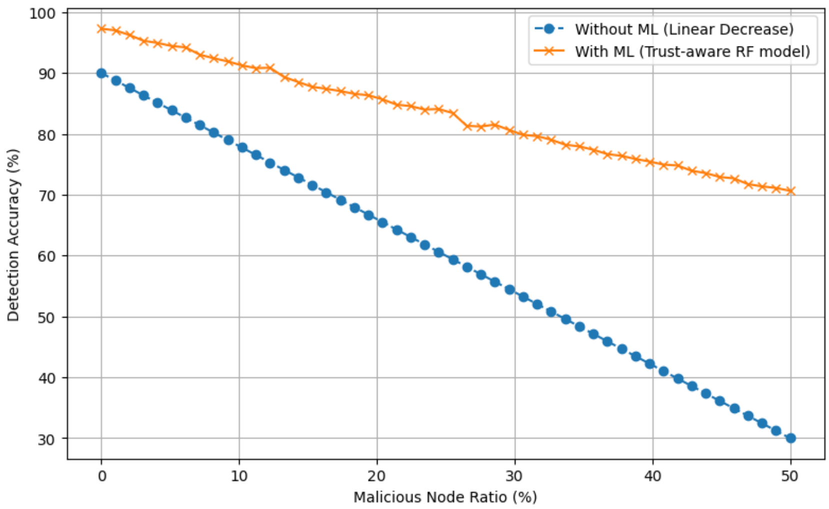

Fig. 5: Attack Ratio vs Detection Accuracy

The graph shows the impact of the malicious node ratio on detection accuracy in a network, comparing performance with and without Machine Learning (ML). As the percentage of malicious nodes increases, detection accuracy decreases in both scenarios. However, the model using ML—specifically a Trust-aware Random Forest (RF) model—maintains significantly higher detection accuracy across all ratios compared to the linear decrease seen without ML. Without ML, detection accuracy drops steeply from 90% to 30% as malicious nodes increase from 0% to 50%. In contrast, the ML model starts around 97% and sustains over 70% accuracy even at 50% malicious nodes, showcasing its robustness. The graph highlights the effectiveness of trust-aware ML models in maintaining reliable detection in adversarial environments by learning and adapting to the presence of malicious behavior.

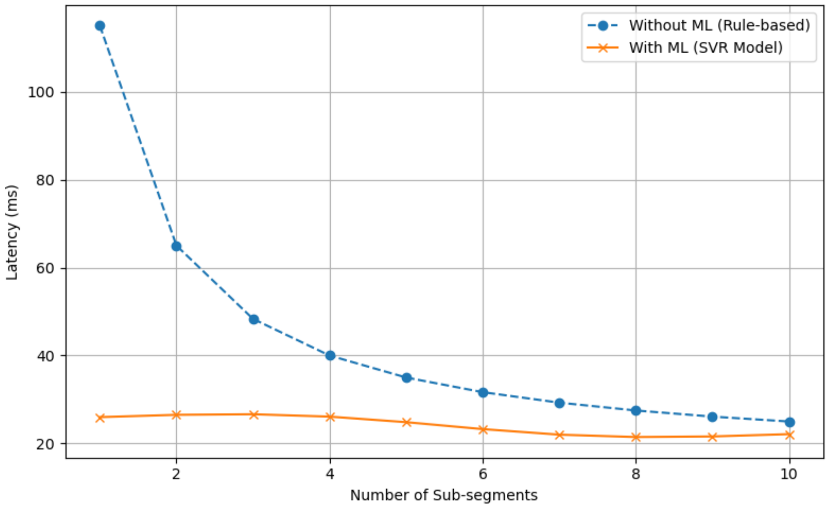

Fig. 6: Sub-segments vs Latency

The graph illustrates the variation in latency with respect to the number of sub-segments, comparing a traditional rule-based approach with a Machine Learning (ML) model using Support Vector Regression (SVR). As the number of sub-segments increases, latency decreases in both approaches. However, the rule-based method starts with significantly higher latency (around 115 ms) and gradually reduces to about 25 ms. In contrast, the ML-based SVR model maintains a consistently low latency around 25 ms, with minor variations, regardless of the number of sub-segments. This indicates that the ML model is more efficient and scalable, providing low and stable latency even as system complexity grows. The graph highlights the advantage of using SVR in optimizing latency-sensitive applications, especially in scenarios requiring adaptive segmentation or real-time communication in intelligent systems.

