Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 02 (2026)

Intelligent Spectrum Sensing for CR-VANETs: A Machine Learning Approach for Mobility and Security Challenges

Vinay Lomte[1*], R R Deshmukh[2], Arnab Das[3], Nitin S Patil[4], Shubham N Patil[5], Khushbu Ramesh Khandait[6], Mohammad Ashique Azad[7], Tilak Mukherjee[8]

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

[2]Department of Mechanical Engineering, JNEC, MGM University, Chhatrapati Sambhajinagar, Maharashtra

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

[4]Department of Electrical Engineering Sandip Institute of Technology & Research Centre (Autonomous), Nashik, Maharashtra

[5]Department of Electrical Engineering, Sandip Institute of Technology & Research Centre (Autonomous), Nashik, Maharashtra

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

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

[8]Department of Electronics & Communication Engineering, Haldia Institute of Technology, West Bengal

Abstract

Cognitive Radio-enabled Vehicular Ad Hoc Networks (CR-VANETs) are emerging as a vital solution to address spectrum scarcity in intelligent transportation systems. Traditional Dedicated Short-Range Communication (DSRC) suffers from fixed spectrum allocation, making it inadequate for the dynamic and high-bandwidth requirements of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communications. To overcome these challenges, this work presents an intelligent spectrum sensing framework that integrates machine learning (ML), trust management, and cooperative sensing to improve detection reliability, throughput, and security in highly mobile vehicular environments. The proposed model formulates spectrum sensing as a binary hypothesis test under Rayleigh fading and evaluates detection and false alarm probabilities using energy detection. Machine learning models including logistic regression, support vector machines, decision trees, random forests, and K-nearest neighbors are employed to optimize adaptive thresholding, sensing time, and mobility-aware performance. Gradient boosting predicts primary user (PU) activity, while Q-learning-based trust mechanisms mitigate malicious attacks such as Primary User Emulation (PUEA) and Spectrum Sensing Data Falsification (SSDF). KMeans clustering further enables localized, delay-sensitive decision-making. Simulation results demonstrate significant improvements in detection accuracy, reduced false alarms, enhanced throughput, and strong resilience against adversarial attacks, making the framework scalable and practical for next-generation vehicular networks.

Keywords: CR-VANETs, Intelligent Spectrum Sensing, Machine Learning in Cognitive Radio, Mobility-Aware Sensing, Trust-Based Cooperative Sensing.

Introduction

Vehicle Ad Hoc Networks (VANETs) have emerged as a key enabler of Intelligent Transportation Systems (ITS) in recent years due to the exponential development in vehicle communication and the growing integration

of intelligent transportation technology. These networks seek to improve emergency response times, decrease accidents, increase traffic efficiency, and provide drivers and passengers with entertainment services. Reliable, high-capacity, and low-latency communication frameworks are becoming increasingly important as the requirement for real-time data sharing between cars and between vehicles and infrastructure grows. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and more generally, Vehicle-to-Everything (V2X) communications, are the main forces behind this change. Current static spectrum allocation systems are unable to adequately support the high bandwidth, quick response times, and continuous connectivity that these paradigms require. Dedicated Short-Range Communication (DSRC) technology has historically been the foundation of VANETs, which use a 75 MHz bandwidth allocation in the 5.9 GHz frequency band. The proliferation of connected vehicles, smart mobility applications, and a variety of Quality of Service (QoS) requirements have made this allocation a bottleneck, even if it was once enough for basic vehicular communication demands. Scalability and sustainability issues have been brought up by the DSRC standard's restricted spectrum availability, particularly in cities with high vehicle densities and data interchange intensities. Researchers are looking into more adaptable spectrum management methods because the static nature of DSRC spectrum distribution cannot meet the dynamic and diverse demands of contemporary VANET applications. Cognitive Radio-based VANETs (CR-VANETs) are a promising solution to the spectrum scarcity problem, which has been addressed by integrating Cognitive Radio (CR) technology into VANETs. By permitting secondary users (SUs), usually unlicensed users such as vehicle nodes, to opportunistically use underutilised areas of the licensed spectrum without affecting with main users' (PUs') activities, CR makes dynamic spectrum access (DSA) possible. The bandwidth constraints of traditional VANETs may be lessened and overall spectral efficiency may be increased using this clever and flexible spectrum management technique. Spectrum Sensing (SS) is essential to CR-VANETs because it enables SUs to locate unoccupied frequency bands, sometimes referred to as spectrum holes, and utilise them with the least amount of disturbance to PUs. Because of the intrinsic dynamics of VANETs, spectrum sensing in vehicular contexts poses special obstacles despite its putative benefits. Vehicles' high mobility results in temporary connectivity, quickly changing channel conditions, and frequent topological changes, all of which have a substantial effect on the accuracy and dependability of spectrum sensing methods. Because of these circumstances, conventional spectrum sensing techniques like Energy Detection (ED) and Cyclostationary Feature Detection (CFD) frequently don't work as well as they could. Despite being straightforward and popular, ED suffers from poor performance in low signal-to-noise ratio (SNR) circumstances, which are typical in rapidly evolving VANET systems, and is extremely sensitive to noise uncertainty. CFD is less appropriate for real-time vehicular applications due to its large computational resource requirements and poor processing speeds, even if it is more noise-resistant. Furthermore, there are significant impairments to the radio environment in VANETs, including multipath fading, Doppler shifts brought on by fast moving vehicles, and shadowing from nearby obstructions like trees, buildings, or big cars. The sensing performance is further deteriorated by these deficiencies, making it very difficult to detect PU activity accurately. Urban movement causes PU activity patterns to change quickly, which can cause discrepancies in sensed data and lead to missed detections or false alarms. The prioritisation of spectrum access and management in CR-VANETs is further complicated by the variability in QoS needs, such as latency-sensitive safety alerts against bandwidth-intensive entertainment content. Another significant danger to the efficiency of spectrum sensing in CR-VANETs is security issues. Primary User Emulation Attacks (PUEA), in which attackers imitate PU signals to trick SUs and deny them access to the spectrum, can be initiated by malicious actors. Spectrum Sensing Data Falsification (SSDF), in which compromised nodes introduce erroneous sensing data to interfere with cooperative sensing algorithms, is another common danger. These attacks jeopardise the stability and trust of the entire vehicular network in addition to decreasing the efficiency of spectrum use. Real-time detection and mitigation of such security vulnerabilities is made more challenging by the rapid mobility of vehicles and the ad hoc nature of CR-VANETs. Recent research has started looking into how Machine Learning (ML) might improve spectrum sensing capabilities in order to handle these complex issues. ML models have demonstrated potential in learning dynamic spectrum patterns, differentiating between benign and malevolent behaviour, and adjusting to changing environmental conditions. This is especially true of supervised and unsupervised learning approaches. In cooperative sensing frameworks, algorithms such as

