

基于时序图神经网络的资产管理反洗钱检测方法

徐鑫, 朱鸿斌, 谌杰, 李青汶, 张霄蓉, 吕智慧

引用本文

徐鑫, 朱鸿斌, 谌杰, 李青汶, 张霄蓉, 吕智慧. [基于时序图神经网络的资产管理反洗钱检测方法](#)[J]. 计算机科学, 2025, 52(10): 60-69.

XU Xin, ZHU Hongbin, CHEN Jie, LI Qingwen, ZHANG Xiaorong, LYU Zhihui. [Anti-money Laundering Detection Method for Asset Management Based on Temporal Graph Neural Networks](#) [J]. Computer Science, 2025, 52(10): 60-69.

相似文章推荐 (请使用火狐或 IE 浏览器查看文章)

Similar articles recommended (Please use Firefox or IE to view the article)

[用于交通预测的时空传播图神经网络](#)

Spatial-Temporal Propagation Graph Neural Network for Traffic Prediction
计算机科学, 2025, 52(10): 90-97. <https://doi.org/10.11896/jsjcx.241000045>

[表格数据生成技术综述](#)

Survey of Tabular Data Generation Techniques
计算机科学, 2025, 52(10): 3-12. <https://doi.org/10.11896/jsjcx.250800044>

[基于动态超图与药物处方信息融合的时序健康事件预测](#)

DHMP: Dynamic Hypergraph-enhanced Medication-aware Model for Temporal Health Event Prediction
计算机科学, 2025, 52(9): 88-95. <https://doi.org/10.11896/jsjcx.250300012>

[基于药物子结构与蛋白质三维图信息的化合物-蛋白质相互作用预测](#)

Graph-based Compound-Protein Interaction Prediction with Drug Substructures and Protein 3D Information
计算机科学, 2025, 52(9): 71-79. <https://doi.org/10.11896/jsjcx.250100116>

[基于双重分类和重建的跨域图异常检测](#)

Cross-domain Graph Anomaly Detection Via Dual Classification and Reconstruction
计算机科学, 2025, 52(8): 374-384. <https://doi.org/10.11896/jsjcx.241000140>

基于时序图神经网络的资产管理反洗钱检测方法

徐鑫¹ 朱鸿斌² 谌杰² 李青汶³ 张霄蓉¹ 吕智慧²

1 上海立信会计金融学院计算机与人工智能学院 上海 201209

2 复旦大学计算与智能创新学院 上海 200433

3 上海财经大学信息管理与工程学院 上海 200433

(20180152@lixin.edu.cn)

摘要 资产管理行业因高频且灵活的资金操作方式,已成为洗钱活动的重要目标。然而,资产管理行业中交易结构的稀疏性、客户间隐性资金流转路径的复杂性,以及交易行为的非统一特征,使得传统显式关系的图建模方法难以有效应对这些挑战。针对上述问题,提出了一种基于时序图神经网络的资产管理反洗钱检测框架(AM-GAML)。该框架通过融合时序模型与图神经网络,构建时间-结构联合嵌入表示,并设计了基于隐式交互关系的图生成机制,能够充分挖掘交易记录中的弱关联特征并捕捉客户间复杂的交易行为模式。在真实交易数据集上的实验验证了 AM-GAML 在准确率、召回率、F1-score 和 AUPRC 等多个关键指标上显著优于多个先进方法,尤其在少数类识别和泛化能力方面表现突出。所提方法为资产管理行业的反洗钱检测提供了高效且可靠的解决方案,并为复杂金融场景下的风险防控研究提供了有力支持。

关键词: 资产管理;反洗钱;时序模型;图神经网络;交易行为分析

中图分类号 TP181;F832.39

Anti-money Laundering Detection Method for Asset Management Based on Temporal Graph Neural Networks

XU Xin¹, ZHU Hongbin², CHEN Jie², LI Qingwen³, ZHANG Xiaorong¹ and LYU Zhihui²

1 School of Computing and Artificial Intelligence, Shanghai Lixin University of Accounting and Finance, Shanghai 201209, China

2 College of Computer Science and Artificial Intelligence, Fudan University, Shanghai 200433, China

3 School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai 200433, China

Abstract The asset management industry, characterized by high-frequency and flexible financial operations, has become a primary target for money laundering activities. However, the sparsity of transaction structures, the complexity of implicit fund transfer paths between accounts, and the non-uniform characteristics of transaction behaviors pose significant challenges for traditional graph modeling methods based on explicit relationships. To address these issues, this paper proposes an Anti-money Laundering Detection Framework for Asset Management based on Temporal Graph Neural Networks(AM-GAML). By integrating temporal models with graph neural networks, the proposed framework constructs a joint temporal-structural embedding representation and designs a graph generation mechanism based on implicit interaction relationships. This enables the framework to effectively capture weakly correlated features in transaction records and uncover complex transaction behavior patterns between users. Experimental results on a real-world transaction dataset demonstrate that AM-GAML significantly outperforms several advanced approaches in terms of accuracy, recall, F1-score, and AUPRC. The framework excels particularly in minority class detection and generalization ability. The proposed method provides an efficient and reliable solution for anti-money laundering detection in the asset management industry and offers valuable support for risk prevention and control research in complex financial scenarios.

Keywords Asset management, Anti-money laundering, Temporal model, Graph neural network, Transaction behavior analysis

到稿日期:2025-08-04 返修日期:2025-09-13

基金项目:国家自然科学基金面上项目(61873309);国家重点研发计划(2023YFC3305304);上海科技创新行动计划(24692111100)

This work was supported by the National Natural Science Foundation of China(61873309), National Key Research and Development Program of China(2023YFC3305304) and Shanghai Science and Technology Innovation Action Plan(24692111100).

通信作者:张霄蓉(zhangxiaorongzj@163.com)

1 引言

资产管理行业是指专业机构或个人通过受托管理客户资金,构建并运作投资组合,以实现资本增值与风险控制。据中国银行业协会发布的《中国资产管理行业发展与创新研究报告》统计,截至2023年,全球资产规模达到118.7万亿美元¹⁾。资产管理高频且灵活的运作方式(如基金申赎、跨境投资等资金操作),为非法资金隐藏、转移与清洗提供了更多隐蔽性通道。例如,洗钱者可利用短期高频申赎行为掩盖非法资金流动轨迹,或利用场外衍生品交易延展资金链条,从而规避传统监管穿透。我国《资管新规》和《反洗钱法》明确要求,资产管理机构应当建立与其业务规模、复杂程度相适应的动态风险评估体系,并依法履行可疑交易报告义务。资产管理机构一旦卷入洗钱案件,不仅面临巨额罚款,还可能因声誉受损导致客户流失,严重影响其业务发展。与商业银行以客户间显性资金流为核心的反洗钱检测相比,资产管理领域的交易路径高度隐蔽,客户之间缺乏明确的资金往来关系。洗钱者更倾向于利用时序性操作、组合式产品、市场行为耦合等复杂手段实现资金清洗。因此,针对资产管理行业的洗钱行为,开发高效、准确的反洗钱(Anti-Money Laundering, AML)检测方法,不仅对于提升金融市场的监管效能至关重要,也在保障金融系统安全和维护投资者权益方面具有深远意义。

