Harmonic Trust Spectrum Modeling for Cognitive Radio Intrusion Detection

S. Jeyaseelan[1], P.G.S. Velmurugan[1], G. Prabhakar[1], and J. Shanthi[2]

[1] *Thiagarajar College of Engineering, Madurai, India,*
[2] *Kamaraj College of Engineering and Technology, Virudhunagar, India*

https://doi.org/10.26636/jtit.2026.3.2747

Abstract — Cognitive radio networks (CRNs) are highly vulnerable to spectrum spoofing, PU emulation (PUE), and harmonic RF manipulation attacks, which significantly degrade dynamic spectrum access reliability and communication security. This paper proposes a harmonic trust spectrum modeling framework for cognitive radio intrusion detection using multi-domain RF intelligence and adaptive machine learning. The proposed system integrates harmonic spectrum analysis, trust oscillation modeling, spectral entropy analysis, wavelet decomposition, and power spectral density (PSD) characterization to detect anomalous RF behaviors. Three heterogeneous RF datasets were used for experimental evaluation: the RadioML 2016.10A modulation dataset, the Oracle RF fingerprinting IQ dataset, normal signals generated by GNU Radio, and malicious PUE RF signals. The proposed methodology extracts advanced harmonic trust features including spectral entropy, spectral flatness, harmonic trust instability index (HTII), and oscillatory trust divergence (OTD), which are subsequently processed using an adaptive XGBoost-based intrusion detection system. Experimental results demonstrate that malicious RF users exhibit significantly higher spectral instability, irregular harmonic distributions, elevated entropy behavior, and oscillatory trust divergence, compared to legitimate users. Furthermore, studies covering fast Fourier transform (FFT) harmonic spectra, PSD analysis, wavelet coefficient analysis, trust oscillation curves, and confusion matrix evaluations confirm the effectiveness of the proposed framework. The proposed harmonic trust spectrum model provides a computationally efficient and scalable solution for next-generation secure cognitive radio communications and RF cyber defense systems.

Keywords — cognitive radio networks, harmonic trust modeling, intrusion detection system, PU emulation, XGBoost

1. Introduction

Cognitive radio networks (CRNs) have emerged as a promising solution for overcoming spectrum scarcity and improving wireless spectrum utilization through intelligent and dynamic spectrum access mechanisms. Traditional fixed spectrum allocation policies often lead to inefficient spectrum usage, as a part of licensed frequency bands remains underutilized, while unlicensed users experience severe bandwidth limitations. Cognitive radio (CR) technology addresses this issue by allowing secondary users to opportunistically access vacant spectrum bands without causing interference to PUs (PU) [1], [2].

Spectrum sensing plays a critical role in CRN environments, since accurate detection of PU activity directly affects communication reliability, spectrum efficiency, and network security. Several spectrum detection techniques, such as energy detection, cyclostationary feature detection, matched filtering, and wavelet-based sensing have been extensively investigated recently [3], [4]. Among these approaches, deep learning and deep learning-based spectrum sensing techniques have gained significant attention due to their ability to learn complex RF patterns and improve detection performance in noisy and dynamic wireless environments [5]–[7].

Despite these advances, CRNs remain highly vulnerable to malicious attacks, particularly PU emulation (PUE), spectrum spoofing, and RF impersonation. In PUE attacks, malicious users mimic the characteristics of PUs to illegally occupy spectrum resources and disrupt normal communication behaviors. These attacks degrade the reliability of spectrum sensing, reduce spectrum utilization efficiency, and compromise the security of intelligent wireless communication systems [1], [3], [8]. Moreover, traditional energy-based sensing techniques are often insufficient for identifying sophisticated harmonic spoofing behaviors, as attackers are capable of imitating legitimate RF signatures with a high degree of accuracy.

Recent studies have explored advanced signal processing approaches including wavelet decomposition, empirical mode decomposition, compressive sensing, and cyclostationary analysis to improve spectrum sensing robustness [9], [10], [11]. Matched filter detection techniques with adaptive thresholds have also demonstrated improved sensing accuracy in dynamic wireless environments [2], [12]. However, existing approaches focus primarily on conventional spectrum occupancy detection and often neglect harmonic trust behavior, oscillatory RF instability, and spectral divergence patterns associated with malicious RF users.

To mitigate these limitations, this paper proposes a novel harmonic trust spectrum modeling (HTSM) framework for CR intrusion detection. The proposed approach integrates harmonic RF analysis, trust oscillation modeling, spectral entropy characterization, wavelet decomposition, and adaptive machine learning techniques to distinguish legitimate spectrum users from malicious PUE attackers.

The overall architecture of the proposed HTSM framework is illustrated in Fig. 1.

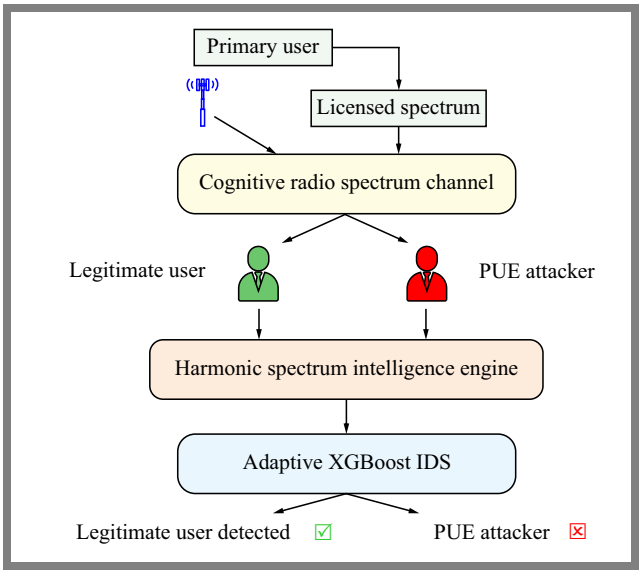

Fig. 1. System architecture of the proposed HTSM framework.