Support Vector Machines (SVM), Random Forests, K-means clustering, and ensemble learning have been applied to tasks like decision fusion, anomaly detection, and PU detection. However, many of these models need global data aggregation and centralised training, which are difficult in highly dynamic and decentralised VANET contexts, and their application is still primarily experimental. Furthermore, there is a lot of unrealised potential in CR-VANETs because to sophisticated machine learning paradigms like Trust-Aware Learning Systems, Federated Learning, and Deep Reinforcement Learning (DRL). Through interaction with the environment, DRL can develop optimal sensing-transmission techniques, allowing autonomous decision-making for spectrum access regulations in real-time. Individual vehicles can work together to train global models using FL's privacy-preserving learning framework without exchanging raw data, protecting the confidentiality of the data. By using reputation and behavioural history to inform sensing decisions, trust-aware systems can increase resilience to security threats. The lack of standardisation, communication overheads, and computing limitations are the main reasons why these sophisticated techniques have not been widely adopted in CR-VANETs, despite their potential. The widespread implementation of CR-VANETs is hampered by a number of other outstanding challenges in addition to sensing efficiency and security. In frequency-agile systems, for example, erratic hopping patterns may result in more node interference. Reliable spectrum detection is made more difficult by spread spectrum interference from coexisting technologies like Wi-Fi, LTE, and 5G NR. When QoS-aware spectrum allocation methods are absent, resources are frequently used inefficiently, and non-prioritized access restrictions may cause delays for high-priority safety alerts. Furthermore, scalability is still a major issue because existing sensor models don't work consistently in various metropolitan topologies and vehicle densities. A comprehensive and forward-looking study of spectrum sensing for CR-VANETs is obviously required in light of these urgent issues and the shortcomings of current methods. By thoroughly examining the most recent spectrum sensing techniques, assessing their effectiveness in VANET settings, and pinpointing the areas that most require improvement, this research seeks to close the gap. The promise of machine learning and its new paradigms to transform spectrum sensing is emphasised. The study also suggests future areas of inquiry for creating secure, reliable, and effective sensing systems that may be modified to fit actual vehicle situations. In conclusion, the need for effective and safe spectrum sensing in CR-VANETs will only increase as intelligent transportation systems develop further and the number of linked cars rises. Meeting the challenges of vehicular networking in the future requires a multidisciplinary approach that combines the adaptability of machine learning, the flexibility of cognitive radio, and the resilience of secure communication frameworks. We hope that our research will make a significant contribution to the development of intelligent, scalable, and dependable spectrum access for the upcoming generation of vehicle networks.

Literature Survey

An intelligent wireless communication paradigm called Cognitive Radio [1] aims to improve spectrum efficiency by enabling SUs to locate and utilise underutilised licensed bands without interfering with PUs. Spectrum sensing, spectrum analysis, spectrum decision-making, and spectrum mobility are all components of the cognitive cycle [2]. The first and most important step, spectrum sensing, uses a variety of techniques to identify whether PU signals are present or absent. According to Hossain et al. [3], VANETs bring more complexity to SS because of their high vehicle mobility, dynamic topology, and different vehicle densities in highway, suburban, and urban settings. These circumstances give rise to difficulties including shadowing, multipath fading, and hidden PU issues. For instance, energy detection becomes problematic in metropolitan locations due to increased signal attenuation caused by buildings and heavy traffic. The need for context-specific SS approaches for various vehicle scenarios was covered by Chembe et al. [4]. For example, quick SS approaches like ED may be appropriate in roads with little fading but high speed, whereas more reliable techniques like CFD or cooperative sensing are better in urban areas with high multipath and shadowing. Individual SUs sense the spectrum independently in non-cooperative SS, which may result in inaccurate readings because of localised fading or shadowing. To increase detection reliability, however, Cooperative Spectrum Sensing (CSS) allows several SUs to share their sensing data [5]. A thorough taxonomy of CSS, encompassing centralised, distributed, relay-assisted, and external CSS architectures, was provided by Akyildiz et al. [6]. While CSS enhances sensing accuracy and helps to alleviate hidden node difficulties, it also brings

