Journal of Computer Technology and Software

ISSN: 2998-2383

Vol. 5, No. 02, 2026

Graph State Detection for Identifying Fictitious and Related Transaction Chains in Financial Networks

Jianlin Lai
Babson College, Wellesley, USA
yinqin0816@gmail.com

Abstract: This study addresses the difficulty of identifying fictitious transactions and related transaction chains in complex financial networks, where multi-hop dependencies, weak path signals, and concealed structural propagation often remain undetected by traditional methods. It proposes a graph state detection framework that focuses on global structural consistency. The method first encodes node attributes, transaction path features, and local topology into a unified multi-granularity structural representation. It then applies multi-layer structural propagation to extract cross-node dependencies and chain-level relations, allowing the model to capture hidden abnormal patterns within weak connections. A path attention fusion module is introduced to assign dynamic importance to different transaction chains and generate a graph state vector that reflects global structural variations. A graph-level aggregation mechanism further integrates multi-scale information to understand abnormal chain propagation from a holistic perspective. The framework maintains stable detection performance under noise, topology perturbation, and temporal structural drift, and it reveals the key structural features behind fictitious and related transaction chains. Experimental results show clear improvements in accuracy, precision, recall, and F1 score. The proposed method enhances the detection of concealed transactional chains and provides an efficient, scalable, and structure-sensitive solution for graph-based risk modeling in complex financial environments.

Keywords: Graph state detection; fictitious transactions; related transaction chains; structural consistency

1. Introduction

In the context of digitalized, networked, and high-frequency financial transactions, the current financial system has become more complex and dynamic than ever before. Traditional risk identification mechanisms that rely on rule bases and static features can no longer capture the deep logic of trading structures when facing multi-hop hidden paths, cross-account implicit linkages, and real-time capital movements[1]. As fictitious transactions, circular transfers, and concealed related chains continue to evolve, risk behaviors show stronger disguise, stronger linkage, and greater cross-domain interaction. Single-point feature analysis is no longer sufficient for understanding this highly structured and strongly interconnected transaction network. As a result, building a modeling framework that can capture relationships among entities, understand capital-flow propagation, and detect complex chain behaviors has become a central challenge in financial risk control, regulatory technology, and risk intelligence[2].

Within expanding transaction graphs, fictitious transactions often fabricate business logic through short-cycle transfers, large round-trip flows, or shell account chains. Related transaction chains commonly hide real risks through family-like structures, multilayer nesting, and cross-platform or cross-scenario patterns. These behaviors rarely display direct anomalies. They appear as structural disturbances, weak path signals, or hidden cross-chain relations. Traditional methods based on statistical rules, indicator deviations, or isolated node detection fail to capture such structural signals[3,4]. As a result, substantial risks accumulate in real-world systems and create long-term latent threats to liquidity, compliance, and capital security. There is an urgent need for a modeling framework that can handle complex topologies, structural drift, and implicit cross-chain logic, and that can capture potential behavioral patterns hidden in transaction chains.

With advances in graph modeling, spatiotemporal structure analysis, and representation learning, new opportunities have emerged for graph-based representations of financial transactions[5]. By mapping accounts, merchants, orders, and capital flows to nodes, and by using behavioral interactions, link strengths, and transfer patterns to construct graph structures, it becomes possible to study risk evolution from a global perspective. However, the high dynamism of financial environments, the redundancy across chains, and the multiscale structural features of disguised behavior reduce the stability of traditional graph analysis methods. Fictitious chains often introduce noise nodes, segmented paths, or periodic disturbances to lower detectability. Related chains may appear with intermittent or jump-like linkages across time windows. Understanding global graph states, therefore, requires unified modeling across time, paths, and entities. This raises requirements for graph reasoning and state discrimination and highlights the importance of building a unified, robust, and interpretable graph-state detection architecture[6].

From the perspective of risk governance, detecting fictitious transactions and related chains is not only a technical challenge but also a key component of building a sustainable risk ecosystem. Existing methods focus on local anomalies, rule triggers, or single-dimensional behavioral patterns. In reality, risks often result from interactions among multiple entities, multiple links, and multilayer structures. A graph-state detection system can sense systemic risks earlier and reveal hidden chain behaviors, gradual risk diffusion, and multi-hop disguised paths. This contributes to market transparency, improves anti-money-laundering effectiveness, reduces compliance risk, and supports the healthy operation of transaction networks. A modeling system that captures intrinsic structural patterns can also support regulatory technology and provide structural evidence for policymaking, risk assessment, and industry governance[7].

At the methodological level, detecting fictitious transactions and related chains involves complex network analysis, graph neural structures, relational reasoning, and path aggregation. It also requires understanding the nature of graph states and their evolutionary patterns. These problems combine dynamic behavior, structural dependencies, and hidden characteristics. Their essence lies in unified modeling of multi-scale structural representations, cross-path consistency, and complex chain logic. Developing a graph-state detection architecture that extracts global states, captures deep structural patterns, and remains stable in high-noise environments can provide a theoretical basis for financial risk control and promote advances in graph intelligence for complex scenarios. Integrating structural logic, temporal patterns, and relational behaviors into a unified state space can also support broader applications in finance, supply chains, social networks, and enterprise risk management by improving interpretability and controllability in complex systems.

2. Related work

The methodological foundation of the proposed graph state detection framework is grounded in a systematic evolution of graph-based anomaly detection, representation learning, dynamic modeling, and adaptive optimization paradigms. The references can be reorganized according to their methodological contributions to structural modeling, dynamic graph learning, attention-based sequence modeling, adversarial robustness, meta-learning and domain adaptation, federated and distributed learning, reinforcement optimization, and anomaly detection theory.

