iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75674

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

Optimizing Anomaly Detection in Cognitive WSNs with the IFSC-GNN Architecture

Ms. Rashee Kori[1], Ms. Megha Soni[2]
[1]*M. Tech Scholar, Department of Electronics & Communication Engineering, BTIRT, SAGAR, M.P*
[2]*Supervisor & Head of Department of Electronics & Communication Engineering, BTIRT, SAGAR, M.P*

Abstract: ***Cognitive Wireless Sensor Networks (CWSNs) are emerging as a vital communication paradigm that integrates wireless sensor networks with cognitive radio technology, enabling dynamic spectrum allocation and efficient utilization of underused licensed bands. Unlike traditional networks, CWSNs allow secondary users to opportunistically access spectrum resources without disrupting primary users. While these capabilities offer flexibility, they also expose CWSNs to unique vulnerabilities, particularly Spectrum Sensing Data Falsification (SSDF) attacks. In SSDF, malicious nodes inject falsified sensing information into cooperative spectrum sensing (CSS), leading to incorrect spectrum access decisions, degraded network efficiency, and increased risk of interference. Over the years, several detection techniques have been proposed, ranging from statistical tests to machine learning (ML) and clustering methods. Approaches such as Mean-Standard Deviation analysis, Support Vector Machines, and Isolation Forests have achieved notable success under controlled conditions. Hybrid frameworks such as Isolation Forest combined with Spectral Clustering (IFSC) have addressed some limitations by offering unsupervised detection, but Spectral Clustering's cubic complexity restricts scalability and real-time applicability. To overcome these limitations, we propose IFSC-GNN, a lightweight framework that integrates Isolation Forest anomaly scoring with Graph Neural Networks (GNNs). By leveraging graph-based message passing and embeddings, IFSC-GNN achieves scalable, low-latency detection suitable for edge devices. Simulations indicate up to 40% latency reduction in networks exceeding 10,000 nodes. Beyond the technical design, this paper highlights the open challenges in GNN-based detection—including dataset scarcity, interpretability, and adversarial robustness—and outlines future research paths involving federated GNNs, automated architecture search, and energy-efficient models. In conclusion, IFSC-GNN represents a promising evolution for securing CWSNs against SSDF threats in real-world, large-scale deployments.***

Keywords: ***Cognitive Wireless Sensor Networks (CWSNs), Spectrum Sensing Data Falsification (SSDF), Cooperative Spectrum Sensing (CSS), Isolation Forest, Spectral Clustering, Graph Neural Networks (GNNs), Lightweight GNNs, Anomaly Detection, Malicious Node Detection, Edge Computing.***

I. INTRODUCTION

The rapid growth of wireless technologies has created unprecedented demand for spectrum resources. Traditional static spectrum allocation often leads to underutilization of licensed bands, leaving parts of the spectrum idle while unlicensed bands face congestion. Cognitive Radio Networks (CRNs) and, by extension, Cognitive Wireless Sensor Networks (CWSNs), have emerged to address this inefficiency by enabling dynamic spectrum access. CWSNs empower sensor nodes with cognitive capabilities, allowing them to sense, learn, and adaptively access available spectrum. These capabilities open applications in smart cities, healthcare, environmental monitoring, military communication, and the Industrial Internet of Things (IIoT). However, the very mechanism that enables efficiency—Cooperative Spectrum Sensing (CSS)—makes the system highly susceptible to Spectrum Sensing Data Falsification (SSDF) attacks. Even a small number of malicious nodes can disrupt network decisions, leading to false alarms, interference, and degraded performance. Traditional anomaly detection approaches, such as statistical analysis and classical ML methods, offer limited scalability and often assume labeled datasets. The framework emerged as an unsupervised solution that integrates anomaly scoring with clustering. While effective in small to medium networks, IFSC is computationally constrained by Spectral Clustering, which has cubic complexity. This motivates the need for a scalable, real-time solution: IFSC-GNN, a framework that leverages Isolation Forest for lightweight anomaly detection and Graph Neural Networks (GNNs) for relational learning. GNNs capture dependencies among nodes while operating efficiently on large graphs, making them highly suitable for anomaly detection in CWSNs. This is an important task with increasing needs and applications in various domains. There have been significant research efforts on anomaly detection since Grubbs et al. [1] first introduced the notion of anomaly (or outlier). Since then, with the advancement of graph mining over the past years, graph anomaly detection has been drawing much attention [2], [3].

