MultiScale Spectral GNN for Fraud Detection

Melike Yildiz Aktas[1][0000−0001−9138−3630], Mustafa Coskun[2][0000−0003−4805−1416], and Chang-Tien Lu[1][0000−0003−3675−0199]

[1] Department of Computer Science, Virginia Tech, Alexandria, VA 22305, USA
[2] Department of Artificial Intelligence and Data Engineering, Ankara University, Ankara, Turkiye
melike@vt.edu, coskun.mustafa@ankara.edu.tr, clu@vt.edu

Abstract. Learning on graphs that exhibit both homophilic and heterophilic structures remains a fundamental challenge in graph representation learning, particularly for critical applications such as fraud detection. Existing studies typically model the underlying graph as either homophilic or heterophilic; however, real-world graphs often display varying degrees of homophily across different subgraphs. To address this limitation, we propose a novel model, the MultiScale Spectral Graph Neural Network (MSSGNN), which tackles this challenge by integrating multi-level spectral filtering with relation-aware subgraph decomposition. Our approach introduces a hierarchical spectral filtering framework employing Beta wavelets at multiple scales, enabling the model to effectively capture diverse heterophily patterns. Node clusters are dynamically extracted based on local edge homophily scores, computed by a lightweight Relation-Aware module. Customized wavelet filters with adaptive propagation depths are applied to each subgraph, and the outputs are fused through a learnable attention mechanism to adaptively integrate multi-level heterophily signals. Experimental results on benchmark fraud detection datasets demonstrate that MSSGNN outperforms existing methods, validating the effectiveness of hierarchical spectral processing and relation-aware subgraph modeling. This work provides a flexible and principled approach for learning robust node representations in highly irregular and adversarial graph environments.

Keywords: Spectral graph neural network · Fraud detection · Heterophily · Homophily.

1 Introduction

In real-world graph-based systems, such as financial transaction networks and e-commerce platforms, fraudsters often associate with legitimate entities to evade detection [1], as illustrated in Figure 1. This behavior introduces heterophily—a phenomenon where connected nodes belong to different classes—posing significant challenges for conventional graph neural networks (GNNs) that typically assume homophily [2]. Effectively learning node representations in the presence of both homophilic and heterophilic structures thus remains a central challenge

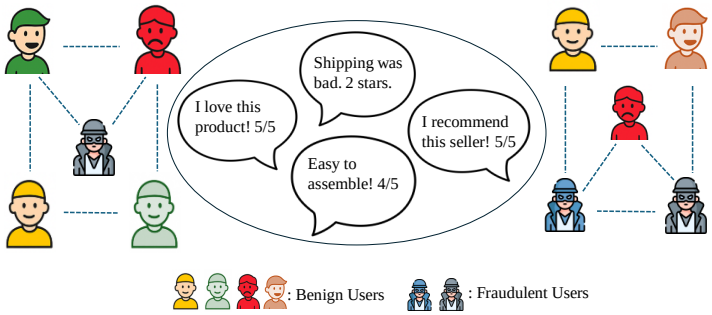

Fig. 1. In online platforms, fraudulent users often connect with benign users and positively interact with shared items (e.g., fake reviews or ratings). This creates a heterophilic graph structure where fraudsters camouflage within legitimate communities, making them difficult to detect using traditional GNNs that assume homophily.

in graph representation learning, particularly for fraud detection applications [3].

Recent studies have analyzed the spectral properties of graphs under varying degrees of heterophily and observed a notable shift in spectral energy from low to high frequencies when fraud or anomalous nodes are present [4]. These observations motivate the development of approaches that operate in the spectral domain to better capture frequency-based patterns. Some existing methods address this issue by employing MLP-based edge classifiers to distinguish homophilic from heterophilic edges [5]. However, such strategies introduce additional learnable parameters, require edge-level supervision, and often suffer from reduced robustness across diverse graph topologies.

To address these limitations, we propose MultiScale Spectral GNN (MSSGNN), a novel framework that leverages hierarchical spectral filtering and relation-aware subgraph decomposition to better model heterophilic and homophilic structures in fraud detection graphs. MSSGNN introduces a multi-scale wavelet-based filtering mechanism, enabling the network to operate across different frequency bands that correspond to mild, medium, and extreme levels of heterophily. Instead of relying on supervised edge classification, we dynamically cluster nodes based on unsupervised local edge homophily scores, computed through a lightweight relation-aware scoring module. Customized Beta wavelet filters with adaptive propagation depths are applied at each scale, and the resulting representations are fused through a learnable attention mechanism. This design allows MSSGNN to adaptively integrate heterophily information at multiple scales while maintaining robustness across diverse and irregular graph structures.

