Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.069776

ARTICLE

Mitigating Sidelobe-Driven Attacks in OFDM-Based Cognitive Radio Networks

Bakhtawar Gul[1], Atif Elahi[1,2], Tahir Saleem[3], Noor Gul[1], Fahad Algarni[4] and Insaf Ullah[5,*]

[1]Department of Electronics, University of Peshawar, Peshawar, Pakistan
[2]Govt. College Mathra, Higher Education Archives & Libraries Department, Peshawar, Pakistan
[3]Department of Computing, Hamdard University Islamabad Campus, Islamabad, Pakistan
[4]College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia
[5]Institute for Analytics and Data Science, University of Essex, Colchester, UK

*Corresponding Author: Insaf Ullah. Email: insaf.ullah@essex.ac.uk

Received: 30 June 2025; Accepted: 07 November 2025; Published: 12 March 2026

ABSTRACT: Orthogonal Frequency Division Multiplexing (OFDM) enables efficient Dynamic Spectrum Access (DSA) but suffers from high sidelobe that causes excessive out-of-band (OOB) emissions and expose the system to spectrum-layer cyberattacks such as man-in-the-middle (MITM), eavesdropping, and primary user emulation (PUE) attacks. To address both spectral leakage and its security implications, this paper introduces a secure and intelligent hybrid optimization strategy that combinesan Eigenspace-based Generalized Sidelobe Canceller (ES-GSC) with a Genetic Algorithm (GA), to derive optimally weighted cancellation carriers. The proposed method jointly suppresses sidelobes and reinforces resistance to leakage-based attacks. MATLAB Simulation demonstrate considerable reductions in OOB emissions and higher resilience against spectrum-layer threats compared with existing techniques.

KEYWORDS: Cybersecurity; cognitive radios network; generalized sidelobe canceler; orthogonal frequency division multiplexing; primary user emulation attack; sidelobe suppression

1 Introduction

Cognitive Radio (CR) enables opportunistic spectrum access to mitigate spectrum scarcity by allowing unlicensed users (ULs) to temporarily use frequency bands that are not being exploited by licensed or primary users (PUs). To prevent interference with PUs, CR systems employ dynamic spectrum allocation (DSA), enabling UL's to adapt in real time to the changing spectrum environment [1,2].

Orthogonal Frequency Division Multiplexing (OFDM) is a popular modulation technique that divides data across subcarriers, simplifying channel management and allowing ULs to activate only unused spectral gaps without overlapping PU channels, as illustrated in Fig. 1. However, OFDM's structure introduces a key vulnerability: even when subcarriers are deactivated to avoid direct overlap, the sidelobes from active subcarriers extend into adjacent bands, causing out-of-band (OOB) radiation that interferes with PUs and creates attack surfaces for spectrum-based cyber intrusions [3–5].

Malicious users can exploit these sidelobes as an entry point into the spectrum. Specifically, attackers can inject forged signals within the sidelobe regions to:

- Launch man-in-the-middle (MITM) attacks by intercepting and altering legitimate data transmissions.
- Conduct denial-of-service (DoS) attacks by flooding sidelobe regions to degrade signal quality or jam communication.

- Perform eavesdropping by exploiting sidelobe leakage to access confidential information.
- Spoof legitimate users, mimicking primary user signals and misleading spectrum sensing mechanisms.

These threats are especially dangerous in CR networks, where the dynamic and open nature of spectrum access can make authentication and intrusion detection more complex. Therefore, minimizing OOB radiation is essential not only for maintaining spectral efficiency but also for fortifying CR systems against spectral-layer attacks [6].

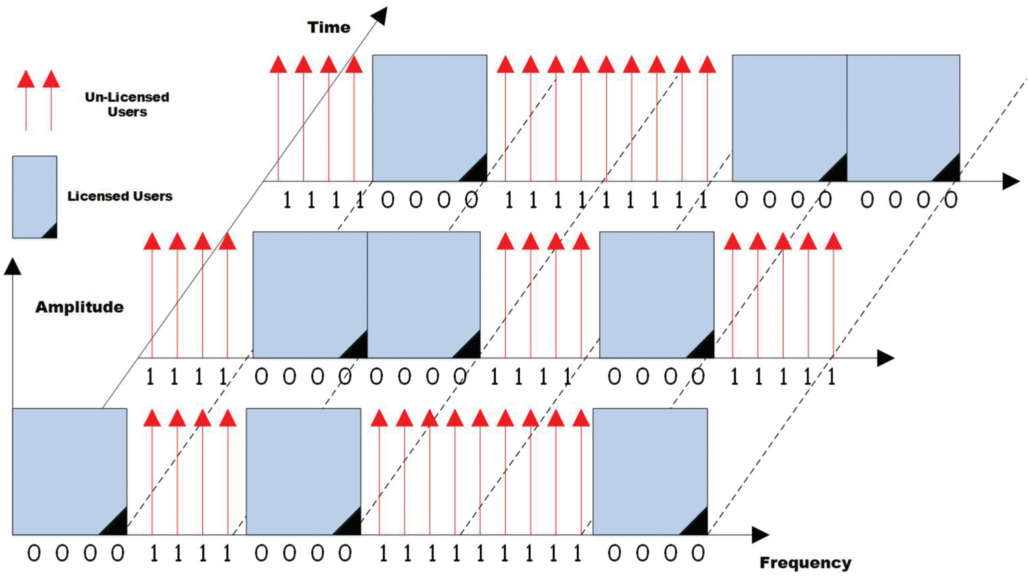

Figure 1: Allocation of PUs (grey blocks) and ULs (arrows) in an OFDM-based cognitive radio system.

To combat this dual challenge of spectral pollution and security risk, various mitigation techniques have been proposed, such as:

- Windowing [7–10]: Signal shaping to suppress leakage.
- Adaptive Symbol Transitions (AST) [11]: Smooth transitions to reduce emissions.
- Subcarrier Weighting (SW) [12,13]: Adjusting subcarrier power for spectral shaping.
- Constellation Expansions (CE) [14–16]: Using advanced constellations for better containment.
- Active Interference Cancellation (AIC) [17–19]: Cancelling emissions with auxiliary signals.
- Phase Adjustment [20] and Cancellation Carriers [21–23]: Fine-tuning signal components to reduce interference.
- Generalized Sidelobe Canceler (GSC) [24,25] and Eigenvalue-Based GSC [4]: Suppressing sidelobes through signal processing.
- Precoding and Hybrid Approaches [26–30]: Combining techniques for enhanced effectiveness.

In this paper, we introduce a novel hybrid nature-inspired approach that not only reduces OOB emissions but also mitigates the associated cybersecurity risks. By combining an Eigenspace-based Generalized Sidelobe Canceller (ES-GSC) with a Genetic Algorithm (GA) for optimized cancellation carrier design, the proposed solution suppresses spectral sidelobes and strengthens resistance against sidelobe-exploiting attacks. Through rigorous simulations, we demonstrate superior performance compared to existing OOB reduction techniques, both in spectral efficiency and resilience to attack.

The main contributions are:

- A cyber-aware hybrid sidelobe suppression framework (ES-GSC-GA optimized CCs) that jointly targets spectral containment and reduction of sidelobe-accessible attack surface.
- A systematic evaluation under five realistic spectrum sharing scenarios that model different PU/UL topologies and attacker capabilities (including synchronization and injection attempts).
- Quantitative performance assessment showing significant reductions in OOB power and leakage (numerical results will be reported in Section 4) and a security discussion that links spectral metrics to attack success rates.

The remainder of the paper is organized as follows: Section 2 provides an overview and detailed system model. Section 3 presents the proposed ES-GSC-GA method. Section 4 discusses the simulation results and analyzes security implications. Finally, Section 5 concludes the paper with a summary and future research directions.

2 Signal Model & Security Implications

An OFDM symbol in discrete time domain can be mathematically represented as:

$$\zeta(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a_k e^{i2\pi kn/N} \tag{1}$$

where $n = 0, 1, 2, \ldots, N-1$.

Here, the input data is denoted by a vector $\mathbf{a}$, where each element a_k corresponds to the k-th subcarrier. This vector is constructed as the transpose of a row vector with N total subcarriers. This formulation establishes the baseline waveform structure; the sidelobe leakage observed in the frequency domain originates from the overlapping of these multiple subcarriers.

To combat inter-symbol interference (ISI) and preserve orthogonality in multipath environments, a cyclic prefix (CP) of M samples is added to the OFDM symbol, defined as:

$$\zeta^{\text{CP}}(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} a_k e^{j2\pi k(N+n)/N} \tag{2}$$

where $n = -M, \ldots, 0, 1, \ldots, N-1$.