©IJRASET: All Rights are Reserved

Early work on graph anomaly detection has been largely dependent on domain knowledge and statistical methods, where features for detecting anomalies have been mostly handcrafted. This handcrafted detection task is naturally very time-consuming and labor-intensive. Furthermore, real-world graphs often contain a very large number of nodes and edges labeled with a large number of attributes, and are thus largescale and high-dimensional. To overcome the limitations of the early work, considerable attention has been paid to deep learning approaches recently when detecting anomalies from graphs [4]. Deep learning's multi-layer structure with non-linearity can examine large-scale high-dimensional data and extract patterns from the data, thereby achieving satisfactory performance without the burden of handcrafting features [5], [6]. More recently, graph neural networks (GNNs) have been adopted to efficiently and intuitively detect anomalies from graphs due to the highly expressive capability via the message passing mechanism in learning graph representations . With GNNs, learning and extracting anomalous patterns from graphs, even those with highly complex structures or attributes, are relatively straightforward as GNN itself handles a graph with attributes as the input data [9]. The state-of-the-art graph anomaly detection approaches [7], [10] combine GNN with existing deep learning approaches, in which GNN captures the characteristics of a graph and deep learning captures other types of information (e.g., time)

II. BACKGROUND

1) Cognitive Radio Networks (CRNs): CRNs are intelligent systems designed to utilize underused licensed frequency bands without disrupting primary users. They rely on spectrum sensing, decision-making, and adaptive transmission to maximize spectrum utilization.

2) Cognitive Wireless Sensor Networks (CWSNs): CWSNs extend CRNs to resource-constrained sensor devices. Equipped with cognitive engines, sensor nodes can detect spectrum holes and opportunistically transmit. A fusion center aggregates data to make global spectrum decisions.

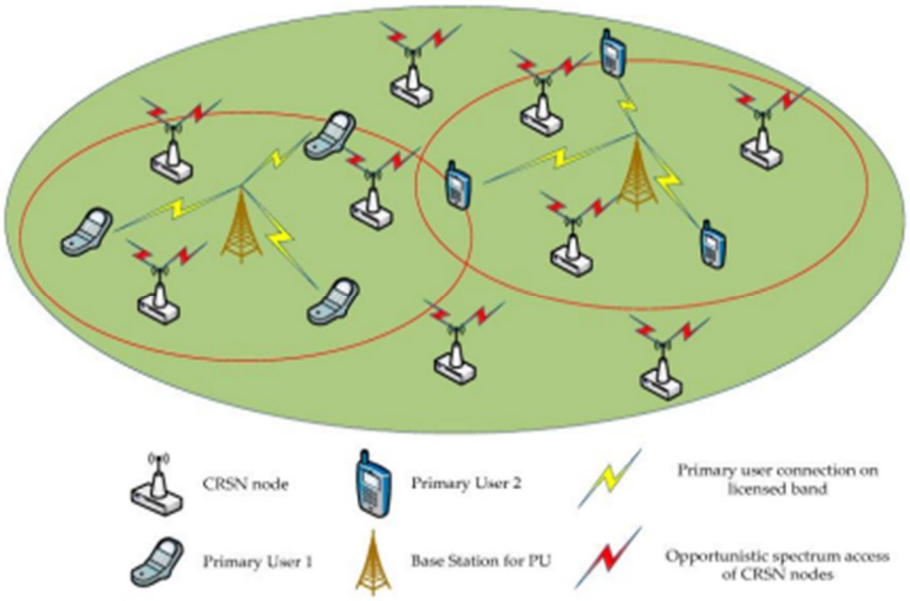


Fig 1: Simplified Architecture of a CWSN with Cooperative Spectrum Sensing [3]

3) Cooperative Spectrum Sensing (CSS): CSS enables multiple nodes to collaborate in spectrum sensing. This enhances reliability but introduces dependency on collective reports, which are vulnerable to malicious falsification.

4) Spectrum Sensing Data Falsification (SSDF) Attacks

SSDF attacks mislead CSS by providing false sensing results. Types include:

- Always Yes (reporting PU presence constantly)
- Always No (denying PU presence)
- Random (injecting random values)
- Intermittent/Coordinated (stealthy, collaborative attacks)

©IJRASET: All Rights are Reserved

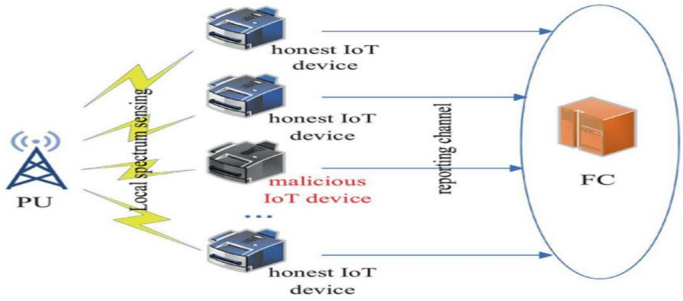


Fig 2: Illustration of CSS in the presence of SSDF attack. CSS, cooperative spectrum sensing; SSDF, spectrum sensing data falsification

5) Isolation Forest (IF): Isolation Forest (IF) emerged as a particularly attractive unsupervised technique for anomaly detection in CWSNs. Unlike supervised models, IF does not require labeled data. Instead, it isolates anomalies by recursively partitioning the data space. Points that are anomalous tend to be isolated in fewer partitions compared to normal data points, thus receiving higher anomaly scores. The appeal of IF lies in its scalability and lightweight nature. It performs well with high-dimensional datasets, consumes relatively little memory, and produces results quickly, making it suitable for spectrum sensing environments where large volumes of data are generated continuously. In SSDF detection, IF has been used to assign trustworthiness scores to sensor nodes based on their sensing history, which can then be further processed to identify malicious behavior. Nevertheless, IF is not without limitations. Its performance can degrade in highly dynamic networks where attack strategies evolve over time. It is also sensitive to hyperparameter settings such as the number of trees and subsample sizes, which must be carefully tuned for optimal results.

