ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20240606001759
Original scientific paper

Supply Chain Financial Fraud Detection Based on Graph Neural Network and Knowledge Graph

Wenying XIE, Juan HE*, Fuyou HUANG, Jun REN

Abstract: Supply chain financial fraud, characterized by extensive false fund circulation and fictitious business events, causes substantial financial losses and undermines the efficiency of supply chain operations. To address this challenge, we introduce an innovative research framework that utilizes knowledge graphs and spatial-temporal neural networks for effective fraud detection. Our approach involves constructing a supplier-customer knowledge graph from data of Chinese listed companies, capturing the complex supply-demand relationships within the supply chain. We designed a spatial-temporal Graph Neural Network (GNN) that models both node attributes and the time-evolving graph topology. By incorporating temporal and spatial dual attention mechanisms, our model adeptly identifies local topology and temporal changes in the knowledge graph. Empirical evaluations demonstrate that our Dual Attention Spatial-Temporal Graph Neural Network (DAST-GNN) outperforms existing methods, achieving an *AUC* of 93.64%, which is 10.41% higher than the leading machine learning methods. Furthermore, analyzing supplier-customer relationships across different historical periods enhances fraud detection, highlighting the robustness of our approach. This research offers a potent tool for regulators, investors, and researchers, advancing the security and efficiency of supply chain operations.

Keywords: financial fraud; graph neural network; knowledge graph; spatial-temporal attention; supply chain network

1 INTRODUCTION

Supply chain finance is a highly efficient approach for maximizing working capital [1, 2]. BCR Publishing Limited reports that the global market size for enterprise supply chain finance reached $1.8 trillion in 2021, reflecting a significant 38% growth compared to the previous year. Despite this growth, fraud has emerged as a critical issue, causing significant financial losses and disrupting supply chain operations. Financial statement fraud, involving deceptive fund movements and fictitious company activities, undermines the effectiveness of supply chain finance and threatens global supply chain stability [3]. According to the International Chamber of Commerce, even a small percentage of fraud within the $5 trillion global trade finance market could result in nearly $5 billion in annual losses. Enhanced fraud detection benefits financial institutions and entities throughout the supply chain, including core enterprises, third-party companies (such as logistics and platform companies), as well as both upstream and downstream enterprises [4]. The integration of the supply chain with the Internet, big data, artificial intelligence (AI), the Internet of Things (IoT), and blockchain technology has resulted in its growing diversity, leading to the establishment of a networked ecosystem [5, 6]. Nevertheless, the rapid development of these technologies has also led to increasingly sophisticated and subtle financial fraud practices. Graph structures have been employed by certain specialists to investigate potential financial fraud behaviors within the supply chain. The researchers discovered that concealing fraudulent activities can be detected by gathering comprehensive global data on the entire supply chain network [7, 8]. However, the interconnections of supply and demand across businesses in the supply chain are becoming increasingly intricate, particularly when businesses collaborate on a worldwide scale [9]. These changes make it easier for companies to quickly trade goods and services with each other, and fraudsters are always changing how they attack. To stop fraudsters from using constantly changing attack tactics, it is important to look into how they gather information in time and space [10]. In practice, most networks are characterized by intertwined spatial and temporal elements, with dynamic attributes at each node. Therefore, it is essential to develop models that accurately represent both the spatial and temporal contexts of graph topologies and node properties. In order to tackle these concerns, we propose the Dual Attention Spatial-Temporal Graph Neural Network (DAST-GNN). This model leverages knowledge graph technology and GNN methods to analyze both local structures and temporal variations in supply and demand graphs. By developing a knowledge graph based on data from publicly traded Chinese companies, we capture the intricate supply-demand relationships across the network. The dual attention mechanism enhances fraud detection by integrating temporal and spatial data, resulting in improved accuracy. Our experimental results demonstrate that DAST-GNN outperforms existing methods, contributing to more effective financial fraud detection. The key contributions of this work are outlined below:

1. Identifying fraudulent entities and monitoring financial fraud through supplier-customer relationship data.
2. Constructing a comprehensive supply chain network using knowledge graph technology.
3. Developing DAST-GNN to simultaneously model node attributes and temporal changes, with rigorous testing showing enhanced detection accuracy.

The structure of this research paper is organized as follows: The next section offers a comprehensive review of the existing literature related to the topic. Section 3 details the methodology used to construct the supplier-customer knowledge graph and provides an in-depth explanation of the DAST-GNN model. Section 4 presents an empirical analysis based on data from Chinese enterprises. Finally, Section 5 summarizes the key findings and contributions of the study.