While the CP effectively maintains orthogonality, it does not mitigate OOB sidelobe radiation. This confirms that sidelobe leakage is an inherent property of the OFDM waveform itself, not an artifact introduced by the transmission channel.

The spectral representation of the OFDM signal can be obtained through an unsampled Discrete Fourier Transform (DFT) applied to Eq. (2). By introducing an upsampling factor P, the resultant upsampled spectrum is expressed as:

$$\psi_m = \frac{1}{N} \sum_{n=-p}^{N-1} \zeta^{\text{CP}}(n)\, e^{-j\frac{2\pi nm}{PN}} \tag{3}$$

where $m = 0, 1, \ldots, PN-1$.

Given that $e^{j2\pi k} = 1$ for the integer $k \in [0, N-1]$ simplifications yield:

$$\psi_m = \frac{1}{N} \sum_{k=0}^{N-1} \sum_{n=-M}^{N-1} a_k e^{\frac{j2\pi n}{N}\left(k-\frac{m}{P}\right)} \tag{4}$$

Eq. (3) can also be compactly written in matrix form as:

$$\boldsymbol{\psi} = \mathbf{Da} \tag{5}$$

where $\boldsymbol{\psi}$ is $PN \times 1$ vector containing the unsampled spectrum $\mathbf{a}$ is an $(N + M) \times 1$ input data vector that includes the original N data points with an additional P data points appended at the beginning to account for the cyclic prefix and $\mathbf{D}$ is an $PN \times (N + M)$ matrix whose element at the $(m + 1)$-th row and $(k + 1)$-th column is given by $\frac{1}{N}\sum_{n=-M}^{N-1} e^{\frac{j2n\pi}{N}(k-\frac{m}{P})}$. The $(m + 1)$-th element of the upsampled spectrum can therefore be expressed as:

$$\psi_m = D_m a \tag{6}$$

where D_m is the $(m + 1)$-th row of D matrix. These Eqs. (3)–(6) transform the time-domain OFDM signal into the frequency domain, where the sidelobe structure becomes visible.

The Normalized power spectral density (PSD) of OFDM can be expressed as follows:

$$P_m = \frac{1}{N} E\left\{|\psi_m|^2\right\} \tag{7}$$

This defines the normalized PSD, which quantifies how signal power leaks into adjacent frequencies. PSD is a key metric for evaluating both spectral efficiency and vulnerability to sidelobe-driven attacks.

Eq. (6) into Eq. (7) yields:

$$P_m = \frac{1}{N} D_m E\{aa^H\} D_m^H \tag{8}$$

The PSD of an OFDM signal is influenced by the statistical properties of the transmitted information symbols, specifically their covariance matrix. Given that the information symbols are independent, identically distributed (iid) with zero mean and unit variance, and considering the autocorrelation matrix of the transmitted signal to be an identity matrix (ignoring CP), Eq. (8) can be simplified to:

$$P_m = \frac{1}{N} D_m D_m^H \tag{9}$$

$$P_m = \frac{1}{N} \sum_{k=0}^{N-1} |d_{mk}|^2 \tag{10}$$

where $d_{mk} = \sum_{n=0}^{N-1} e^{-j\frac{2n\pi}{N}(k-\frac{m}{M})}$.

Assuming only the $(l + 1)$-th subcarrier is active and all others are inactive, the PSD equation simplifies to:

$$P_m = \frac{1}{N} |d_{ml}|^2 = \frac{1}{N}\left(\frac{1}{N}\sum_{n=0}^{N-1} e^{\frac{j2n\pi}{N}(l-\frac{m}{M})}\right)\left(\frac{1}{N}\sum_{r=0}^{N-1} e^{-\frac{j2r\pi}{N}(l-\frac{m}{M})}\right) \tag{11}$$

The equation can be simplified to:

$$P_m = \frac{1}{N}\left(\frac{\operatorname{sinc}\left(\pi\left(l - \frac{m}{M}\right)\right)}{\operatorname{sinc}\left(\frac{\pi}{N}\left(l - \frac{m}{M}\right)\right)}\right)^2 \tag{12}$$

The above equation demonstrates that the spectral shape of a single OFDM subcarrier follows a sinc-squared envelope, where, Maximum PSD Occurs solely at the frequencies of the active subcarrier, specifically at $m = lM$, flanked by sidelobes that decay slowly. This slow decay of sidelobes mathematically explains the significant spectral leakage in OFDM, which attackers can exploit for covert injection or PUE attacks.

For the idealized case of perfect subcarrier orthogonality, the PSD is:

$$P_m = \frac{1}{N}\left(\frac{\text{sinc}\left(\pi\left(l-r\right)\right)}{\text{sinc}\left(\frac{\pi}{N}\left(l-r\right)\right)}\right)^2 = 0 \tag{13}$$

Consequently, an active subcarrier does not induce interference on other subcarrier channels. In other words, perfect subcarrier synchronization eliminates Inter-Carrier Interference (ICI).

However, security concerns arise from the sidelobes inherent in the OFDM waveform. Fig. 2 illustrates the normalized PSD for a single active subcarrier. The sidelobes are evident, with the first sidelobe only 7 dB below the main lobe indicating significant spectral leakage. These sidelobes are not just a signal processing artifact but represent potential cybersecurity attack surfaces, allowing attackers to:

- Inject covert signals near the sidelobe regions (spectrum injection attacks),
- Jam adjacent channels by exploiting sidelobe overlap,
- Spoof legitimate user activity (primary user emulation) by mimicking the sidelobe signature,
- Intercept and manipulate ongoing transmissions via MITM attacks.

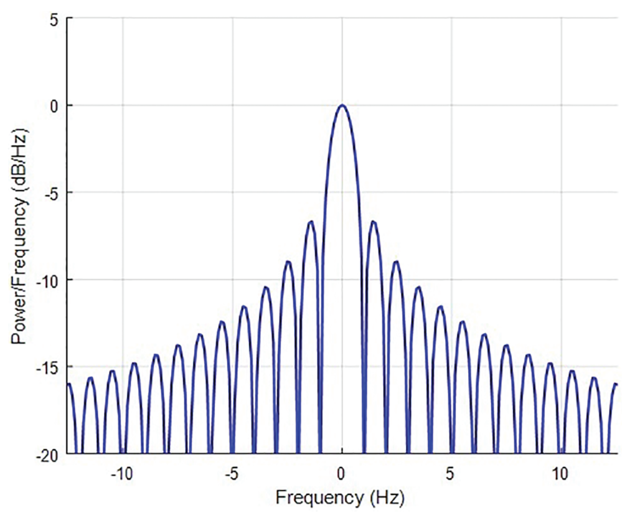

Figure 2: Normalized PSD of an OFDM signal with a single active subcarrier.

Fig. 3 illustrates a realistic scenario: PUs occupies subcarriers 41–64 and 81–105, while an UL transmits in the spectrum hole (subcarriers 65–80). Though subcarriers overlapping PUs are deactivated, OOB radiation from sidelobes still causes interference up to −25 dB in PU bands. This leakage not only degrades performance but also provides attackers with a stealthy path for spectral intrusion, bypassing traditional sensing or spectrum occupancy checks. Therefore, the sidelobe profile of OFDM signals acts as a cybersecurity vulnerability vector, emphasizing the urgent need for advanced sidelobe suppression techniques not merely for spectral efficiency, but as a line of defense in secure cognitive radio operations.

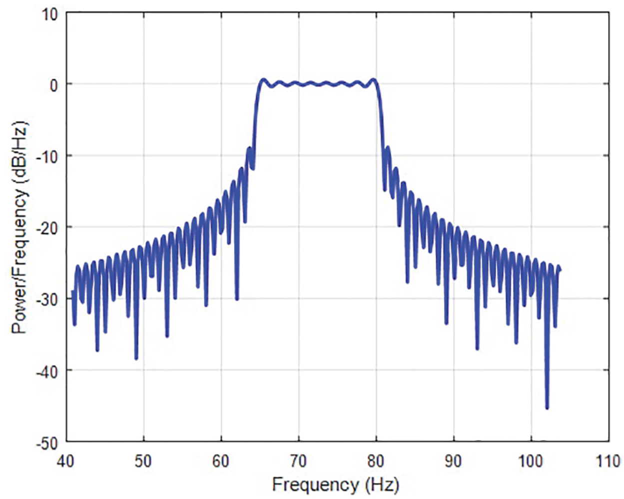

Figure 3: Single UL band (subcarriers 65–80) flanked by PU bands (subcarriers 41–64, 81–105).