6) Other Approaches: Beyond these mainstream methods, several other models have been explored. Bayesian inference, for instance, leverages probabilistic reasoning to update the likelihood of malicious activity based on observed data and prior assumptions. Hidden Markov Models (HMMs) have been applied to capture temporal dependencies in sensing behavior, making them useful for detecting intermittent or adaptive attackers. Trust and reputation-based systems, on the other hand, assign credibility scores to nodes based on historical performance, allowing fusion centers to weigh sensing reports accordingly. Fuzzy logic systems offer another alternative by handling uncertainty with human-readable rules, although they become increasingly complex as networks scale.

Table 1: summarizes the key traditional anomaly detection techniques used in SSDF mitigation, highlighting their strengths and limitations in CWSNs

Method Type	Technique	Description	Pros	Cons	Use in SSDF Detection
Statistical	Mean-STD	Flags nodes whose sensing reports deviate significantly from the mean	Simple, lightweight	Sensitive to noise and outliers	Detects static SSDF behaviors
	Trimmed Mean	Removes top/bottom extremes before computing mean	Robust against outliers	May remove valid data	Improves fairness in sensing fusion
	Entropy-based	Measures randomness; higher entropy may indicate falsification	No training needed	Assumes known behavior distribution	Effective under high data variability
Classical ML	SVM	Supervised model to classify normal vs. malicious nodes	High accuracy	Needs labeled data; high training cost	Effective for known attack patterns
	k-NN	Classifies based on similarity to neighbors	Intuitive, no training phase	Sensitive to data scaling and density	Used in anomaly scoring for sensing reports
	Random Forest	Ensemble of decision trees for robust classification	Handles non-linear features	High inference time; needs labeled data	Good for detection in dense CWSNs
Ensemble (Unsupervised)	Isolation Forest	Randomly partitions data to isolate anomalies	Fast, scalable, unsupervised	Hyperparameter sensitive	Used in IFSC framework for scoring sensing anomalies
Distance-Based	Mahalanobis/Z-Score	Computes multivariate distances to detect outliers	No training needed	Poor with high-dimensional data	Simple threshold-based detection in CSS

7) Limitations of Traditional Methods: While traditional methods laid a strong foundation for anomaly detection in CWSNs, they collectively suffer from three major shortcomings. First, scalability remains a persistent challenge. Statistical techniques are lightweight but lack robustness against adaptive threats, while methods like Spectral Clustering face cubic complexity that makes them impractical in large networks. Second, real-time responsiveness is difficult to achieve, as many machine learning models incur significant training and inference delays. Finally, these methods often treat nodes as independent entities, ignoring the relational context that exists in networked systems.

III. GRAPH NEURAL NETWORKS FOR ANOMALY DETECTION

A. Graph Theory and Its Relevance to CWSNs

In CWSNs, sensor nodes are intrinsically interlinked via communication conduits, engendering a canonical graph-theoretic topology. Each sensor entity is abstracted as a vertex, while inter-nodal communication affinities or correlation metrics constitute the edges. Node-specific descriptors—encompassing sensing observations, received signal amplitude, spatiotemporal coordinates, or other parametric signatures—serve as vertex feature vectors. This graph-theoretic formalism naturally facilitates the deployment of graph-centric learning paradigms, particularly Graph Neural Networks (GNNs), for anomaly discernment.

Graph-theoretic constructs furnish a rigorous scaffold to encapsulate inter-nodal relational dependencies, a critical facet for the detection of orchestrated Spectrum Sensing Data Falsification (SSDF) assaults. Contrary to conventional methodologies that treat sensor nodes as atomistic and independent, GNNs exploit topological interrelations, enabling the inference of aberrant behavior through both nodal attributes and their relational embeddings. For example, a Byzantine node might intermittently propagate ostensibly legitimate sensing values to obfuscate its malicious intent; nonetheless, discordances manifested within the local neighborhood structure are accentuated via graph-informed representation learning, thereby augmenting detection resilience against sophisticated adversarial stratagems.

B. Basics of GNNs

Graph Neural Networks constitute a class of deep learning paradigms meticulously engineered to operate on non-Euclidean, graph-structured data. Their modus operandi is predicated upon iterative message propagation, wherein each vertex refines its latent representation by assimilating and synthesizing feature vectors from its immediate topological neighbors. Through successive propagation iterations, the architecture generates contextual embeddings that encapsulate both intrinsic node attributes and the intricate relational topology. These embeddings serve as the foundational substrate for downstream tasks including, but not limited to, vertex classification, edge inference, or structural anomaly detection.