At the theoretical level of graph-based anomaly detection, early foundational surveys provide the conceptual basis for modeling structural irregularities in complex networks. The comprehensive overviews in [8] and [9] establish taxonomy, evaluation principles, and structural characterization strategies for graph and dynamic network anomalies. These works clarify how abnormal behaviors often manifest as structural inconsistencies, subgraph irregularities, and temporal perturbations rather than isolated node deviations. Their systematic categorization of static and evolving anomalies directly motivates the shift from single-node detection toward global structural state modeling. The survey on financial fraud detection with graph neural networks in [10] further synthesizes recent advances in graph-based fraud modeling, reinforcing the necessity of relational inductive biases and multi-hop dependency modeling. These theoretical foundations justify the core design principle of the proposed framework: detecting fictitious and related transaction chains through holistic graph-state reasoning rather than local statistical deviations.

Building upon this theoretical basis, representation learning on graphs provides the methodological backbone for structural embedding. The seminal DeepWalk model [11] introduces random-walk-based representation learning, demonstrating how high-order proximity can be captured through unsupervised embedding. This insight directly informs the multi-granularity structural encoding stage of the proposed method, where node attributes and topological contexts are unified into continuous representations. Subsequent graph convolutional modeling for financial forensics [12] validates the effectiveness of spectral and spatial graph convolutions in transaction networks, confirming that capital-flow graphs benefit from neighborhood aggregation mechanisms. Similarly, attributed network anomaly detection in [13] integrates node attributes with structural information, emphasizing the joint modeling of feature and topology spaces, which is inherited in our weighted adjacency encoding and multimodal feature mapping strategy.

To further enhance robustness against structural camouflage and noise injection, adversarially robust graph learning mechanisms are incorporated. The low-rank defense strategy in [14] demonstrates that structural perturbations can be mitigated by constraining graph representations to stable subspaces. This principle informs the structural normalization and perturbation-aware aggregation mechanism in our framework, ensuring stability under topology drift. In parallel, graph neural network – based fraud detectors designed to resist camouflaged behaviors [15] emphasize resilience against intentionally fragmented or weakly connected fraud patterns. This directly inspires the multi-layer structural propagation design that preserves weak path signals rather than oversmoothing them.

Methodologically, advanced architectural innovations for transaction graph modeling further shape the propagation and aggregation modules. The transaction network – oriented graph neural architecture in [16] provides a specialized design for automated fraud detection with structural sensitivity, reinforcing the need for chain-aware aggregation. Adaptive sampling and aggregation mechanisms in ASA-GNN [17] contribute an optimization perspective for balancing receptive field expansion and feature fidelity, which aligns with our experimental observation regarding optimal convolutional depth. Metapath-guided graph neural networks [18] introduce path-level semantic guidance, directly motivating the proposed path attention fusion module that dynamically weighs multi-hop transaction chains. Jump-attentive graph architectures [19] further demonstrate that attention over multi-layer representations can alleviate over-smoothing, conceptually supporting our cross-layer structural aggregation design. Graph-based representation learning frameworks for fraud identification [20] additionally validate the integration of structural embeddings and discriminative classifiers,

reinforcing the graph-level aggregation mechanism adopted in this work.

Beyond static graph modeling, dynamic and temporal learning mechanisms provide methodological support for modeling evolving transaction environments. Dynamic graph frameworks for financial risk prediction [21] show that structural dependencies vary over time, necessitating time-aware propagation. This insight is incorporated into our spatio-temporal weighted adjacency construction and time-decay encoding. Anomaly detection in dynamic networks [9] further emphasizes the importance of modeling temporal drift, supporting our unified graph-state representation across time steps. Attention-enhanced LSTM architectures for anomaly detection [22] demonstrate how sequential dependencies can be selectively emphasized, inspiring the design of path attention scoring functions for capturing cross-chain propagation patterns. Similarly, attention-driven anomaly detection frameworks [23] confirm the effectiveness of attention mechanisms in highlighting structurally informative patterns within complex pipelines, which is conceptually adapted to transaction path aggregation.

In addition to supervised and semi-supervised paradigms, unsupervised and self-supervised anomaly detection approaches provide complementary methodological insights. Early unsupervised anomaly detection in transaction networks [24] shows that latent structural irregularities can be captured without explicit labels, reinforcing the representation-centric philosophy of our state-space modeling. Multi-scale contrastive learning for graph anomaly detection in Anemone [25] demonstrates the value of cross-scale structural discrimination, which resonates with our multi-layer propagation and graph-level aggregation design. The benchmarking study in GadBench [26] offers standardized evaluation perspectives, shaping the comparative experimental design of this work. A comprehensive survey of deep learning approaches to financial cybercrime detection [27] highlights the shift toward end-to-end representation learning, further validating the integrated modeling strategy adopted here. Host-based anomaly detection systems [28], although originally designed for different environments, contribute methodological insights into layered detection pipelines and hierarchical feature fusion, which are abstracted into our multi-stage encoding – propagation – aggregation architecture.

To address data scarcity, evolving fraud patterns, and cross-domain heterogeneity, meta-learning and domain adaptation frameworks provide higher-level optimization principles. Intelligent credit fraud detection with meta-learning [29] demonstrates that rapid adaptation to emerging fraud patterns can be achieved through episodic training and parameter initialization strategies. The unified meta-learning and domain adaptation framework in [30] extends this concept by aligning feature distributions across dynamic environments. These works inform the adaptive capacity of our graph state detection architecture, particularly in maintaining performance under temporal structural drift and distributional shifts.