3 Proposed Secure OFDM-Based CR System with Cyber-Aware Sidelobe Suppression

As cyberattacks increasingly exploit physical-layer vulnerabilities in cognitive radio networks, particularly through spectral leakage and OFDM sidelobes, robust defense mechanisms at the waveform level have become essential. In OFDM-based cognitive radio systems, high OOB radiation even when PU-occupied subcarriers are deactivated poses a critical security risk. This leakage can be maliciously used by attackers to launch MITM attacks, Denial of Service (DoS) through spectral pollution, or Primary User Emulation (PUE) attacks that hijack spectral resources.

To mitigate these threats, we propose a novel hybrid signal processing framework that enhances spectral containment and fortifies the system against such adversarial exploitation is illustrated in Fig. 4 illustrating the integration of cancellation carriers and subspace decomposition for sidelobe suppression. Our approach synergistically combines ES-GSC with Genetically Optimized Cancellation Carriers (CCs), resulting in a secure and spectrally robust OFDM waveform.

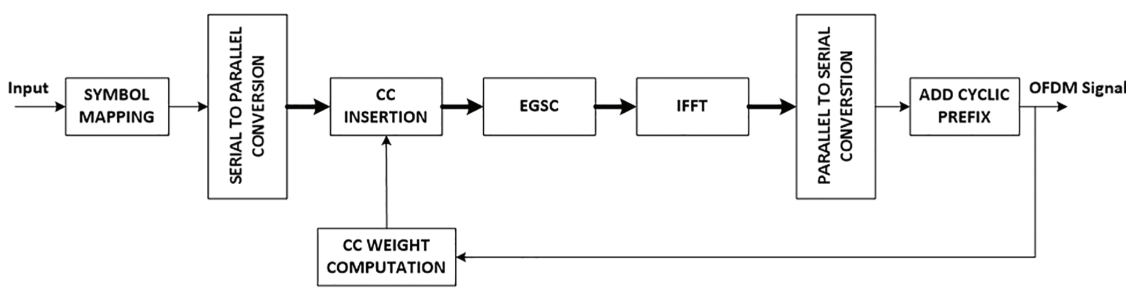

Figure 4: System model of proposed technique.

3.1 Cybersecurity Role of Cancellation Carriers

The CC method introduces a set of strategically positioned subcarriers at the edges of the OFDM spectrum. These carriers, modulated with complex coefficients optimized via GA, serve as active defense lines attenuating unwanted OOB radiation that could otherwise expose the system to spectral intrusion.

GA was selected because it is highly effective in solving nonlinear, multi-objective optimization problems with large and irregular search spaces, such as simultaneously minimizing OOB power and avoiding predictable leakage patterns. Unlike deterministic methods, GA does not require gradient information and can efficiently explore diverse solutions, reducing the risk of getting trapped in local optima. While other metaheuristics like Particle Swarm Optimization (PSO) and Differential Evolution (DE) were considered, GA was preferred for its greater flexibility in constraint handling and its ability to balance spectral shaping with security objectives.

An OFDM system comprising a total of N_c subcarriers is considered. Of these, N subcarriers are allocated for data transmission, carrying complex symbols $\mathbf{a} = [a_1, a_2, \ldots, a_N]^T$ modulated using PSK or QAM. The remaining $M = N_c - N$ subcarriers, traditionally employed as a guard band to mitigate out-of-band interference, are instead populated with CCs.

These CCs are no longer passive guard bands but cyber-aware spectral guards, actively suppressing sidelobes and reducing attack surfaces are strategically positioned at the spectrum edges of the OFDM signal as depicted in in Fig. 5. The CCs are modulated with complex weighting factors $\mathbf{g} = [g_1, g_2, \ldots, g_{M-1}, g_M]^T$, determined through GA using our proposed fitness function to counteract the original signal's sidelobe structure. This process aims to minimize the combined sidelobe levels within a specified spectral region.

$$\mathbf{x} = \left[g_1, \ldots, g_{M/2}, a_1, \ldots, a_N, g_{M/2+1}, \ldots, g_M\right]^T \tag{14}$$

This represents the transmitted OFDM vector including data symbols a_k and cancellation carriers g_m. Unlike passive guard bands, these GA-optimized carriers actively suppress sidelobe leakage, serving as spectral guards that harden the waveform against injection and spoofing attacks.

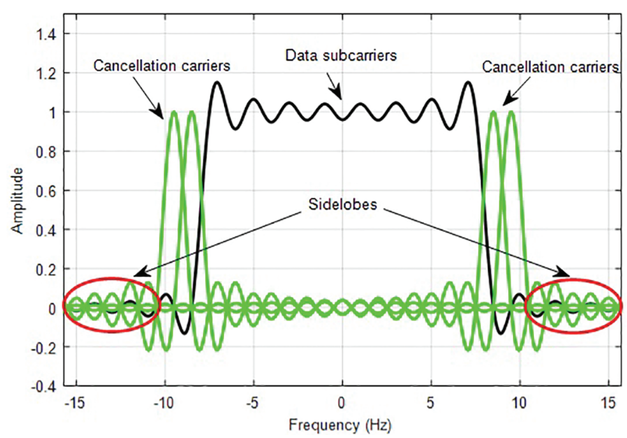

Figure 5: Concept of CCs, optimized via GA, for sidelobe suppression and attack surface reduction.

3.2 *ES-GSC as an Intrusion Mitigation Technique*

The ES-GSC is a signal processing method used to reduce unwanted signals (called sidelobe interference). It does this by using a technique called subspace decomposition, which breaks the signal into parts to identify and cancel out interference. The ES-GSC technique treats the incoming signal as a mix of basic building blocks (called basis vectors). It then splits the signal space into two parts. One part called the signal subspace contains the useful or desired signal. The other part called the noise subspace holds the interference or unwanted signals. The noise subspace (the part containing interference) is used to create special weights that help reduce the unwanted sidelobe signals. This leads to better signal quality. This approach usually works better than older GSC methods especially when the signal is weak or noisy (low SNR conditions). The ES-GSC technique is used in many areas like medical imaging, radar, and communications systems. It helps these systems works better by reducing or removing unwanted signals (interference or noise).

Key components and processes of ES-GSC are:

1. Signal Model: The received signal is modeled as a linear combination of desired signal components and interference.
2. Subspace Decomposition: Eigenvalue decomposition or Singular Value Decomposition (SVD) is employed to partition the signal space into signal and noise subspaces.
3. Weight Calculation: Weights are computed based on the noise subspace to minimize the power of the output error signal.
4. Sidelobe Cancellation: The calculated weights are applied to the received signal to suppress sidelobe components.
5. Output Signal: The processed signal with reduced sidelobe interference is obtained.

The ES-GSC technique involves a two-step process. Initially, signal and noise subspaces are derived from the GSC's correlation matrix, suppose it is **R**. Subsequently, a specialized weight vector is generated by projecting the GSC's weight vector onto the signal subspace. The correlation matrix, **R**, is a Hermitian matrix with specific properties.

1. The eigenvalues of Hermitian matrices are real.
2. Eigen vectors corresponding to different eigen values are orthogonal.
3. Matrix **R** can be decomposed as given by the equation:

$$\mathbf{R} = \boldsymbol{\Sigma}\boldsymbol{\Omega}\boldsymbol{\Sigma}^{\boldsymbol{H}} \tag{15}$$

The spectral theorem is applied to decompose the GSC's correlation matrix, **R**, into a diagonal matrix, $\boldsymbol{\Omega}$, containing eigenvalues, and a unitary matrix, $\boldsymbol{\Sigma}$, composed of eigenvectors. Due to the strong coherence of on-axis signals, the dominant eigenvectors associated with the largest eigenvalues are attributed to the main lobe. These eigenvectors constitute the signal subspace, while the remaining eigenvectors form the noise subspace. Orthogonality between these subspaces is ensured. By projecting the GSC's weight vector onto the signal subspace, a new weight vector is derived that preserves the desired signal component while enhancing sidelobe suppression given by equation.

$$\mathbf{w}_{\text{ES-GSC}} = \boldsymbol{\Sigma}\boldsymbol{\Sigma}^{\boldsymbol{H}}\mathbf{w}_{\text{GSC}} \tag{16}$$

Unlike static sidelobe suppression techniques, ES-GSC adapts dynamically to real-time changes in the interference environment. This adaptability is crucial in hostile spectrum-sharing conditions, where:

- Attack characteristics can change (frequency hopping, power variation, spectral spreading).
- Multiple simultaneous threats may appear at different sidelobe locations.
- Legitimate signals may coexist alongside malicious ones, requiring fine discrimination.