As shown in Fig. 1, the licensed spectrum is initially occupied by the PU, while both legitimate secondary users (SUs) and malicious PUE attackers attempt to access the CR channel. The observed RF transmissions are collected by a spectrum monitoring node and forwarded to the harmonic spectrum intelligence engine for spectral feature extraction. The extracted trust-aware harmonic features are subsequently processed by an adaptive XGBoost-based intrusion detection system to identify legitimate spectrum access and malicious spectrum spoofing activities.

The proposed framework introduces two novel metrics, i.e. harmonic trust instability index (HTII) and oscillatory trust divergence (OTD), for quantifying spectral instability and malicious oscillatory divergence in RF trust behavior. HTII measures the harmonic instability of RF spectral distributions, while OTD evaluates the divergence between legitimate and malicious trust harmonics across frequency-domain representations. These metrics enable an accurate characterization of spoofed RF behavior and enhance intrusion detection performance in CRN environments.

To validate the effectiveness of the proposed framework, experiments were conducted using three heterogeneous RF data sets. An experimental analysis focusing on fast Fourier transform (FFT), power spectral density (PSD), wavelet analysis, spectral entropy computation, trust oscillation modeling, and confusion matrix evaluation, was performed to assess the proposed framework. The extracted RF features were subsequently utilized to evaluate the effectiveness of the proposed intrusion detection methodology under various spectrum sensing scenarios.

An adaptive XGBoost-based intrusion detection model was developed using the extracted harmonic trust features to classify legitimate and malicious RF behaviors. Experimental results demonstrate that malicious RF users exhibit significantly higher spectral entropy, unstable harmonic distributions, elevated trust oscillations, and larger harmonic divergence compared to legitimate users. The proposed framework achieved effective RF anomaly detection performance while preserving computational complexity.

The remainder of this paper is organized as follows. Section 2 presents the related works. Section 3 presents the architecture of the proposed system. Section 4 presents the proposed harmonic trust spectrum modeling framework and feature extraction methodology. Section 5 presents the experimental results and performance evaluation. Finally, Section 6 concludes the article and discusses future research directions.

2. Related Works

The authors of [9] proposed a spectrum sensing framework based on random forest classification combined with wavelet transform and empirical mode decomposition. Their approach demonstrated improved sensing performance under varying channel conditions. The superior results were achieved by exploiting machine learning-based feature extraction techniques. Similarly, in [1] a comprehensive review of spectrum sensing in CR Internet of Things (CR-IoT) environments is presented and the challenges associated with reliable spectrum access, security threats, and intelligent sensing strategies are discussed.

The authors of [3] reviewed recent advances in spectrum sensing and highlighted the importance of robust sensing algorithms for future CR systems. In [4], a detailed review of conventional spectrum sensing approaches is provided including energy detection, matched filtering, and cyclostationary feature detection techniques. Deep learning-based spectrum sensing methods have also gained attention due to their ability to learn complex RF characteristics. Article [5] investigates deep learning classification techniques for CR spectrum sensing and demonstrates improved sensing accuracy in dynamic wireless environments.

Advanced signal processing techniques have been extensively explored to enhance spectrum sensing performance, e.g. in [10], [11], where compressive sensing and various radio spectrum monitoring approaches in CRNs are researched, emphasizing reduced sampling requirements and efficient spectrum monitoring. Paper [2] presents a comprehensive survey on spectrum management in CRNs and discusses spectrum sharing, sensing, and dynamic access strategies. Furthermore, in [12], a matched filter detection approach with adaptive threshold selection is proposed to improve sensing reliability under varying channel conditions, while in [13], the effectiveness of cyclostationary feature analysis is demonstrated to identify unique RF signatures in CR applications.

Recent studies have also explored machine learning-based intrusion detection approaches. The authors of [9] utilized the XGBoost algorithm combined with SHAP analysis for attack detection and explainable security analytics. In [12], the KNN and ANN-based methods are proposed to detect PU emulation attacks (PUEA) in CRNs is proposed. Similarly, in [13], a machine learning-based intrusion detection system is presented that is capable of identifying anomalous network behavior using supervised learning techniques.

Tab. 1. Comparison of existing CR security and spectrum sensing approaches.

Ref.	Method	Technique	Limitation
[1]	CR-IoT spectrum sensing and spectrum management survey	CR-IoT survey	No intrusion detection framework
[2]	Spectrum management survey for CRNs	Survey	No RF intrusion detection framework
[3]	Review of recent advances in spectrum sensing	Spectrum sensing	No trust-aware RF analysis
[4]	Comparative survey of conventional spectrum sensing methods	Survey	Limited security considerations
[5]	Deep learning-based RF signal classification for spectrum sensing	Deep learning	Limited attack detection capability
[6]	XGBoost and SHAP based attack detection framework	XGBoost along with SHAP	General IoT security application
[7]	Machine learning based intrusion detection system	Machine learning IDS	Not specifically designed for CRNs
[8]	KNN and ANN based PUE attack detection	KNN + ANN	Limited harmonic spectrum intelligence
[9]	Random forest with wavelet and EMD based spectrum sensing	RF + wavelet + EMD	No intrusion detection capability
[10]	Compressive spectrum sensing for CRNs	Compressive sensing	No intrusion detection support
[11]	Comprehensive review of spectrum sensing techniques	Spectrum sensing	No malicious user identification capability
[12]	Matched filter detection with adaptive thresholding	Matched filtering	Vulnerable to sophisticated spoofing attacks
[13]	Cyclostationary feature extraction for RF signature identification	Cyclostationary analysis	No trust behavior modeling

The comparison of existing CR security and spectrum sensing approaches is provided in Tab. 1

Although existing studies have demonstrated significant progress in spectrum sensing, RF signal classification, and intrusion detection, most approaches focus primarily on spectrum occupancy detection, signal classification, or conventional machine learning-based attack detection. Limited attention has been paid to harmonic trust behavior, oscillatory RF instability, spectral divergence analysis, and trust-aware harmonic modeling. To address these limitations, the proposed HTSM framework integrates harmonic spectrum intelligence, trust oscillation analysis, spectral entropy characterization, and adaptive XGBoost-based intrusion detection to provide enhanced protection against malicious RF activities and PUE attacks.