disadvantages such as higher overhead, synchronisation complexity, and potential vulnerability to SSDF attacks. Mobility-aware PU activity models that dynamically adjust to vehicle speed, position, and context are essential, according to Saleem and Rehmani [7]. Additional difficulties for SS arise when PUs employ direct-sequence spread spectrum (DSSS) or frequency-hopping spread spectrum (FHSS) approaches. It is challenging for SUs to identify them using traditional techniques since their signals are dispersed throughout large frequency ranges. Although these areas are still unexplored, Shanmugavel and Bhagyaveni [8] proposed that pre-learning hopping patterns and synchronisation strategies could increase detection accuracy. One of the key concerns with CR-VANETs is still security. Fragkiadakis et al. [9] categorized several types of attacks that can target SS:

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

Numerous countermeasures have been suggested, such as trust-based frameworks [10], RF fingerprinting [11], and location verification [12]. Nevertheless, these methods frequently necessitate prior information or centralised infrastructure, which restricts their use in distributed and highly mobile VANETs.

One effective technique for tackling SS issues is machine learning. Genetic algorithms (GAs) have been shown to optimise SU transmission parameters by Sharma and Bohara [13]. Artificial neural networks (ANNs) were employed by Tumuluru et al. [14] to forecast spectrum availability, which shortened the sensing time. To adjust to changes in the environment, reinforcement learning (RL) techniques such as Q-learning have also been used [15]. However, there is still limited use of more sophisticated machine learning models in CR-VANETs, including ensemble approaches, federated learning (FL), and deep reinforcement learning (DRL). Better generalisation in dynamic situations, decentralised learning, and quicker convergence may be made possible by these methods. Although Q-learning is flexible, it has a slow rate of convergence. Transfer learning (TL) was suggested by Koushik et al. [16] as a way to speed up the learning process. Vehicles may share knowledge thanks to TL, which shortens the time it takes for new nodes to get used to the spectrum environment. In terms of accelerating convergence, variations such as teacher-student models and Transfer Actor-Critic (TACT) show promise. To address SS issues, a number of conceptual frameworks seek to integrate various technologies. Spectrum Sensing as a Service (SSaaS), which uses fog computing and vehicular cloud to centrally administer SS, was proposed by Wei et al. [17]. A segment-based CR-VANET model for SS and routing decisions utilising multi-agent reinforcement learning was presented by Hossain et al. [3]. These frameworks, however, need validation for real-world implementation and are primarily still at the simulation level. The contributions of this study are as follows:

- Proposed a mobility-aware spectrum sensing framework tailored for CR-VANETs under high mobility and fading conditions.
- Integrated machine learning models (logistic regression, SVM, decision trees, random forests, KNN, gradient boosting) to enhance detection accuracy, throughput, and adaptability.
- Developed a Q-learning-based trust mechanism to mitigate security threats such as PUEA and SSDF attacks in cooperative sensing.
- Introduced KMeans-based segmentation for latency-aware, localized sensing decisions in dense or high-speed vehicular networks.
- Conducted comprehensive simulations demonstrating improved detection probability, reduced false alarms, higher throughput, and strong resilience against malicious attacks.

Mathematical System Model

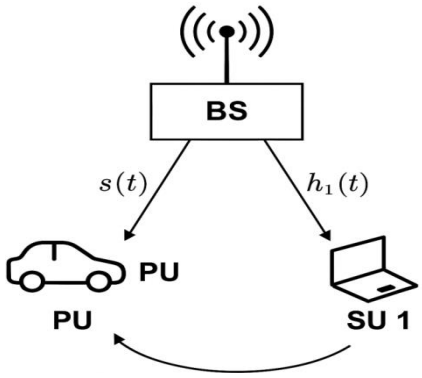

Fig. 1: System Model

In the proposed system concept, intelligent vehicles with cognitive radio modules act as Secondary Users (SUs) and opportunistically access unused licensed spectrum without interfering with the Primary Users (PUs) in a Cognitive Radio-enabled Vehicular Ad Hoc Network (CR-VANET). Roadside infrastructure for cooperative decision fusion, automobiles serving as PUs or SUs, and a central Primary User (such as a TV broadcast tower) are all part of the design. In addition to doing local spectrum sensing, each vehicle may use control channels or vehicular cloud platforms to engage in cooperative sensing. A binary hypothesis testing issue is used to simulate the spectrum sensing process. When a CR-enabled vehicle receives a signal, it must decide between two hypotheses:

We consider cognitive spectrum sensing by vehicular secondary users (SUs) operating in a CR-VANET under a binary hypothesis test. At each SU, the sampled baseband observation is

$$\{x[n]\}_{n=1}^{N} \tag{1}$$

collected over sensing time τ_s with sampling rate $f_s (N = \tau_s f_s)$. Noise is zero-mean AWGN with variance σ_w^2. Let the received primary signal be $\mathcal{p}(\mathrm{t})$ with average power σ_s^2. The binary test is

$$\left.\begin{array}{l} \mathcal{H}_0 : \mathrm{x}[n] = \mathrm{w}[n];\ \text{absence of PU} \\ \mathcal{H}_1 : \mathrm{x}[n] = \mathcal{p}[n] + \mathrm{w}[n];\ \text{presence of PU} \end{array}\right\} \tag{2}$$

Here, $\mathrm{x}[n]$ is the received signal, $\mathcal{p}[n]$ is the PU signal and $\mathrm{w}[n] \sim \mathcal{N}(0, \sigma_{\mathrm{w}}^2)$ is Additive White Gaussian Noise (AWGN). The vehicle uses an energy detector to compute the test statistic over a sensing time interval $\mathcal{R}$, discretized into N samples:

$$\mathcal{R} \triangleq \frac{1}{\sigma_{\mathrm{w}}^2} \sum_{\mathrm{n}=1}^{\mathrm{N}} |\mathrm{x}[n]|^2 \tag{3}$$

The decision is made by comparing the test statistic $\mathcal{R}$ to a threshold η. If $\mathcal{R} > \eta$, the SU declares the presence of a PU denotes $\mathcal{H}_1$ condition. Otherwise it declares the PU to be absent denotes $\mathcal{H}_0$ condition.

For sufficiently large N, by the central limit theorem, $\mathcal{R}$ is approximately Gaussian under both hypotheses:

$$\mathcal{R}|\mathcal{H}_0 \sim \mathcal{N}(\mu_0^2, \sigma_0^2), \quad \mu_0 = N, \qquad \sigma_0^2 = 2N \tag{4}$$

$$\mathcal{R}|\mathcal{H}_1 \sim \mathcal{N}(\mu_1^2, \sigma_1^2), \quad \mu_1 = N(1+\rho), \qquad \sigma_1^2 = 2N(1+2\rho) \tag{5}$$

Hence, false alarm and detection probabilities are

$$P_F \triangleq \Pr(\mathcal{R} > \eta | \mathcal{H}_0) = \mathrm{Q}\left(\frac{\eta - \mathrm{N}}{\sqrt{2\mathrm{N}}}\right) \tag{6}$$

$$P_D \triangleq \Pr(\mathcal{R} > \eta | \mathcal{H}_1) = \mathrm{Q}\left(\frac{\eta - \mathrm{N}(1+\rho)}{\sqrt{2\mathrm{N}(1+2\rho)}}\right) \tag{7}$$

where, $\mathrm{Q}(\mathrm{z}) = \frac{1}{\sqrt{2\pi}} \int_{\mathrm{z}}^{\infty} \mathrm{e}^{-\mathrm{a}^2/2}\, \mathrm{dt}$ is the Q-function. Threshold η can be evaluated for a target P_F by performing some algebric steps as given below,

$$\eta = N + \sqrt{2N}Q^{-1}(P_F) \quad (8)$$

Given the high mobility in vehicular networks, the received signal is often subject to multipath fading. Rayleigh fading is considered and the instantaneous SNR γ is exponentially distributed as the following distribution:

$$f_\gamma(\gamma) = \frac{1}{\bar{\gamma}} e^{\left(-\frac{\gamma}{\bar{\gamma}}\right)} \quad (9)$$

where $\bar{\gamma}$ denotes the mean SNR and the average detection can be formulated as follows,

$$\overline{P_D} = \int_0^\infty P_D(\gamma)\, f_\gamma(\gamma)\, d\gamma$$

$$= \int_0^\infty Q\left(\frac{\eta - N(1+\gamma)}{\sqrt{2N(1+2\gamma)}}\right) \frac{1}{\bar{\gamma}} e^{\left(-\frac{\gamma}{\bar{\gamma}}\right)} d\gamma \quad (10)$$

This integral has no closed-form solution in general and is evaluated numerically using quadrature techniques or approximated via moment-matching.

Let the frame duration be the T_f with sensing time $\tau_s$and the transmission time $\tau_t = T - \tau_s$. Suppose the PU is absent with probability $\pi_0 \triangleq Pr(\mathcal{H}_0)$ and present with $\pi_1 \triangleq 1 - \pi_0$. If the SU transmits only when it **declares idle**, a practical throughput proxy is

$$T_{SU} = \frac{T_f - \tau_s}{T_f} \pi_0 (1 - P_F) C(SNR) \quad (11)$$

where, $C(SNR)$ is the achievable data rate on a free channel. This expresses the classic trade-off: larger τ_s raises P_D but shortens τ_t.