By continuously updating the correlation matrix R and recalculating subspace projections, ES-GSC can track and suppress both unintentional interference and malicious sidelobe injections. This real-time adaptability makes it well-suited for scenarios where attackers modify their strategy mid-transmission to evade fixed defenses.

4 Simulation Results: Cybersecurity-Enhanced Evaluation of the Proposed OFDM-Based Cognitive Radio System

To validate the cyber-resilience and signal integrity of our proposed sidelobe suppression framework, extensive simulations were conducted using MATLAB R2021a. The testbed evaluated OFDM-based cognitive radio systems with varying subcarrier configurations (16, 32, 128, and 256) under adversarial spectrum sharing conditions. Each scenario simulated potential physical-layer security threats such as eavesdropping via sidelobes, spectrum hijacking, and malicious interference injection through high OOB radiation.

To ensure robust defense against cyber-physical spectrum attacks, each OFDM symbol was supplemented with a cyclic prefix or zero-padding to combat ISI, a common vulnerability leveraged in DoS conditions.

4.1 Scenario 1: Single Spectrum Hole with Borderline Threats

In this setting, an UL occupies a narrow spectrum hole flanked by PU bands, which makes the system highly prone to cross-band interference and MITM-style attacks. The proposed method achieved the strongest sidelobe suppression, with significant OOB reduction completely outperforming GSC+GA and other benchmarks. This result highlights the technique's ability to secure spectrum edges in tightly packed environments (Figs. 6 and 7, Table 1).

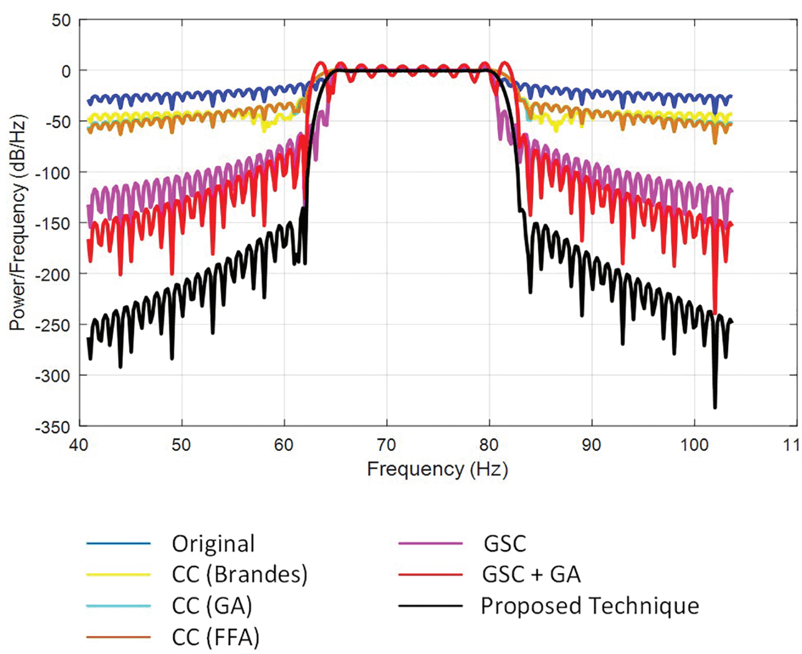

Figure 6: Comparison of PSD before and after applying the proposed technique, highlighting enhanced spectral containment and improved resilience against borderline spectrum injection attacks.

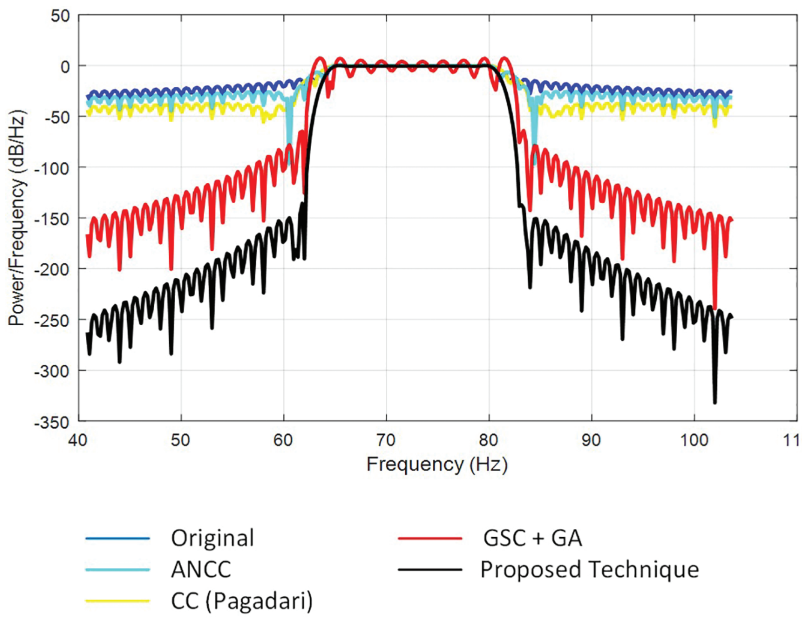

Figure 7: Comparison of PSD before and after applying the proposed technique, highlighting enhanced spectral containment and improved resilience against borderline spectrum injection attacks.

Table 1: PSD and % OOB Reduction relative to original signal (−29 dB).

Technique	PSD (dB)	% OOB Reduction
Original signal	−29	0.00
ANCC	−34	17.24
CC (Pagadari)	−44	51.72
CC (Brandes)	−45	55.17
CC (GA)	−55	89.66
CC (FFA)	−57	96.55
GSC	−132	355.17
GSC + GA	−166	472.41
Proposed technique	−263	806.90

4.2 Scenario 2: Distributed Access under Uniform Load

Here, multiple ULs access distributed spectrum holes across a wideband allocation, a situation where sidelobe leakage can enable lateral interference or covert channel formation. The proposed method consistently maintained spectral isolation, delivering significant OOB reduction, compared to EGSC and from GSC+GA. These gains confirm the robustness of our framework in fragmented spectral environments (Figs. 8 and 9, Table 2).

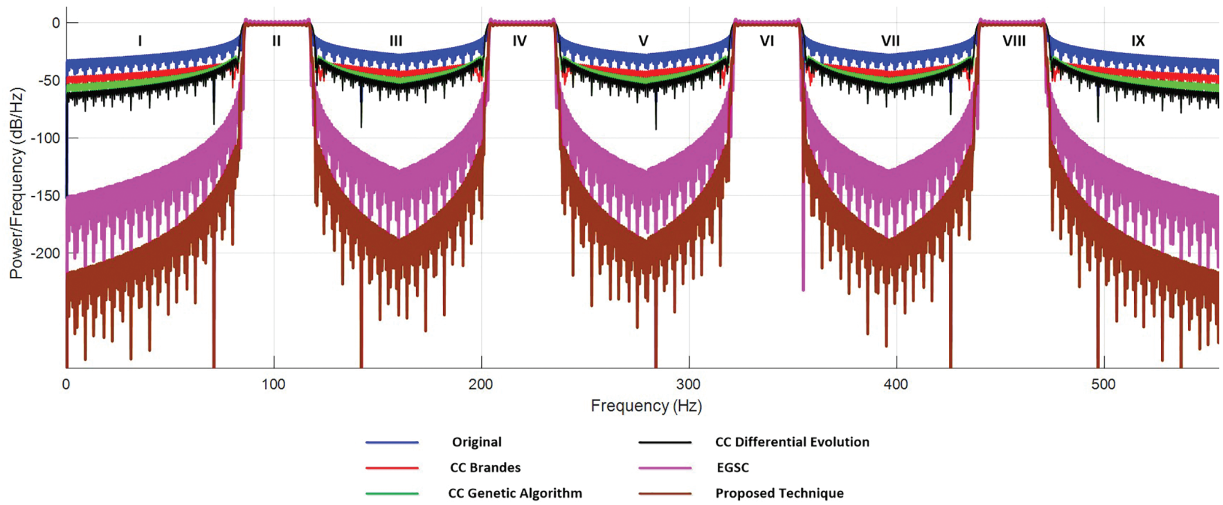

Figure 8: Normalized PSD for Scenario 2 illustrating effective sidelobe suppression across multiple spectrum holes, enhancing spectral containment and defending against distributed spectrum injection attacks in cognitive radio networks.