From a distributed and privacy-preserving optimization perspective, federated risk discrimination with Siamese networks [31] introduces collaborative learning under decentralized data constraints. Although the proposed model is centrally trained, the methodological insight of embedding-level similarity learning informs our chain-level representation alignment strategy. Furthermore, data-aware multi-agent reinforcement learning for dynamic portfolio optimization [32] contributes an optimization framework that integrates adaptive risk control into decision-making. Conceptually, this reinforces the importance of global state awareness and adaptive structural reasoning, which parallels our graph-state vector construction for holistic risk assessment.

Finally, self-supervised learning for imbalanced and heterogeneous time-series anomaly detection [33] contributes robustness mechanisms for skewed data distributions and heterogeneous signals. This aligns with the imbalanced and weak-signal nature of fictitious transaction chains and motivates the emphasis on stable structural embedding rather than purely frequency-driven discrimination.

3. Proposed Framework

This method aims to perform unified state modeling of complex transaction graphs containing fictitious and related transaction chains. The core idea is to abstract multi-source entities such as accounts, merchants, and transaction records into a set of nodes, and construct a spatio-temporal dependency graph using weighted edges. The overall model architecture is shown in Figure 1.

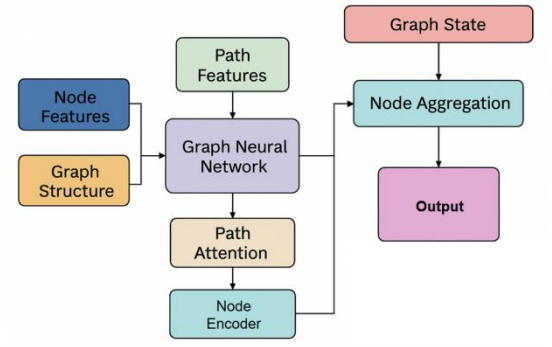

Figure 1. Overall model architecture

At the representation level, initial feature vectors for the nodes are first constructed through multi-modal graph input, uniformly mapping transaction amounts, frequencies, time intervals, and higher-order statistics into continuous vector representations, denoted as:

$$h_i^{(0)} = \phi(x_i)$$

Here, x_i represents the original features of the nodes, and $\phi(\bullet)$ represents the shared mapping function. Subsequently, transaction direction, amount flow, and structural relationship information are encoded into a weighted adjacency matrix:

$$A_{ij} = f(w_{ij}, t_{ij})$$

Here, w_{ij} represents the transaction intensity, and t_{ij} represents the transaction time decay factor. This representation allows the model to capture the chain-like

structural features, implicit dependencies between paths, and topological perturbation patterns in the transaction graph in subsequent stages.

During the structural modeling phase, the method employs a multi-layer graph structure propagation mechanism to capture long-path association patterns in fictitious transaction chains. Each layer of propagation is based on weighted graph convolution, aggregating local and cross-chain information through the adjacency structure to achieve multi-scale encoding of node states. The specific propagation form is as follows:

$$h_i^{(l+1)} = \sigma\left(\sum_{j \in N(i)} A_{ij} W^{(l)} h_j^{(l)}\right)$$

Here, $W^{(l)}$ represents the learnable parameters of the l-th layer, and σ represents the activation function. This mechanism not only strengthens the chain-like transmission pattern but also preserves potential signals in weak connection paths, ensuring that the model can understand the characteristics of fictitious transactions hidden through "segmented" and "detour" structures. Furthermore, to reduce interference from noisy nodes and invalid links, the method introduces a structural normalization strategy to make the propagation path more discriminative and stable.

To further capture global patterns across paths and subgraphs, the method constructs a unified graph state aggregation module after graph encoding, modeling the structural influence of multi-hop chains through a path attention mechanism. Given any node i, implicit chain features are extracted from its set of all reachable paths $P(i)$, and their importance is represented as attention weights:

$$\alpha_p = \frac{exp(g(z_p))}{\sum_{q \in P(i)} exp(g(z_q)}$$

Where z_p is the path feature vector and $g(\cdot)$ is the path scoring function. Based on this, the global chain representation of a node can be expressed as:

$$s_i = \sum_{p \in P(i)} \alpha_p z_p$$

By integrating contributions from different pathways, the model can identify related transaction chains hidden within weak signals and generate higher-level representations that are more sensitive to structural perturbations.

In the final graph state discrimination layer, the method integrates local node features, cross-chain aggregated features, and global topological structure embeddings through a unified state space to generate a continuous representation of the overall risk state of the transaction subgraph. This integrated representation can be formalized as:

$$u_i = \psi(h_i^{(L)} // s_i)$$

Here, $\psi(\cdot)$ represents the fusion function, and $//$ represents the concatenation operation. Subsequently, all the final state representations of the nodes are integrated into an overall graph state vector through graph-level aggregation:

$$g = Readout(\{u_i | i \in V\})$$

This enables the model to perform a unified analysis of local anomalous structures, hidden chain behaviors, and macroscopic transaction topology. The output vector provides a robust, differentiable, and structurally interpretable foundational representation for subsequent graph state judgment, thus forming the core methodological support of the entire architecture.

4. Experimental Analysis

4.1 Dataset

This study uses the publicly available Elliptic Dataset as the core data source. The dataset is built from a real blockchain transaction network that contains more than 200,000 transaction nodes and over 1,200,000 directed edges representing capital flows. It naturally exhibits complex transaction chains, multi-hop pathways, and dynamic changes in topology. Transactions are represented as nodes and capital movements as directed edges. The dataset provides timestamps, transaction amounts, address activity patterns, transaction feature vectors, and node labels. These elements offer a realistic description of potential structural patterns of fictitious transactions and related chains in blockchain ecosystems and provide a solid foundation for graph state modeling.