3. Proposed Model

Unlike conventional spectrum sensing approaches that mainly rely on energy detection or signal strength measurements, the proposed framework investigates harmonic patterns, spectral uncertainty, trust oscillations, and spectrum occupancy behavior to identify abnormal RF activities.

The overall framework begins with the acquisition of RF signals from the selected benchmark datasets. The collected RF signals are then processed through a spectrum monitoring stage, where both time- and frequency-domain characteristics are analyzed to capture the underlying behavior of spectrum users.

FFT is utilized to reveal the harmonic spectrum structure of the received signals, while PSD analysis provides information regarding signal energy distribution across the frequency spectrum. Spectral entropy is used to measure the randomness and uncertainty present within RF transmissions, whereas wavelet analysis captures localized spectral variations and transient behaviors that may indicate malicious activity. The combination of these techniques enables comprehensive multidomain RF signal characterization.

The extracted spectral information is forwarded to the harmonic spectrum intelligence engine which constitutes the main processing analytical component of the proposed framework. This module evaluates harmonic stability, spectral consistency, transmitter reliability, and spectrum occupancy behavior to construct a trust-aware representation of each RF transmission. By continuously monitoring these spectral attributes, the framework establishes a dynamic trust profile capable of distinguishing legitimate spectrum occupancy from suspicious RF activities.

To evaluate the intrusion detection capability, two metrics are introduced. The first is the harmonic trust instability index (HTII), which quantifies the degree of instability within the harmonic spectrum. Legitimate spectrum users generally exhibit stable harmonic structures, whereas malicious users often generate irregular spectral fluctuations due to spoofing behavior and transmission inconsistencies. Consequently, higher HTII values indicate increased harmonic instability and greater likelihood of malicious activity.

The second metric, i.e. oscillatory trust divergence (OTD), measures the deviation between trusted harmonic behavior and suspicious RF transmissions. This metric captures the spectral divergence observed between legitimate users and potential attackers by analyzing variations in harmonic energy distributions and trust oscillations. Larger OTD values indicate substantial deviations from expected spectrum behavior and serve as indicators of spectrum spoofing and PUE attacks.

The extracted features are combined to form a multidimensional feature representation of each spectrum user. These features are subsequently fed to an adaptive extreme gradient boosting (XGBoost)-based intrusion detection system (IDS). The classifier learns discriminative patterns associated with legitimate and malicious RF activities and performs automated classification of spectrum users.

The proposed HTSM framework establishes a unified relationship between harmonic spectrum intelligence, trust-based signal analysis, and machine learning-based intrusion detection. By introducing trust-oriented RF metrics and integrating them with advanced signal processing techniques, the framework provides an additional layer of spectrum security that complements traditional spectrum sensing approaches.

4. Experimental Setup and Methodology

The proposed implementation of the HTSM framework was performed using the Google Collaboratory environment, using Python libraries that include NumPy, SciPy, Scikit-Learn, PyWavelets, Matplotlib, and XGBoost. In addition, the GNU radio companion (GRC) was employed to generate custom RF datasets that represent legitimate and malicious spectrum users.

4.1. Data Set Acquisition and RF Signal Sources

To investigate the behavior of the RF spectrum in diverse communication scenarios, three different datasets were used. The first dataset, RadioML2016.10A, was used to analyze modulation-specific RF characteristics under varying channel conditions. This data set contains eleven modulation schemes, including BPSK, QPSK, 8PSK, PAM4, QAM16, QAM64, GFSK, CPFSK, WBFM, AM-DSB and AM-SSB, across signal-to-noise ratio (SNR) values ranging from –20 to +18 dB. The data set was used primarily for modulation-aware harmonic analysis, spectral entropy extraction, power spectral density estimation, and wavelet decomposition.

The second data set is a subset of the Oracle RF Fingerprinting dataset. It provides real-world RF fingerprints captured from multiple USRP X310 software-defined radio devices. Unlike its synthetic modulation counterparts, this dataset contains device-specific hardware impairments and transmitter fingerprints, making it suitable for trust-aware RF intelligence modeling. The dataset was used to investigate harmonic stability, RF reliability, transmitter-specific spectrum characteristics, and trust signal generation. IQ samples were processed as complex-valued RF signals as:

$$x(n) = I(n) + jQ(n)\,, \tag{1}$$

where $I(n)$ and $Q(n)$ represent the in-phase and quadrature components of the RF signal, respectively.

The third dataset was generated using the GNU radio companion to emulate both legitimate spectrum users and malicious PUE attackers under realistic RF conditions. Modulated communication signals such as BPSK and QPSK were utilized to represent practical wireless transmission behavior.

To simulate realistic wireless environments, channel impairments including Rayleigh fading, Doppler shift, additive white Gaussian noise (AWGN), and phase variations were implemented. The attacker behavior was designed to mimic legitimate transmissions while introducing controlled spectral distortions and power fluctuations, thereby representing sophisticated RF spoofing scenarios. Although a simplified signal model is used for initial validation, the proposed framework is further evaluated using real-world RF datasets, including RadioML 2016.10A and Oracle to ensure robustness under realistic wireless conditions.