2 LITERATURE REVIEW

Researchers and industry experts have increasingly turned to big data analysis and machine learning to monitor and mitigate supply chain financial fraud. This field has seen various methodological advancements aimed at addressing fraud risks. DuHadway et al. proposed a methodology for managing purposeful hazards in supply chain risk management, focusing on the practical application of risk mitigation strategies [11]. Similarly, Kara et al. utilized data mining techniques to identify risks and fraud within supply chains [12]. Zhou et al. implemented Apache Spark and Hadoop big data architecture combined with convolutional neural networks (CNNs) for fraud detection [13]. Wu et al. introduced MultiFraud, a multi-task learning framework leveraging heterogeneous graph neural networks (GNNs) to tackle complex fraud scenarios with reasonable interpretability [14]. Initial research predominantly relied on rule-based systems derived from historical transaction data, which often overlooked the intricate correlations among multiple entities involved in fraud. This approach neglected valuable relational information and was limited in its ability to capture dynamic interactions [15]. The integration of graph structures has significantly advanced the field by enabling the capture of correlations among fraudsters through the creation of knowledge graphs. For example, Microsoft developed a comprehensive knowledge graph that integrates user interactions, transactions, and connections to reduce e-commerce fraud [16]. Cai et al. proposed an interpretable fraud detection method using a two-layer knowledge graph combined with fraud pattern mining strategies [17]. Li et al. constructed a supplier-customer knowledge graph to map complex interactions within the supply chain, improving financial statement fraud detection [18]. The advent of deep learning technologies has further enhanced fraud detection capabilities. Graph neural networks (GNNs) have demonstrated considerable potential in analyzing knowledge graphs due to their ability to process graph-structured data, capturing both local and global information to identify fraudulent patterns [19]. Consequently, anti-fraud models based on knowledge graphs and GNNs have become a research hotspot. Cheng et al. proposed a 3D convolutional neural network based on a Spatial-temporal attention mechanism for credit card fraud detection, leveraging the characteristics of fraudsters-"temporal aggregation" and "spatial aggregation"-and extracting spatial features from location-based transaction graphs through GNNs [10]. Chen et al. introduced SCN_GNN, a method combining node sampling algorithms with graph topology to improve detection accuracy [20]. Xu et al. enhanced Gated Recurrent Units (GRU) with a spatial-temporal dual attention mechanism to better learn node embeddings [21]. Yang et al. developed a spatial-temporal perception graph neural network to address credit-related changes in small and medium-sized enterprises [7]. Despite these advancements, many studies remain narrowly focused on single-task scenarios, often failing to fully leverage the complex and dynamic nature of network relationships. The integration of spatial and temporal aspects in GNNs has not been extensively explored, leaving a significant knowledge gap in effectively detecting supply chain financial fraud. This gap is particularly evident in understanding how spatial-temporal rules related to hidden fraudulent behavior can be extracted from complex supplier-customer relationships. To address these challenges, this study focuses on extracting spatial-temporal rules related to concealed fraud from intricate supplier-customer interactions. The existing literature highlights the need for a comprehensive approach that models both spatial and temporal dimensions of graph data. This research introduces a dual attention spatial-temporal graph neural network (DAST-GNN) to enhance fraud detection by summarizing supply and demand relationships through a knowledge graph. The proposed model aims to bridge the gap in understanding between supplier-customer relationships and fraudulent activities, offering a more robust framework for detecting financial fraud within supply chains.

3 METHOD

3.1 Graph Construction

Fig. 1 illustrates a supplier-customer knowledge graph with the entity, relationship, and attribute included. Here's how the extraction procedure works:

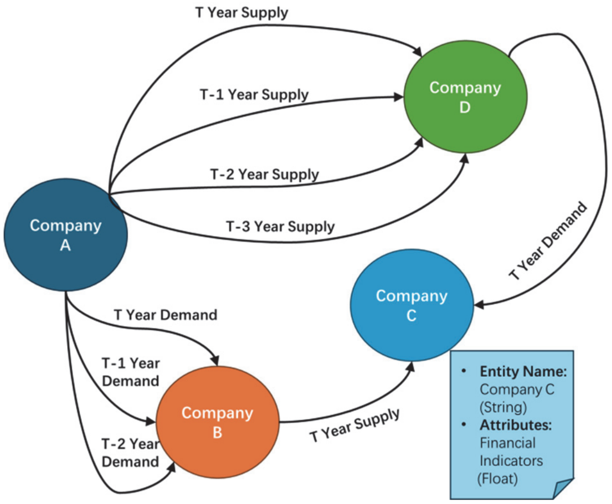

Figure 1 Knowledge graphs between suppliers and customers: examples

(1) Extracting entities. The entity node set contains the company's name, as well as the names of its suppliers and customers.

(2) Extraction of relationships. The supply chain created a knowledge graph with two types of relationships: supply and demand links. The relationship between the business and its revealed suppliers is known as the demand relationship, and it indicates that the business requires goods from the suppliers shown in the diagram. A business establishes a supply relationship when it provides its products to customers and discloses the customers to the business.

(3) Extraction of attributes. company financial information is represented in a knowledge graph by using financial indicators from company statements as entity attributes. These attributes are derived from accounting items in financial statements, which provide insights into the company's financial health. Bao et al. identified 28 crucial financial data points necessary for detecting financial statement fraud [22]. Li et al. examined governance indicators related to financial fraud in China and noted that these indicators manifest in various aspects of financial statements, including debt solvency, operational capability, profitability, cash flow, and development capacity [23].

Chen et al. found that profitability and asset quality positively impact financial fraud detection when analyzing data from Chinese A-share listed companies [24]. Given these findings and the diverse national contexts, this study selects 12 financial indicators for fraud analysis, covering debt solvency, operational capability, and profitability, as detailed in Tab. 1.

Table 1 Financial indicators for financial fraud detection

No.	Financial indicators
1	Gross Profit Margin
2	Net Profit Margin
3	Current Ratio
4	Quick Ratio
5	Debt to Asset Ratio
6	Inventory Turnover Ratio
7	Accounts Receivable Turnover Ratio
8	Operating Cash Flow to Net Income Ratio
9	Capital Expenditure to Cash Flow Ratio
10	Revenue Growth Rate
11	Accounts Receivable Growth Rate
12	Operating Expense Ratio

3.2 Definitions

Definition 1. Supplier-Customer Knowledge Graph. The temporal Supplier-Customer Knowledge Graph is denoted as an ordered set of T graph snapshots $\xi=\left\{\xi^{t}\right\}_{t=1}^{T}=\left\{v,\varepsilon^{t},\lambda^{t},X^{t},E^{t}\right\}_{t=1}^{T}$. Here, v and ε denotes the node and the edge set, including company and its suppliers and customers, λ^t denotes entity's financial attributes, ε^t denotes the edge set at time t. $X^{t}\in R^{|v|\times fv}$ and $E^{t}\in R^{|\varepsilon|\times f\varepsilon}$. Note that the Supplier-Customer Knowledge Graph ξ_{sc} is also treated as temporal graph with multiple graph snapshots, and each of them is a subset of ξ^t with all the companies.