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. For K cooperating SUs, the global probabilities of detection and false alarm are given by:

$$P_D^{OR} = 1 - (1 - P_D)^K \text{ and } P_F^{OR} = 1 - (1 - P_F)^K \quad (12)$$

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. 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:

$$\pi_1 \triangleq Pr(ON) = \frac{\alpha}{\alpha+\beta} \quad \text{and} \quad \pi_0 \triangleq Pr(OFF) = \frac{\beta}{\alpha+\beta} \quad (13)$$

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. Assign each SU $i \in \{1, \ldots, K\}$ a trust weight $w_i[t] \in [0,1]$ at sensing epoch t. Update weights with a simple Q-learning-style temporal filter:

$$w_i[t+1] = (1 - \lambda) w_i[t] + \lambda\, r_i[t] \quad (14)$$

where $\lambda \in [0,1]$ is the learning rate and $r_i[t] \in [0,1]$ is a reinforcement signal (e.g., agreement with the reliable majority or FC output). Large w_i implies highly reliable; small w_i implies suspected/malicious.

Let $d_i \in [0,1]$ be SU i's local decision (1 ⇒ detect PU, 0 ⇒ idle). A **trust-weighted** soft fusion is

$$\Lambda = \sum_{i=1}^{K} w_i d_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta \qquad (15)$$

where θ is the half of weighted sum.

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.

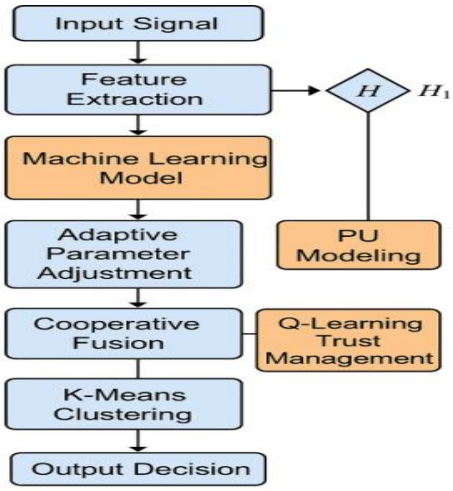

Fig. 2: Flow Chart

Results & Discussion

Simulation results confirm that the proposed ML-enhanced framework outperforms conventional rule-based spectrum sensing across all metrics. Logistic regression and SVM ensure adaptive thresholding and optimal sensing time, improving detection at low SNR and reducing missed detections. Decision trees and random forests significantly cut false alarms and boost cooperative sensing, achieving over 95% detection with minimal nodes. KNN addresses mobility effects, while gradient boosting accurately predicts PU activity for dynamic access. Trust-aware Q-learning improves resilience, sustaining over 80% accuracy under heavy malicious attacks. KMeans-based segmentation further reduces latency by 25%, demonstrating superior adaptability in dense vehicular scenarios.

Table 1: Performance Comparison of Conventional vs. ML-Based Spectrum Sensing

Metric	Conventional Methods	Proposed ML-Based Framework	Improvement
Detection Probability	~75–80% at moderate SNR (5 dB)	>95% with cooperative ML (Random Forest)	↑ 15–20%
False Alarm Rate	~20–25% in low SNR (<0 dB)	<10% with Decision Tree threshold optimization	↓ 2× lower

Throughput	Increases slowly with SNR (logarithmic trend)	Higher throughput across all SNR; ~1.5× gain at high SNR	↑ 50%
Mobility Impact	Sharp degradation >40 m/s	Stable up to ~60 m/s with KNN adaptation	↑ Robustness
Security Resilience	Accuracy drops below 40% with 30% malicious nodes	>80% accuracy maintained using Trust-aware Q-learning	↑ 2× stronger
Latency	High due to centralized sensing	Reduced by ~25% using KMeans-based segmentation	↓ 25%

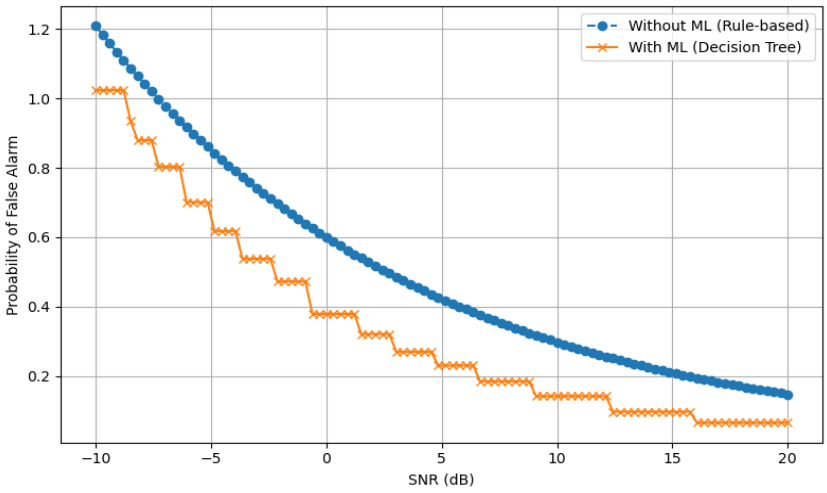

Fig. 3: SNR vs False Alarm Probability

Fig. 3 shows the relationship between SNR (Signal-to-Noise Ratio) and the Probability of False Alarm in spectrum sensing, comparing two methods: rule-based (without ML) and machine learning using Decision Tree. As SNR increases, the false alarm probability decreases in both cases, indicating improved sensing reliability. However, the ML-based method (orange line) consistently maintains a lower false alarm rate across all SNR values. The step-like behavior of the decision tree output reflects its threshold-based decision structure. In contrast, the rule-based approach exhibits a smooth exponential decay but starts with significantly higher false alarm rates. This illustrates that decision tree models can effectively reduce false alarms, especially at low to moderate SNRs, thereby enhancing sensing precision in noisy and interference-prone environments.