4.2. RF Signal Preprocessing

The acquired IQ samples from all datasets were first converted into numerical arrays and preprocessed for further analysis. The RadioML dataset was loaded from the serialized dictionary format and individual modulation samples were extracted. The Oracle RF dataset was loaded as complex-valued IQ samples using a complex128 representation to preserve the information from the transmitter's fingerprint. The GNU radio generated datasets were loaded using 64 complex representations.

To support machine learning-based analysis, the RF signals were partitioned into fixed-size windows.

Let the RF sequence be represented as:

$$X = \{x_1, x_2, x_3, \ldots, x_N\}\,, \tag{2}$$

where N denotes the total number of IQ samples.

The signal was segmented into windows of length $L = 2048$ samples according to the following:

$$W_i = \{x_{iL}, x_{iL+1}, \ldots, x_{(i+1)L-1}\}\,, \tag{3}$$

where W_i denotes the i-th signal segment.

This segmentation process transforms long RF recordings into multiple independent observations, thereby increasing the number of training samples available for machine learning.

4.3. Time-domain RF Signal Analysis

Time-domain visualization was performed to examine the temporal characteristics of legitimate and malicious RF transmissions. The real component of each IQ signal was analyzed to identify waveform stability and oscillatory behavior. Normal users generally produce periodic and stable RF waveforms, whereas malicious users introduce irregular fluctuations and noise-induced distortions. Time-domain analysis provides an initial understanding of the behavior of RF signals before frequency-domain processing.

4.4. Frequency-domain Spectrum Analysis

Frequency domain analysis was conducted using the FFT, which converts the RF signal from the time domain into its spectral representation and reveals harmonic structures associated with legitimate and malicious transmissions. The discrete Fourier transform is defined as:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-\frac{j2\pi kn}{N}}\,, \tag{4}$$

where $x(n)$ is the input RF signal, N is the signal length, and $X(k)$ denotes the spectral representation.

FFT analysis enables visualization of harmonic peaks, spectral spreading, and frequency domain anomalies. The normal user signals generated in GNU Radio exhibited narrow harmonic

peaks, whereas the PUE attack signals produced broader spectral distributions due to the presence of AWGN.

4.5. Power Spectral Density Estimation

To evaluate spectral energy distribution, PSD estimation was performed using the Welch method. PSD provides information on energy concentration across frequency bands and is widely employed in CR spectrum sensing applications. PSD is calculated in the following manner:

$$PSD(f) = \frac{|X(f)|^2}{N} \,, \tag{5}$$

where $X(f)$ denotes the Fourier spectrum and N represents the signal length.

PSD analysis allows for comparison of normal and malicious spectrum occupancy behavior and assists in identifying abnormal RF energy patterns.

4.6. Wavelet-based Harmonic Analysis

Although FFT provides global spectral information, it lacks temporal localization capability. Therefore, discrete wavelet transform (DWT) analysis was employed to investigate localized spectral variations and transient RF disturbances. Daubechies wavelets (db4) were selected because of their effectiveness in capturing RF signal irregularities. The wavelet transform is expressed as:

$$W(a,b) = \int_{-\infty}^{\infty} x(t)\, \psi_{a,b}(t)\, dt \,, \tag{6}$$

where $\psi_{a,b}(t)$ denotes the scaled and shifted mother wavelet.

Wavelet coefficients were extracted from all RF signals and analyzed to distinguish stable harmonic behavior from malicious oscillatory activity.

4.7. Trust-aware Harmonic Spectrum Modeling

Trust is represented as a dynamic spectrum-dependent quantity derived from the characteristics of the RF signal. The trust function is formulated as:

$$T(t) = \alpha\, S(t) + \beta\, C(t) + \gamma\, R(t) + \delta\, O(t) \,, \tag{7}$$

where $S(t)$ denotes spectrum stability, $C(t)$ represents channel consistency, $R(t)$ corresponds to RF reliability, and $O(t)$ indicates spectrum occupancy behavior.

The weighting coefficients satisfy the following:

$$\alpha + \beta + \gamma + \delta = 1 \,, \tag{8}$$

and were empirically selected as:

$$T(t) = 0.3\, S + 0.2\, C + 0.3\, R + 0.2\, O \,. \tag{9}$$

The generated trust sequence forms a trust oscillation curve that reflects the stability of the behavior of the RF spectrum over time. Legitimate users generally exhibit smooth trust variations, whereas malicious users produce significant trust oscillations.

4.8. Feature Extraction and RF Intelligence Metrics

Several RF features were extracted from the processed signals to characterize spectral behavior and detect anomalies associated with the use of the malicious spectrum. The first feature is spectral entropy, which quantifies the uncertainty within the RF spectrum. Spectral entropy is computed as:

$$H = -\sum_{i=1}^{N} p_i \log_2(p_i) \,, \tag{10}$$

where:

$$p_i = \frac{P_i}{\sum\limits_{i=1}^{N} P_i} \,, \tag{11}$$

P_i represents the spectral power of the i-th frequency component. Higher entropy values indicate increased spectral randomness and potentially malicious behavior.

To quantify harmonic instability, a harmonic trust instability index (HTII) is proposed. HTII measures the variation of harmonic spectral energy by relating the variance of the FFT power spectrum to its mean power. This metric provides an indication of the stability of the received RF signal and helps distinguish legitimate users from malicious occupants of the spectrum. HTII is defined as:

$$HTII = \frac{\sigma_P^2}{\mu_P} \,, \tag{12}$$

where the mean FFT spectral power is computed as:

$$\mu_P = \frac{1}{N} \sum_{i=1}^{N} P(i) \,, \tag{13}$$

where σ_P^2 denotes the variance of the FFT power spectrum, μ_P represents the mean FFT spectral power, $P(i)$ denotes the FFT power of the i-th spectral component, and N is the total number of FFT spectral components.