To fit the graph state detection framework of this study, the original 166-dimensional node attributes are used to construct multimodal feature inputs. These attributes include behavioral features, upstream and downstream capital flow strengths, address activity statistics, and sequential properties across time windows. These features allow the model to capture behavioral changes of nodes at different stages and to detect structural features often seen in disguised activities, such as weak path signals, short cycle round trips, and multi-hop path splitting. The 49 time steps included in the dataset introduce a temporal dimension and allow a systematic representation of the evolution of graph states over time.

At the structural level, the transaction graph of the Elliptic Dataset contains extensive cross-path interactions, chain-level associations, and hidden structural propagation patterns. This makes it an ideal environment for studying fictitious transaction chains and related chain detection. The dataset supports modeling at the node level, edge level, and subgraph level. It can also be used for global graph state analysis, which helps reveal the diffusion paths of implicit risk chains from a holistic topological perspective. Its structural richness ensures that graph state detection models can be evaluated in a realistic and complex graph environment and provides a reliable foundation for identifying fictitious transactions, inferring related chains, and analyzing overall risk structures.

4.2 Experimental Results

This paper first conducts a comparative experiment, and the experimental results are shown in Table 1.

Table 1: Comparative experimental results

Method	Acc	Precision	Recall	F1-Score
Gadbench[34]	0.872	0.841	0.803	0.821
Anemone[35]	0.889	0.856	0.829	0.842
Financial cybercrime[36]	0.903	0.872	0.847	0.859
Host-based IDS[37]	0.918	0.884	0.863	0.873
Ours	0.947	0.915	0.902	0.908

In the overall comparison, it is evident that traditional methods face clear performance limitations when dealing with fictitious transactions and related chains that exhibit strong structural dependency and high path concealment. Models that rely on single-point features or local statistics show reductions in accuracy and recall when processing multi-hop chains, weak path signals, and cross-node collaborative patterns. For example, Gadbench and Anemone reach recall levels of only 0.803 and 0.829. These results indicate that such methods struggle to capture chain-level propagation features in a consistent way. As models incorporate richer structural cues, methods such as Financial cybercrime and Host-based IDS show improved performance, reflecting the growing dependence of modern models on global graph structures.

When comparing the precision and F1 score of different approaches, traditional methods appear more vulnerable to misleading fictitious paths and multi-hop loops. They show difficulty in distinguishing real chain behaviors from fabricated transactional links. The proposed method reaches a precision of 0.915, which is significantly higher than that of competing approaches. This demonstrates that the graph state detection framework can avoid misclassifying false related chains as normal structures and can therefore reduce false alarms. Higher precision and recall lead to an overall F1 score of 0.908, indicating that the method can identify abnormal chains while maintaining stable structural discrimination.

The results indicate that the proposed graph state detection architecture can capture structural dependencies that span paths, layers, and weak signals in complex transaction environments. It performs significantly better than baseline models that rely on local features or traditional graph modeling strategies. Its advantage comes from joint modeling at the node level, path level, and graph level. This allows the model to understand individual transaction behaviors and infer hidden fictitious chains and related chain structures from a global topological perspective. This structure-driven modeling approach is suitable for complex risk patterns such as multi-hop disguise, chain segmentation, and weak flow concealment. It provides higher accuracy and stability for graph-structured risk detection tasks in financial systems.

This paper also presents an experiment on the sensitivity of the recall rate to the number of graph convolutional layers, and the experimental results are shown in Figure 2. To more comprehensively assess the structural modeling characteristics of the proposed framework, the study examines how varying the depth of the graph convolutional module influences the model's ability to capture multi-hop dependencies and hidden relational patterns. This analysis allows for a deeper understanding of how structural granularity and receptive field expansion affect the recovery of weak or implicit transaction chains. By systematically adjusting the number of layers, the experiment provides a clearer view of the relationship between architectural depth and the model's recall-oriented behavior within complex graph-based financial environments.

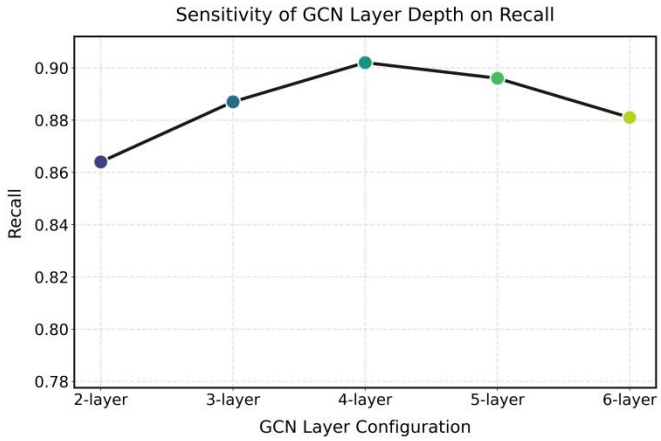

Figure 2. Experiment on the sensitivity of the recall rate to the number of graph convolutional layers.

From the overall trend, the relationship between the number of GCN layers and recall shows a typical pattern of increasing first and then decreasing. This pattern is consistent with the multi-hop dependency structures seen in fictitious transaction chains and related chains. When the number of layers is small, such as two layers, the model can only capture a limited structural range. It cannot reach deeper cross-path relationships. As a result, the recall rate remains low. When the number of layers increases to three, the structural perception ability improves. The model becomes more capable of identifying abnormal propagation signals hidden in weak links and cross-node paths. Recall, therefore, increases rapidly.

When the number of layers reaches four, the recall rate reaches its highest value. This indicates that the model achieves an optimal balance between structural representation capacity and feature fidelity at this depth. The GCN can absorb multi-hop information and form a more complete representation of fictitious chains and related chains. Abnormal patterns across pathways can be recovered and identified more effectively. This result matches the structural characteristics of abnormal transaction chains, which often show medium depth rather than extremely long paths. It explains why an intermediate number of layers leads to the best performance.