Our approach is evaluated on real-world fraud detection datasets, where it consistently demonstrates strong performance. Comparative analyses against strong baseline models highlight the superior predictive performance achieved by the MultiScale Spectral Graph Neural Network (MSSGNN). These results highlight the value of combining hierarchical spectral filtering with relation-aware subgraph decomposition for modeling heterophilic structures in fraud detection.

The main contributions of our study are summarized as follows:

- **Proposing a novel multi-scale spectral GNN framework (MSSGNN) for fraud detection:** MSSGNN integrates hierarchical spectral filtering and adaptive subgraph modeling to effectively handle graphs with mixed homophilic and heterophilic structures, commonly seen in fraud detection scenarios.
- **Introducing a relation-aware, unsupervised subgraph decomposition strategy:** We develop a lightweight edge scoring module that computes continuous homophily scores between nodes, enabling the dynamic partitioning of nodes into subgraphs based on local structural heterogeneity—without requiring edge labels.
- **Designing scale-specific Beta wavelet filters with adaptive propagation depths:** To extract frequency-aware representations, each subgraph is processed through customized Beta wavelet kernels. These are tailored by propagation depth (K) to target different spectral bands aligned with varying degrees of heterophily.
- **Developing a learnable attention-based fusion mechanism across heterophily scales:** The multi-scale embeddings generated from each subgraph are fused through an attention module that adaptively weighs each subgraph's contribution, enhancing robustness to topology shifts and noise.
- **Conducting comprehensive evaluations on real-world fraud detection datasets:** We validate the effectiveness of MSSGNN on two benchmark datasets (YelpChi and Amazon), where it consistently outperforms strong baselines in both AUC and F1 score, demonstrating its practical advantage in identifying fraudulent behavior on graphs.

2 Related Work

This section reviews the related literature in three main categories: (1) general approaches to fraud detection; (2) the application of graph neural networks to fraud detection; and (3) spectral graph neural networks.

2.1 Fraud Detection

Any type of fraud, which involves deceptive practices to obtain financial gain, has become a serious concern for businesses and organizations. Detecting fraudulent activities is inefficient and expensive with traditional methods, such as manual verification and auditing [6]. With advances in artificial intelligence [7], machine learning techniques [8] have gained prominence as effective tools to analyze large volumes of financial data and identify fraud more intelligently and efficiently.

Some researchers address the fraud detection problem as an anomaly detection task [4], given that fraudulent instances typically constitute a very small portion of the entire dataset. Data mining [9], data engineering [10], and blockchain [11] are widely applied for fraud detection task.

Different application domains, such as credit card transactions [12–15], insurance claims [16–19], and e-commerce platforms [20–24], have motivated the design of various specialized fraud detection models. However, major challenges remain, including severe class imbalance, the evolving strategies of fraudsters (concept drift), and the scarcity of labeled fraudulent instances.

2.2 Graph Neural Networks for Fraud Detection

Recently, graph-based approaches have gained increasing attention especially in social networks because graphs have ability to model complex relationships between entities, such as transactions, users, and products [25–27]. Unlike traditional feature-based methods, graph-based models can exploit relational patterns and detect subtle fraudulent behaviors that may be difficult to capture otherwise [2].

Graph Neural Networks (GNNs) have emerged as a powerful class of models designed to operate directly on graph-structured data. By aggregating and transforming information from neighboring nodes, GNNs can effectively capture both local and global structural patterns [28, 29]. This makes them particularly well-suited for fraud detection tasks, where understanding the interactions between different entities is crucial for identifying anomalous or deceptive behavior.

Several variants of GNNs have been proposed to enhance model expressiveness, including convolutional [30, 31], attention-based [32–34], and spectral approaches [5, 35]. Among these, spectral GNNs leverage graph signal processing techniques to perform convolutions in the spectral domain, offering a principled way to analyze graph frequency components.

2.3 Spectral Graph Neural Networks

Spectral Graph Neural Networks (Spectral GNNs) form a subclass of GNNs that utilize graph signal processing techniques to learn representations in the spectral domain, typically through graph Laplacian-based filters [36]. Despite their potential in capturing global graph structures and contributing to both graph signal processing and representation learning, spectral methods have received comparatively less attention than spatial approaches, leaving important theoretical and practical aspects underexplored [37, 38].

Traditional spectral GNNs often rely on scalar-to-scalar filtering over individual eigenvalues using fixed-order polynomial approximations, which limits their flexibility and ability to model complex spectral patterns [39]. More recent developments have begun to address these limitations through automated and adaptive frameworks, enhancing the versatility of spectral GNNs across diverse graph types—ranging from homophilic to heterophilic—while also reducing the dependency on manual architecture design [40, 41].