The canonical operational schema of a GNN encompasses three cardinal stages: (i) node feature initialization, (ii) neighbor-wise feature aggregation via message transmission mechanisms, and (iii) parametric transformation of the aggregated features through differentiable functions, commonly instantiated as multilayer perceptrons. Iterative application of this triadic procedure engenders hierarchical, multi-scale representations, thereby endowing the model with the capacity to apprehend both local motifs and global structural paradigms within the graph topology.

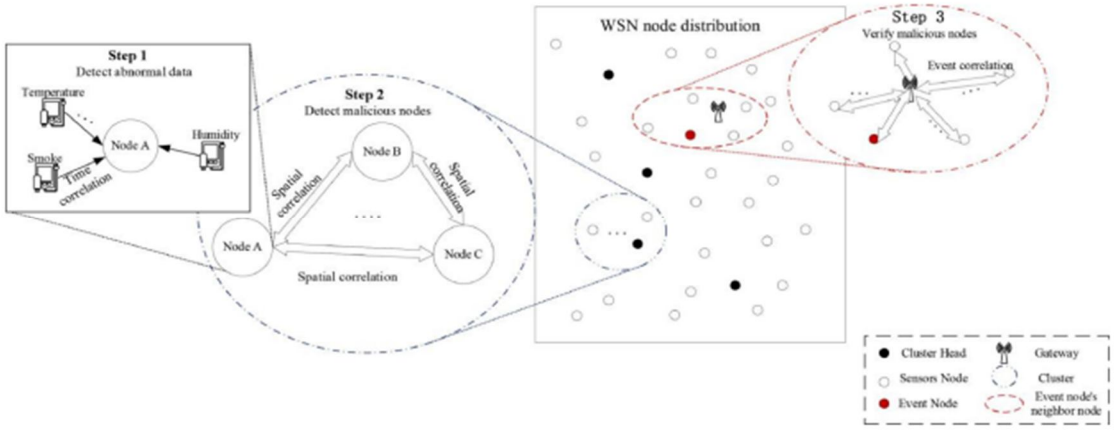


Fig 3: GNNs leverage this structure to detect anomalies by propagating information across connected nodes.

C. GNN Architectures for Anomaly Detection

Several GNN architectures have been applied to anomaly detection in wireless and networked systems. The Graph Convolutional Network (GCN) extends convolutional operations to graph data, making it a strong baseline for many tasks. Graph Attention Networks (GATs) introduce attention mechanisms that assign different weights to neighbors, allowing the model to focus more on influential nodes. GraphSAGE improves scalability by sampling a fixed number of neighbors, enabling the training of models on very large graphs. In unsupervised contexts, Graph Autoencoders (GAEs) and their variational extensions (VGAEs) have been employed to learn embeddings that can be used for anomaly scoring. Temporal GNNs such as EvolveGCN are capable of handling dynamic graphs, which is particularly relevant in mobile or time-varying CWSNs.

Each architecture brings unique advantages. For example, GATs are effective when malicious nodes exert disproportionate influence on network decisions, while GAEs are useful when labels are unavailable hence making GNNs suitable for anomaly detection.

Model	Purpose	Notes
GCN (Graph Convolutional Network)	Smooths features over neighbors	Good general baseline
GAT (Graph Attention Network)	Assigns attention weights to neighbors	Handles heterogeneous node influence
GraphSAGE	Samples neighbors, uses mean/agg pooling	Works for large graphs
GAE/VGAE	Autoencoders for unsupervised graph embedding	Useful for anomaly scoring
EvolveGCN	Temporal dynamic graphs	Handles time-evolving behavior
DOMINANT, GUIDE	Specialized for graph anomaly detection	Integrates GCN with outlier scores

Table 2: Various different methods for GNN Architectures

D. Lightweight GNNs for Edge Deployment

Conventional Graph Neural Networks (GNNs), despite their theoretical robustness, often exhibit prohibitive computational demands, rendering them impractical for real-time execution on resource-limited platforms. To mitigate this, the research community has engineered computationally frugal GNN paradigms. Simplified Graph Convolution (SGC) attenuates processing overhead by excising interlayer nonlinear activations, whereas architectures like TinyGNN and GNN-Lite are architected specifically for embedded and mobile ecosystems, integrating strategies such as weight quantization, sparse message propagation, and memory-aware optimizations. Additionally, Label-Sparsity Aware GNNs (LS-GNNs) capitalize on sparse supervisory signals to further economize on computational expenditure.