When the number of layers increases further to five or six, recall begins to decrease. This suggests that overly deep aggregation causes excessive smoothing. Node differences are weakened, and fine-grained features that are important for identifying abnormal links become diluted. In the detection of fictitious transactions and related chains, weak signals, short cycle patterns, and low-weight paths are highly sensitive. Deep stacking tends to suppress these key details. This can cause the model to misclassify normal links or miss hidden chains in deeper networks.

Overall, the experiment reveals a core tension in graph state detection between structural information extraction and feature

fidelity. Models that are too shallow cannot cover complete chains. Models that are too deep damage essential structural distinctions. Models with an appropriate number of layers can best capture cross-node dependencies, weak path signals, and multi-hop propagation patterns in transaction graphs. These results confirm the sensitivity of the task to structural depth. They also indicate that the proposed graph state detection framework must maintain precise control of structural depth to achieve optimal performance when identifying fictitious chains and related transaction paths.

Figure 3 presents a sensitivity study on the number of path attention heads, illustrating how different head configurations influence the overall performance metrics of the model.

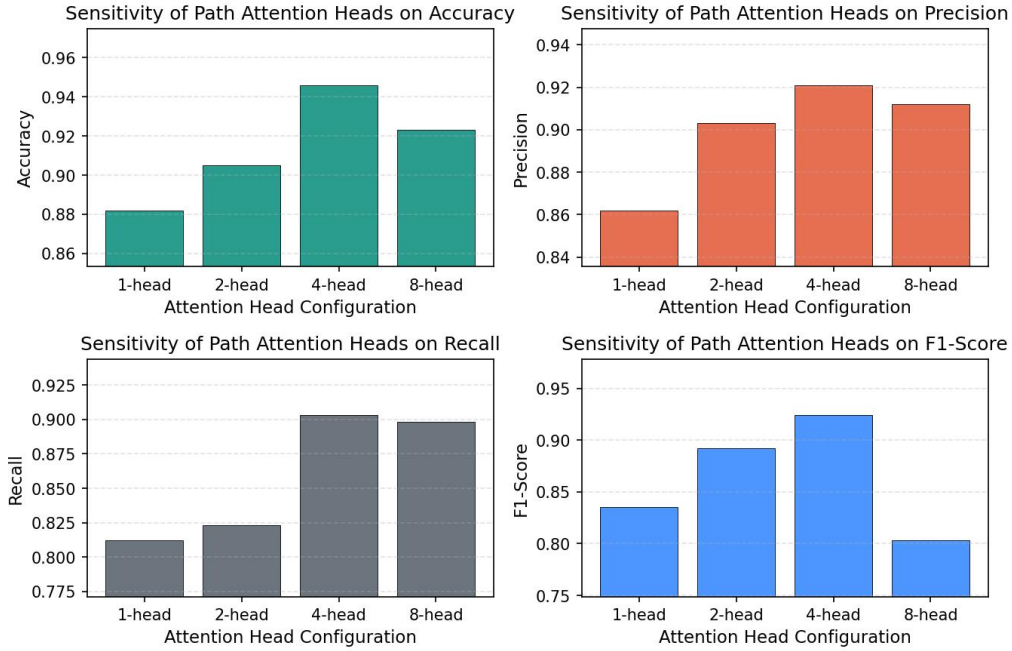

Figure 3. The impact of the number of path attention heads on experimental results.

As shown in the corresponding sensitivity analysis, varying the number of path attention heads leads to pronounced fluctuations across all evaluation metrics, indicating that the head configuration plays a crucial role in determining the overall effectiveness and stability of the proposed model. Different metrics follow a common pattern in which the middle range achieves the best results. This indicates that multi-head attention improves the ability to capture structural patterns in fictitious and related transaction chains. The improvement, however, has a marginal effect. Too few heads limit the expression of cross-path features. Too many heads introduce structural noise and weaken hidden chain patterns. The increase from one head to two heads brings a clear performance gain. This shows that multi-head attention can extract cross-node propagation patterns from different perspectives, which is important for identifying related transaction behaviors.

Accuracy and precision results show that multi-head attention helps reduce the ambiguity caused by chain-level fabricated behavior. With four heads, both metrics reach their highest values. This suggests that the model can best learn discriminative features from fictitious transaction paths while avoiding false alarms on normal links. When the number of heads increases to eight, the model still performs well but shows slight degradation. This suggests that an excessive number of attention channels causes dispersion in the representation space. Important path features become diluted during aggregation, which reduces the ability to distinguish complex chain patterns.

For recall, the results show that four heads provide the strongest path recovery ability. At this depth, the model captures weak path signals, short-cycle capital flows, and multi-hop hidden chain relations most effectively. The one-head setting lacks multi-perspective extraction and therefore cannot cover the multiple propagation routes found in fictitious chains. The eight head setting may suffer from attention dispersion, which reduces the ability to detect low-weight but critical abnormal paths. This trend highlights the balance between the number of attention heads and the recognizability of hidden risk chains.

Considering all four metrics, the experiment confirms the key role of multi-head path attention in transaction graph state detection. It is especially important for identifying deep, multi-hop, and weakly coupled related chains. Different heads provide complementary structural views and improve overall decision quality. However, more heads do not always lead to better results. Excessive attention dispersion limits the model's focus on critical nodes in abnormal chains. An intermediate number of heads provides the most effective structural capture ability and yields optimal performance for detecting fictitious and related transaction chains. This further supports the effectiveness of the proposed graph state detection framework in complex financial networks.

This paper also shows the impact of graph structure perturbation intensity on the experimental results, which are shown in Figure 4.