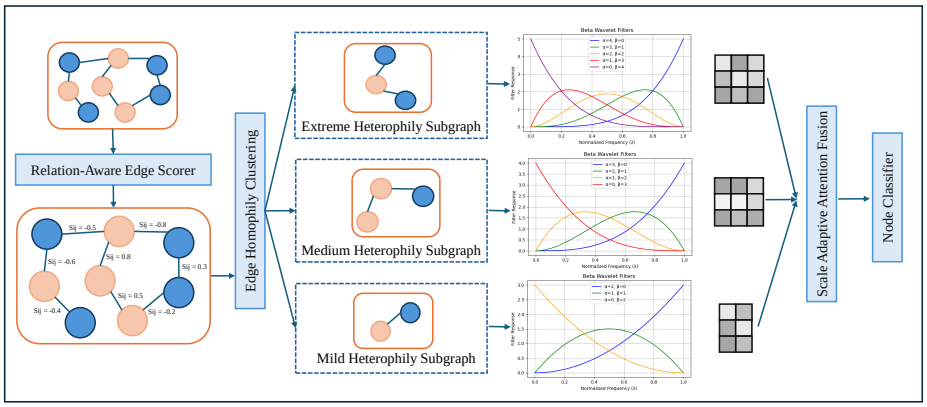

Fig. 2. Framework of Proposed MSSGNN: From left to right, the model comprises three key components: (1) a Relation-Aware Edge Scoring module that estimates edge-level homophily; (2) Subgraph Decomposition and Hierarchical Spectral Filtering, which leverages Beta wavelets to process subgraphs at multiple spectral scales; and (3) a Scale-Adaptive Fusion module that employs an attention mechanism to integrate multi-scale representations.

3 Methodology

In this section, we present the detailed architecture of MultiScale Spectral GNN (MSSGNN) and provide theoretical and practical insights into its design. MSSGNN is designed to effectively capture both homophilic and heterophilic patterns in fraud-related graphs by leveraging spectral filtering across multiple frequency bands, adaptive subgraph decomposition, and a learnable attention-based fusion mechanism as can be seen in Figure 2.

MSSGNN consists of three main components: (1) Relation-Aware Edge Scoring for estimating edge-level homophily, (2) Subgraph Decomposition and Hierarchical Spectral Filtering based on Beta wavelets, and (3) Scale-Adaptive Fusion using an attention mechanism to integrate multi-scale representations. This pipeline enables MSSGNN to learn robust and discriminative node representations across heterogeneous graph structures.

3.1 Preliminaries

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ denote a graph, where $\mathcal{V}$ is the set of $n = |\mathcal{V}|$ nodes and $\mathcal{E}$ is the set of $m = |\mathcal{E}|$ edges. Each node $v_i \in \mathcal{V}$ is associated with a feature vector $\mathbf{x}_i \in \mathbb{R}^d$, and the collection of all node features forms the feature matrix $\mathbf{X} \in \mathbb{R}^{n \times d}$. The adjacency matrix is denoted by $\mathbf{A} \in \{0,1\}^{n \times n}$, and the diagonal degree matrix by $\mathbf{D}$, where $D_{ii} = \sum_j A_{ij}$.

The (normalized) graph Laplacian is defined as $\mathbf{L} = \mathbf{I} - \mathbf{D}^{-1/2}\mathbf{A}\mathbf{D}^{-1/2}$, and admits an eigen-decomposition $\mathbf{L} = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^\top$, where $\mathbf{U}$ contains eigenvectors and $\boldsymbol{\Lambda}$ contains the corresponding eigenvalues.

Before presenting the technical details, we first define the following terms, which are used consistently throughout the paper.

- **Homophily Score** (s_{ij}): a relation-aware similarity score computed for each edge $(i, j) \in \mathcal{E}$, indicating homophily (positive) or heterophily (negative).
- **Wavelet Filter** ($\Psi_k(\mathbf{L})$): a Beta wavelet filter at scale k applied to the Laplacian, capturing specific graph frequency bands.
- **Subgraph Partition** ($\mathcal{G}_s$): a node-induced subgraph corresponding to mild, medium, or extreme levels of heterophily, extracted based on local edge scores.
- **Scale-wise Propagation Depth** (K_s): the number of propagation steps (filtering depth) assigned to each subgraph scale.
- **Attention Fusion** ($\alpha_s^{(i)}$): learnable attention weights used to fuse node embeddings from different subgraphs into a unified representation $\mathbf{h}^{(i)}$.