Definition 2. Fraud detection based on Supplier-Customer Knowledge Graph. Given the temporal Supplier-Customer Knowledge Graph $\xi_{sc}=\left\{\xi_{sc}^{t}\right\}_{t=1}^{T}$ and a set of labeled companies as training set D_{fd} = $\{(u, y)\}$, here $y = 1$ denotes fraud otherwise $y = 0$, the goal of fraud detection based on Supplier-Customer Knowledge Graph is to predict the future fraud probability of companies.

3.3 Dual Attention Mechanism Spatial-Temporal Graph Neural Network

The structure of DAST-GNN is shown in Fig. 2. It is made up of two main parts: a spatial-temporal perception aggregator and a spatial-temporal attention mechanism. Fig. 2 shows that the suggested DAST-GNN uses a spatially aware aggregator in each time graph snapshot to learn about the nodes and edges that are close to node u. Subsequently, we can acquire individual spatial embeddings for each node in T graph snapshots. The time-aware aggregator incorporates all T spaces as inputs to capture the temporal variations in continuous graph snapshots and produces the temporal embeddings as outputs. Ultimately, DAST-GNN employs a dual spatial-temporal attention method that involves spatial embedding and temporal embedding. This mechanism produces the final node embedding, subsequently merging it with downstream learning objectives to form an end-to-end model.

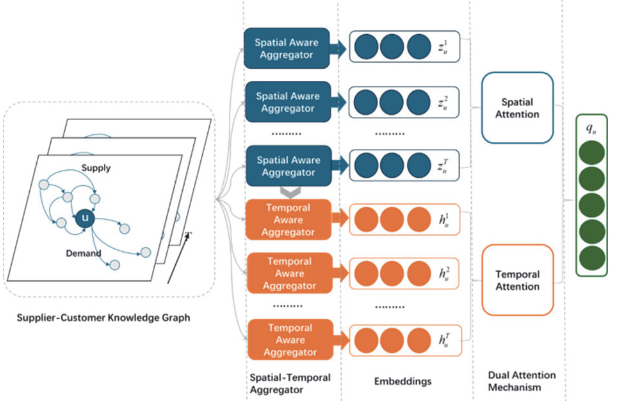

Figure 2 Illustration of Dual Attention mechanism Spatial-temporal Graph Neural Network (DAST-GNN)

3.3.1 Spatial-Temporal Aware Aggregator

(1) Spatial Aware Aggregator.

Generally, given a targeted node u and its neighborhood at t time, the N_u^t spatial-aware aggregator $\phi(\cdot)$ can be defined as:

$$z_{u}^{t}=\phi\left(x_{u}^{t},\left\{\left(x_{v}^{t},e_{u,v}^{t}\right):v\in N_{u}^{t}\right\};\Theta_{\phi}^{t}\right) \tag{1}$$

where x_v^t and $e_{u,v}^t$ are the original feature vectors of node u and edge (u, v) at time t, and Θ_ϕ^t is the set of parameters that the spatially aware aggregator can learn at time t. To make it work, the linear attention operator $\phi(\cdot)$ is used. This is because different neighbors have different effects on the chosen node. In particular, the following changes are made to Eq. (1):

$$\alpha_{u,v}^{t}=\frac{\exp\left(v_{\phi}^{t\;T}\sigma\left(W_{\phi1}^{t}[\left[x_{u}^{t},x_{v}^{t},e_{u,v}^{t}\right]]\right)\right)}{\sum_{v'\in N_{u}^{t}}\exp\left(v_{\phi}^{t\;T}\sigma\left(W_{\phi1}^{t}\left[x_{u}^{t},x_{v'}^{t},e_{u,v'}^{t}\right]\right)\right)} \tag{2}$$

$$z_{u}^{\prime t}=\sigma\left(W_{\phi2}^{t}\sum_{v\in N_{u}^{t}}\alpha_{u,v}^{t}\left[x_{u}^{t},e_{u,v}^{t}\right]\right) \tag{3}$$

$$z_{u}^{t}=\sigma\left(W_{\phi3}^{t}\left[x_{u}^{t},z_{u}^{\prime t}\right]\right) \tag{4}$$

where σ is a nonlinear activation function (sigmoid), $[\cdots]$ denotes the concatenation of vectors, $W_{\phi1}^t, W_{\phi2}^t, W_{\phi3}^t$ and v_ϕ^t are learnable parameters of the spatial-aware aggregator at t time. Use node u and its neighboring nodes N_u^t, as well as the vector of edges, to calculate the weights of neighboring nodes during aggregation. Use the calculated weights to aggregate the information of surrounding nodes and edges onto node u to obtain the updated vector z'^{t}_{u}. By stacking this aggregator iteratively for *K* times, the final spatial embedding is able to absorb the topological and attributed information in *K*-hops neighborhood. For simplification, we still use z^t_u to denote the final spatial embedding for node *u* at time *t*.

(2) Temporal Aware Aggregator.