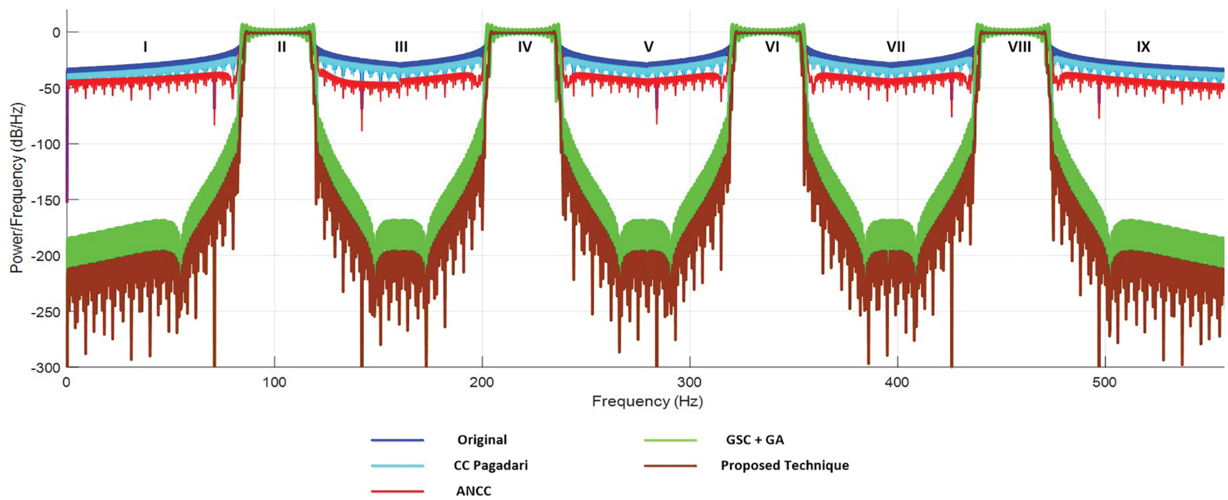

Figure 9: Normalized PSD for Scenario 2 illustrating effective sidelobe suppression across multiple spectrum holes, enhancing spectral containment and defending against distributed spectrum injection attacks in cognitive radio networks.

Table 2: Power spectral density and OOB reduction.

Technique	PSD (dB)	% OOB Reduction
Original signal	−33	0.00
CC Pagadari	−37	12.12
ANCC	−43	30.30
CC (Brandes)	−47	42.42
CC GA	−54	63.64
CC + DE	−61	84.85

(Continued)

Table 2 (continued)

Technique	PSD (dB)	% OOB Reduction
GSC	−135	309.09
EGSC	−152	360.61
GSC + GA	−170	415.15
Proposed technique	−220	566.67

4.3 Scenario 3: Uneven White Hole Utilization with Fixed LU Load

In this irregular allocation, uneven gaps between PUs and ULs create localized OOB peaks that attackers can exploit. The proposed method suppressed these leakage points effectively, achieving significant OOB reduction, outperforming GSC+GA and all other methods. This shows the framework's strength in countering unpredictable sidelobe patterns caused by uneven spectral use (Figs. 10 and 11, Table 3).

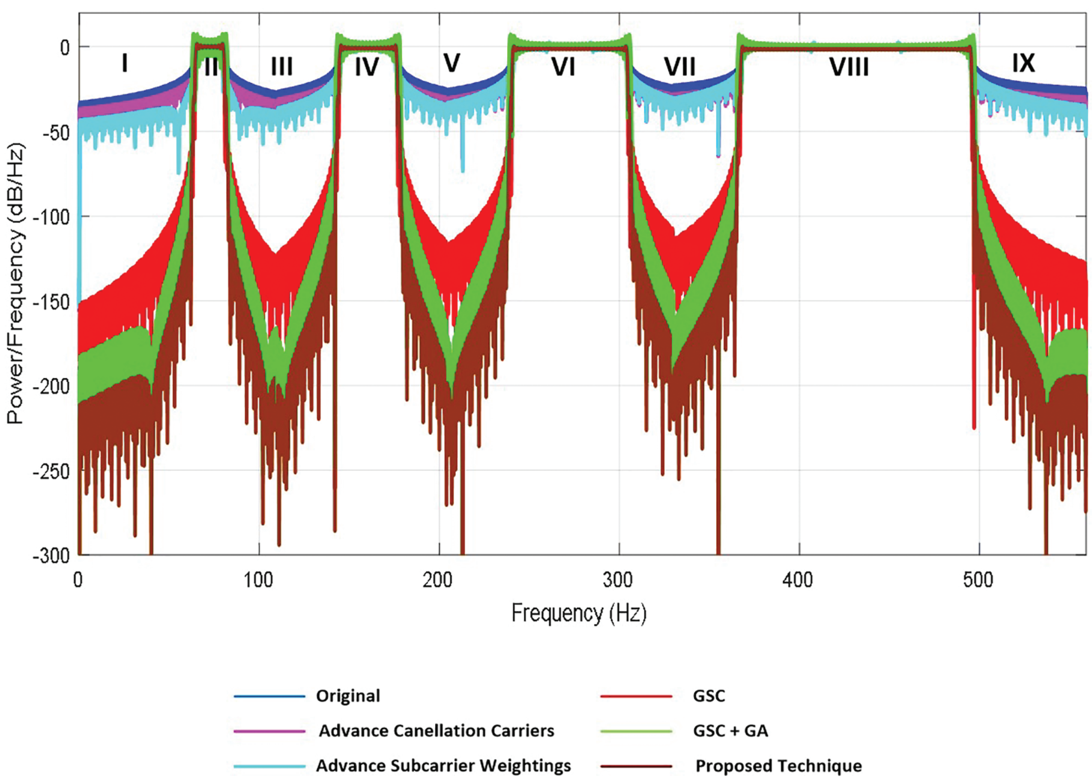

Figure 10: Normalized PSD analysis under irregular spectrum allocation, highlighting the proposed method's effectiveness in minimizing sidelobe leakage and enhancing cybersecurity in cognitive radio networks.

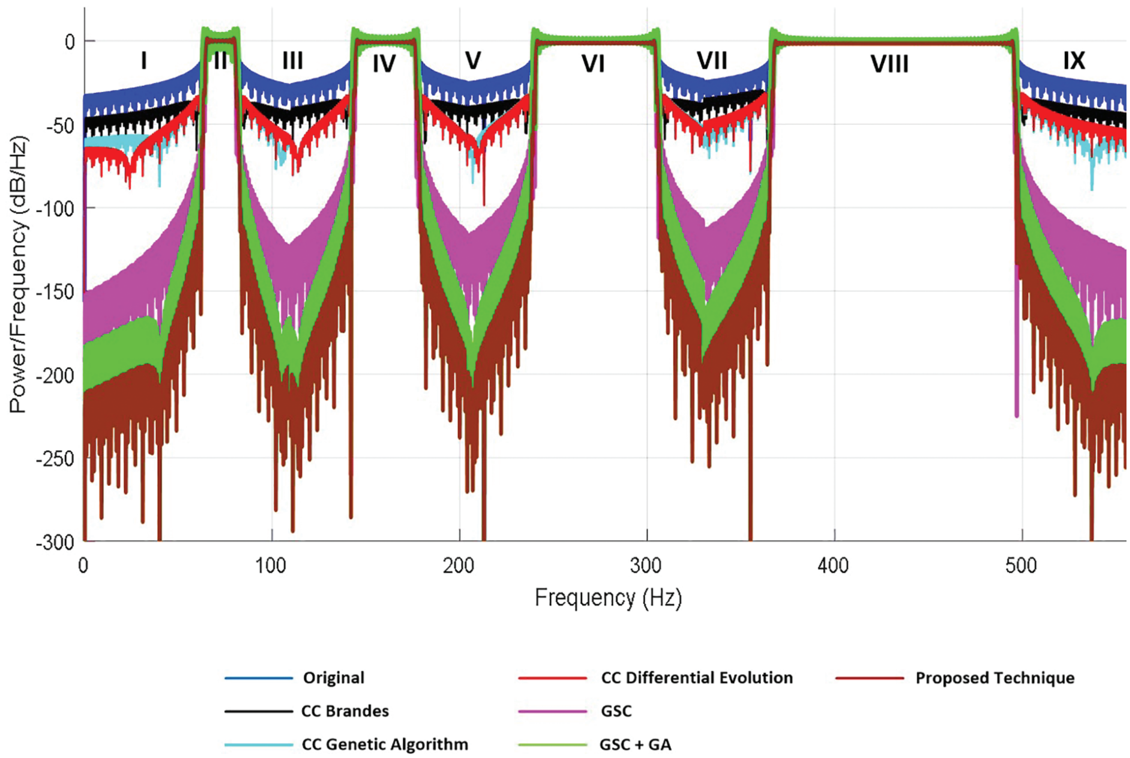

Figure 11: Normalized PSD analysis under irregular spectrum allocation, highlighting the proposed method's effectiveness in minimizing sidelobe leakage and enhancing cybersecurity in cognitive radio networks.