3.2 Relation-Aware Edge Scoring

The method starts with computing a relation-aware homophily score s_{ij} for each edge $(i, j) \in \mathcal{E}$. This score is produced using a lightweight neural module that jointly encodes node features $\mathbf{x}_i$ and $\mathbf{x}_j$, capturing both feature similarity and their semantic difference. The resulting score guides the subsequent subgraph partitioning process.

Homophily score s_{ij} is computed by a relation-aware module:

$$s_{ij} = \tanh\left(\mathbf{w}^\top \cdot \text{Dropout}\left([\mathbf{W}_h\mathbf{x}_i, \mathbf{W}_h\mathbf{x}_j, \mathbf{W}_h\mathbf{x}_i - \mathbf{W}_h\mathbf{x}_j]\right)\right), \tag{1}$$

where $\mathbf{x}_i, \mathbf{x}_j$ are node features, $\mathbf{W}_h$ is a projection layer, and $\mathbf{w}$ is a scoring weight vector. The result $s_{ij} \in [-1, 1]$ indicates the degree of homophily for that edge.

3.3 Subgraph Decomposition via Edge Homophily Clustering

Each node v_i is assigned a local homophily score by averaging over its incident edges:

$$s_i = \frac{1}{|\mathcal{N}(i)|} \sum_{j \in \mathcal{N}(i)} s_{ij}. \tag{2}$$

Then the nodes are partitioned into three groups based on score quantiles:

$$\mathcal{V} = \mathcal{V}_{\text{mild}} \cup \mathcal{V}_{\text{medium}} \cup \mathcal{V}_{\text{extreme}},$$

resulting in subgraphs $\mathcal{G}_s = (\mathcal{V}_s, \mathcal{E}_s)$ for $s \in \{\text{mild}, \text{medium}, \text{extreme}\}$. This unsupervised partitioning allows MSSGNN to dynamically adapt to graph heterogeneity without additional labeling requirements.

3.4 Hierarchical Spectral Filtering with Beta Wavelets

For each subgraph, we apply a polynomial Beta wavelet filter which are polynomial approximations designed to capture band-pass behavior in the spectral domain:

$$\Psi^{(K_s)}(\mathbf{L}) = \sum_{k=0}^{K_s} \theta_k \cdot \mathbf{L}^k, \tag{3}$$

where $\mathbf{L}$ is the normalized graph Laplacian and $\{\theta_k\}$ are coefficients derived from Beta functions [5]. This filter captures structural information up to K_s hops and targets specific frequency bands depending on the heterophily level.

Different propagation depths K are assigned to each subgraph to capture multi-level heterophily, reflecting their expected structural smoothness. Specifically, we set $K = 1$ for the *mild* heterophily subgraph, $K = 2$ for *medium*, and $K = 3$ for *extreme* heterophily. This design is grounded in spectral graph theory: subgraphs with low heterophily tend to have smoother signals concentrated in low-frequency bands, which can be effectively captured with shallow propagation [42]. In contrast, highly heterophilic subgraphs exhibit more irregular, high-frequency behavior that requires deeper propagation to model. By progressively increasing the value of K, the model adapts its receptive field to the spectral complexity of each subgraph, enabling more precise representation learning across different structural regimes.

The node representation after wavelet filtering becomes:

$$\mathbf{h}_s = \Psi^{(K_s)}(\mathbf{L}_s) \cdot \mathbf{X}_s, \tag{4}$$

where $\mathbf{X}_s$ and $\mathbf{L}_s$ are the feature matrix and Laplacian of subgraph $\mathcal{G}_s$.

Each subgraph is assigned a scale-specific propagation depth K_s, controlling how far node information propagates. Lower K_s values are used for mildly heterophilic regions, while higher K_s values capture complex, high-frequency structures common in fraud scenarios.

3.5 Scale-Adaptive Attention Fusion

The filtered representations from each subgraph are projected independently, normalized, and passed through a learnable attention module. The attention mechanism computes weights $\alpha_s^{(i)}$ for each subgraph output per node i, allowing the final embedding $\mathbf{h}^{(i)} = \sum_s \alpha_s^{(i)} \mathbf{h}_s^{(i)}$ to adaptively emphasize the most informative scales.