Higher HTII values indicate greater harmonic instability, suggesting irregular RF spectral behavior and an increased likelihood of malicious spectrum occupancy, including PUE attacks.

The second proposed metric is the oscillatory trust divergence (OTD), which measures the deviation between the trust behavior of legitimate spectrum users and malicious PUE attackers. OTD quantifies the cumulative difference in trust values over a sequence of RF observations and is defined as:

$$OTD = \sum_{i=1}^{N} \left| T_{\mathrm{Normal}}(i) - T_{\mathrm{Attack}}(i) \right| \,, \tag{14}$$

where $T_{\mathrm{Normal}}(i)$ denotes the trust value of the legitimate spectrum user at the i-th observation, $T_{\mathrm{Attack}}(i)$ represents the trust value of the suspected PUE attacker, and N is the total number of analyzed RF observations.

Larger OTD values indicate greater divergence from normal spectrum behavior, thereby providing a strong indication of malicious spectrum occupancy and RF spoofing activities.

4.9. Machine Learning-based Intrusion Detection

The extracted RF intelligence features were assembled into feature vectors for intrusion detection. Each signal window generated a feature vector containing spectral entropy and HTII values. The resulting feature matrix is represented as:

$$X = \begin{bmatrix} H_1 & HTII_1 \\ H_2 & HTII_2 \\ \vdots & \vdots \\ H_n & HTII_n \end{bmatrix}, \tag{15}$$

where each row corresponds to an RF signal segment.

Class labels were assigned as:

$$y = \begin{cases} 0, & \text{normal user} \\ 1, & \text{PUE attacker} \end{cases}, \tag{16}$$

The data set was divided into training and testing subsets using a 70:30 ratio. A stratified train-test split was employed to prevent data leakage and all performance metrics were evaluated on previously unseen testing samples. XGBoost was selected as the classifier due to its robustness, computational efficiency, and ability to capture non-linear relationships within RF features.

4.10. Performance Evaluation

The effectiveness of the proposed HTSM framework was evaluated using well-known classification metrics and CR performance indicators:

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

$$Precision = \frac{TP}{TP + FP}, \tag{18}$$

$$Recall = \frac{TP}{TP + FN}, \tag{19}$$

$$F1 = 2 \cdot \frac{Precision \times Recall}{Precision + Recall}. \tag{20}$$

To provide a more balanced evaluation, the Matthews correlation coefficient (MCC) was defined as:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}. \tag{21}$$

The consistency was further evaluated using Cohen's kappa coefficient:

$$\kappa = \frac{p_o - p_e}{1 - p_e}, \tag{22}$$

where p_o denotes observed agreement and p_e represents expected agreement.

For CR security evaluation, the probability of detection and the probability of false alarm were determined:

$$P_d = \frac{TP}{TP + FN}, \tag{23}$$

$$P_{fa} = \frac{FP}{FP + TN}. \tag{24}$$

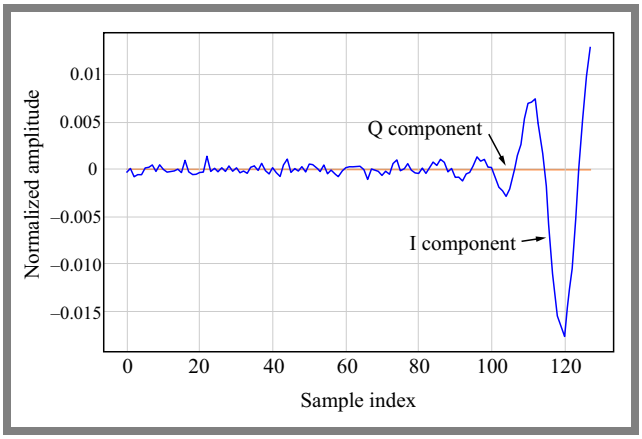

Fig. 2. Time-domain representation of the selected RadioML RF signal.

The generated experimental outputs include time-domain RF waveforms, FFT harmonic spectra, power spectral density plots, wavelet coefficient visualizations, trust oscillation curves, confusion matrices, and machine learning performance metrics.

5. Simulations Results

The evaluation was carried out using multiple heterogeneous RF datasets representing diverse spectrum sensing scenarios. The objective of the evaluation was to investigate harmonic spectrum behavior, trust oscillation characteristics, spectral entropy variations, and the effectiveness of the proposed HTII and OTD metrics.

5.1. RadioML2016.10A

This data set was used as the first benchmark dataset to validate the ability of the proposed framework to analyze the harmonic spectrum. The dataset contains multiple modulation schemes and SNR levels, allowing investigation for RF signal behavior under realistic communication conditions.

Figure 2 illustrates the temporal behavior of the selected RF signal. The waveform exhibits stable amplitude characteristics with limited fluctuations, indicating a communication environment for trust modeling.

The FFT spectrum shown in Fig. 3 shows dominant spectral components concentrated within specific frequency bins. Such a spectral concentration indicates efficient spectrum utilization and reduced harmonic instability.

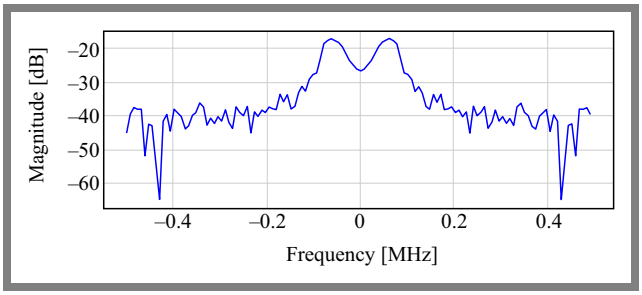

Fig. 3. FFT spectrum of the RadioML.