Table 3: Power spectral density and OOB reduction.

Technique	PSD (dB)	% OOB Reduction
Original signal	−33	0.00
ACC	−37	12.12
ASW	−43	30.30
CC (Brandes)	−46	39.39
CC GA	−59	78.79
CC + DE	−75	127.27
GSC	−153	363.64
GSC + GA	−184	457.58
Proposed technique	−210	536.36

4.4 Scenario 4: Consistent UL Load with Variable LU Occupancy

With equal UL bandwidth but varying PU occupancy, predictable sidelobe harmonics usually emerge, which attackers can exploit for synchronization or spoofing. By combining GA-based CC optimization with ES-GSC, our method disrupted harmonic sidelobe patterns, yielding better OOB reduction, a clear improvement over GSC+GA. This demonstrates its ability to prevent long-term targeted interference in dynamic PU distributions (Figs. 12 and 13, Table 4).

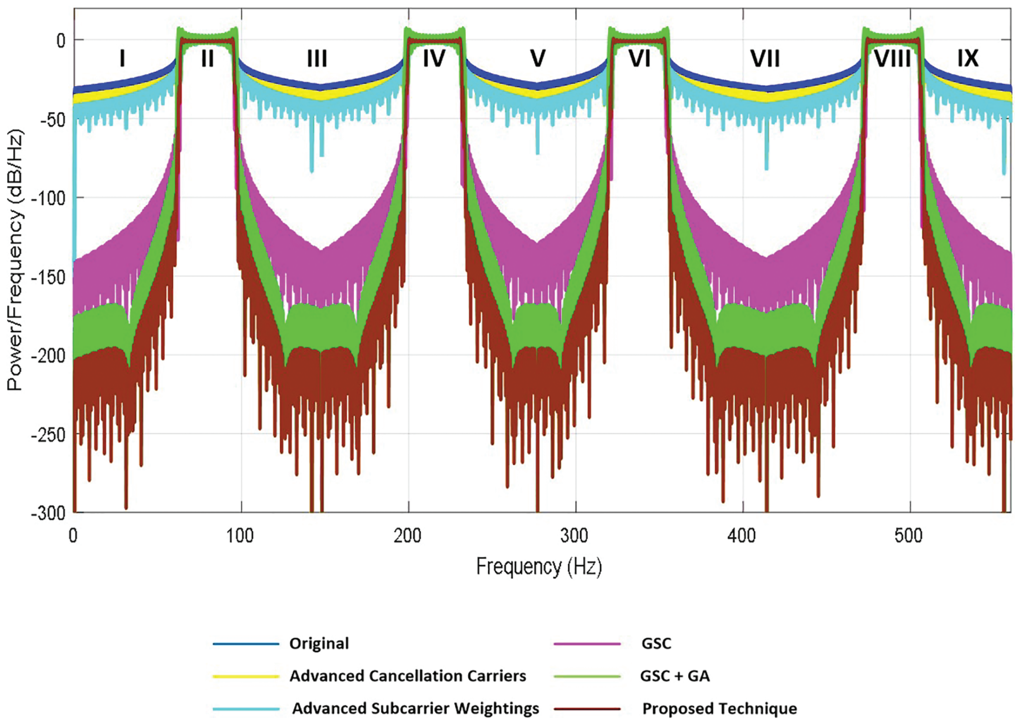

Figure 12: Normalized PSD for equal-sized white holes with variable black hole bandwidths, highlighting enhanced cybersecurity through sidelobe suppression against spectrum injection attacks.

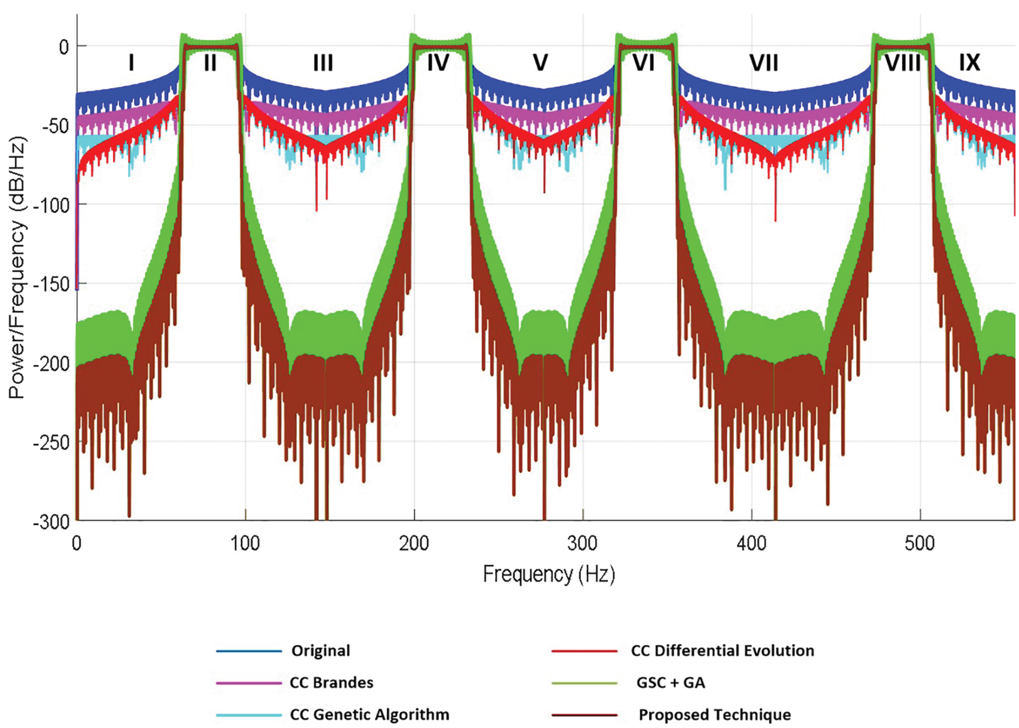

Figure 13: Normalized PSD for equal-sized white holes with variable black hole bandwidths, highlighting enhanced cybersecurity through sidelobe suppression against spectrum injection attacks.

Table 4: Power spectral density and OOB reduction.

Technique	PSD (dB)	% OOB Reduction
Original signal	−31	0.00
ACC	−36	16.13
ASW	−42	35.48
CC (Brandes)	−45	45.16
CC GA	−57	83.87
CC + DE	−80	158.06
GSC	−142	358.06
GSC + GA	−190	512.90
Proposed technique	−220	609.68

4.5 Scenario 5: Fully Dynamic Spectrum Topology

This most challenging case models rapid PU–UL reallocation, where attackers may attempt spectrum hijacking and PUE through fast hopping. The proposed hybrid method adapted in real time, achieving significant OOB reduction, exceeding GSC+GA. This confirms the technique's resilience under fast-changing spectrum conditions and its ability to prevent adversarial synchronization (Figs. 14 and 15, Table 5).