Each node receives embeddings from all scales. Attention weights are computed:

$$\alpha_s^{(i)} = \frac{\exp\left(\mathbf{a}^\top \cdot \tanh(\mathbf{W}_a \mathbf{h}_s^{(i)})\right)}{\sum_{s'} \exp\left(\mathbf{a}^\top \cdot \tanh(\mathbf{W}_a \mathbf{h}_{s'}^{(i)})\right)}, \tag{5}$$

where $\mathbf{W}_a$ and $\mathbf{a}$ are learnable parameters. The final node representation is a weighted sum:

$$\mathbf{h}^{(i)} = \sum_s \alpha_s^{(i)} \cdot \mathbf{h}_s^{(i)}. \tag{6}$$

3.6 Training Objective

The final node embeddings are used to predict fraud labels via a supervised cross-entropy loss. Each final node embedding $\mathbf{h}^{(i)}$ is passed through a softmax classifier:

$$\hat{\mathbf{y}}^{(i)} = \text{softmax}(\mathbf{W}_{\text{out}}\mathbf{h}^{(i)}), \tag{7}$$

We optimize a hybrid loss function combining node classification and edge-level structure learning. The total loss is:

$$\mathcal{L} = \mathcal{L}_{\text{cls}} + \gamma \cdot \mathcal{L}_{\text{edge}}, \tag{8}$$

where $\mathcal{L}_{\text{cls}}$ is cross-entropy loss for node labels, and $\mathcal{L}_{\text{edge}}$ is a hinge loss on edge homophily scores:

$$\mathcal{L}_{\text{edge}} = \sum_{(i,j)\in\mathcal{E}} \max(0, 1 - y_{ij} \cdot s_{ij}), \tag{9}$$

with $y_{ij} \in \{-1, +1\}$ representing edge labels indicating heterophily or homophily. The standard cross-entropy objective is:

$$\mathcal{L}_{\text{cls}} = -\sum_{i\in\mathcal{V}_{\text{train}}} \sum_{c=1}^{C} y_i^{(c)} \log \hat{y}_i^{(c)}, \tag{10}$$

where C is the number of classes (e.g., fraud/non-fraud), $y_i^{(c)}$ is the ground truth label (one-hot encoded), and $\hat{y}_i^{(c)}$ is the predicted softmax probability for node i belonging to class c.

4 Experiments

To assess the performance of our proposed model, MSSGNN, it's performance is validated empirically through comprehensive experiments on fraud detection benchmarks.

4.1 Datasets

YelpChi [43] and Amazon [44] datasets are widely used for fraud detection task in the literature [2, 45–47]. Dataset description and some statistics are shown in Table 1. The number of classes for both datasets are two.

1) YelpChi Dataset: MSSGNN is performed on spam review detection using the YelpChi dataset, which consists of hotel and restaurant reviews labeled as either filtered (spam) or recommended (legitimate) by Yelp. Each review is represented as a node with 32 handcrafted features. The graph is constructed with three types of relations: (1) R-U-R connects reviews written by the same user, (2) R-S-R connects reviews of the same product with identical star ratings, and (3) R-T-R connects reviews of the same product posted within the same month [5].

2) Amazon Dataset: For fraudulent user detection, an Amazon product review dataset is utilized. Users are labeled as fraudulent if less than 20% of their reviews receive helpful votes, and as benign if more than 80% do, following previous work [2, 5]. To avoid label leakage caused by the feature "minimum number of unhelpful votes" [2, 47], it is excluded. 24-dimensional node features are used. The heterogeneous graph is built with three types of relations: (1) U-P-U connects users who reviewed at least one common product, (2) U-S-V connects users who gave the same star rating within one week, and (3) U-V-U connects users with top 5% mutual review text similarity.

Table 1. Dataset Description

Dataset	Task	Number of Nodes	Number of Node Features	Percentage of Fraud	Relation Types
YelpChi	Spam Review Detection	45,954	32	14.53%	R-U-R: same user R-S-R: same product & star R-T-R: same product & month
Amazon	Fraudulent User Detection	11,944	24	6.87%	U-P-U: common product U-S-V: same star within a week U-V-U: top 5% text similarity

4.2 Baselines

Our proposed method is compared with six baselines which includes a traditional machine-learning model MLP and graph-based methods.

- **MLP**: This method uses only node features as input and does not incorporate edges or graph structure.
- **GCN** [28]: A graph neural network that classifies nodes by aggregating feature information from their immediate neighbors.
- **GPRGNN** [42]: A generalized PageRank-based spectral GNN that adaptively learns propagation weights to capture long-range dependencies in graphs.
- **BWGNN** [4]: A bandpass filter-based GNN that leverages both low- and high-frequency information to better capture complex patterns in graph signals.
- **SplitGNN** [5]: A spectral graph learning framework that partitions the graph into subgraphs for local message passing, followed by global feature aggregation to improve scalability.
- **Arnoldi-GCN** [41]: A variant of GCN that guides Spectral GNN propagation using explicit filters, enabling effective learning from multi-hop neighborhood information by adaptively learning propagation weights.

4.3 Evaluation Metrics and Experiment Settings

A comparative analysis is conducted between our model and several baseline methods. Given the inherently imbalanced nature of fraud detection datasets,

model performance is evaluated using F1-Score and AUC, which are more informative metrics than accuracy in imbalanced classification settings.