传统反洗钱方法主要依赖静态规则与浅层统计模型,通过预设规则(如交易金额阈值、交易频率限制)标记可疑交易,并结合人工审查验证^[1]。随着数字支付手段和复杂金融工具的广泛应用,交易数据呈现出大规模、高维度的特征,洗钱行为也日益隐蔽化、网络化。在此背景下,传统基于静态规则的方法难以及时适应不断演化的洗钱技术,也无法有效建模复杂交易网络中的异常行为模式^[2],由此产生的高误报率显著提升了机构的合规运营成本。为突破传统基于规则方法在适应性及准确性方面的局限性,近年来已有大量研究在银行^[3-7]、虚拟货币^[8-9]、区块链^[10]等多个场景的反洗钱领域中引入机器学习(Machine Learning, ML)与深度学习(Deep Learning, DL)技术,通过从历史数据中学习非线性模式来提升检测效果。该类模型部署简单,且能够在一定程度上提升检测精度^[3-4,11]。例如,Zhang等^[3]利用美国金融机构提供的实际交易数据,系统比较了5种机器学习算法和2种采样技术在洗钱识别上的性能表现。然而,上述方法普遍依赖高质量的标注数据,而在实际场景中,洗钱行为标签获取成本高,因此标注数据稀缺。为应对这一问题,研究者进一步引入了半监督与无监督学习方法以降低对标签的依赖^[6,9,12]。这类方法更适合处理高维、弱标注的数据。例如,Bakry等^[12]提出了凝聚层次聚类与多种降维技术(ICA, KPCA, SVD, LPP)相结合的方式,来降低反洗钱系统中高维数据的复杂性并提升聚类性能。实验结果表明,KPCA与凝聚层次聚类相结合时,在多种评估指标下均表现最佳。此外,Transformer架构也被应用于交易序列分析中,其对长程依赖关系的建模能力,进一

步增强了交易行为识别的效果^[13-14]。

随着洗钱行为日益呈现网络化、团伙化的发展趋势,交易数据中的图结构信息对揭示隐蔽的资金流动路径尤为关键。因此,近期研究考虑使用图神经网络(Graph Neural Network, GNN)方法开展AML的相关探索^[15-17]。图神经网络结合了图结构表达与深度学习能力,能够通过聚合客户邻域信息建模资金流动关系。Qin等^[5]提出的BTDF-GNN方法通过融合特征工程、不平衡样本处理、GraphSAGE和GAT模型集成等技术,在真实的银行交易数据上展示出优异的检测性能。Cheng等^[7]提出的群体感知图学习框架GAGNN,结合图注意力网络与社区中心编码器建模用户之间的拓扑与属性特征,动态聚合可疑账户形成洗钱团伙,实现了对有组织洗钱行为的有效识别。

本研究旨在使用时序图神经网络技术识别复杂的洗钱交易模式,实现更有效的资产管理领域反洗钱检测。尽管GNN在银行等传统金融场景中的AML检测任务中表现出显著优势,但其在资产管理行业中的应用仍面临多重挑战。一方面,不同客户的交易历史具有不定长、非统一的结构特征,如交易频率、周期、金额波动等存在巨大的个体差异。在构建基于客户节点的图表示时,如何衡量客户之间在不定长交易历史下的相似性,成为图建模过程中的关键难题。这一问题不仅影响图中边权的定义与边构建策略,也直接关系到模型对可疑客户之间“潜在共谋行为”的刻画能力。现有方法主要依赖简单的统计摘要或阈值规则处理,难以充分利用交易记录中隐含的微弱行为关联。另一方面,相较于银行等传统金融机构,资产管理行业的客户交易之间缺乏明确的资金流转路径,其洗钱行为通常是通过伪装正常交易或借助第三方账户构建间接链路,从而掩盖真实的资金流向。由于缺少显性转账关系,传统基于显著边结构构图的GNN方法在该场景下难以直接适用。这种结构稀疏、弱关联的图网络,在边定义、图连通性及信号传播等方面存在天然劣势。此外,已有图神经网络方法主要依赖银行交易数据开发,其图结构假设与行为模式在资产管理场景下存在显著偏差,直接迁移可能导致图结构扭曲、模型泛化能力下降,从而降低识别的有效性。

基于上述研究背景和挑战,本文针对资产管理行业,提出一种基于时序图神经网络的资产管理行业反洗钱检测框架(Asset Management-tailored Graph Neural Network for Anti-Money Laundering, AM-GAML)。该框架融合时序模型和图神经网络,在缺乏显性交易路径的背景下重建交易实体间的交互结构,有效捕捉更加复杂的洗钱行为模式,从而提高反洗钱检测表现。研究的具体贡献如下:

1)首次将GNN方法应用于资产管理行业的反洗钱检测任务中,针对资产管理场景中客户交易关系隐蔽、结构稀疏的特点,构建融合交易行为序列与图结构信息的实体级检测框架。通过引入统一的时间-结构联合嵌入表示,模型能够有效表征不同客户间复杂且异质的交易行为特征,为资产管理行业反洗钱实践提供了新的技术路径。

2)提出一种新颖的图生成机制,用于刻画客户交易之间

¹⁾ <https://www.china-cba.net/Index/show/catid/14/id/44301.html>

的潜在关联关系。该机制基于客户历史行为序列数据挖掘隐式交互关系,在缺乏显性交易路径的情况下构建高质量的实体关系图,从而提升图神经网络在弱连接图结构下的建模能力,显著增强了模型对洗钱客户的识别效果。

3)实验结果表明,所提出的方法在资产管理行业的真实交易环境中展现出优异的反洗钱检测性能,能够在保障识别结果精确性的同时兼顾覆盖率,在高风险客户识别中实现精度与召回的有效平衡,显著提升其在实际反洗钱场景中的筛查能力与应用潜力。