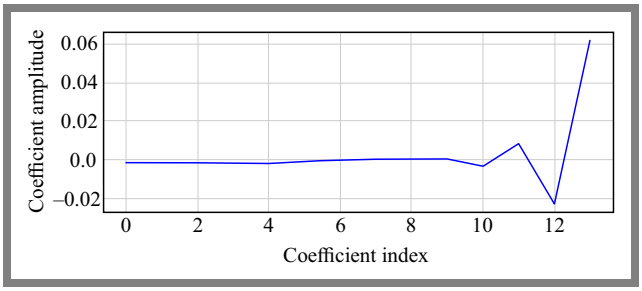

Fig. 4. Wavelet approximation coefficients obtained from RadioML.

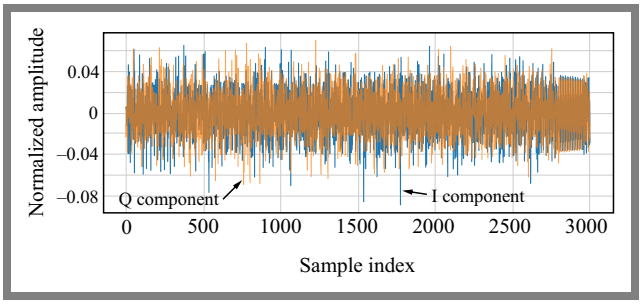

Fig. 5. Oracle RF fingerprint signal.

Figure 4 presents the wavelet approximation coefficients generated using the Daubechies wavelet transform. The smooth coefficient evolution indicates stable low-frequency harmonic structures that are characteristic of legitimate communication signals. The results obtained demonstrate low spectral randomness and stable harmonic characteristics, which form a baseline for the proposed HTSM framework.

5.2. Oracle RF Fingerprinting Dataset

Unlike RadioML, this dataset contains real-world transmitter fingerprints generated from physical wireless devices.

Figure 5 demonstrates the temporal variation of the Oracle RF signal. The observed fluctuations represent hardware-specific non-linearities and manufacturing imperfections that naturally occur in real transmitters.

The FFT presented in Fig. 6 exhibits spectral energy patterns associated with device-specific RF fingerprints. These spectral variations contribute significantly to the estimation of the trust.

Figure 7 illustrates the evolution of trust values over time. Variations in trust indicate changes in spectrum behavior and provide an effective mechanism for identifying abnormal RF activities.

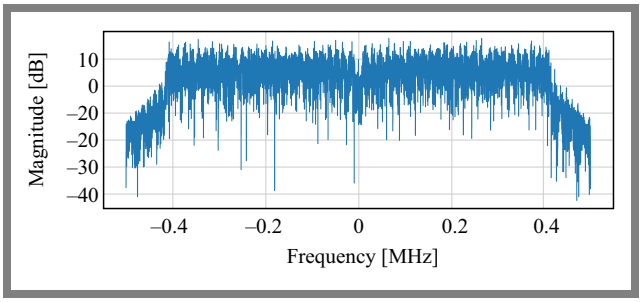

Fig. 6. FFT spectrum of the Oracle RF signal.

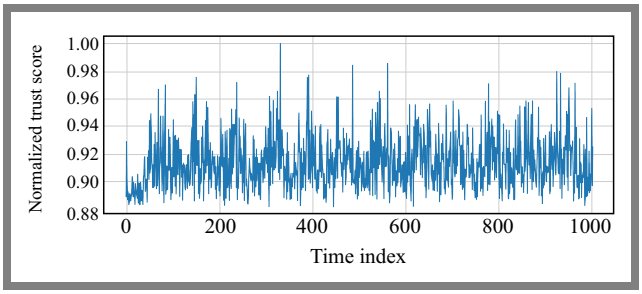

Fig. 7. Trust oscillation curve generated by the proposed HTSM framework.

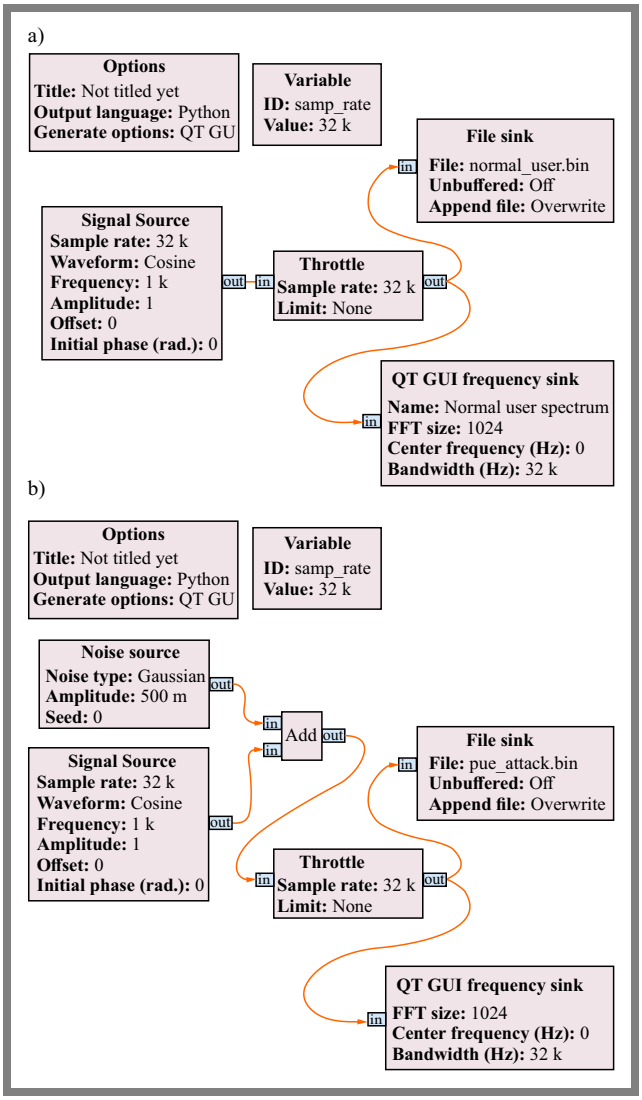

Fig. 8. GNU Radio flowgraph used to generate legitimate user signals a) and for PUE attack b).