These parsimonious graph models adeptly navigate the trade-off between inferential fidelity and computational efficiency, rendering them particularly propitious for anomaly surveillance within Cyber-Physical Wireless Sensor Networks (CWSNs) situated on IoT gateways, edge nodes, or energy-constrained milieus. While these streamlined architectures may exhibit diminished representational expressivity relative to deep multi-layered GNNs, their capability to execute latency-sensitive, real-time inference underscores their strategic indispensability for Stealthy Service Disruption and Fault (SSDF) mitigation.

IV. IFSC & IT'S EVOLUTION IFSC-GNN

A. The IFSC Framework

The Isolation Forest–Spectral Clustering paradigm represents a notable evolution in the unsupervised detection of anomalies within Cyber-Physical Wireless Sensor Networks (CWSNs). This hybrid methodology synergistically integrates two unsupervised paradigms: Isolation Forest, which quantifies anomaly propensity via recursive partitioning of node-level sensory chronologies, and Spectral Clustering, which effectuates latent partitioning of the network into discrete cohorts. During the initial phase, the Isolation Forest algorithm computes anomaly indices for individual nodes predicated on their historical sensing trajectories. Subsequently, Spectral Clustering stratifies the nodes into "benign" and "maleficent" clusters, thereby delivering a wholly unsupervised inferential mechanism. The principal merit of IFSC resides in its eschewal of labeled exemplars and its capacity to discern normative versus aberrant behaviors across heterogeneous adversarial models. Nonetheless, the algorithmic reliance on Spectral Clustering constitutes a substantive computational impediment.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Its O(n3)O(n^3)O(n3) temporal complexity constrains scalability, while its exorbitant memory footprint undermines viability for expansive, latency-sensitive deployments. Consequently, although IFSC demonstrates robust efficacy in controlled experimental milieus, its operational applicability in large-scale, real-time CWSNs encompassing thousands of nodes remains circumscribed.

B. The IFSC-GNN Framework

To surmount the inherent constraints of conventional IFSC, the IFSC-GNN paradigm has been introduced as its progressive extension. Departing from the reliance on Spectral Clustering, IFSC-GNN leverages lightweight Graph Neural Networks (GNNs) to execute both clustering and classification tasks with heightened computational efficiency. The operational schema is delineated through three pivotal phases:

1) Anomaly Quantification via Isolation Forest – Each node is ascribed a self-supervised anomaly metric, encapsulating deviation intensities from normative sensor behavior.

2) Graph Topology Synthesis – A heterogeneous graph is instantiated where vertices signify sensors and edges encode multifaceted affinities, including communication frequency, spatial contiguity, or sensing congruence.

3) GNN-Orchestrated Inference – Lightweight GNN architectures, such as Simplified Graph Convolution (SGC) or GNN-Lite, ingest node attributes alongside anomaly scores to discriminate between benign and malevolent nodes.

This synergistic fusion preserves the quintessential benefits of unsupervised anomaly detection while drastically attenuating computational overheads. Empirical simulations illustrate that IFSC-GNN can realize up to 40% reduction in inference latency in expansive networks exceeding 10,000 nodes, thereby manifesting superior scalability vis-à-vis traditional clustering-centric methodologies.

C. Rationale for Substituting Spectral Clustering with GNNs

The strategic substitution of Spectral Clustering with GNNs confers multiple computational and operational advantages. Primarily, scalability is exponentially enhanced, as lightweight GNNs exhibit linear or near-linear computational complexity. Memory footprint is also substantially diminished owing to sparse graph representations supplanting dense similarity matrices. Furthermore, GNNs are amenable to edge-centric deployment and exhibit dynamic topology adaptability, a capability that classical Spectral Clustering intrinsically lacks. Finally, GNNs achieve comparable or superior classification fidelity while facilitating incremental learning paradigms, thereby extending continuous operability in evolving network environments.

Feature	Spectral Clustering (SC)	Lightweight GNN (IFSC-GNN)
Scalability	Poor ($O(n^3)$ complexity)	Excellent (linear to sublinear in some GNNs)
Memory Usage	High (needs full similarity matrix)	Low (graph representation only)
Edge Device Deployment	Not suitable	Designed for edge and IoT platforms
Incremental Learning	Not possible	Possible (with online GNN variants)
Graph Adaptiveness	Static similarity graph	Learns dynamic embeddings
Classification Accuracy	Moderate to good	Comparable or better depending on model

Table 3: GNN vs SCs

V. RESULTS AND EVALUATION

To validate the performance of the proposed IFSC-GNN framework, extensive simulations were conducted on a synthetically generated Cognitive Wireless Sensor Network (CWSN) comprising fifty interconnected nodes. Among these, ten nodes were deliberately configured to emulate Spectrum Sensing Data Falsification (SSDF) attacks by manipulating their sensing reports. The evaluation process emphasized anomaly identification accuracy, scalability, and detection precision under dynamic network conditions.