2 问题定义

定义 1(客户关联网络) 在资产管理反洗钱检测任务中,定义客户关联网络 $\mathcal{G}=(\mathcal{V}, \mathcal{E})$,描述客户间的潜在关联及个体特征。该网络由客户节点集合 \mathcal{V} 和客户间关联边集合 \mathcal{E} 构成。具体而言,节点集合 $\mathcal{V}=\{v_1, v_2, \dots, v_N\}$ 表示客户账户,每个节点 v_i 代表一个独立的客户 i ,其历史交易行为可表示为交易序列:

$$\mathbf{X}_i = \langle x_{i,1}, x_{i,2}, \dots, x_{i,T_i} \rangle \quad (1)$$

其中, $x_{i,t} \in \mathbb{R}^d$ 为客户 i 的第 t 条交易记录,包含多维交易行为特征; T_i 为客户 i 的交易序列长度。边集合 $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$,表示客户间潜在关联关系。由于资产管理行业缺乏明确的资金流转路径, \mathcal{E} 的构造并非基于真实转账关系,而是基于客户间的属性相似性或行为模式相似性在建模阶段构造。具体构造

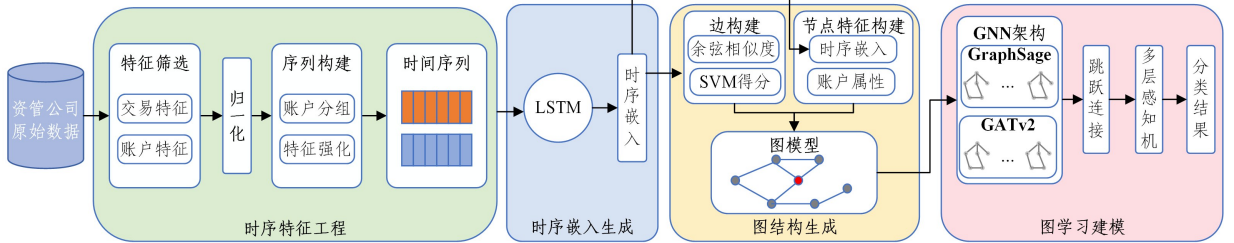


图 1 AM-GAML 流程图

Fig.1 Flowchart of AM-GAML

3.2 时序特征工程模块

为提升模型对洗钱行为的识别能力,本研究设计了系统化的时序特征工程模块,包括数据预处理、交易序列构建、特征增强等步骤,为后续图结构构建与模型训练奠定基础。

1)数据预处理:对于缺失值较少且缺失模式较为随机的特征,使用均值填充以减小噪声对模型训练的影响。为了避免特征量纲差异导致模型偏置,对连续型特征进行最小-最大缩放(Min-Max Normalization),将其线性映射至 $[0,1]$ 区间。对于类别变量,则采用 One-Hot 编码处理。

2)交易序列构建:在该阶段,依据客户编号对原始交易数据进行分组,提取每个客户 v_i 的时间序列交易记录 $\mathbf{X}_i = \langle x_{i,1}, x_{i,2}, \dots, x_{i,T_i} \rangle$ 。为保证输入数据维度一致,采用以下固定长度序列处理方式:

$$\tilde{\mathbf{X}}_i = \begin{cases} \langle x_{i,1}, \dots, x_{i,T_i}, \mathbf{0}_{d \times (L-T_i)} \rangle, & T_i < L \\ \langle x_{i,T_i-L+1}, \dots, x_{i,T_i} \rangle, & T_i \geq L \end{cases} \quad (2)$$

其中, L 为预设序列长度, $\mathbf{0}$ 表示零值填充向量。

3)特征增强:在数据清洗和交易序列构建的基础上,为刻

过程详见第 3.4 节。

定义 2(基于图的资产管理洗钱客户识别) 基于上述客户关联网络,本研究的目标是构建图神经网络模型,对每个客户 v_i 进行分类,预测其对应的二元类别标签 $y_i \in \{0,1\}$ 。其中, $y_i=1$ 表示该客户存在洗钱嫌疑; $y_i=0$ 表示客户不存在洗钱嫌疑。

本文涉及的主要符号及其含义如表 1 所列。

表 1 符号及含义

Table 1 Symbols and their meanings

符号	含义
$\mathcal{G}=(\mathcal{V}, \mathcal{E})$	客户关联网络
$\mathcal{V}=\{v_1, v_2, \dots, v_N\}$	客户节点集合,其中节点 v_i 表示第 i 个客户节点
$\mathbf{X}_i=\langle x_{i,1}, x_{i,2}, \dots, x_{i,T_i} \rangle$	客户 i 的交易行为序列,其中 $x_{i,t}$ 表示该客户第 t 条交易记录, T_i 表示该客户的交易序列长度
$y_i \in \{0,1\}$	客户 i 对应标签,1表示涉嫌洗钱,0表示交易正常
$\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$	图中的边集合,表示客户节点间的潜在行为关联

3 AM-GAML 模型设计

3.1 总体思路

针对资产管理行业反洗钱检测问题,本文提出了 AM-GAML 框架,其流程图如图 1 所示,可分为 4 个模块:时序特征工程模块、时序嵌入生成模块、图结构生成模块和图学习建模模块。该框架通过融合客户时序交易数据以及客户间的潜在交互关系,提升模型对可疑洗钱客户的检测能力。

画资产管理领域洗钱活动的典型行为模式,在时间维度、交易信息、发起方账户信息等多维特征基础上^[5,18],进一步引入了领域增强特征,包括五日累积交易额($f_{intensity}$)和闲置账户激活标识(f_{active})。

首先,五日累计交易额特征($f_{intensity}$)主要用于捕捉洗钱账户特有的资金流动时序模式。根据以往研究,洗钱账户通常采用“分散-集中”的资金转移策略^[19],即在短时间内将大额资金拆分为多笔交易,并在特定时间窗口内完成转移。基于这一行为特征,采用式(3)所示方式来计算 $f_{intensity}$:

$$f_{i,intensity} = \sum_{k=0}^4 a_{i,t-k} \quad (3)$$

其中, $a_{i,t}$ 表示客户 v_i 在第 t 条交易中的金额。该特征兼顾洗钱的短期特征和金融交易规律,既覆盖完整的交易周期,又在捕捉账户资金异常资金流动与保持特征稳定性之间取得平衡^[20]。

其次,构建闲置账户激活标识 f_{active} ,以识别长期处于闲置状态但近期交易突然激增的账户。在反洗钱检测中,客户“休眠-激活”行为模式具有重要的风险监测价值^[21]。现有研究

表明,洗钱者常利用交易记录稀少的休眠账户,这类账户由于缺乏足够的行为特征,在常规风险评估模型中往往被归类为低风险,而后通过突然激活并实施密集资金操作来完成非法资金转移^[20,22-23]。基于上述现象,式(4)给出 f_{active} 的计算方式:

$$f_{i,\text{active}} = \left(\frac{f_{i,\text{recent}} + \epsilon}{f_{i,\text{past}} + \epsilon} \right) \cdot I(f_{i,\text{past}} < \delta) \cdot I(f_{i,\text{recent}} > \theta) \quad (4)$$