5.3. GNU Radio Generated RF Dataset

To validate the proposed framework under controlled attack conditions, a custom RF dataset was generated using GNU Radio Companion. Two binary datasets were created: a legitimate spectrum user represented by `normal_user.bin` and a malicious attacker represented by `pue_attack.bin`. The generated datasets were subsequently analyzed in Google Colab.

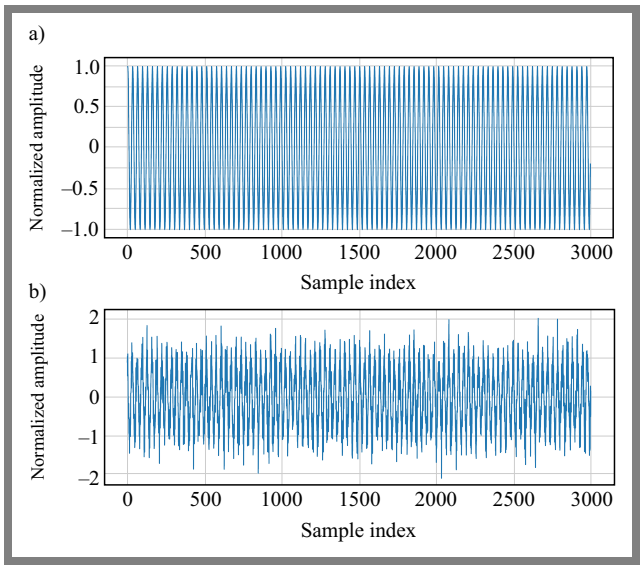

Fig. 9. Legitimate user RF signal a) and PUE attack RF signal b).

Figure 8a shows the signal generation architecture for the legitimate user employing modulated RF transmission schemes, while in Fig. 8b the PUE attack scenario generated by introducing controlled interference, channel impairments, and spectral distortions is presented to emulate malicious spectrum access behavior under realistic conditions. This process emulates an attacker trying to mimic a licensed spectrum occupant.

The legitimate signal shown in Fig. 9a exhibits highly periodic behavior with consistent amplitude characteristics. In contrast, Fig. 9b shows significant fluctuations introduced by malicious interference, resulting in higher spectral uncertainty and trust instability.

The most significant result is presented in Fig. 10. The PSD comparison clearly illustrates the difference between the occupancy of trusted and malicious spectrum. The legitimate user shows concentrated spectral energy, whereas the PUE attacker introduces broadband spectral spreading and increased harmonic distortion. The results confirm that the proposed HTSM framework successfully captures the spectral instability, trust oscillation behavior, and harmonic divergence introduced by malicious spectrum users.

Table 2 presents the classification performance of the proposed framework integrated with the XGBoost classifier on the GNU Radio-generated RF dataset. The dataset consisted of 331 555 feature instances extracted from both legitimate user transmissions and PUE attack signals.

Experimental results demonstrated an overall classification precision of 99.99%, with a precision of 100% and an F1 score of 99.51%, indicating highly reliable discrimination between legitimate and malicious spectrum activities. The probability of detection reached 99.03%, while the probability of false alarm remained at zero, confirming the capability of the proposed framework to identify the occupancy of spoofed spectrum without misclassifying legitimate users. Furthermore, the obtained MCC (0.9951) and Cohen kappa score

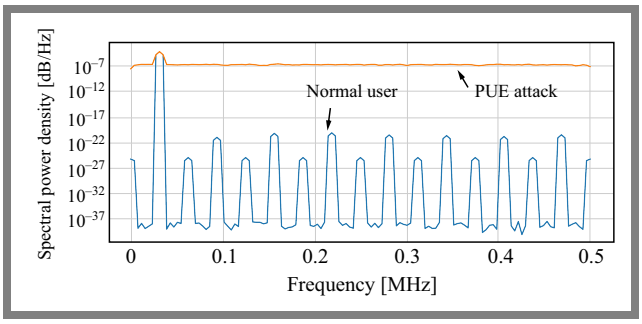

Fig. 10. PSD comparison between legitimate and PUE attack signals.

Tab. 2. Performance evaluation of the proposed framework using the GNU Radio RF dataset.

Performance metric	Value
Accuracy	99.9919%
Precision	100.0000%
Recall	99.0326%
F1-score	99.5139%
Matthews correlation coefficient	0.9951
Cohen kappa score	0.9951
Probability of detection	0.9903
Probability of false alarm	0.0000

(0.9951) indicate an excellent agreement between predicted and actual classes.

These results validate the effectiveness of the proposed HTII and OTD metrics in capturing trust-related spectral variations and demonstrate the suitability of harmonic trust intelligence for next-generation CR intrusion detection systems. It should be noted that the exceptionally high classification performance achieved by the proposed HTSM framework is influenced by the controlled GNU Radio attack generation environment used in this study. The generated PUE attack signals exhibit distinguishable spectral and trust-related characteristics, enabling effective separation between legitimate and malicious spectrum users. Although the results obtained demonstrate the effectiveness of the proposed HTII and OTD metrics, further experimental evaluation of the proposed framework is envisaged using real-world software-defined radio (SDR) platforms such as USRP and ADALM-Pluto devices, under real wireless channel conditions involving fading, interference, noise uncertainty, and mobility effects.