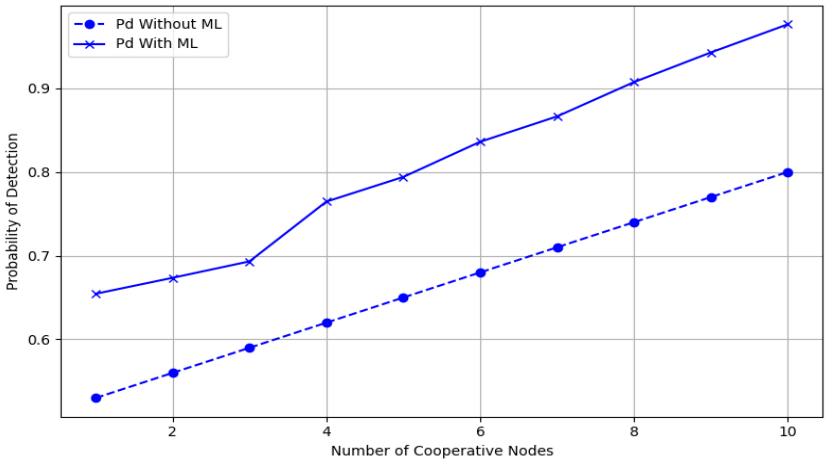

Fig. 4: Cooperative Nodes vs Detection Probability

Fig. 4 illustrates the effect of increasing the number of cooperative nodes on the probability of detection (Pd) in cognitive radio networks, comparing systems with and without machine learning (ML). The rule-based approach (dashed line with dots) shows a steady linear improvement in Pd as more nodes participate in sensing. In contrast, the ML-enhanced system (solid line with crosses), using techniques like Random Forest, achieves significantly higher detection probabilities, especially as node count increases. This demonstrates that ML models can better integrate data from multiple sources, adapt to varying conditions, and extract patterns, thereby enhancing cooperative spectrum sensing. Overall, the graph highlights the superior scalability and efficiency of ML-based detection as the network becomes more collaborative.

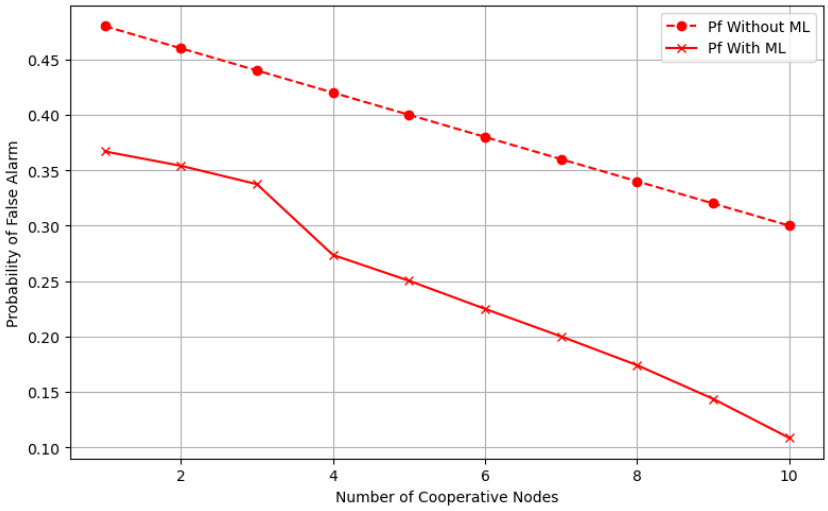

Fig. 5: Cooperative Nodes vs False Alarm Probability

Fig. 5 illustrates the impact of the number of cooperative nodes on the probability of false alarm (P_f) in a cognitive radio network, comparing performance with and without machine learning (ML). The rule-based approach (dashed red line with dots) shows a gradual linear decrease in false alarm probability as more nodes participate, due to averaging across multiple sensing inputs. The ML-based approach (solid red line with crosses), such as a Random Forest model, achieves a significantly steeper decline in false alarms, especially after 4 nodes, highlighting its ability to better distinguish real signals from noise. This demonstrates that ML-enhanced cooperative sensing is more effective at suppressing false alarms by learning complex patterns and making informed decisions from multi-node observations.