其中, $f_{i,\text{recent}} = \frac{N_{i,\text{recent}}}{T_r}$ 表示客户 v_i 近期平均日交易频率; $f_{i,\text{past}} = \frac{N_{i,\text{past}}}{T_p}$ 表示历史平均日交易频率; ϵ 为固定小数; δ 为闲置判定阈值; θ 为激活阈值; $I(\cdot)$ 为指示函数,满足条件时为1,否则为0。

通过上述操作,该模块为每个客户生成交易序列特征 $\tilde{\mathbf{X}}_i$,该序列用于刻画与客户洗钱相关行为的特征,并被用作后续时序嵌入生成模块的输入。

3.3 时序嵌入生成模块

洗钱行为往往呈现出高度异步且复杂的动态特征,例如在短时间内出现的大额金额突变、非正常的交易频次波动,以及特定产品或渠道的偏好切换。这类模式难以通过静态或单一时点的特征全面刻画。为有效建模客户交易行为中的时间动态特征,本文采用长短期记忆网络(Long Short-Term Memory, LSTM)对每个客户节点 v_i 的交易序列 $\tilde{\mathbf{X}}_i$ 进行编码,提取反映客户行为演化的动态表征。

具体而言,时序嵌入生成模块接收经过时序特征工程处理后的交易序列 $\tilde{\mathbf{X}}_i$,通过LSTM对其进行编码,以生成定长的时序嵌入。在每个时间步 t ,LSTM更新隐藏状态 $\mathbf{h}_{i,t}$ 和单元状态 $\mathbf{c}_{i,t}$,其计算过程可表示为:

$$\mathbf{h}_{i,t}, \mathbf{c}_{i,t} = \text{LSTM}_\theta(\mathbf{x}_{i,t}, \mathbf{h}_{i,t-1}, \mathbf{c}_{i,t-1}), \mathbf{h}_{i,t}, \mathbf{c}_{i,t} \in \mathbb{R}^h, t = 1, \dots, L \quad (5)$$

其中, LSTM_θ 表示模型的参数化函数。经过 L 个时间步后,最终隐藏状态 $\mathbf{h}_{i,L}$ 被用作客户节点 v_i 的时序表征:

$$\mathbf{z}_i = \mathbf{h}_{i,L}, \mathbf{z}_i \in \mathbb{R}^h \quad (6)$$

时序表征 \mathbf{z}_i 捕捉了客户交易行为在时间维度上的动态特征,并作为后续图结构生成模块的输入,用于刻画客户行为相似性并构建潜在关联。

3.4 图结构生成模块

在资产管理场景中,客户之间缺乏直接的转账记录或显性资金流路径,传统依赖直接交易记录的图构建方法难以有效刻画节点间的联系。本模块旨在根据客户历史交易行为相似性来刻画其相互之间的关联,进而提升模型在反洗钱检测任务中的表现。具体而言,本文创新性地引入代理模型 $f_{\text{proxy}}(\cdot)$,通过基于行为模式的监督学习方式挖掘节点之间的潜在相似性,从而在无显性交易关系的情况下构建客户关联网络。

根据定义1,每个客户被映射为图中的节点 v_i ,其交易行为通过时序嵌入模块编码为时序表征 $\mathbf{z}_i \in \mathbb{R}^h$ 。代理模型 $f_{\text{proxy}}(\cdot)$ 以 \mathbf{z}_i 作为输入,在训练阶段仅使用训练集中的标注客户学习洗钱概率 \hat{y}_i 与 \mathbf{z}_i 之间的映射关系。训练完成后,代理模型在不使用测试集标签的前提下,直接输出每个节点的

洗钱概率 $p_i = f_{\text{proxy}}(\mathbf{z}_i) \in \mathbb{R}^C$,其中 C 表示类别总数。本研究为二分类任务,即 $C=2$,分别对应正常客户与洗钱嫌疑客户。代理模型的输出过程可形式化表示为:

$$f_{\text{proxy}}(\mathbf{z}_i) = \mathbf{p}_i, \mathbf{p}_i = [p_{i,1}, \dots, p_{i,C}], \sum_{c=1}^C p_{i,c} = 1 \quad (7)$$

其中,第 c 个分量 $p_{i,c}$ 表示节点 v_i 属于类别 c 的概率。通过代理模型 $f_{\text{proxy}}(\cdot)$,可以得到节点集合 \mathcal{V} 中所有节点的概率分布矩阵 $\mathbf{P} \in \mathbb{R}^{N \times C}$,其第 i 行即为节点 v_i 的概率分布 \mathbf{p}_i 。

基于节点的类别概率分布矩阵 \mathbf{P} ,本文模型可以在缺乏显性关联的情况下挖掘客户之间的洗钱倾向关联程度。具体地,通过计算节点之间的余弦相似度构建相似度矩阵 $\mathbf{S} \in \mathbb{R}^{N \times N}$ 。对于任意两个节点 v_i 和 v_j ,其相似度计算式为:

$$\text{Sim}(v_i, v_j) = \frac{\mathbf{p}_i \cdot \mathbf{p}_j}{\|\mathbf{p}_i\| \cdot \|\mathbf{p}_j\|}, \forall i, j \in \{1, 2, \dots, N\} \quad (8)$$

在此基础上,基于相似度矩阵 \mathbf{S} 构建无向同构图 $G = (\mathcal{V}, \mathcal{E})$ 。其中,节点集合定义为 $\mathcal{V} = \{v_1, v_2, \dots, v_N\}$, N 为节点总数。边集合 \mathcal{E} 的构造步骤如下:

1)对于节点 v_i ,在满足 $S_{ij} > \tau$ 的候选节点中选取相似度最高的前 K 个节点,构建边集合 $\mathcal{E}_1 = \{(v_i, v_j) \mid v_j \in \text{Top}K(\{v_k \mid S_{ik} > \tau\}, K), i \neq j\}$;

2)对于未满足阈值条件的节点 v_i ,选取相似度最高的节点 $v_j = \arg \max_{k \neq i} S_{ik}$,补充边集合 $\mathcal{E}_2 = \{(v_i, v_j) \mid S_{ij} = \max_{k \neq i} S_{ik}, S_{ik} \leq \tau\}$;

3)将上述两类边集合合并,得到完整的边集合 $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$ 。

最终,构建得到无向同构图 $G = (\mathcal{V}, \mathcal{E})$,其中节点集合 \mathcal{V} 表示所有交易主体,边集合 \mathcal{E} 刻画交易主体之间的潜在行为关联。节点特征由矩阵 $\mathbf{X} \in \mathbb{R}^{N \times F}$ 提供,其中 F 为节点特征维度,包括客户交易序列特征 $\tilde{\mathbf{X}}$ 及LSTM获得的动态行为表征 \mathbf{z}_i 。节点分类信息由标签向量 $\mathbf{y} \in \{0, 1\}^N$ 表示。图结构 G 与节点特征矩阵 \mathbf{X} 、标签向量 \mathbf{y} 一并用于后续的反洗钱检测任务。