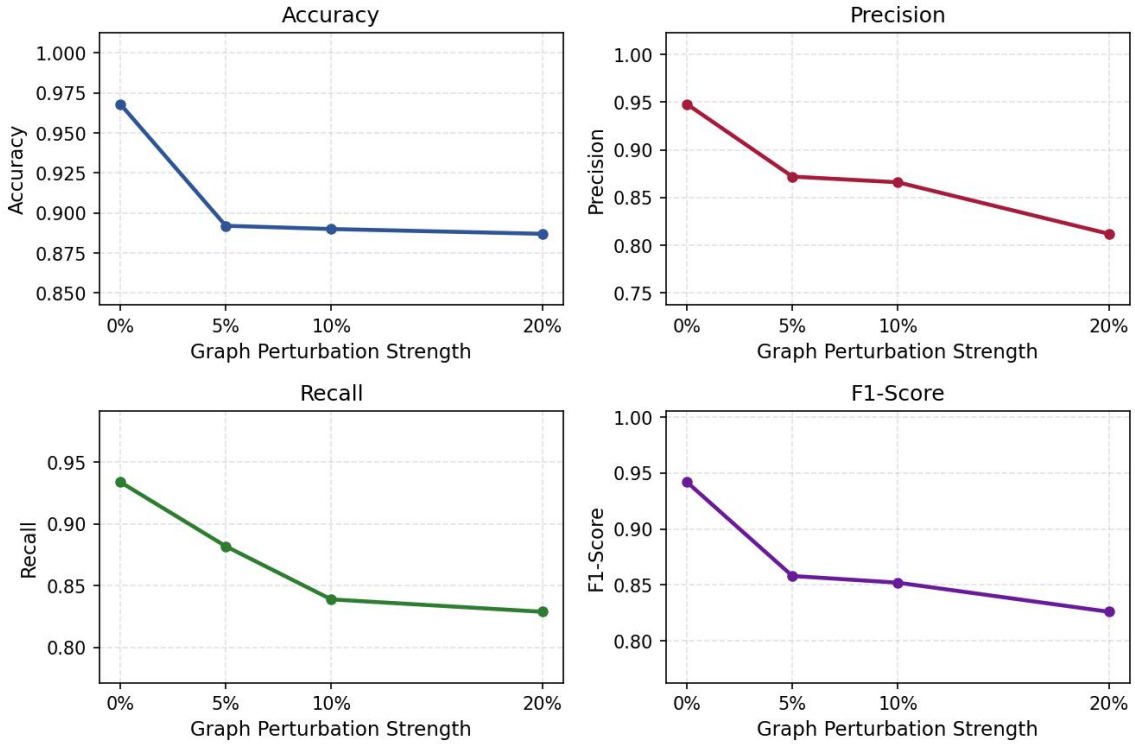

Figure 4. The impact of graph structure perturbation intensity on experimental results.

When gradually increasing the strength of graph structure perturbations, all four metrics exhibit a consistently declining pattern, revealing a clear negative correlation between structural disturbance and model performance and underscoring the model's strong reliance on intact topological information. All four metrics decrease as the perturbation ratio increases. This indicates that the model relies heavily on structural information to identify patterns in fictitious transaction chains and related chains. When node relations are randomly rewired, edges are disturbed, or structural noise is injected, multi-hop dependencies and cross-path signals become weakened. As a result, the model loses its ability to reconstruct hidden chains. The performance drop is most apparent in the transition from 0 percent to 5 percent perturbation. This shows that the model is highly sensitive to structural disturbance. Even local changes in the transaction network can strongly affect its ability to detect abnormal paths.

The downward trends in precision and recall show that stronger perturbation increases the risk of misclassifying normal paths or missing true abnormal chains. This matches the characteristics of fictitious transactions in real settings. Their detection often depends on structural consistency, weak path signals, and chain-level propagation cues, all of which are disrupted by structural noise. When the perturbation reaches 10 percent or 20 percent, precision drops sharply. The breakage of adjacency relations prevents the model from maintaining accurate focus on abnormal chains. Recall also decreases, which indicates that the model fails to recover full abnormal propagation paths. The simultaneous decline of both metrics shows that structure is one of the most important factors in transaction graph state detection.

Overall, the experiment demonstrates the strong reliance of the model on structural consistency in complex financial transaction networks. It also highlights the importance of maintaining graph structure integrity in risk detection tasks. Fictitious transactions and related chains often hide within specific paths, low-weight edges, and weakly connected node sequences. Structural perturbation disrupts these critical patterns and prevents the model from capturing cross-node dependencies. Therefore, the proposed graph state detection framework is highly sensitive to noise, drift, and abnormal disturbances in graph structure. This reinforces the importance of data quality, structural stability, and link consistency in dynamic financial systems.

Figure 5 reports how the classification accuracy changes as the noise injection ratio increases, providing a detailed view of the model's robustness under different noise levels.

The experimental results show a clear monotonic decline, indicating that increasing the noise injection ratio directly weakens the model's structural discrimination ability. With zero noise, the model can fully use both local and global structural information in the transaction graph. It can accurately identify key nodes and paths in fictitious and related transaction chains, which leads to the highest accuracy. Once noise is introduced, the topology becomes disturbed, and true dependencies among nodes are diluted. The model can no longer maintain consistent structural reasoning in complex chains, and performance drops quickly.