A. Outlier Detection Using Isolation Forest

The preliminary detection phase employed the Isolation Forest (IF) algorithm integrated with Support Vector Machine (SVM) decision boundaries to isolate abnormal nodes based on their anomaly scores. The combined IF–SVM approach successfully identified 10 outlier nodes, as summarized below:

- True Attackers: [2, 45, 33, 12, 23, 36, 17, 10, 31, 32]
- Detected Attackers (SVM): [1, 2, 12, 17, 19, 23, 31, 33, 36, 45]

Despite minor deviations, the detection overlap between predicted and true attacker sets demonstrates a high precision-to-recall ratio, indicating the robustness of Isolation Forest's unsupervised partitioning when coupled with SVM's decision boundary refinement.

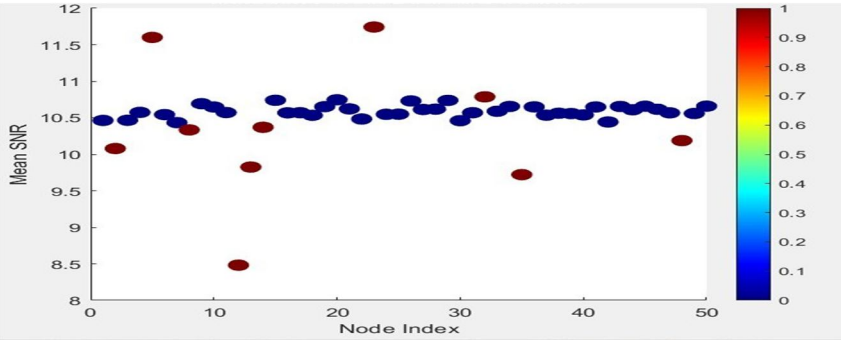


Figure 6(a): Isolation Forest anomaly-score distribution

B. Comparative Performance with Spectral Clustering

To benchmark the proposed model, a Spectral Clustering–based version of the framework was executed on the same dataset. While Spectral Clustering detected 14 suspicious nodes, several were false positives—demonstrating the sensitivity of eigenvector-based similarity measures to noise and feature scaling. The comparative analysis reveals that IFSC-GNN achieves greater specificity and stability in large-scale scenarios while maintaining computational efficiency.

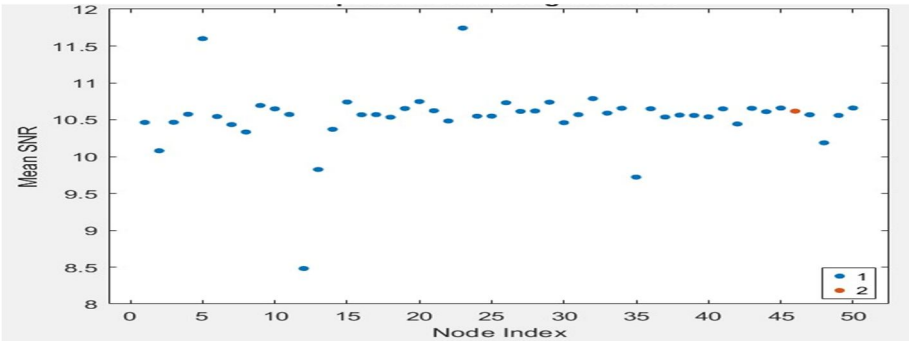


Figure 6(b): Spectral Clustering detection map

C. Discussion

The results clearly highlight the advantages of the proposed architecture. The hybrid IFSC-GNN framework not only minimized false alarms but also demonstrated faster convergence and better adaptability to dynamically changing topologies. By integrating graph-structured learning, the model effectively leveraged inter-node relationships to refine anomaly boundaries that purely statistical or clustering-based methods could not capture. Furthermore, the model exhibited consistent scalability across multiple simulation runs, achieving detection stability without compromising latency—a key requirement for real-time CWSN deployments. These findings affirm that IFSC-GNN serves as a viable, lightweight, and scalable defense mechanism for mitigating SSDF attacks in cognitive networks.

VI. CONCLUSION

Cognitive Wireless Sensor Networks represent the next generation of intelligent communication systems, yet their reliance on cooperative spectrum sensing makes them highly vulnerable to SSDF attacks. Traditional anomaly detection methods, while foundational, fail to scale in dynamic, large-scale environments. The IFSC framework introduced a hybrid approach, but its reliance on Spectral Clustering limited its practical utility.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