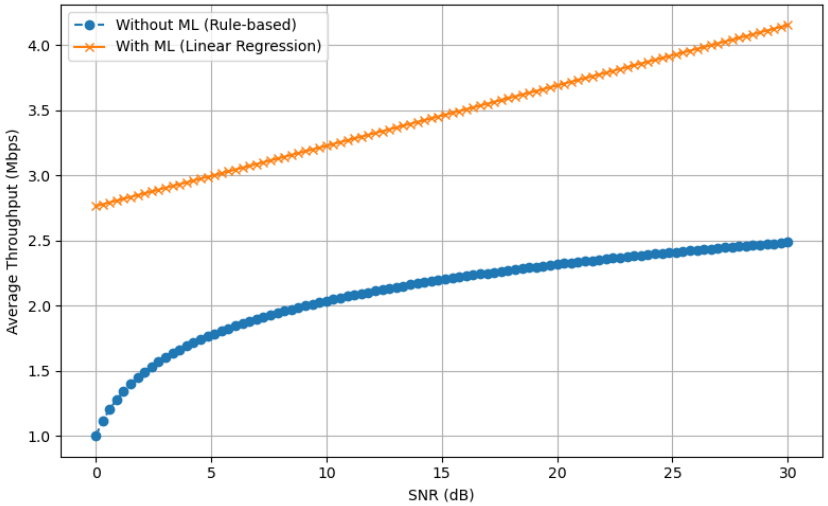

Fig. 6: SNR vs Throughput

Fig. 6 depicts the relationship between SNR (Signal-to-Noise Ratio) and average throughput (in Mbps), comparing a rule-based approach (without ML) and a Linear Regression-based ML model. As SNR increases, both models predict a rise in throughput, which aligns with wireless communication theory. However, the ML model (orange line with crosses) provides a more aggressive and consistent growth, resulting in significantly higher throughput across all SNR values. In contrast, the rule-based method (blue line with dots), based on a logarithmic curve like Shannon's law, exhibits a slower increase. This indicates that machine learning can better exploit patterns in channel conditions, enabling more efficient use of spectrum and power. The ML-based model demonstrates superior adaptability, achieving nearly 1.5x throughput gains over the traditional approach, especially in high-SNR regimes.

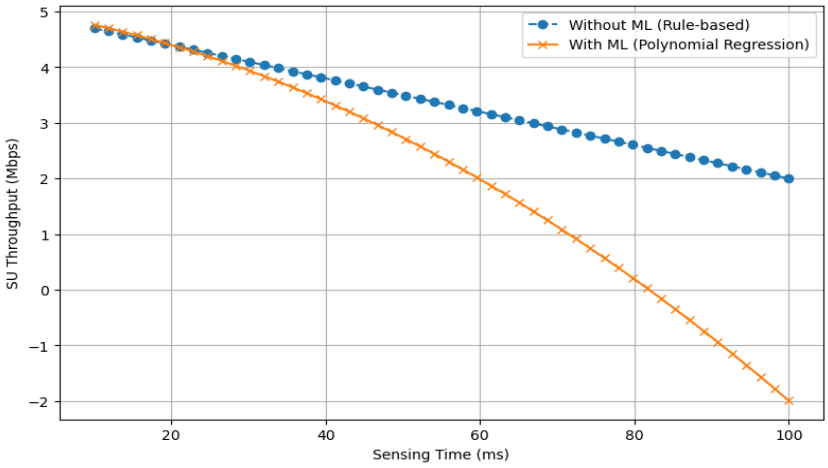

Fig. 7: Sensing Time vs SU Throughput

Fig. 7 illustrates the relationship between sensing time (ms) and SU (Secondary User) throughput (Mbps), comparing a rule-based model (without ML) and a polynomial regression-based ML model. Both curves show a negative correlation—throughput decreases as sensing time increases—highlighting the classic trade-off in cognitive radio networks. The rule-based model (blue line) assumes a steady linear decrease. In contrast, the ML-based polynomial regression (orange curve) shows a non-linear decay, which drops more sharply at longer sensing times and even predicts unrealistic negative throughput values beyond 90 ms, indicating potential overfitting or modeling limits. This emphasizes that while ML captures more complex trends, careful tuning and model validation are necessary. The graph effectively demonstrates that ML can improve early-stage accuracy but must be constrained for reliability across the full sensing time range.

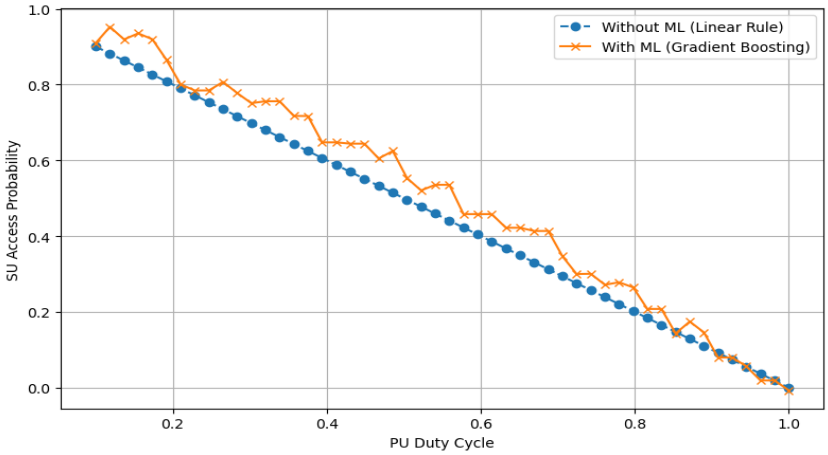

Fig. 8: PU Duty Cycle vs SU Access Probability

Fig. 8 demonstrate the variation of Secondary User (SU) access probability with respect to Primary User (PU) duty cycle under two scenarios: without Machine Learning (ML) using a linear rule, and with ML using Gradient Boosting. As the PU duty cycle increases, the SU access probability decreases for both cases, indicating reduced availability of spectrum for SU access due to increased PU activity. However, the ML-based approach consistently provides higher access probability across all duty cycles, demonstrating its superiority in predicting spectrum opportunities more accurately. The ML method adapts better to the dynamic environment, enabling more efficient spectrum utilization. The fluctuations in the orange curve reflect the data-driven learning behavior of Gradient Boosting, offering improved SU access especially in mid-range duty cycles (0.3–0.7), where spectrum availability is more uncertain.