Generally, given a targeted node *u* and its spatial embeddings generated from *T* graph snapshots $\left\{z^t_u\right\}^T_{t=1}$, the temporal aware aggregator *φ*(·) can be defined as:

$$h^t_u = \varphi\left(\left\{z^t_u\right\}^T_{t=1}; \Theta_\varphi\right) \tag{5}$$

where the learnable parameter set of the temporal aware aggregator is denoted as *Θ_φ*. In order to represent the temporal changes in the *T* graph snapshots, we propose using two stacked LSTM models to generate temporal embeddings for *u*, as below:

$$f^t_u = \sigma\left(W_{\varphi f}\cdot\left[h^{t-1}_u, z^t_u\right]\right) \tag{6}$$

$$i^t_u = \sigma\left(W_{\varphi i}\cdot\left[h^{t-1}_u, z^t_u\right]\right) \tag{7}$$

$$\tilde{c}^t_u = f^t_u \cdot \tilde{c}^{t-1}_u + i^t_u \cdot \tan h\left(W_{\varphi C}\cdot\left[h^{t-1}_u, z^t_u\right]\right) \tag{8}$$

$$o^t_u = \sigma\left(W_{\varphi o}\cdot\left[h^{t-1}_u, z^t_u\right]\right) \tag{9}$$

$$h^t_u = o^t_u \cdot \tan h\left(\tilde{c}^t_u\right) \tag{10}$$

Note that the hidden states computed by the first LSTM layer act as inputs for the second LSTM Layer. The temporal embedding h^t_u encodes the temporal information of node *u* until the *t* time.

3.3.2 Dual Attention Mechanism

After collecting all of node *u*'s spatial and temporal embeddings, we use the attention operator to aggregate significant spatial and temporal information across all *T* graph snapshots. The set of spatial and temporal embeddings for node *u* is denoted as $E = \left\{z^t_u\right\}^T_{t=1} \cup \left\{h^t_u\right\}^T_{t=1}$.

(1) Spatial Attention.

The impact of different neighbors on node representation also varies, and attention mechanism can adaptively capture relevant information. Apply spatial attention to the aggregator during the aggregation process. β_e is a standardized attention value located relative to embedded *e*, indicating the importance of *u* to embedded *e*. β_e is generated by our spatial attention module, which takes the representation of nodes and their neighbors as input and is described as:

$$\beta_e = \frac{\exp\left({v_{f2}}^T\sigma(e)\right)}{\sum_{e'\in E}\exp\left({v_{f2}}^T\sigma(e')\right)} \tag{11}$$

(2) Temporal Attention.

For temporal attention, it refers to multiple static snapshot times around a single node. After obtaining the state embeddings of nodes at different static snapshot times, the time attention weights for a single time are as:

$$\alpha_t = \frac{\exp\left({v_{f1}}^T\tan h\left(h'_t\right)\right)}{\sum_{e'\in E_{enb}}\exp\left({v_{f1}}^T\tan h\left(h'_t\right)\right)} \tag{12}$$

where α_t indicates the importance of time step t for determining the target node's label compared to others. The concatenation of all the state vectors is denoted by:

$$H = [h'_1 \oplus \cdots \oplus h'_T] \tag{13}$$

And the algorithm ultimately needs to combine the state embeddings of multiple static snapshots, and the proportion of each static snapshot embedding is the use of temporal attention weights, which includes:

$$\alpha = soft\max\left({v_{f1}}^T\tan h\left(H^T\right)\right) \tag{14}$$

Then we sum up all the state vectors scaled by *α*, for the final embedding of a single node as *q*, it can be passed to downstream learning objectives to form an end-to-end model:

$$q_u = \sigma\left({v_{f1}}^T\sum_{e\in E_{emb}}\beta_e e\right) \tag{15}$$

3.4 Fraud Detection Task

As stated previously, we define the issue of fraud detection as a problem of classifying nodes. More precisely, while considering the given set of labeled nodes *Dfd* = {(*u*, *y*)}, we utilize a Multilayer Perceptron (MLP) with cross entropy loss, which is dependent on the final embeddings *q* of the nodes, as follows:

$$L_{fd} = -\frac{1}{\left|D_{fd}\right|}\sum_{(u,y)\in D_{fd}} y\log\left(\hat{y}\right) + \left(1-y\right)\log\left(1-\hat{y}\right) \tag{16}$$

$$\hat{y} = MLP_{fd}\left(q_u\right) \tag{17}$$

where two fully connected layers, built upon the matching node embedding, comprise the multi-layer perception known as $MLP_{fd}(\cdot)$. These two fully connected layers process node embeddings sequentially, mapping them to the final output $\hat{y}$. The cross-entropy loss Eq. (16) is employed during training to refine the model's predictions, ensuring they align closely with the true labels *y*. Specifically, this loss function penalizes discrepancies between the predicted probability distribution and the actual labels, thereby guiding the network to improve its predictive accuracy.

4 RESULTS AND DISCUSSION

4.1 Experimental Dataset and Data Description

(1) Data source.

This study constructs a supplier-customer knowledge graph using supplier, customer, and financial information from the financial statements of Chinese enterprises to identify instances of financial statement fraud. Data, including both legitimate and fraudulent entries, is sourced from the WIND database. The sample comprises all Chinese companies publicly traded on the Shanghai, Shenzhen, and Beijing stock exchanges between 2018 and 2021, along with their disclosed suppliers and customers. In the knowledge graph, the relationship between a company and its disclosed clients is categorized as a supply relationship, while the relationship between the company and its disclosed suppliers is categorized as a demand relationship. Identification of companies involved in financial fraud is primarily based on official penalty announcements by the China Securities Regulatory Commission. Seven categories of financial statement fraud, as identified by Liao et al. [21] and Xiong et al. [25], include profit and asset manipulation, fraudulent statements, delayed disclosure of significant information, omission of important details, provision of incorrect information, and violations of accounting principles. Companies committing these infractions are classified as fraudulent samples, while others are considered non-fraudulent. The study focuses on using data from 2021 to build the knowledge graph and analyze fraudulent activities. After manual processing of the "violation type" and "specific violation behavior" fields in the WIND database, we filtered out observations lacking financial and supplier-customer data. The final dataset includes 104 fraud cases and 567 non-fraudulent samples. The proportion of fraudulent samples ranges from 15.49% to 16.70% [8], justifying the selection of fraudulent cases for this study.