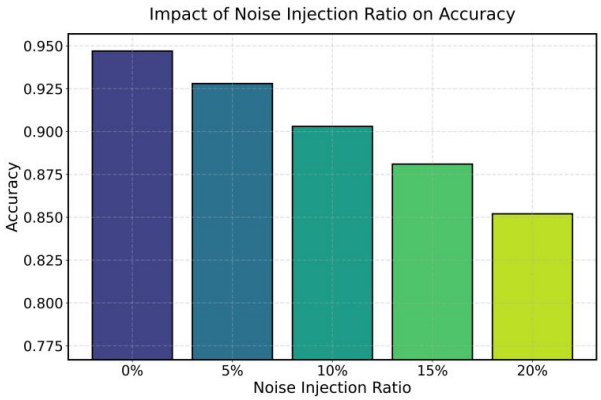

Figure 5. The impact of noise injection ratio on accuracy

Between zero percent and ten percent noise, accuracy decreases sharply. This shows that the model is highly sensitive to early structural noise. Fictitious and related transaction chains often rely on weak path signals, low-weight links, and multi-hop hidden relationships. Noise introduced at this stage first disrupts these subtle but important clues. As a result, the model's ability to capture risk features that spread across paths declines significantly. This characteristic reflects the fragility of financial graph structures. Even small perturbations can strongly weaken the expression of chain patterns.

As noise increases to fifteen percent and twenty percent, accuracy continues to decline and then stabilizes. This suggests that the model can no longer rely on structural information to reconstruct true chains. The overall quality of the graph state representation is severely degraded. Heavy noise makes the structure close to random. Local correlations and global consistency are lost, and the model cannot distinguish real transaction chains from fabricated paths. For graph state detection tasks that depend on multi-scale structural reasoning, this marks a critical point of degradation.

Overall, the experiment demonstrates the strong dependence of the graph state detection model on structural integrity. Noise injection disrupts chain-level associations, disturbs propagation paths, and weakens the modeling of multi-hop relationships. These factors directly affect the identification of fictitious and related transaction chains. The results show that in real financial systems, maintaining data quality, controlling structural noise, and stabilizing the transaction graph are essential for ensuring reliable performance in high-risk scenarios.

5. Conclusion

This study addresses the challenge of identifying fictitious transactions and related transaction chains by building a graph state detection framework for complex financial networks. The framework constructs a unified representation at the node, path, and global graph levels. It captures multi-hop weak signals, cross-path propagation patterns, and hidden chain relationships. It also provides stable and fine-grained structural reasoning for detecting abnormal chains. The experimental results show that the framework can handle disguised chain patterns that traditional methods fail to identify. It extracts deep structural patterns from transaction networks and offers strong technical support for risk control, anti-money laundering, and cross-account behavior modeling.

At the methodological level, the proposed path attention fusion mechanism and structural consistency modeling enhance the model's sensitivity to graph topology changes. The model maintains strong detection performance under structural perturbation, noise, and temporal evolution. Through a unified graph state space, it can aggregate and infer related chains at a higher level and capture network dynamics from a global perspective. This is important for financial risks that are dynamic, strongly coupled, and highly concealed. The structured reasoning mechanism improves the model's expressive power in transaction scenarios and also provides insights for broader multi-relation graph analysis tasks.

From an application perspective, the proposed graph state detection framework can be directly applied to banking risk control, fraud monitoring, anti-money laundering, supply chain capital flow analysis, and digital asset regulation. As transaction networks grow in scale and complexity, traditional rule-based or local feature-based methods struggle to handle complex risk patterns. The findings of this study can support future regulatory technologies. They can provide financial institutions with structured risk profiling and allow systems to detect high-risk chains earlier and more accurately. This improves operational security and market transparency.

Looking ahead, the framework has several potential directions for further development. It can be extended with temporal enhancement models, dynamic graph neural networks, and adaptive structure learning. This would allow stable performance in large-scale, cross-platform, and cross-network environments. Generative modeling could also be explored to simulate potential risk chains and enable early prediction of unknown fraud patterns and more complex disguises. As regulatory technology and large-scale financial models continue to advance, the graph reasoning mechanism proposed in this study can be integrated with multimodal models. This will support the development of interpretable, transferable, and adaptive financial risk intelligence systems with long-term value across real-world applications.

References

[1] Y. Motie and B. Raahemi, "Financial fraud detection using graph neural networks: A systematic review," Expert Systems with Applications, vol. 240, p. 122156, 2024.

[2] J. Qian and G. Tong, "Metapath-guided graph neural networks for financial fraud detection," Computers and Electrical Engineering, vol. 126, p. 110428, 2025.

[3] P. Kadam, "Financial fraud detection using jump-attentive graph neural networks," Proceedings of the 2024 International Conference on Machine Learning and Applications (ICMLA), pp. 628-635, 2024.

[4] X. Guo, Y. Wu, W. Xu and et al., "Graph-Based Representation Learning for Identifying Fraud in Transaction Networks," Proceedings of the 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), pp. 1598-1602, 2025.

[5] N. Bakhshinejad, U. T. Nguyen, S. Ghahremani and et al., "A Graph-Based Deep Learning Model for the Anti-Money Laundering Task of Transaction Monitoring."

[6] Y. Tian, G. Liu, J. Wang and et al., "ASA-GNN: Adaptive sampling and aggregation-based graph neural network for transaction fraud detection,"

IEEE Transactions on Computational Social Systems, vol. 11, no. 3, pp. 3536-3549, 2023.

[7] Y. Zhou, M. Sun and F. Zhang, "Graph Neural Network-Based Anomaly Detection in Financial Transaction Networks," Journal of Computing Innovations and Applications, vol. 1, no. 2, pp. 87-101, 2023.

[8] L. Akoglu, H. Tong and D. Koutra, "Graph based anomaly detection and description: a survey," Data Mining and Knowledge Discovery, vol. 29, no. 3, pp. 626-688, 2015.

[9] S. Ranshous, S. Shen, D. Koutra, S. Harenberg, C. Faloutsos and N. F. Samatova, "Anomaly detection in dynamic networks: a survey," Wiley Interdisciplinary Reviews: Computational Statistics, vol. 7, no. 3, pp. 223-247, 2015.