The learning rate is set to 0.01 for YelpChi dataset and 0.1 for Amazon in MSSGNN. The weight decay is 0.00005, the dimension of node embedding is 6, the number of epochs is 1000, and the dropout rate is 0.1. Training, validation, and test ratios are 40%, 20%, and 40%, respectively. All methods are optimized with the Adam optimizer.

5 Results

5.1 Fraud Detection Results

In this section, the comparison between MSSGNN and baseline models are presented in Table 2.

Table 2. Performance Comparison

Dataset	**YelpChi**		**Amazon**	
Metric	**AUC Score**	**F1 Score**	**AUC Score**	**F1 Score**
MLP	0.8172	0.4608	0.8975	0.4822
GCN	0.547	0.4608	0.7714	0.4822
GPRGNN	0.6983	0.4615	0.8792	0.5879
BWGNN	0.836	0.7057	0.836	0.6332
SplitGNN	<u>0.9135</u>	<u>0.7151</u>	<u>0.9283</u>	<u>0.6881</u>
Arnoldi-GCN	0.7333	0.6047	0.874	0.6924
MSSGNN	**0.8987**	**0.7222**	**0.9109**	**0.7064**

The experimental results presented in Table 2 demonstrate the effectiveness of the proposed MSSGNN model across two real-world fraud detection datasets: YelpChi and Amazon. MSSGNN results are highlighted in bold, while the best-performing baseline results are underlined. MSSGNN achieves the highest F1 scores on both datasets, surpassing all baseline models, including recent state-of-the-art methods such as SplitGNN and Arnoldi-GCN. Notably, while SplitGNN achieves the best AUC scores, MSSGNN provides a better balance between detection accuracy and robustness, as indicated by its superior F1 scores. This highlights the advantage of our hierarchical spectral filtering and relation-aware subgraph decomposition in capturing heterophilic structures. The consistent performance gains across datasets confirm the generalizability of MSSGNN and its suitability for complex fraud detection scenarios where both homophilic and heterophilic patterns are present.

5.2 Ablation Study

Table 3 presents an ablation study evaluating the impact of key components in MSSGNN on the YelpChi dataset. The full model achieves the highest F1 score,

demonstrating the overall effectiveness of integrating spectral filtering, subgraph partitioning, and attention-based fusion. When the subgraph decomposition is removed, performance drops noticeably in both AUC and F1, underscoring the value of separating nodes based on homophily levels for scale-specific processing. Removing the relation-aware scoring module results in a moderate decline, confirming its role in guiding meaningful subgraph formation. Notably, the model without attention fusion achieves comparable AUC but slightly lower F1, suggesting that the learnable fusion mechanism contributes to improved classification precision. These results collectively validate that each architectural component of MSSGNN enhances its ability to detect fraud in heterophilic networks.

Table 3. Ablation Study on YelpChi Dataset

Model Variant	AUC Score	F1 Score
MSSGNN (full)	0.8987	0.7222
w/o Subgraphs	0.8866	0.7065
w/o Relation-Aware Scoring	0.8925	0.7105
w/o Attention Fusion	0.8949	0.7215

6 Conclusion

In this work, we introduced MSSGNN, a novel graph neural network designed to address the challenges of learning on graphs with both homophilic and heterophilic structures—particularly in the context of fraud detection. By combining hierarchical spectral filtering with a relation-aware subgraph decomposition strategy, MSSGNN effectively captures varying levels of structural heterogeneity across different frequency bands. Our model incorporates customized Beta wavelet filters, adaptive propagation depths, and an attention-based fusion mechanism to robustly integrate multi-scale information. Extensive experiments on real-world datasets demonstrate that MSSGNN consistently outperforms existing baselines, confirming its effectiveness in detecting fraudulent behavior in complex social networks. These results highlight the importance of frequency-aware, heterophily-sensitive modeling in advancing the state of graph-based fraud detection.

Acknowledgment

Melike Yildiz Aktas is financially supported by the Turkish Ministry of National Education for her PhD research.