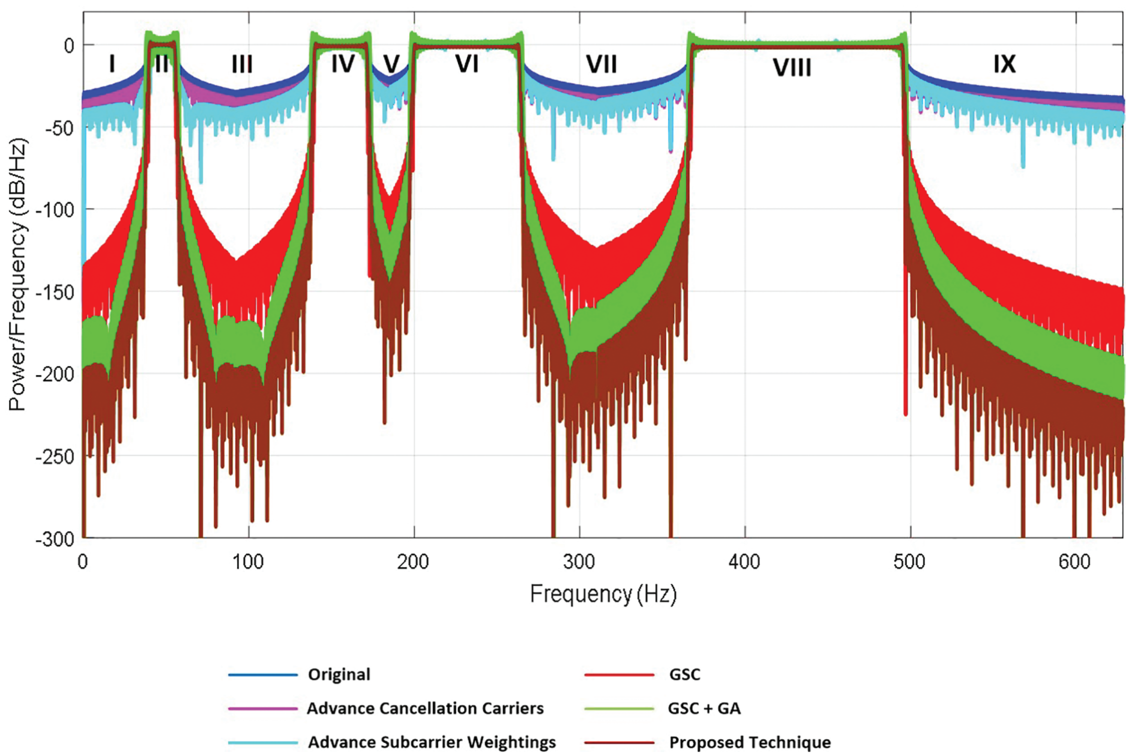

Figure 14: Normalized PSD for variable-sized white and black holes, demonstrating improved spectral security and resilience against sidelobe-based cyber threats using the proposed technique.

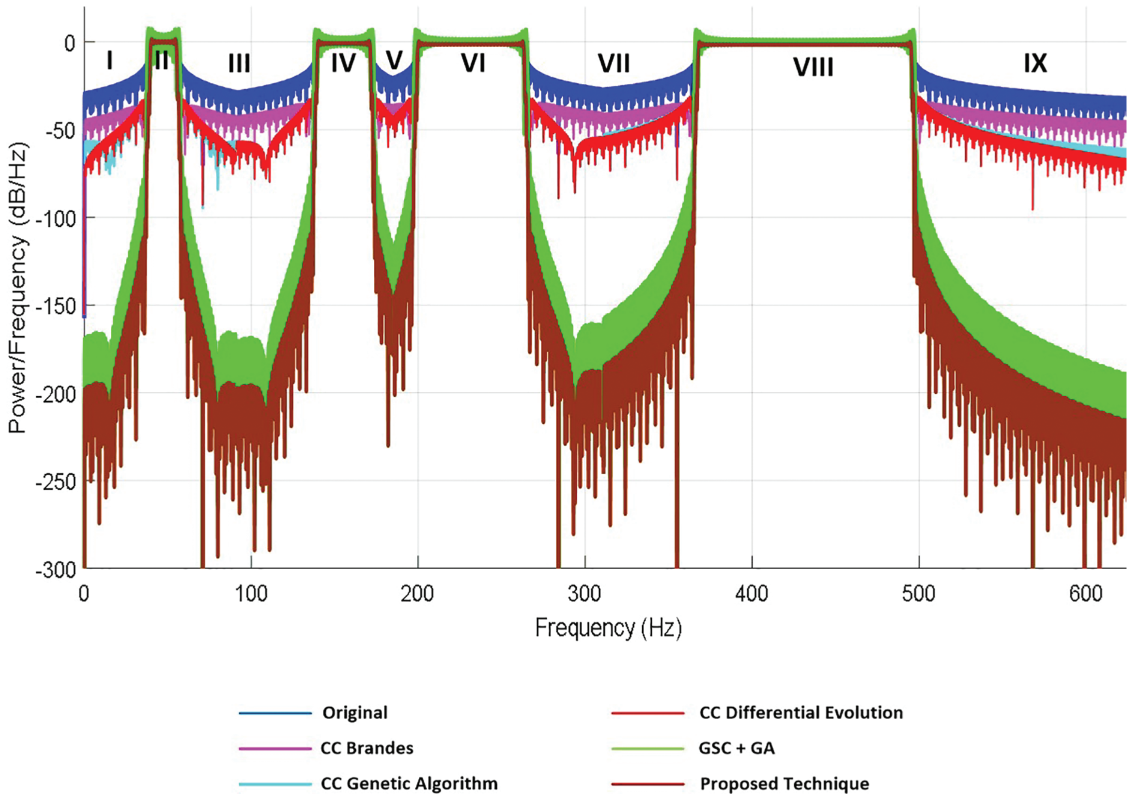

Figure 15: Normalized PSD for variable-sized white and black holes, demonstrating improved spectral security and resilience against sidelobe-based cyber threats using the proposed technique.

Table 5: Power spectral density and OOB reduction.

Technique	PSD (dB)	% OOB Reduction
Original signal	−30	0.00
ACC	−35	16.13
ASW	−40	35.48
CC (Brandes)	−45	45.16
CC GA	−57	83.87
CC + DE	−70	158.06
GSC	−135	358.06
GSC + GA	−190	512.90
Proposed technique	−220	609.68

4.6 Conclusion of Results

Across all scenarios, the proposed hybrid method combining Genetically Optimized Cancellation Carriers and ES-GSC proved highly effective in containing spectral emissions, thereby reducing the physical-layer attack surface. By strengthening the spectral isolation of ULs, the system resists advanced threats such as DoS via spectrum flooding, side-channel injection, and PU impersonation. These findings validate the approach as a cyber-aware waveform design strategy for secure cognitive radio networks.

5 Conclusion & Future Work

This research presented a hybrid cybersecurity-enhanced sidelobe suppression technique for OFDM-based CR systems, addressing the dual challenge of spectral efficiency and vulnerability to spectrum-based attacks. By integrating ES-GSC with GA optimized CCs, the proposed method achieves notable reduction in OOB emissions and significant improvement in sidelobe suppression as compared to conventional techniques. Simulations across five spectrum-sharing scenarios results validate the superior performance of our approach in mitigating interference, improving spectral containment, and enhancing system resilience against potential cybersecurity threats such as jamming, spoofing, and unauthorized access through sidelobe leakage. The proposed technique not only enhances coexistence with legitimate licensed users but also fortifies the dynamic spectrum environment against sophisticated intrusions.

Future work will focus on real-time implementation, using software-defined radio platforms, integration with machine learning for dynamic threat detection and extension to MIMO and multi-user systems, Additionally incorporating hybrid cryptographic techniques and analyzing time complexity will further enhance security and scalability of OFDM-based CR networks.

Acknowledgement: The authors would like to express their sincere gratitude for the collaborative efforts of the research team in addressing the cybersecurity vulnerabilities arising from sidelobe emissions in OFDM-based cognitive radio systems. The conceptualization and design of the Eigen space-based Generalized Sidelobe Canceller were made possible through the combined contributions of Bakhtawar Gul, Atif Elahi, Tahir Saleem, Noor Gul,Fahad Algarni and Insaf Ullah. Their collective efforts in system modeling, simulation, result analysis, and manuscript preparation were instrumental in the successful completion of this study.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Atif Elahi and Fahad Algarni supervised the research, conceptualized the core problem related to sidelobe-induced cybersecurity vulnerabilities in OFDM-based cognitive radio systems, and proposed the use of the Eigenspace-based Generalized Sidelobe Canceller (ES-GSC) as a solution. He also guided the simulation design and led the manuscript preparation. Bakhtawar Gul implemented the proposed methodology under supervision, conducted system modeling and simulations, and contributed to the analysis and writing of the manuscript. Tahir Saleem, Insaf Ullah, and Noor Gul critically reviewed and endorsed the proposed framework. They contributed to refining the system design, assisted in simulation troubleshooting, offered technical insights, and proofread the manuscript to enhance its coherence and academic rigor. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors. The data that support the findings of this study are available from the Corresponding Author, [Insaf Ullah], upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Nomenclature

AST	Adaptive Symbol Transition
AIC	Active Interference Cancellation
CE	Constellation Expansions
CC	Cancellation Carriers
CP	Cyclic Prefix
CR	Cognitive Radio
DFT	Discrete Fourier Transform
DSA	Dynamic Spectrum Access