(2) Supplier-customer knowledge graph.

We constructed a supplier-customer knowledge graph for Chinese companies following the method outlined in Section 3.1. Initially, we extracted entities (companies) and relationships (supply or demand) from the supply chain information disclosed by the companies, creating triples that systematically describe the relationships between listed companies and their suppliers and customers. Ultimately, we developed a supplier-customer knowledge graph for Chinese companies comprising 4687 entity nodes and 10780 relationships. Statistics on the entities and relationships in the supplier-customer knowledge graph are shown in Tab. 2.

Table 2 Statistics of the Datasets.

Dataset	Fraud detection
Nodes	4687
Edges	10780
Node Features	126549

Fig. 3 illustrates the part of supplier-customer knowledge graph for Chinese enterprises in 2021. As demonstrated by the example in Fig. 3, the knowledge graph can systematically and clearly describe the complex supply and demand relationships between companies. The five listed companies with stock codes 002163, 200012, 002006, 002541, and 603128, which have been exposed for fraudulent activities, are shown to have had transactions with each other and are also interconnected with five other companies 600550, 000420, 601618, 837302, and 870881 through supply and demand relationships over the past four years.

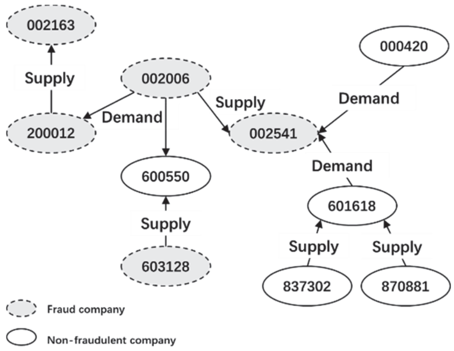

Figure 3 Supplier-customer knowledge graph of Chinese companies: an illustrative example

4.2 Comparative Experimental Design

4.2.1 Evaluation Indicators

The Confusion Matrix is a commonly used performance evaluation matrix for supervised machine learning classification models, which evaluates the confusion that classifiers may cause in multiple types of classification problems. To accurately evaluate the performance of the model in handling imbalanced problems, this paper evaluates the performance of the model based on confusion matrix, sampling Accuracy, $F1$ Score, and AUC (Area Under ROC Curve) indicators. More specifically,

(1) Accuracy, refers to the percentage of correctly identifying fraudulent companies.

$$Accuracy = \frac{TN + TP}{TN + FN + TP + FP} \tag{18}$$

(2) $F1$ Score, a robust metric that quantifies the accuracy of binary classification models. It is calculated as the harmonic mean of accuracy and recall. A model with a higher $F1$ Score is more resilient.

$$F1\ Score = \frac{2TP}{TN + 2TP + FP} \tag{19}$$

(3) AUC, refers to the area under the Receiver Operating Characteristic (ROC) curve. The model does a better job of classifying things when the AUC number is close to 1. AUC can clearly tell the difference between fraud and non-fraud categories. Changes in the distribution of categories do not affect it, making it a superior choice as a global evaluation indicator. In order to do our empirical study, we looked at the AUC value and compared how well different fraud detection methods worked.

$$FPR = \frac{FP}{TN + FP} \tag{20}$$

$$TPR = \frac{TP}{TP + FN} \tag{21}$$

Among them, True Positive (TP) refers to the accurate identification of fraudulent companies as fraudulent. False Negative (FN) represents the incorrect identification of fraudulent companies as non-fraudulent. True Negative (TN) means non-fraudulent companies are appropriately detected. Fake Positive (FP) means misidentifying non-fraudulent companies as fraudulent.

4.2.2 Baselines

We evaluated the static graph performance of DAST-CNN by comparing it with several popular GNN baseline methods, including DeepWalk [26], node2vec [27], GCN [28], and GraphSAGE [29], which are not designed to model temporal patterns in sequential data. To perform this comparison, we first applied these methods to each time step to generate node representations. We then concatenated the representations from different time steps into a single vector and used logistic regression to predict labels based on these vectors. In particular, we used the PyG library where GraphSAGE employs a mean aggregator and requires heterogeneous convolution processing of input graph data. Each GNN model contains two hidden layers, each with a size of 10. Additionally, we assessed the impact of incorporating node characteristics and supplier-customer relationships in the knowledge graph.To analyze temporal patterns, we also used LSTM [30], GRU [31], DynGEM [32], and DynAERNN [33]. LSTM and GRU focus on the evolution of node attributes over time, while DynGEM and DynAERNN capture and analyze surrounding contextual information. These methods were employed to provide a comprehensive evaluation of how different models handle temporal attributes and graph-structured data.

4.2.3 Experimental Design

The model training method utilizes 80% of the sample dataset for training and reserves the remaining 20% for testing purposes. Due to the imbalance in the experimental data, fraudulent samples are typically much less common than non-fraudulent samples. During GNN model training, we employ cost-sensitive learning to address the distinction between fraudulent and non-fraudulent data. Grid search is commonly employed to determine the optimal weight ratio between fraudulent and non-fraudulent classes in the loss function of the GNN model. This modification adjusts the penalty linked to misclassifying fraudulent cases, enhancing the importance of fraudulent samples during training [34]. Calculate the average of five cross-validations to obtain the model assessment index.