It is worth noting that the GNU Radio dataset incorporates realistic modulation schemes and channel effects. However, further validation using real-world SDR platforms remains an important direction for future work.

6. Conclusions

This paper proposed a harmonic trust spectrum modeling framework for intrusion detection in CRNs. The framework combines harmonic spectrum analysis, trust-aware signal modeling, and machine learning to identify malicious spec-

trum activities, including PUE attacks. The proposed approach was validated using multiple heterogeneous RF data sets under diverse spectrum sensing scenarios. Signal processing techniques such as FFT, PSD, wavelet analysis, and spectral entropy were employed to extract RF spectrum characteristics. Furthermore, two trust-oriented metrics, HTII and OTD, were introduced to quantify spectral trust variations and malicious oscillatory behavior.

The experimental results demonstrated clear distinctions between legitimate and malicious RF activities, with spoofed users exhibiting greater spectral entropy, greater harmonic instability, and increased trust divergence. The integration of these features with an IDS confirmed the effectiveness of the proposed framework for adaptive spectrum security.

Acknowledgments

The authors wish to thank the management, principal, and Head of the Department of Thiagarajar College of Engineering, Madurai, India, for their support and facilities provided for this research.

Data Availability

Data used in this study include publicly available RadioML2016.10A and Oracle RF Fingerprinting datasets, along with a GNU Radio generated RF dataset. The custom dataset is available from the corresponding author upon a reasonable request.

References

[1] A.A. Raji and T.O. Olwal, "Spectrum Sensing in Cognitive Radio Internet of Things: State-of-the-art, Applications, Challenges, and Future Prospects", *Journal of Sensor and Actuator Networks*, vol. 14, art. no. 109, 2025 (https://doi.org/10.3390/jsan14060109).

[2] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, and S. Mohanty, "A Survey on Spectrum Management in Cognitive Radio Networks", *IEEE Communications Magazine*, vol. 46, pp. 40–48, 2008 (https://doi.org/10.1109/MCOM.2008.4481339).

[3] A. Nasser *et al.*, "Spectrum Sensing for Cognitive Radio: Recent Advances and Future Challenge", *Sensors*, vol. 21, art. no. 2408, 2021 (https://doi.org/10.3390/s21072408).

[4] S. Samala, S. Mishra, and S.S. Singh, "Spectrum Sensing Techniques in Cognitive Radio Technology: A Review Paper", *Journal of Communications*, vol. 15, pp. 577–582, 2020 (https://doi.org/10.12720/jcm.15.7.577-582).

[5] S. Zheng *et al.*, "Spectrum Sensing Based on Deep Learning Classification for Cognitive Radios", *ArXiv*, 2019 (https://arxiv.org/abs/1909.06020).

[6] M.F. Habibi and P. Sukarno, "Analysis of Attack Detection on IoT Using XGBoost Algorithm and SHAP", *2025 International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia, 2025 (https://doi.org/10.1109/ICoICT66265.2025.11193104).

[7] A. Kiran *et al.*, "Intrusion Detection System Using Machine Learning", *2023 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2023 (https://doi.org/10.1109/ICCCI56745.2023.10128363).

[8] M.A. Inamdar and H.V. Kumaraswamy, "Accurate Primary User Emulation Attack (PUEA) Detection in Cognitive Radio Network using KNN and ANN Classifier", *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2020 (https://doi.org/10.1109/ICOEI48184.2020.9143015).

[9] G.K. Gole, S. Morya, and R.K. Nagar, "Spectrum Sensing in Cognitive Radio Using Random Forest with Wavelet and Empirical Mode Decomposition", *International Journal of Environmental Services*, vol. 11, art. no. 24s, 2025.

[10] F. Salahdine, "Compressive Spectrum Sensing for Cognitive Radio Networks", *ArXiv*, 2018 (https://arxiv.org/abs/1802.03674).

[11] F. Salahdine, "Spectrum Sensing Techniques for Cognitive Radio Networks", *ArXiv*, 2017 (https://arxiv.org/abs/1710.02668).

[12] F. Salahdine, H. El Ghazi, N. Kaabouch, and W.F. Fihri, "Matched Filter Detection with Dynamic Threshold for Cognitive Radio Networks", *International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Marrakech, Morocco, 2015 (https://doi.org/10.1109/WINCOM.2015.7381345).

[13] P.D. Sutton, K.E. Nolan, and L.E. Doyle, "Cyclostationary Signatures in Practical Cognitive Radio Applications", *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 13–24, 2008 (https://doi.org/10.1109/JSAC.2008.080103).

S. Jeyaseelan, M.Sc.
https://orcid.org/0009-0009-6556-0491
E-mail: jeyaseelanjeyas@gmail.com
Thiagarajar College of Engineering, Madurai, India
https://www.tce.edu

P.G.S. Velmurugan, Ph.D.
https://orcid.org/0000-0002-3507-9797
E-mail: pgsvels@tce.edu
Thiagarajar College of Engineering, Madurai, India
https://www.tce.edu

G. Prabhakar, Ph.D.
https://orcid.org/0000-0003-4760-7646
E-mail: gpece@tce.edu
Thiagarajar College of Engineering, Madurai, India
https://www.tce.edu

J. Shanthi, Ph.D.
https://orcid.org/0000-0002-7282-7854
E-mail: shanthiece@kamarajengg.edu.in
Kamaraj College of Engineering and Technology, Virudhunagar, India
https://www.kamarajengg.edu.in