DE	Differential Evolution
DOS	Denial of Service
ES-GSC	Eigen Space Based Generalized Sidelobe Canceler
GSC	Generalized Sidelobe Canceler
iid	independent, identically distributed
ICI	Inter-Carrier Interference
LU	Licensed User
MITM	Man in the Middle
OOB	Out-of-Band
OFDM	Orthogonal Frequency Division Multiplexing
PSD	Power Spectral Density
PSO	Particle Swarm Optimization
PU	Primary User
PUE	Primary User Emulation
SW	Subcarrier Weightings
SNR	Signal-to-Noise Ratio

References

1. Haykin S. Cognitive radio: brain-empowered wireless communications. IEEE J Sel Areas Commun. 2005 Feb 7;23(2):201–20. doi:10.1109/JSAC.2004.839380.
2. Khozeimeh F, Haykin S. Brain-inspired dynamic spectrum management for cognitive radio ad hoc networks. IEEE Trans Wirel Commun. 2012 Aug 21;11(10):3509–17. doi:10.1109/TWC.2012.081312.111538.
3. Solaija MS, Zegrar SE, Arslan H. Orthogonal frequency division multiplexing: the way forward for 6G physical layer design? IEEE Vehicular Technol Mag. 2024 Jan 8;19(1):45–54. doi:10.1109/MVT.2023.3344432.
4. Elahi A, Gul N, Khan SU. EigenSpace-based generalized sidelobe canceler applied for sidelobe suppression in cognitive radio systems. Wirel Pers Commun. 2021 Dec;121(4):3009–28. doi:10.1007/s11277-021-08861-x.
5. Proakis JG, Salehi M. Digital communications. New York, NY, USA: McGraw-Hill; 2008 [cited 2025 Sep 20]. Available from: https://www.tbooks.solutions/digital-communications-john-g-proakis-masoud-salehi-5th-edition/.
6. Giménez J, Cortés JA, Cañete FJ, Martos-Naya E, Díez L. A modified pulse and design framework to halve the complexity of OFDM spectral shaping techniques. IEEE Commun Lett. 2024;28(9):2146–50. doi:10.1109/LCOMM.2024.3432155.
7. Tank HB. Optimizing windowed filters for enhanced OFDM performance in 5G networks: a comprehensive analysis of PAPR, BER, and PSD. Journal Electr Syst. 2024;20(7s):1845–52. doi:10.52783/jes.3862.
8. Debnath S, Ahmed S, Alam SS. Analysis of filtered multicarrier modulation techniques using different windows for 5G and beyond wireless systems. Wirel Commun Mob Comput. 2024;2024:9428292. doi:10.1155/2024/9428292.
9. Siluveru M, Nanda D, Kesoju M. Evaluation of OFDM system in terms of PAPR and BER using PAPR reduction techniques: windowing and Clipping. Babylonian J Netw. 2024;2024:1–8. doi:10.58496/BJN/2024/001.
10. Devi P, Bharti MR. An efficient spectrum shaping method for OFDM-based cognitive radio system. Int J Wirel Mob Comput. 2025;29(1):83–92. doi:10.1504/IJWMC.2025.147618.
11. Mahmoud HA, Arslan H. Sidelobe suppression in OFDM-based spectrum sharing systems using adaptive symbol transition. IEEE Commun Lett. 2008;12(2):133–5. doi:10.1109/LCOMM.2008.071729.
12. Cosovic I, Brandes S, Schnell M. Subcarrier weighting: a method for sidelobe suppression in OFDM systems. IEEE Commun Lett. 2006;10(6):444–6. doi:10.1109/LCOMM.2006.1638610.
13. Selim A, Doyle L. Real-time sidelobe suppression for OFDM systems using advanced subcarrier weighting. In: Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC); 2013 Apr 7–10; Shanghai, China. p. 4043–7. doi:10.1109/WCNC.2013.6555224.
14. Jon JH, Han CW. Reduction of signal envelope fluctuations in OFDM systems using ACE with double extension. Wirel Pers Commun. 2023;132(2):1177–92. doi:10.1007/s11277-023-10652-5.

15. Dang TH, Tran VN, Nguyen LC. Active constellation modification technique for PAPR reduction of OFDM signals. IEEE Access. 2023;11:137779–97. doi:10.1109/ACCESS.2023.3340437.
16. Begh GR, Mir AH. Constellation expanded active interference cancellation technique for suppression of out-of-band radiation in OFDM based cognitive radios. AEU-Int J Electr Communicat. 2017;76:36–45. doi:10.1016/j.aeue.2017.03.016.
17. Yamaguchi H. Active interference cancellation technique for MB-OFDM cognitive radio. In: Proceedings of the 34th European Microwave Conference, 2004 Oct 12–14; Amsterdam, The Netherlands. Vol. 2, p. 1105–8. doi:10.1109/icwmc.2010.53.
18. Qu D, Wang Z, Jiang T. Extended active interference cancellation for sidelobe suppression in cognitive radio OFDM systems with cyclic prefix. IEEE Trans Vehicular Technol. 2010;59(4):1689–95. doi:10.1109/TVT.2010.2040848.
19. Wang Z, Qu D, Jiang T, He Y. Spectral sculpting for OFDM based opportunistic spectrum access by extended active interference cancellation. In: Proceedings of the IEEE GLOBECOM 2008—2008 IEEE Global Telecommunications Conference; 2008 Nov 30–Dec 4; New Orleans, LA, USA. p. 1–5. doi:10.1109/GLOCOM.2008.ECP.852.
20. Alian EH, Mitran P. A phase adjustment approach for interference reduction in OFDM-based cognitive radios. IEEE Trans Wirel Commun. 2013;12(9):4668–79. doi:10.1109/TW.2013.072213.121994.
21. Lopes FR, Panaro JS. OFDM sidelobe suppression combining active and null cancellation carriers in the guard bands. In: Proceedings of the 2013 SBMO/IEEE MTT-S International Microwave & Optoelectronics Conference (IMOC); 2013 Aug 4–7; Rio de Janeiro, Brazil. p. 1–5. doi:10.1109/IMOC.2013.6646597.
22. Brandes S, Cosovic I, Schnell M. Reduction of out-of-band radiation in OFDM systems by insertion of cancellation carriers. IEEE Commun Lett. 2006;10(6):420–2. doi:10.1109/LCOMM.2006.1638602.
23. Kryszkiewicz P, Bogucka H. Out-of-band power reduction in NC-OFDM with optimized cancellation carriers selection. IEEE Commun Lett. 2013;17(10):1901–4. doi:10.1109/LCOMM.2013.081813.131515.
24. Elahi A, Qureshi IM, Khan ZU, Zaman F. Sidelobe reduction in non-contiguous OFDM-based cognitive radio systems using a generalized sidelobe canceller. Appl Sci. 2015;5(4):894–909. doi:10.3390/app5040894.
25. Kaleem A, Gul N, Elahi A, Haq SU, Kim SM, Kim J. Multiple generalized sidelobe cancellers for minimization of interference in cognitive radio system. Wirel Pers Commun. 2023;133(1):641–66. doi:10.1007/s11277-023-10784-8.
26. Arulkarthick VJ, Srihari K, Arvind C, Mukunthan MA, Sundar R. A hybrid precoded-companding scheme for PAPR reduction in OFDM systems. Natl Acad Sci Lett. 2024;47(3):285–91. doi:10.1007/s40009-023-01354-4.
27. Sathish Kumar S, Arulkarthick VJ, Chakrapani A, Sasikala G. A new hybrid precoding-partial transmit sequence method for PAPR reduction in multicarrier wireless communication systems. Proc Nat Acad Sci India Sec A Phys Sci. 2024;94(2):193–9. doi:10.1007/s40010-023-00866-4.
28. Raghavendra CG, Ashish D, Chaitanya VC. A novel approach to control the sidelobe levels in OFDM radar waveform design using hybrid of sub-carrier weighting and time domain windowing. Int J Wirel Mob Comput. 2023;25(4):322–7. doi:10.1504/IJWMC.2023.135382.
29. Elahi A, Qureshi IM, Atif M, Gul N. Sidelobe reduction in cognitive radio systems using hybrid technique. World Acad Sci Eng Technol Int J Electr Comput Energ Electron Commun Eng. 2017;11(3):213–6.
30. Elahi A, Qureshi IM, Zaman F, Gul N, Saleem T. Suppression of mutual interference in noncontiguous orthogonal frequency division multiplexing based cognitive radio systems. Wirel Commun Mob Comput. 2017;2017:1860134. doi:10.1155/2017/1860134.