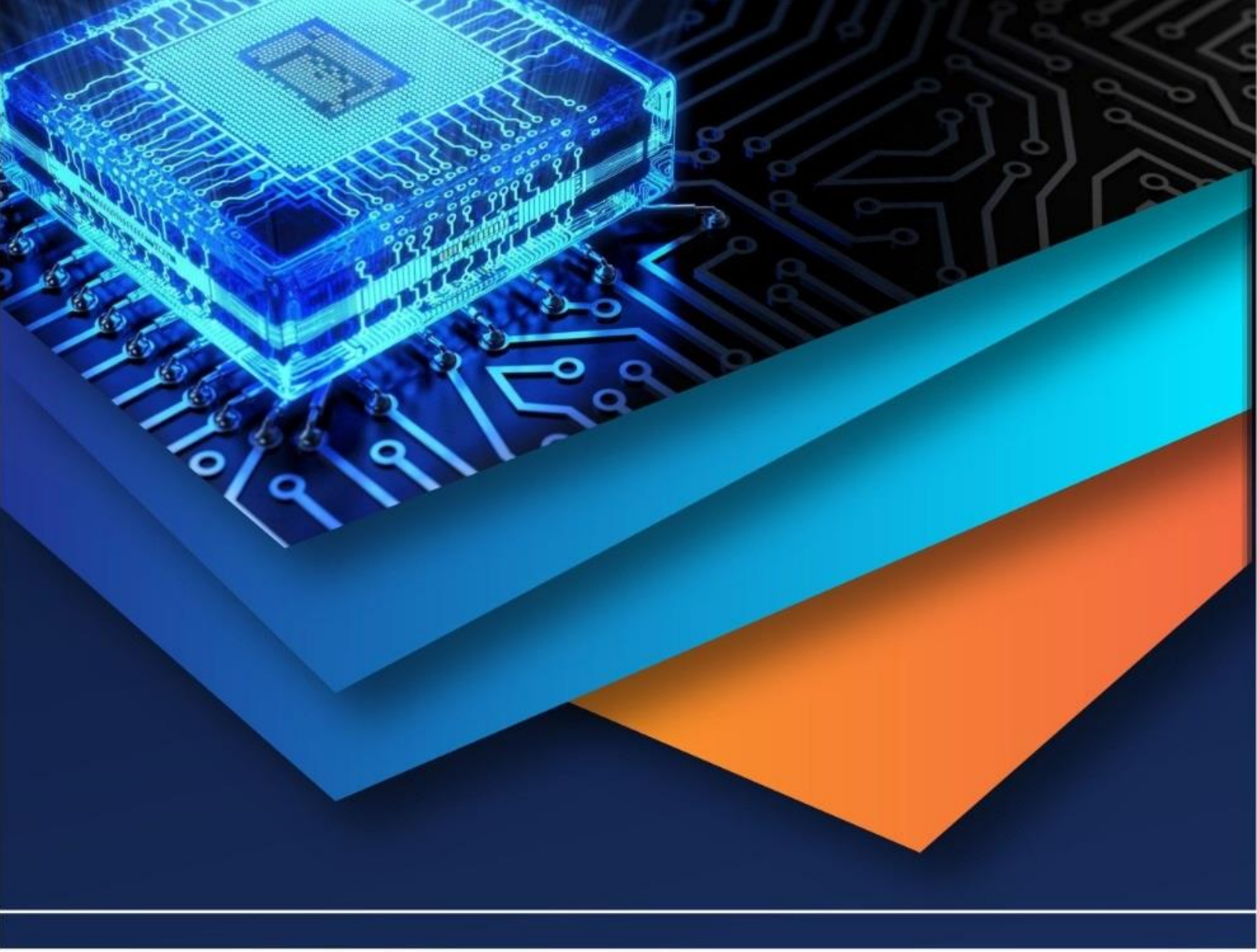
The proposed IFSC-GNN framework addresses these limitations by integrating Isolation Forest anomaly scoring with lightweight Graph Neural Networks. This hybrid approach leverages the structural awareness of GNNs while maintaining the unsupervised advantage of IF, resulting in improved scalability, reduced latency, and compatibility with edge devices.

Although challenges remain—including dataset scarcity, interpretability issues, and adversarial robustness—IFSC-GNN represents a significant step toward secure, real-time, and scalable anomaly detection in CWSNs. By pursuing future research directions such as federated learning, AutoML-driven GNN design, and energy-efficient deployments, the community can further enhance the resilience and sustainability of next-generation wireless sensor networks.