3.5 图学习建模模块

在图学习建模阶段,本文设计了一种改进的GNN模型,通过结合多种先进机制,提升了图表示学习性能。该模块包括输入与特征变换、图卷积分层、特征融合与全局表示。

3.5.1 输入与特征变换

模型以节点特征矩阵 $\mathbf{X} \in \mathbb{R}^{N \times F}$ 作为输入。为了增强特征表达能力,首先通过一层线性变换将输入特征映射到更高维度的隐藏空间:

$$\mathbf{H}^{(0)} = \mathbf{X}\mathbf{W}_{\text{in}} + \mathbf{b}_{\text{in}} \quad (9)$$

其中, $\mathbf{W}_{\text{in}} \in \mathbb{R}^{F \times F_{\text{hid}}}$ 和 $\mathbf{b}_{\text{in}} \in \mathbb{R}^{F_{\text{hid}}}$ 为可学习参数, F_{hid} 为隐藏特征维度。

为应对图数据中节点数量不均、批量大小不固定等问题,每次特征变化后采用LayerNorm对隐藏特征 $\mathbf{H}^{(l)}$ 进行归一化处理^[24]:

$$\hat{\mathbf{h}}_i^{(l)} = \frac{h_i^{(l)} - \mu}{\sigma + \epsilon} \cdot \boldsymbol{\gamma} + \boldsymbol{\beta} \quad (10)$$

其中, $\mathbf{h}_i^{(l)} \in \mathbb{R}^{F_{\text{hid}}}$ 是节点 v_i 的隐藏特征; μ 和 σ 分别为特征维度上的均值和标准差; $\boldsymbol{\gamma}$ 和 $\boldsymbol{\beta}$ 为可学习的缩放和偏移参数; ϵ 为平滑项。

3.5.2 图卷积层

图卷积层是模型的核心部分,用于提取节点的局部和全局特征。本研究设计了4层图卷积操作,交替使用改进型图注意力网络(GATv2卷积)^[25]和GraphSAGE卷积^[26],以充分捕捉邻居节点的重要性和多层次结构信息。

1) GATv2 卷积

GATv2基于多头注意力机制,通过动态计算节点与其邻居之间的注意力权重,捕捉重要的邻居关系并更新节点特征。注意力权重计算式为:

$$a_{ij} = \text{softmax}(\sigma_{\text{LeakyReLU}}(\mathbf{a}^T [\mathbf{W}_q \mathbf{h}_i^{(l)} \parallel \mathbf{W}_k \mathbf{h}_j^{(l)}])) \quad (11)$$

其中, $\mathbf{h}_i^{(l)}$ 和 $\mathbf{h}_j^{(l)}$ 分别为第 l 层节点 v_i 和邻居 v_j 的隐藏特征, $\mathbf{W}_q, \mathbf{W}_k \in \mathbb{R}^{F_{\text{hid}} \times F_{\text{hid}}}$ 为线性变换矩阵, \mathbf{a} 为注意力向量, \parallel 表示拼接。

基于注意力权重,节点特征通过多头机制进行更新。具体而言,GATv2卷积采用 K 个注意力头并行计算邻居特征的加权聚合,并将结果拼接以增强表示能力。其更新式为:

$$\mathbf{h}_i^{(l+1)} = \parallel_{k=1}^K \sigma_{\text{ELU}} \left(\sum_{j \in N(i)} a_{ij}^{(k)} \mathbf{W}_v^{(k)} \mathbf{h}_j^{(l)} \right) \quad (12)$$

其中, $a_{ij}^{(k)}$ 和 $\mathbf{W}_v^{(k)}$ 分别为第 k 个注意力头的权重和值变换矩阵。

2) GraphSAGE

GraphSAGE采用均值聚合学习邻居节点的特征信息,其更新式为:

$$\mathbf{h}_i^{(l+1)} = \sigma_{\text{LeakyReLU}}(\mathbf{W}_{\text{sage}} \cdot \text{mean}(\{\mathbf{h}_i^{(l)}\} \cup \{\mathbf{h}_j^{(l)}, \forall j \in N(i)\})) \quad (13)$$

此外,为缓解深层网络中可能出现的梯度消失和特征退化问题,在图卷积层中引入残差连接机制^[27]。具体实现为,将每层图卷积的输出与上一层输入直接相加:

$$\mathbf{H}^{(l+1)} = \text{GNN}(\mathbf{H}^{(l)}) + \mathbf{H}^{(l)} \quad (14)$$

其中, $\mathbf{H}^{(l)}$ 是第 l 层的输入特征; $\text{GNN}(\mathbf{H}^{(l)})$ 表示当前层的图卷积操作。

在每一层卷积操作后,使用LayerNorm对特征进行归一化,以确保多层传播中的特征分布稳定性。为防止过拟合,每层卷积操作后加入Dropout,对部分输出特征进行随机丢弃。

3.5.3 特征融合与嵌入表示

在多层图卷积操作后,为整合多层次结构信息并生成高质量全局表示,引入跳跃连接(Jumping Knowledge, JK)机制^[28]。该机制通过逐元素最大化池化融合各层输出节点表示, $\mathbf{H}_{\text{JK}} = \text{max pool}(\mathbf{H}^{(1)}, \mathbf{H}^{(2)}, \dots, \mathbf{H}^{(L)})$, 在保留浅层局部特征的同时捕获深层全局信息,并有效缓解梯度消失与特征退化问题。

在此基础上,为突出任务相关的重要节点特征,进一步引入注意力机制。对于每个节点表示 \mathbf{h}_i , 其注意力权重计算为:

$$a_i = \frac{\exp(\mathbf{w}_{\text{att}}^T \cdot \tanh(\mathbf{W}_{\text{att}} \mathbf{h}_i + \mathbf{b}_{\text{att}}))}{\sum_{j=1}^N \exp(\mathbf{w}_{\text{att}}^T \cdot \tanh(\mathbf{W}_{\text{att}} \mathbf{h}_j + \mathbf{b}_{\text{att}}))} \quad (15)$$

通过注意力权重 a_i 调整每个节点的嵌入,得到最终节点表示 $\mathbf{h}_i' = a_i \cdot \mathbf{h}_i$ 。

对于节点分类任务,节点嵌入 \mathbf{h}_i' 输入至由3层全连接层和PReLU激活函数组成的多层感知机(Multilayer Perceptron, MLP),最终通过Softmax函数映射得到类别概率分布 $\hat{y}_{i,c}$, 其表示节点 v_i 属于类别 c 的预测概率。

训练过程中,采用交叉熵损失函数 $L = -\frac{1}{N} \sum_{i=1}^N \sum_{c=1}^C y_{i,c} \log(\hat{y}_{i,c})$, 最小化预测分布 $\hat{y}_{i,c}$ 与真实标签 $y_{i,c}$ 之间的差异,从而优化模型并实现节点分类。