4.2.4 Experimental Results and Discussion

(1) Fraud detection results.

Using the GNN model, we effectively detect and address fraudulent activities by leveraging financial indicators and the extensive supply-demand relationships within the supplier-customer knowledge network. As shown in Tab. 3, the DAST-GNN model significantly outperforms other models in fraud detection. The comparison reveals that all four GNN models consistently achieve higher detection rates than traditional machine learning techniques. Specifically, Node2vec, DeepWalk, and GraphSAGE report Area Under the Curve (AUC) values of 91.72%, 89.37%, 85.63%, and 78.19%, respectively. These values are notably higher compared to those of conventional methods. DeepWalk and Node2vec, in particular, demonstrate the effectiveness of incorporating graph topology information into fraud detection. The supplier-customer knowledge graph benefits greatly from these models' ability to utilize graph data processing to uncover insights into intercompany relationships. The integration of financial relationships between businesses further enhances fraud detection, underscoring the value of graph-based approaches in revealing hidden fraudulent patterns. These findings highlight the superior performance of GNN models in capturing complex relationships and temporal dynamics, which are critical for accurate fraud detection.

Table 3 Fraud detection results using different methods (%)

Method		Features	ACC	AUC	$F1$ Score
Graph neural networks	Node2vec	Supply and demand relationships + Financial indicators	83.81	91.72	85.68
	DeepWalk		82.12	89.37	84.46
	GCN		72.64	85.63	73.31
	GraphSAGE		63.54	77.89	67.88
Common machine learning methods	LSTM	Financial indicators	81.42	83.23	79.94
	GRU		79.89	82.16	77.75
	DynGEM		75.37	80.34	71.66
	DynAERNN		61.33	76.63	65.21
	DAST-GNN		86.32	93.64	89.72

(2) Robust test.

In order to enhance the reliability of the findings, we performed fraud detection trials on companies from different years. More precisely, we created a knowledge graph of suppliers and customers using the organization's financial data and supply chain information, spanning from 2018 to 2021. We employ the Graph Neural Network (GNN) model to identify instances of financial fraud across several years. Additionally, we utilize the most effective machine learning technique as a standard against which to compare our results.

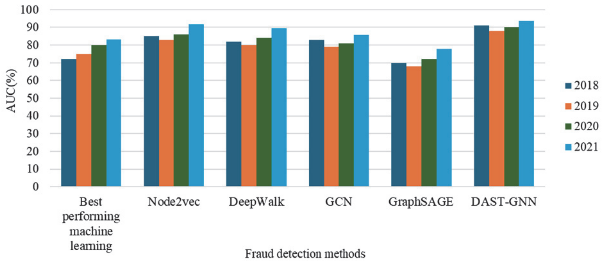

Figure 4 AUC value of fraud detection in different years

Fig. 4 presents the fraud detection outcomes for the years 2018 to 2020. The detection results for these years show consistent patterns with those observed for 2021. Notably, the GNN models generally achieve a higher Area

Under the Curve (*AUC*) compared to other machine learning algorithms, with the exception of GraphSAGE. This trend underscores the efficacy of the GNN approach, which leverages supplier-customer relationships and knowledge graph data, in outperforming traditional machine learning methods that do not account for these relationships. The empirical evidence confirms that incorporating supplier-customer relationships into the knowledge graph significantly enhances fraud detection capabilities. The GNN models, particularly DAST-GNN, demonstrate superior performance in extracting and analyzing hidden relationships among firms, compared to conventional methods that rely solely on financial indicators. Additionally, we explored the impact of incorporating supply and demand data from various historical periods on fraud detection. By constructing a comprehensive knowledge graph that integrates supply and demand data spanning 1 to 6 years, we applied the DAST-GNN model to detect financial fraud. Fig. 4 illustrates the results of fraud detection using this extended temporal knowledge graph. The analysis indicates that the DAST-GNN model remains effective across different historical periods, further validating its robustness and adaptability in identifying fraudulent activities.

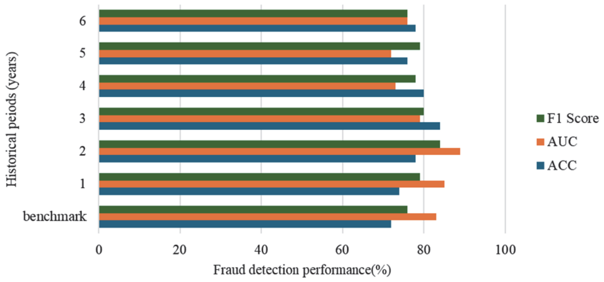

Figure 5 Fraud detection performance over various historical periods

Fig. 5 illustrates that incorporating historical supplier-customer relationships can significantly enhance financial fraud detection. Specifically, using supplier-customer data that spans multiple years provides a valuable supplement to an organization's current knowledge. Detection models utilizing relationships extending over two or more years consistently outperform those based on a single year of data. This effect is especially pronounced when the supplier-customer relationships extend back four years or more. These findings corroborate the work of Damberg et al. [35] and Li et al. [8], which emphasize that multi-year supply and demand relationships offer critical insights for fraud detection. The extended temporal scope allows for a more comprehensive understanding of the patterns and anomalies in business interactions, thereby improving the accuracy and reliability of fraud detection. Integrating historical data into the knowledge graph not only enriches the context but also enhances the model's ability to identify fraudulent activities that may be obscured in shorter-term analyses.