References

1. Y. Ma, X. Liu, N. Shah, and J. Tang, "Is homophily a necessity for graph neural networks?" *arXiv preprint arXiv:2106.06134*, 2021.
2. Y. Dou, Z. Liu, L. Sun, Y. Deng, H. Peng, and P. S. Yu, "Enhancing graph neural network-based fraud detectors against camouflaged fraudsters," in *Proceedings of the 29th ACM international conference on information & knowledge management*, 2020, pp. 315–324.
3. J. Zhu, Y. Yan, L. Zhao, M. Heimann, L. Akoglu, and D. Koutra, "Beyond homophily in graph neural networks: Current limitations and effective designs," *Advances in neural information processing systems*, vol. 33, pp. 7793–7804, 2020.
4. J. Tang, J. Li, Z. Gao, and J. Li, "Rethinking graph neural networks for anomaly detection," in *International conference on machine learning*. PMLR, 2022, pp. 21 076–21 089.
5. B. Wu, X. Yao, B. Zhang, K.-M. Chao, and Y. Li, "Splitgnn: Spectral graph neural network for fraud detection against heterophily," in *Proceedings of the 32nd ACM international conference on information and knowledge management*, 2023, pp. 2737–2746.
6. A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: a systematic literature review," *Applied Sciences*, vol. 12, no. 19, p. 9637, 2022.
7. Y. Bao, G. Hilary, and B. Ke, "Artificial intelligence and fraud detection," *Innovative Technology at the Interface of Finance and Operations: Volume I*, pp. 223–247, 2022.
8. R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," *Human-Centric Intelligent Systems*, vol. 2, no. 1, pp. 55–68, 2022.
9. M. N. Ashtiani and B. Raahemi, "Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review," *Ieee Access*, vol. 10, pp. 72 504–72 525, 2021.
10. B. Baesens, S. Höppner, and T. Verdonck, "Data engineering for fraud detection," *Decision Support Systems*, vol. 150, p. 113492, 2021.
11. J. Gera, A. R. Palakayala, V. K. K. Rejeti, and T. Anusha, "Blockchain technology for fraudulent practices in insurance claim process," in *2020 5th international conference on communication and electronics systems (ICCES)*. IEEE, 2020, pp. 1068–1075.
12. M. Seera, C. P. Lim, A. Kumar, L. Dhamotharan, and K. H. Tan, "An intelligent payment card fraud detection system," *Annals of operations research*, vol. 334, no. 1, pp. 445–467, 2024.
13. A. Urunkar, A. Khot, R. Bhat, and N. Mudegol, "Fraud detection and analysis for insurance claim using machine learning," in *2022 IEEE international conference on signal processing, informatics, communication and energy systems (SPICES)*, vol. 1. IEEE, 2022, pp. 406–411.
14. P. Tiwari, S. Mehta, N. Sakhuja, J. Kumar, and A. K. Singh, "Credit card fraud detection using machine learning: a study," *arXiv preprint arXiv:2108.10005*, 2021.
15. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *Ieee Access*, vol. 10, pp. 39 700–39 715, 2022.

16. E. Nabrawi and A. Alanazi, "Fraud detection in healthcare insurance claims using machine learning," *Risks*, vol. 11, no. 9, p. 160, 2023.
17. S. K. Pala, "Investigating fraud detection in insurance claims using data science," *International Journal of Enhanced Research in Science, Technology & Engineering ISSN*, pp. 2319–7463, 2022.
18. S. Vyas and S. Serasiya, "Fraud detection in insurance claim system: A review," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*. IEEE, 2022, pp. 922–927.
19. S. Agarwal, "An intelligent machine learning approach for fraud detection in medical claim insurance: A comprehensive study," *Scholars Journal of Engineering and Technology*, vol. 11, no. 9, pp. 191–200, 2023.
20. S. Ray, "Fraud detection in e-commerce using machine learning," *BOHR International Journal of Advances in Management Research*, vol. 1, no. 1, pp. 7–14, 2022.
21. N. Tax, K. J. de Vries, M. de Jong, N. Dosoula, B. van den Akker, J. Smith, O. Thuong, and L. Bernardi, "Machine learning for fraud detection in e-commerce: A research agenda," in *Deployable Machine Learning for Security Defense: Second International Workshop, MLHat 2021, Virtual Event, August 15, 2021, Proceedings 2*. Springer, 2021, pp. 30–54.
22. A. Mutemi and F. Bacao, "E-commerce fraud detection based on machine learning techniques: Systematic literature review," *Big Data Mining and Analytics*, vol. 7, no. 2, pp. 419–444, 2024.
23. G. Zhang, Z. Li, J. Huang, J. Wu, C. Zhou, J. Yang, and J. Gao, "efraudcom: An e-commerce fraud detection system via competitive graph neural networks," *ACM Transactions on Information Systems (TOIS)*, vol. 40, no. 3, pp. 1–29, 2022.
24. J. Li, "E-commerce fraud detection model by computer artificial intelligence data mining," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 8783783, 2022.
25. T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," *Decision Support Systems*, vol. 133, p. 113303, 2020.
26. D. Cheng, X. Wang, Y. Zhang, and L. Zhang, "Graph neural network for fraud detection via spatial-temporal attention," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 8, pp. 3800–3813, 2020.
27. P. Li, H. Yu, X. Luo, and J. Wu, "Lgm-gnn: A local and global aware memory-based graph neural network for fraud detection," *IEEE Transactions on Big Data*, vol. 9, no. 4, pp. 1116–1127, 2023.
28. T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," *arXiv preprint arXiv:1609.02907*, 2016.
29. P. Velickovic, G. Cucurull, A. Casanova, A. Romero, P. Lio, Y. Bengio *et al.*, "Graph attention networks," *stat*, vol. 1050, no. 20, pp. 10–48 550, 2017.
30. O. Atkinson, A. Bhardwaj, C. Englert, V. S. Ngairangbam, and M. Spannowsky, "Anomaly detection with convolutional graph neural networks," *Journal of High Energy Physics*, vol. 2021, no. 8, pp. 1–19, 2021.
31. Y. Hu, A. Qu, and D. Work, "Graph convolutional networks for traffic anomaly," *arXiv preprint arXiv:2012.13637*, 2020.
32. C. Liu, L. Sun, X. Ao, J. Feng, Q. He, and H. Yang, "Intention-aware heterogeneous graph attention networks for fraud transactions detection," in *Proceedings of the 27th ACM SIGKDD conference on knowledge discovery & data mining*, 2021, pp. 3280–3288.