4 实验结果与分析

4.1 实验数据集

本实验采用资产管理领域某基金销售公司提供的2024年1月至2025年3月脱敏交易数据,以支持资产管理场景下的AML检测任务。原始数据包括客户基本信息表、交易确认表、反洗钱个人信息表、反洗钱机构信息表及洗钱标识表。基于客户编号(CUST_ID)、基金账号(ACCO_ID)、交易账号(TRADE_ID)等关键字段,关联多表后构建统一视图,并通过属性筛选,删除冗余及缺失率较高的字段,最终保留与交易行为密切相关的特征用于建模。

在交易数据处理方面,原始交易确认表包含54072条交易记录,按客户维度重组为时间序列数据。为保留最长客户的完整交易行为,统一将交易序列长度设定 $L=1980$, 不足部分采用零向量填充以对齐维度。最终形成1956个客户的交易序列数据集,每条交易记录包含16个特征。关键特征如表2所列。

表2 特征列表

Table 2 Features list

变量	特征
时间维度	CONF_YEAR, CONF_MONTH, CONF_DAY
交易信息	CUST_TYPE, BUSI_CODE, FUND_CODE, CONF_AMTS
发起方账户信息	NET_CODE, COUNTY_PROV, COUNTY_CITY, COUNTY_DIST, TELL_PREFIX, GENDER, AGE, RISK_LEV
特征强化	5D_TOTAL, ACTIVE

根据企业针对洗钱行为的标注结果,数据集中洗钱嫌疑客户占17.2%(共337个),正常客户占82.8%(共1619个),反映出类别分布差异。此外,从客户类型分布来看,个人客户、机构客户及基金客户占比分别为63.1%, 26.8%和10.1%,体现了资产管理领域客户主体的多样性。整体来看,本数据集通过多源数据的整合与关键行为特征的提取,为后续基于时序图神经网络的反洗钱检测方法提供了可靠的数据支撑。

在模型训练阶段,将数据按照4:3:3的比例划分为训练集、验证集、测试集。为保证模型在不同客户类型下的泛化能力,划分过程中采用按客户类型的分层采样策略,以确保各数据子集中客户类型和类别标签均衡分布。数据集分布如表3所列。

表3 数据集划分

Table 3 Datasets split

变量	节点数	正例	负例	交易笔数
训练集 train	781	151	630	22767
验证集 val	586	93	493	14775
测试集 test	589	93	496	16530

4.2 实验设置

4.2.1 实验环境

本实验在配备4张NVIDIA GeForce RTX 4090显卡的

服务器上完成,服务器操作系统为 Ubuntu 20.04 LTS (64 位),具体软硬件环境配置如表 4 所列。

表 4 实验环境配置
Table 4 Experimental environment

项目	配置
服务器显卡	4 × NVIDIA GeForce RTX 4090
操作系统	Ubuntu 20.04 LTS(64 位)
CUDA 版本	CUDA Toolkit 12.0, cuDNN 8.9.2
Python 版本	Python 3.10

4.2.2 参数配置

表 5 详细介绍了模型的关键参数配置,包括交易序列数据的时序生成、代理模型的选用、同构图构建规则,以及 GNN 模型的结构设计。

表 5 参数配置
Table 5 Parameters configuration

模块	参数	值
时序嵌入生成 (LSTM)	优化器	Adam
	隐藏层维度	64
	训练轮数	100
	批处理大小	64
图结构生成	代理模型选择	SVM
	核函数	径向基核 (RBF)
	阈值 τ	0.7
	K	5
图学习建模	隐藏层维度	128
	图卷积层	4
	GATv2Conv 多头数量	4

4.3 评价指标

在资产管理场景下的反洗钱检测任务中,洗钱嫌疑客户占比较低,呈现类别分布不均衡的特点。为全面评估模型性能,除准确率 (Accuracy) 外,本文还重点关注模型在识别少数类 (即洗钱嫌疑客户) 方面的表现。为此,采用召回率 (Recall) 衡量模型对洗钱嫌疑客户的识别能力。在本研究中,召回率定义为模型正确识别出的洗钱嫌疑客户数量占所有真实洗钱嫌疑客户总数的比例。召回率得分越高,表明模型漏报越少,能够检测出更多真实存在的洗钱嫌疑客户。

同时,考虑到误报 (即模型将正常客户错误地判定为洗钱嫌疑客户) 会带来较高的运营成本,本文采用 F1-score 作为综合评价指标。该指标通过平衡精确率 Precision (预测为洗钱客户的客户中实际为洗钱客户的比例) 与召回率 Recall (真实洗钱客户中被正确识别的比例) 来评估模型在识别洗钱嫌疑客户的同时控制误报的整体性能。其计算式如下:

$$F1\text{-score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (16)$$

此外,为进一步评估模型在类别极度不均衡条件下对洗钱嫌疑客户的检测性能,本文采用 AUPRC (Area Under the Precision-Recall Curve) 作为关键指标。传统的 AUROC (Area Under the Receiver Operating Characteristic Curve) 衡量模型区分正负类的整体能力,其得分范围为 0.5~1.0 (1.0 表示完全区分,0.5 表示接近随机预测)。然而,在严重类别不均衡的情况下,AUROC 会被大量负类样本 (正常客户) 主导,从而高估模型对洗钱嫌疑客户的实际检出能力。相比之下,AUPRC 更加关注模型对洗钱嫌疑客户的识别表现。其

曲线在不同阈值下综合反映了精确率与召回率的平衡。AU-PRC 得分越高,说明模型能够在保持较低误报的同时发现更多洗钱嫌疑客户;而当其值接近洗钱客户比例时,则表明模型性能接近随机预测水平。

综上所述,本文使用 Accuracy, Recall, F1-score 和 AU-PRC 作为主要评价指标,从多个维度全面评估模型在反洗钱检测任务中的性能。

4.4 基准模型

为了全面评估所提出的 AM-GAML 框架在资产管理行业反洗钱检测任务中的有效性,本研究分别构建以下方法作为基准模型进行对比实验。其中,SVM,GBDT,XGBoost,LSTM 以时序特征工程提取的客户交易序列作为输入;GraphSAGE,GAT,HGT,R-GCN,MAGNN 使用原始交易数据构建客户-基金有向异构图,节点和边特征分别编码客户静态信息与交易行为,并在此基础上进行节点分类任务。