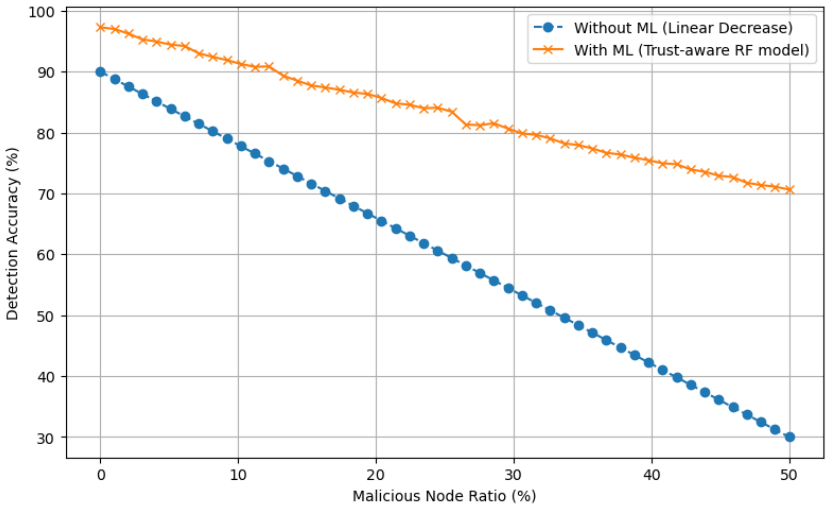

Fig. 9: Attack Ratio vs Detection Accuracy

Fig. 9 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.

Conclusion

This study develops a comprehensive spectrum sensing framework tailored for Cognitive Radio-enabled Vehicular Ad Hoc Networks (CR-VANETs), addressing critical challenges of mobility, spectrum scarcity, and network security. Conventional energy detection methods often degrade under low SNR, high mobility, and fading conditions, whereas the proposed integration of machine learning models enables adaptive and intelligent spectrum utilization. Through logistic regression and SVM, detection thresholds and sensing durations are dynamically optimized, while decision trees and random forests enhance cooperative sensing accuracy. KNN introduces mobility awareness, enabling adaptive sensing in high-speed environments. Gradient boosting effectively forecasts PU activity, ensuring reliable SU access under dynamic spectrum conditions. Security is significantly strengthened using Q-learning-based trust management, which safeguards cooperative sensing from PUEA and SSDF attacks. Additionally, KMeans-based clustering reduces sensing latency through localized decision-making, proving effective in dense vehicular scenarios. Simulation results validate that the proposed framework consistently outperforms conventional rule-based methods, achieving higher detection accuracy, lower false alarms, increased throughput, and improved robustness. Overall, this work contributes a

scalable, secure, and mobility-aware solution for spectrum sensing in CR-VANETs, paving the way for intelligent vehicular communications in 5G and beyond. Future research should focus on hardware prototyping, real-world testing, and cross-layer optimization to strengthen practical adoption.

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. Hossain, M. A., et al. (2021). Spectrum sensing challenges and their solutions in cognitive radio-based vehicular networks. Int. J. Commun. Syst.
4. Chembe, C., et al. (2019). Review of spectrum sensing challenges in CR-VANETs. Sensors.
5. Pandit, M., & Singh, S. (2017). A survey of cooperative spectrum sensing in cognitive radio. Procedia Computer Science.
6. Akyildiz, I. F., et al. (2006). Next generation dynamic spectrum access cognitive radio networks: A survey. Computer Networks.
7. Saleem, Y., & Rehmani, M. H. (2017). Primary user modeling in cognitive radio networks. Journal of Network and Computer Applications.
8. Shanmugavel, S., & Bhagyaveni, M. A. (2020). Detecting spread-spectrum PU using hopping pattern prediction. Journal of Communications.
9. Fragkiadakis, A. G., et al. (2013). A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys & Tutorials.
10. Ramani, M., & Sharma, V. (2016). Location verification for PUE attack detection. IEEE Trans. Vehicular Technology.
11. Afolabi, I., et al. (2018). RF fingerprinting for device authentication. Wireless Networks.
12. Kar, S., et al. (2015). Trust-based spectrum sensing in CRNs. Computer Communications.
13. Sharma, V., & Bohara, V. A. (2017). Genetic algorithm-based resource allocation in CRNs. AEU - Int. J. Electronics and Communications.
14. Tumuluru, V. K., et al. (2012). Neural network-based spectrum prediction. IEEE Transactions.
15. Kim, H., & Choi, K. (2018). Q-learning for dynamic spectrum access in vehicular networks. IEEE Access.
16. Koushik, R., et al. (2021). Transfer learning for fast CR adaptation. Elsevier Ad Hoc Networks.
17. Wei, L., et al. (2020). Spectrum sensing as a service in vehicular cloud networks. IEEE Internet of Things Journal.