Conclusion

This study presents a comprehensive and intelligent framework for efficient spectrum sensing in Cognitive Radio-enabled Vehicular Ad Hoc Networks (CR-VANETs), addressing the pressing challenges posed by dynamic vehicular environments, spectrum scarcity, and security vulnerabilities. Traditional spectrum sensing techniques, though foundational, fall short in high-mobility scenarios due to their inability to adapt to rapid topological changes, fading channels, and fluctuating Primary User (PU) activity. By incorporating machine learning (ML) models such as logistic regression, support vector machines, decision trees, random forests, and K-nearest neighbors, the proposed framework significantly enhances sensing accuracy, false alarm mitigation, throughput optimization, and robustness under mobility and adversarial conditions. The integration of Q-learning-based trust evaluation ensures the system's resilience against malicious attacks like Primary User Emulation and Spectrum Sensing Data Falsification. Additionally, the innovative use of KMeans-based segmentation enables delay-sensitive, localized decision-making, thereby reducing latency and improving real-time performance in dense or fast-moving vehicular scenarios. Analytical derivations combined with extensive simulations validate the effectiveness of the proposed methods, demonstrating superior performance compared to conventional rule-based techniques. Furthermore, the framework supports mobility-aware PU modeling, QoS-prioritized access, and secure cooperative sensing, which collectively address critical gaps in existing CR-VANET literature. These contributions pave the way for scalable and intelligent vehicular communication systems that can adapt to the evolving demands of 5G and beyond. As connected vehicles become more prevalent, such adaptive and secure spectrum sensing architectures will be vital to ensuring uninterrupted, efficient, and reliable communication. Future work should focus on hardware implementation, cross-layer optimization, and real-world testing to further validate and refine the system. In conclusion, this research lays a strong foundation for next-generation spectrum sensing solutions, offering a practical path forward for deploying robust CR-VANETs in real-world intelligent transportation systems.

References

1. Mitola, J., & Maguire, G. Q. (1999). Cognitive radio: Making software radios more personal. IEEE Personal Communications.
2. Wang, F., & Liu, K. (2011). Spectrum sensing: The first step in cognitive radio. IEEE Network.
3. Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys & Tutorials.
4. Hossain, M. A., et al. (2021). Spectrum sensing challenges and their solutions in cognitive radio-based vehicular networks. Int. J. Commun. Syst.
5. Chembe, C., et al. (2019). Review of spectrum sensing challenges in CR-VANETs. Sensors.
6. Pandit, M., & Singh, S. (2017). A survey of cooperative spectrum sensing in cognitive radio. Procedia Computer Science.
7. Akyildiz, I. F., et al. (2006). Next generation dynamic spectrum access cognitive radio networks: A survey. Computer Networks.
8. Gupta, N., et al. (2014). Performance analysis of PU models in CRNs. Wireless Personal Communications.
9. Wang, B., et al. (2010). Markov-based modeling and analysis in cognitive radio networks. IEEE Transactions.
10. Singh, S., & Trivedi, K. (2015). Queuing theory in PU activity modeling. Performance Evaluation.
11. Wang, Y., & Salous, S. (2017). Spectrum occupancy modeling using ARIMA. IEEE Access.
12. Saleem, Y., & Rehmani, M. H. (2017). Primary user modeling in cognitive radio networks. Journal of Network and Computer Applications.
13. Shanmugavel, S., & Bhagyaveni, M. A. (2020). Detecting spread-spectrum PU using hopping pattern prediction. Journal of Communications.
14. Fragkiadakis, A. G., et al. (2013). A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys & Tutorials.
15. Ramani, M., & Sharma, V. (2016). Location verification for PUE attack detection. IEEE Trans. Vehicular Technology.
16. Afolabi, I., et al. (2018). RF fingerprinting for device authentication. Wireless Networks.
17. Kar, S., et al. (2015). Trust-based spectrum sensing in CRNs. Computer Communications.
18. Sharma, V., & Bohara, V. A. (2017). Genetic algorithm-based resource allocation in CRNs. AEU - Int. J. Electronics and Communications.
19. Tumuluru, V. K., et al. (2012). Neural network-based spectrum prediction. IEEE Transactions.
20. Kim, H., & Choi, K. (2018). Q-learning for dynamic spectrum access in vehicular networks. IEEE Access.
21. Koushik, R., et al. (2021). Transfer learning for fast CR adaptation. Elsevier Ad Hoc Networks.
22. Wei, L., et al. (2020). Spectrum sensing as a service in vehicular cloud networks. IEEE Internet of Things Journal.