SVM^[29]:经典的二分类模型,适用于小样本、结构化特征的分类任务。

GBDT^[30]:梯度提升决策树模型,通过集成多个弱分类器提升整体性能,适用于非线性关系建模。

XGBoost^[31]:改进的梯度提升框架,优化了模型并行性与正则化能力,具有较强的泛化能力。

LSTM^[32]:长短期记忆网络,用于捕捉客户交易行为中的时间依赖性,仅考虑时间序列特征,无图结构信息。

GraphSAGE^[26]:基于邻居采样与特征聚合机制的图神经网络,实现对大规模图数据的高效表示学习。

GAT^[33]:图注意力网络,通过引入自注意力机制,动态调整邻居节点权重,捕捉邻接关系差异。

HGT^[34]:基于 Transformer 架构的异构图神经网络模型,引入节点类型与边类型的注意力机制,实现对图异构性的有效建模。

R-GCN^[35]:关系图卷积网络,基于关系类型的权重变换,建模多关系图的结构与语义特征。

MAGNN^[36]:基于元路径的异构图神经网络,通过节点内部与元路径级别的多重聚合机制,提升节点表征。

4.5 实验结果与分析

4.5.1 实验结果

表 6 列出了不同模型在反洗钱检测任务中的性能。

表 6 实验结果

Table 6 Experimental results

方法	Accuracy	Precision	Recall	F1-score	AUPRC
SVM	0.9219	0.8730	0.5914	0.7051	0.7529
GBDT	0.8506	0.5177	0.7849	0.6239	0.7768
XGBoost	0.8421	0.5000	0.8817	0.6381	0.8197
LSTM	0.9253	0.9093	0.7940	0.8374	0.7825
GraphSAGE	0.9542	0.7895	0.9146	0.8475	0.8749
GAT	0.9253	0.7639	0.6707	0.7143	0.7204
HGT	0.9161	0.7231	0.6512	0.6838	0.7008
R-GCN	0.9379	0.7222	0.9000	0.8013	0.8151
MAGNN	0.9273	0.8893	0.5464	0.6766	0.6710
AM-GAML	0.9610	0.9168	0.9419	0.9287	0.9351

可以看出,AM-GAML 模型在所有指标上均表现出色,特别是在 Recall (0.9419), F1-score (0.9287) 和 AUPRC (0.9351) 方面,显著领先于其他模型。机器学习模型中,

SVM的准确率较高(0.9219),但 Recall 偏低(0.5914),表明其对洗钱嫌疑客户的识别能力有限,存在较高的漏报风险;GBDT 和 XGBoost 虽然在 Recall 指标上表现较好,但 Precision 分别为 0.5177 和 0.5000,且 F1-score 和 AUPRC 指标均处于较低水平,表明模型在平衡识别洗钱嫌疑客户的准确性与全面性方面存在不足。

通过对比 LSTM 和 AM-GAML 模型的性能,可以进一步说明引入图结构在反洗钱检测任务中的重要性。一方面,图结构显著提升了模型的复杂建模能力。相较于 LSTM 模型,AM-GAML 的 Recall 从 0.7940 提升至 0.9419,增长了 18.63%,扩大了对洗钱嫌疑客户的覆盖范围;F1-score 提升了 10.90%,表明模型在精准率和召回率之间实现了更优的平衡。同时,AM-GAML 的 Accuracy 达到 0.9610,提升了 3.86%,进一步验证了其在全局分类性能上的优势。这些指标的提升表明,本文提出的框架能够更有效地捕捉复杂的交易模式,显著减少漏报,在资产管理行业反洗钱任务中具备更强的检测能力。另一方面,图结构增强了模型对不平衡数据的处理表现。AM-GAML 的 AUPRC 达到 0.9351,显著优于 LSTM 的 0.7825。AUPRC 的提升,反映了 AM-GAML 在不同概率阈值下均能保持高效的分类性能。在反洗钱场景中,洗钱嫌疑客户占比较低且交易行为复杂,单纯依赖交易序列的模型难以充分利用客户间的行为关系。通过引入图结构,AM-GAML 能够利用客户间的潜在行为关联,将交易网络中关键节点和交互模式的信息融入模型,使其即使在低置信度

样本中也能有效识别潜在洗钱嫌疑客户,显著提升洗钱客户的检出能力。

在图神经网络模型中,GraphSAGE 和 R-GCN 整体表现较为优异,准确率分别为 0.9542 和 0.9379,召回率也达到 0.9146 和 0.9000,但各项指标仍低于 AM-GAML。相比之下,GAT,HGT 和 MAGNN 在 Recall 和 AUPRC 上表现较差。它们通过基于客户与基金之间的实际交易关系构建“客户-基金”异构图,能较好地刻画客户与金融产品之间的显性交互路径。然而,在实际反洗钱检测场景中,这类方法难以揭示客户间的潜在行为关联。即便多个客户持有同一基金,也会因为购买时机、交易频率、金额分布等因素而存在较大差异,使得基于显性交易构建的边所反映的相关性较弱,难以真实体现客户间的潜在风险关联,从而限制了模型在资产管理场景下的洗钱检测能力。相较之下,AM-GAML 通过挖掘客户交易行为的相似性,构建更具辨识力的弱连接结构,从而显著提升了对洗钱嫌疑客户的检测能力。

图 2 展示了主要基准模型与 AM-GAML 在训练过程中的评估指标随训练轮次(Epoch)的变化曲线。从图中可以看出,AM-GAML 在训练初期(约第 10 至 20 轮)即在各项指标上取得较高性能,整体展现出更快的收敛趋势,优于 LSTM 与多种主流图神经网络模型。此外,AM-GAML 的各项指标在训练后期保持稳定,波动较小,这表明其在处理交易行为建模时,不仅训练效率高,而且具有较强的稳定性,能够更好地适应资产管理场景下动态复杂的交易网络。