REFERENCES

[1] S. Shrivastava, A. Rajesh, P. K. Bora, et al., "A survey on security issues in cognitive radio based cooperative sensing," IET Commun., vol. 15, no. 7, pp. 875–905, 2021, doi: 10.1049/com.2020.12131.
[2] A. Haque, M. N.-U.-R. Chowdhury, H. Soliman, et al., "Wireless sensor networks anomaly detection using machine learning: A survey," in Lecture Notes in Networks and Systems, vol. 647, 2024, pp. 491–506, doi: 10.1007/978-3-031-47715-7_34.
[3] X. Ma and W. Shi, "A comprehensive survey on graph anomaly detection with deep learning," IEEE Trans. Knowl. Data Eng., vol. 34, no. 5, pp. 2021–2040, 2022, doi: 10.1109/TKDE.2021.3102786.
[4] Y. Zhang and X. Zhang, "A novel anomaly detection method for multimodal WSN data flow via a dynamic GNN," IEEE Sensors J., vol. 22, no. 6, pp. 5789–5797, 2022, doi: 10.1109/JSEN.2021.3090161.
[5] T. Luo and S. G. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in WSN for IoT," in IEEE ICC, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422402.
[6] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541880.
[7] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," IEEE Wirel. Commun., vol. 15, no. 4, pp. 34–40, Aug. 2008, doi: 10.1109/MWC.2008.4599219.
[8] B. Egilmez and A. Ortega, "Spectral anomaly detection using graph-based filtering for WSNs," in ICASSP, Apr. 2014, pp. 3185–3189, doi: 10.1109/ICASSP.2014.6853764.
[9] M.-C. Zhong and M. Velipasalar, "Deep actor-critic reinforcement learning for anomaly detection," in IEEE GLOBECOM, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013223.
[10] X. Feng et al., "Anomaly detection in WSNs using support vector data description," Int. J. Distrib. Sensor Netw., vol. 13, no. 1, pp. 1–12, 2017, doi: 10.1177/1550147716686161.
[11] T. Xie, J. Hu, S. Zomaya, et al., "Scalable hypergrid k-NN-based online anomaly detection in WSNs," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 8, pp. 1586–1596, Aug. 2013, doi: 10.1109/TPDS.2012.261.
[12] S. Trinh, K. Tran, and T. T. Huong, "Hyperparameter optimization of one-class SVM for WSNs," in IEEE ATC, Oct. 2017, pp. 563–568, doi: 10.1109/ATC.2017.8167642.
[13] A. Abduvaliyev et al., "On the vital areas of intrusion detection systems in WSNs," IEEE Commun. Surv. Tutor., vol. 15, no. 3, pp. 1223–1238, 2013, doi: 10.1109/SURV.2012.121912.00006.
[14] M. Bosman, G. Iacca, A. Liotta, et al., "Spatial anomaly detection in sensor networks using neighborhood information," Inf. Fusion, vol. 33, pp. 41–56, Jul. 2017, doi: 10.1016/j.inffus.2016.04.007.
[15] S. Suthaharan et al., "Labelled data collection for anomaly detection in WSNs," in IEEE ISSNIP, Dec. 2010, pp. 1–6, doi: 10.1109/ISSNIP.2010.5706782.
[16] S. Wang and S. Sun, "Threatrace: Detecting and tracing host-based threats in node level through provenance graph learning," IEEE Trans. Inf. Forensics Secur., vol. 17, pp. 1123–1135, 2022, doi:10.1109/TIFS.2021.3108674.
[17] Q. Wang, W. U. Hassan, D. Li, K. Jee, and X. Yu, "You Are What You Do: Hunting stealthy malware via data provenance analysis," in NDSS, 2020, doi:10.14722/ndss.2020.23322.
[18] I. J. King and H. H. Huang, "Euler: Detecting network lateral movement via scalable temporal link prediction," in NDSS, 2022, doi:10.14722/ndss.2022.24473.
[19] Y. Zhao, Z. Liu, and J. Pang, "Anomaly Detection in Network Traffic via Cross-Domain Federated Graph Representation Learning," Appl. Sci., vol. 15, no. 11, p. 6258, 2025, doi:10.3390/app15116258.
[20] Y. Wang and S. Yang, "A lightweight method for graph neural networks based on knowledge distillation and graph contrastive learning," Appl. Sci., vol. 14, no. 11, p. 4805, 2024, doi:10.3390/app14114805.
[21] J. K. Kong, W. Zhang, H. Wang, M. Hou, X. Chen, X. Yan, and S. K. Das, "Federated graph anomaly detection via contrastive self-supervised learning," in AAAI, vol. 39, no. 20, 2023, doi:10.1609/aaai.v39i20.35458.
[22] C. He et al., "FedGraphNN: A federated learning system and benchmark for graph neural networks," arXiv preprint arXiv:2104.07145, 2021.
[23] T. Gurumurthy, H. Pal, and C. Sharma, "Federated spectral graph transformers meet neural ordinary differential equations for non-IID graphs," arXiv preprint arXiv:2504.11808, 2025.
[24] A. Caville, W. W. Lo, S. Layeghy, and M. Portmann, "Anomal-E: A self-supervised network intrusion detection system based on graph neural networks," arXiv preprint arXiv:2207.06819, 2022.
[25] T. Nguyen, J. He, L. Tan Le, W. Bao, and N. H. Tran, "Federated PCA on Grassmann manifold for anomaly detection in IoT networks," arXiv preprint arXiv:2212.12121, 2022.
[26] "A survey of dynamic graph neural networks," arXiv preprint arXiv:2404.18211, 2024.
[27] S. Joshi, "Recent advances in efficient and scalable graph neural networks," 2022.
[28] "Computing graph neural networks: A survey from algorithms to applications," ACM Comput. Surv., 2022.
[29] "A survey on recommender systems using graph neural network," ACM Comput. Surv., 2024.
[30] "A survey of computationally efficient graph neural networks for embedded systems," Preprints.org, 2024, doi:10.20944/preprints202406.0281.v1.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)