[10] S. Motie and B. Raahemi, "Financial fraud detection using graph neural networks: A systematic review," Expert Systems with Applications, vol. 240, p. 122156, 2024.

[11] B. Perozzi, R. Al-Rfou and S. Skiena, "DeepWalk: Online learning of social representations," Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 701-710, 2014.

[12] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson and C. E. Leiserson, "Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics," arXiv preprint arXiv:1908.02591, 2019.

[13] K. Ding, J. Li, R. Bhanushali and H. Liu, "Deep anomaly detection on attributed networks," Proceedings of the 2019 SIAM International Conference on Data Mining, pp. 594-602, 2019.

[14] N. Entezari, S. A. Al-Sayouri, A. Darvishzadeh and E. E. Papalexakis, "All you need is low (rank): Defending against adversarial attacks on graphs," Proceedings of the 13th International Conference on Web Search and Data Mining, pp. 169-177, 2020.

[15] Y. Dou, Z. Liu, L. Sun, Y. Deng, H. Peng and P. S. Yu, "Enhancing graph neural network-based fraud detectors against camouflaged fraudsters," Proceedings of the 29th ACM International Conference on Information & Knowledge Management, pp. 315-324, 2020.

[16] R. Fang, "Transaction network graph neural networks for automated and robust financial fraud detection in corporate auditing," Transactions on Computational and Scientific Methods, vol. 4, no. 7, 2024.

[17] Y. Tian, G. Liu, J. Wang and et al., "ASA-GNN: Adaptive sampling and aggregation-based graph neural network for transaction fraud detection," IEEE Transactions on Computational Social Systems, vol. 11, no. 3, pp. 3536-3549, 2023.

[18] J. Qian and G. Tong, "Metapath-guided graph neural networks for financial fraud detection," Computers and Electrical Engineering, vol. 126, p. 110428, 2025.

[19] P. Kadam, "Financial fraud detection using jump-attentive graph neural networks," Proceedings of the 2024 International Conference on Machine Learning and Applications (ICMLA), pp. 628-635, 2024.

[20] X. Guo, Y. Wu, W. Xu and et al., "Graph-based representation learning for identifying fraud in transaction networks," Proceedings of the 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), pp. 1598-1602, 2025.

[21] C. F. Chiang, D. Li, R. Ying, Y. Wang, Q. Gan and J. Li, "Deep learning-based dynamic graph framework for robust corporate financial health risk prediction," 2025.

[22] J. Li, Q. Gan, Z. Liu, C. Chiang, R. Ying and C. Chen, "An improved attention-based LSTM neural network for intelligent anomaly detection in financial statements," 2025.

[23] H. Wang, C. Nie and C. Chiang, "Attention-driven deep learning framework for intelligent anomaly detection in ETL processes," 2025.

[24] T. Pham and S. Lee, "Anomaly detection in bitcoin network using unsupervised learning methods," arXiv preprint arXiv:1611.03941, 2016.

[25] M. Jin, Y. Liu, Y. Zheng and et al., "Anemone: Graph anomaly detection with multi-scale contrastive learning," Proceedings of the 30th ACM International Conference on Information & Knowledge Management, pp. 3122-3126, 2021.

[26] J. Tang, F. Hua, Z. Gao and et al., "Gadbench: Revisiting and benchmarking supervised graph anomaly detection," Advances in Neural Information Processing Systems, vol. 36, pp. 29628-29653, 2023.

[27] J. Nicholls, A. Kuppa and N. A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," IEEE Access, vol. 9, pp. 163965-163986, 2021.

[28] I. Martins, J. S. Resende, P. R. Sousa and et al., "Host-based IDS: A review and open issues of an anomaly detection system in IoT," Future Generation Computer Systems, vol. 133, pp. 95-113, 2022.

[29] H. Hanrui, Y. Yi, W. Xu, Y. Wu, S. Long and Y. Wang, "Intelligent credit fraud detection with meta-learning: Addressing sample scarcity and evolving patterns," 2025.

[30] S. Huang, Y. Zheng, Y. Zhao, R. Ying, K. Cao and X. Liang, "A unified meta learning and domain adaptation framework for credit fraud detection in dynamic environments," 2026.

[31] H. Feng, Y. Wang, R. Fang, A. Xie and Y. Wang, "Federated risk discrimination with Siamese networks for financial transaction anomaly detection," 2025.

[32] R. Ying, J. Lyu, J. Li, C. Nie and C. Chiang, "Dynamic portfolio optimization with data-aware multi-agent reinforcement learning and adaptive risk control," 2025.

[33] Y. Shu, K. Zhou, Y. Ou, R. Yan and S. Huang, "A self-supervised learning framework for robust anomaly detection in imbalanced and heterogeneous time-series data," 2025.

[34] J. Tang, F. Hua, Z. Gao and et al., "Gadbench: Revisiting and benchmarking supervised graph anomaly detection," Advances in Neural Information Processing Systems, vol. 36, pp. 29628-29653, 2023.

[35] M. Jin, Y. Liu, Y. Zheng and et al., "Anemone: Graph anomaly detection with multi-scale contrastive learning," Proceedings of the 30th ACM International Conference on Information & Knowledge Management, pp. 3122-3126, 2021.

[36] J. Nicholls, A. Kuppa and N. A. Le-Khac, "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape," IEEE Access, vol. 9, pp. 163965-163986, 2021.

[37] I. Martins, J. S. Resende, P. R. Sousa and et al., "Host-based IDS: A review and open issues of an anomaly detection system in IoT," Future Generation Computer Systems, vol. 133, pp. 95-113, 2022.