33. S. Wei and S. Lee, "Financial anti-fraud based on dual-channel graph attention network," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 19, no. 1, pp. 297–314, 2024.
34. H. Zhao, Y. Wang, J. Duan, C. Huang, D. Cao, Y. Tong, B. Xu, J. Bai, J. Tong, and Q. Zhang, "Multivariate time-series anomaly detection via graph attention network," in *2020 IEEE international conference on data mining (ICDM)*. IEEE, 2020, pp. 841–850.
35. J. Zheng, C. Yang, T. Zhang, L. Cao, B. Jiang, X. Fan, X.-m. Wu, and X. Zhu, "Dynamic spectral graph anomaly detection," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 39, no. 12, 2025, pp. 13 410–13 418.
36. X. Wang and M. Zhang, "How powerful are spectral graph neural networks," in *International conference on machine learning*. PMLR, 2022, pp. 23 341–23 362.
37. D. Bo, X. Wang, Y. Liu, Y. Fang, Y. Li, and C. Shi, "A survey on spectral graph neural networks," *arXiv preprint arXiv:2302.05631*, 2023.
38. S. M. Geisler, A. Kosmala, D. Herbst, and S. Günnemann, "Spatio-spectral graph neural networks," *Advances in Neural Information Processing Systems*, vol. 37, pp. 49 022–49 080, 2024.
39. D. Bo, C. Shi, L. Wang, and R. Liao, "Specformer: Spectral graph neural networks meet transformers," *arXiv preprint arXiv:2303.01028*, 2023.
40. S. Mo, K. Wu, Q. Gao, X. Teng, and J. Liu, "Autosgnn: automatic propagation mechanism discovery for spectral graph neural networks," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 39, no. 18, 2025, pp. 19 493–19 502.
41. M. Coşkun, A. Grama, and M. Koyutürk, "Generalized learning of coefficients in spectral graph convolutional networks," *arXiv preprint arXiv:2409.04813*, 2024.
42. E. Chien, J. Peng, P. Li, and O. Milenkovic, "Adaptive universal generalized pagerank graph neural network," *arXiv preprint arXiv:2006.07988*, 2020.
43. S. Rayana and L. Akoglu, "Collective opinion spam detection: Bridging review networks and metadata," in *Proceedings of the 21th acm sigkdd international conference on knowledge discovery and data mining*, 2015, pp. 985–994.
44. J. J. McAuley and J. Leskovec, "From amateurs to connoisseurs: modeling the evolution of user expertise through online reviews," in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 897–908.
45. Z. Liu, Y. Dou, P. S. Yu, Y. Deng, and H. Peng, "Alleviating the inconsistency problem of applying graph neural network to fraud detection," in *Proceedings of the 43rd international ACM SIGIR conference on research and development in information retrieval*, 2020, pp. 1569–1572.
46. H. Peng, R. Zhang, Y. Dou, R. Yang, J. Zhang, and P. S. Yu, "Reinforced neighborhood selection guided multi-relational graph neural networks," *ACM Transactions on Information Systems (TOIS)*, vol. 40, no. 4, pp. 1–46, 2021.
47. F. Shi, Y. Cao, Y. Shang, Y. Zhou, C. Zhou, and J. Wu, "H2-fdetector: A gnn-based fraud detector with homophilic and heterophilic connections," in *Proceedings of the ACM web conference 2022*, 2022, pp. 1486–1494.