5 CONCLUSION

This paper presents a novel methodology for detecting financial fraud within supply chains through the use of knowledge graphs and spatial-temporal neural networks. We introduce the Dual Attention Spatial-Temporal Graph Neural Network (DAST-GNN), which integrates a dual attention mechanism to effectively represent both the spatial structure and temporal dynamics inherent in financial data. Empirical results from actual financial datasets validate that this approach adeptly captures the temporal patterns of attribute changes and the spatial characteristics of neighboring nodes. Rigorous evaluations indicate that the DAST-GNN model exhibits exceptional efficiency in identifying financial fraud within supply chains. The theoretical contributions of this study include advancing the application of spatial-temporal graph neural networks to the domain of fraud detection, thereby providing a more comprehensive understanding of the interaction between spatial and temporal factors in financial data. Practically, this framework offers a sophisticated tool for enhancing fraud detection processes, potentially mitigating financial losses and improving operational efficiency within supply chains. Future work will focus on deploying this framework in real-world settings, particularly among small and medium-sized enterprises. Additionally, we intend to extend the framework by integrating additional logistical and operational data into the supply chain knowledge graph. We will also optimize the DAST-GNN model to enhance its adaptability to various application scenarios. These enhancements are expected to significantly improve the model's performance, thereby offering more robust and effective solutions for financial fraud detection across diverse contexts.

Acknowledgments

This article was supported by National Natural Science Foundation of China (grant numbers 71802100, 71873111); Key R & D Program of China State Railway Group Co., Ltd. (N2022Z022);China National Railway Group Science and Technology Research and Development Program (JGYJS-2023-0026).

6 REFERENCES

[1] Gelsomino, L. M., Mangiaracina, R., Perego, A., & Tumino, A. (2016). Supply chain finance: a literature review. *International Journal of Physical Distribution & Logistics Management, 46*(4). https://doi.org/10.1108/IJPDLM-08-2014-0173

[2] Wuttke, D. A., Blome, C., Heese, H. S., & Protopappa-Sieke, M. (2016). Supply chain finance: Optimal introduction and adoption decisions. *International Journal of Production Economics, 178*, 72-81. https://doi.org/10.1016/j.ijpe.2016.05.003

[3] Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. *The Innovation, 2*(4), 100176. https://doi.org/10.1016/j.xinn.2021.100176

[4] Randall, W. S. & Theodore Farris, M. (2009). Supply chain financing: using cash-to-cash variables to strengthen the supply chain. *International Journal of Physical Distribution & Logistics Management, 39*(8), 669-689. https://doi.org/10.1108/09600030910996314

[5] Zhou, H., Sun, G., Fu, S., Fan, X., Jiang, W., Hu, S., & Li, L. (2020). A distributed approach of big data mining for financial fraud detection in a supply chain. *Comput Mater Continua, 64*(2), 1091-1105.

https://doi.org/10.32604/cmc.2020.09834

[6] Zaidi, M. & Hasan, S. M. (2022). Supply Chain Risk Prioritization Using AHP and Framework Development: A Perspective of the Automotive Industry. *International Journal of Industrial Engineering and Management, 13*(4), 283-293. https://doi.org/10.24867/IJIEM-2022-4-319

[7] Yang, S., Zhang, Z., Zhou, J., Wang, Y., Sun, W., Zhong, X., Fang, Y., Yu, Q., & Qi, Y. (2021, January). Financial risk analysis for SMEs with graph-based supply chain mining. *Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence*, 4661-4667. https://doi.org/10.24963/ijcai.2020/643

[8] Li, J., Chang, Y., Wang, Y., & Zhu, X. (2023). Tracking down financial statement fraud by analyzing the supplier-customer relationship network. *Computers & Industrial Engineering, 178*, 109118. https://doi.org/10.1016/j.cie.2023.109118

[9] Fiedler, A. (2022). An agent-based negotiation protocol for supply chain finance. *Computers & Industrial Engineering, 168*, 108136. https://doi.org/10.1016/j.cie.2022.108136

[10] Cheng, D., Wang, X., Zhang, Y., & Zhang, L. (2020). Graph neural network for fraud detection via spatial-temporal attention. *IEEE Transactions on Knowledge and Data Engineering, 34*(8), 3800-3813. https://doi.org/10.1109/TKDE.2020.3025588

[11] DuHadway, S. & Carnovale, S. (2019). Malicious supply chain risk: A literature review and future directions. *Revisiting supply chain risk*, 221-231. https://doi.org/10.1007/978-3-030-03813-7_13

[12] Kara, M. E., Fırat, S. Ü. O., & Ghadge, A. (2020). A data mining-based framework for supply chain risk management. *Computers & Industrial Engineering, 139*, 105570. https://doi.org/10.1016/j.cie.2018.12.017

[13] Wu, B., Chao, K. M., & Li, Y. (2024). Heterogeneous graph neural networks for fraud detection and explanation in supply chain finance. *Information Systems, 121*, 102335. https://doi.org/10.1016/j.is.2023.102335

[14] Gianini, G., Fossi, L. G., Mio, C., Caelen, O., Brunie, L., & Damiani, E. (2020). Managing a pool of rules for credit card fraud detection by a Game Theory based approach. *Future Generation Computer Systems, 102*, 549-561. https://doi.org/10.1016/j.future.2019.08.028

[15] Nanduri, J., Jia, Y., Oka, A., Beaver, J., & Liu, Y. W. (2020). Microsoft uses machine learning and optimization to reduce e-commerce fraud. *INFORMS Journal on Applied Analytics, 50*(1), 64-79. https://doi.org/10.1287/inte.2019.1017

[16] Cai, S. & Xie, Z. (2024). Explainable fraud detection of financial statement data driven by two-layer knowledge graph. *Expert Systems with Applications, 246*, 123126. https://doi.org/10.1016/j.eswa.2023.123126

[17] Li, J., Chang, Y., Wang, Y., & Zhu, X. (2023). Tracking down financial statement fraud by analyzing the supplier-customer relationship network. *Computers & Industrial Engineering*, *178*, 109118. https://doi.org/10.1016/j.cie.2023.109118

[18] Motie, S. & Raahemi, B. (2023). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*, 122156. https://doi.org/10.1016/j.eswa.2023.122156

[19] Chen, J., Chen, Q., Jiang, F., Guo, X., Sha, K., & Wang, Y. (2024). SCN_GNN: A GNN-based fraud detection algorithm combining strong node and graph topology information. *Expert Systems with Applications, 237*, 121643. https://doi.org/10.1016/j.eswa.2023.121643

[20] Xu, D., Cheng, W., Luo, D., Liu, X., & Zhang, X. (2019, August). Spatio-temporal attentive RNN for node classification in temporal attributed graphs. *Proceedings of the 28th International Joint Conference on Artificial Intelligence*, 3947-3953. https://doi.org/10.24963/ijcai.2019/548

[21] Liao, L., Chen, G., & Zheng, D. (2019). Corporate social responsibility and financial fraud: evidence from China. *Accounting & Finance, 59*(5), 3133-3169. https://doi.org/10.1111/acfi.12572

[22] Bao, Y., Ke, B., Li, B., Yu, J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. *Journal of Accounting Research, 58*(1), 199-235. https://doi.org/10.1111/1475-679X.12292

[23] Li, W. & Xu, X. (2023). Ensemble learning algorithm-research analysis on the management of financial fraud and violation in listed companies. *Decision Making: Applications in Management and Engineering, 6*(2), 722-733. https://doi.org/10.31181/dmame622023785

[24] Chen, X. & Zhai, C. (2023). Bagging or boosting? Empirical evidence from financial statement fraud detection. *Accounting & Finance, 63*(5), 5093-5142. https://doi.org/10.1111/acfi.13159

[25] Xiong, J., Ouyang, C., Tong, J. Y., & Zhang, F. F. (2021). Fraud commitment in a smaller world: Evidence from a natural experiment. *Journal of Corporate Finance, 70*, 102090. https://doi.org/10.1016/j.jcorpfin.2021.102090

[26] Perozzi, B., Al-Rfou, R., & Skiena, S. (2014, August). Deepwalk: Online learning of social representations. *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*, 701-710. https://doi.org/10.1145/2623330.2623732

[27] Grover, A. & Leskovec, J. (2016, August). node2vec: Scalable feature learning for networks. *Proceedings of the 22nd ACM SIGKDD international conference on Knowledge discovery and data mining*, 855-864. https://doi.org/10.1145/2939672.2939754.

[28] Van Den Berg, R., Thomas, N. K., & Welling, M. (2017). Graph convolutional matrix completion. *arXiv preprint arXiv:1706.02263, 2*(8), 9.

[29] Velickovic, P., Cucurull, G., Casanova, A., Romero, A., Lio, P., & Bengio, Y. (2017). Graph attention networks. *stat, 1050*(20), 10-48550.

[30] Hochreiter, S. & Schmidhuber, J. (1997). Long short-term memory. *Neural computation, 9*(8), 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

[31] Chung, J., Gulcehre, C., Cho, K., & Bengio, Y. (2014). Empirical evaluation of gated recurrent neural networks on sequence modeling. *arXiv preprint arXiv:1412.3555*.

[32] Goyal, P., Chhetri, S. R., & Canedo, A. (2020). dyngraph2vec: Capturing network dynamics using dynamic graph representation learning. *Knowledge-Based Systems, 187*, 104816. https://doi.org/10.1016/j.knosys.2019.06.024

[33] Goyal, P., Kamra, N., He, X., & Liu, Y. (2018). Dyngem: Deep embedding method for dynamic graphs. *arXiv preprint arXiv:1805.11273.*

[34] Höppner, S., Baesens, B., Verbeke, W., & Verdonck, T. (2022). Instance-dependent cost-sensitive learning for detecting transfer fraud. *European Journal of Operational Research, 297*(1), 291-300. https://doi.org/10.1016/j.ejor.2021.05.028

[35] Damberg, S., Schwaiger, M., & Ringle, C. M. (2022). What's important for relationship management? The mediating roles of relational trust and satisfaction for loyalty of cooperative banks' customers. *Journal of Marketing Analytics, 10*(1), 3-18. https://doi.org/10.1057/s41270-021-00147-2

Contact information:

Wenying XIE
School of Transportation and Logistics, Southwest Jiaotong University,
Chengdu, Sichuan 611756, China
Institute for Supply Chain Finance Studies, National Engineering Laboratory
of Application Technology of Integrated Transportation Big Data
Southwest Jiaotong University,
Chengdu, Sichuan 611756, China

Juan HE
(Corresponding author)
School of Transportation and Logistics, Southwest Jiaotong University,
Chengdu, Sichuan 611756, China
Institute for Supply Chain Finance Studies, National Engineering Laboratory
of Application Technology of Integrated Transportation Big Data
Southwest Jiaotong University,
Chengdu, Sichuan 611756, China
E-mail: hejunlin93@163.com

Fuyou HUANG
Institute of Transportation Development Strategy & Planning of Sichuan
Province,
Chengdu, Sichuan 610041, China

Jun REN
China State Railway Group Company Limited, Beijing 100080, China