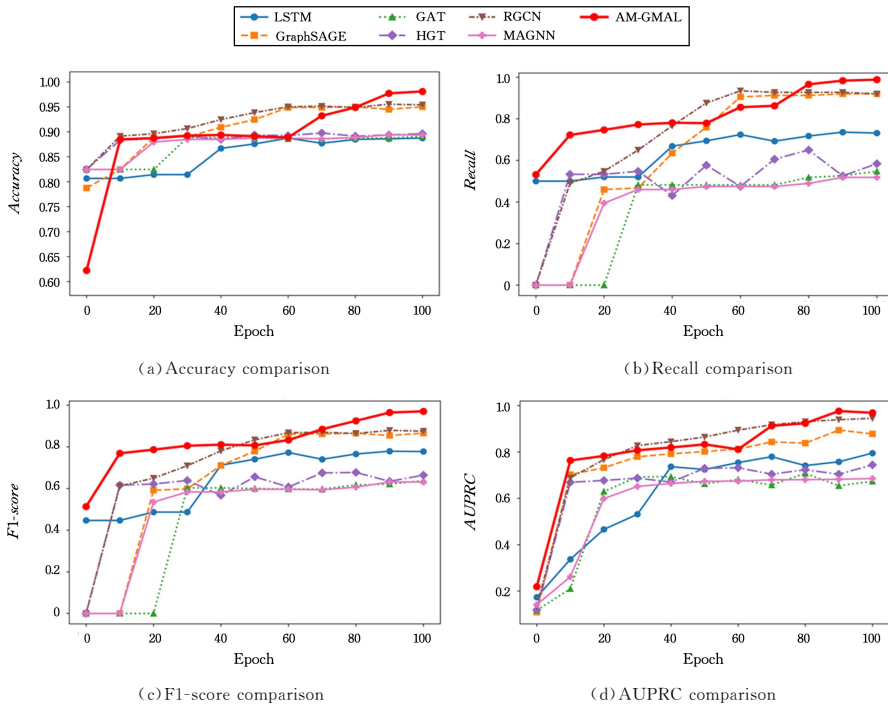


图 2 训练轮次中评估指标的变化趋势

Fig. 2 Trends of evaluation metrics across training epochs

图 3 展示了 AM-GAML 模型在训练集和验证集上的指标随训练轮次变化的情况,以评估其拟合能力和泛化能力。从图中可以观察到,模型在训练初期实现了快速收敛,所有评估指标均从初始值迅速提升至接近最终稳定值。这表明,AM-GAML 能够高效学习交易行为中的特征模式。此外,在

整个训练过程中,验证集的各项指标曲线与训练集保持一致,未出现显著的性能偏差,反映了模型具有良好的泛化性能。特别是在后期,各项指标曲线趋于平稳且波动幅度较小,未观察到过拟合现象,这进一步体现了 AM-GAML 在复杂数据场景下的稳健性。

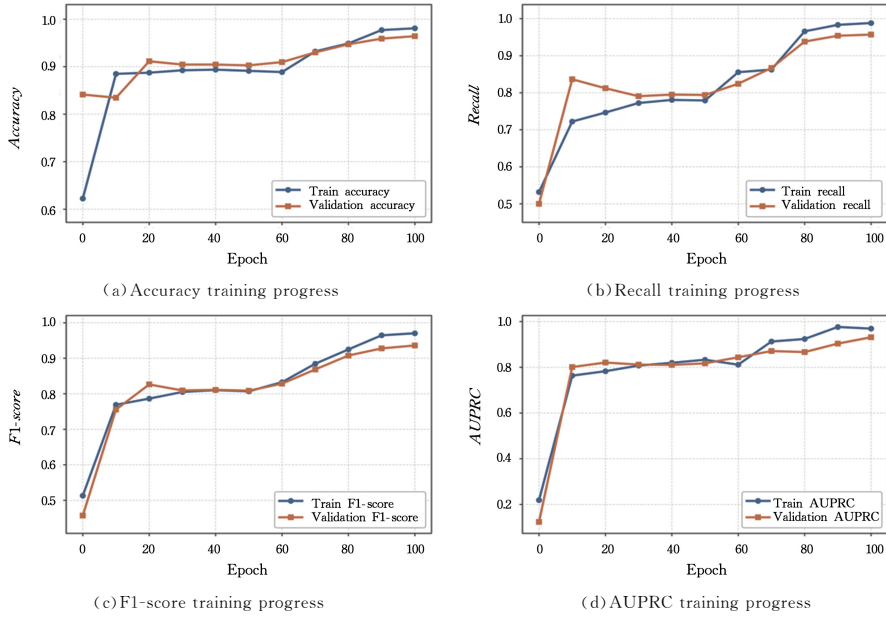


图3 AM-GAML 训练与验证评估指标的变化趋势

Fig. 3 Trends of evaluation metrics for AM-GAML training and validation

4.5.2 构图策略对比

为进一步验证图结构构建方式对模型性能的影响,设计了两组实验,并在保持其他模块不变的前提下,系统评估构图方式对最终分类效果的影响。首先,为验证 AM-GAML 框架中用于边构建的代理模型的稳健性,将原本基于 SVM 的代理模型替换为基于 XGBoost 的代理模型。其次,为验证基于客户洗钱倾向构建的交易网络相较于基于实际属性构建的网络在反洗钱检测中的优越性,选取客户的城市级属性 (COUNTY_CITY) 作为连边依据。将地理位置相同的客户节点相连,形成反映空间邻近关系的无向图,并将其作为另一种边构建策略。

如图 4 所示,采用 XGBoost 作为代理模型的构图方案在各项关键指标上均略优于基于 SVM 的代理模型,显示了其在捕捉复杂行为模式上的潜力。同时,两种代理模型均能有效支持图结构构建并提升最终识别性能,表明所提 AM-GAML 在代理模型选择上具有一定的鲁棒性。

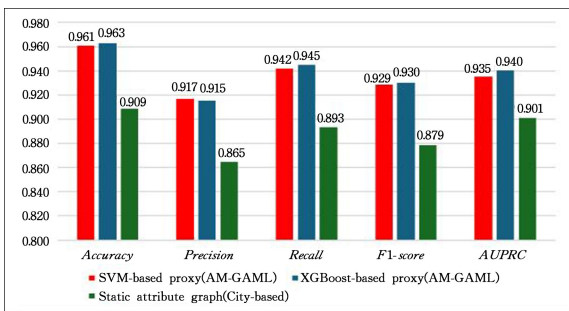


图4 不同图构建方式下模型的性能指标对比

Fig. 4 Performance comparison under different graph construction strategies

相比之下,基于城市属性构建的图结构虽表现差于代理模型构图,但整体仍优于大部分基线模型,表明静态属性信息在一定程度上反映了客户间的潜在关联。然而,此类基于静态信息的构图策略在实际反洗钱场景中存在局限性,主要体

现在客户静态属性维度较少且区分度有限,难以刻画潜在洗钱行为。相较之下,AM-GAML 在此基础上进一步提升了建图维度,将关注重点从低维静态特征扩展至高维动态行为特征,通过代理模型刻画客户在交易频率、金额变化、时序模式等方面的深层相似性,从而构建更加贴近真实风险关系的弱连接结构。上述结果验证了基于行为相似性学习的代理模型在刻画客户交互特征及提升反洗钱检测效果方面的优势。

4.5.3 参数敏感性分析

1) 邻居数 K 的敏感性分析

为进一步探索图结构生成模块中关键参数 K 对模型性能的影响,本研究保持其他模型设置不变,设置 $K = \{3, 4, 5, 6, 7, 8, 9, 10\}$ 并记录在不同参数设置下的具体性能对比。实验结果如表 7 和图 5 所示。

表7 不同 K 值下的模型性能对比Table 7 Model performance comparison under different K values

K 值	Acc	Precision	Recall	F1-score	AUPRC
3	0.9559	0.9060	0.9359	0.9200	0.9034
4	0.9609	0.9215	0.9346	0.9276	0.9435
5	0.9604	0.9216	0.9313	0.9263	0.9149
6	0.9593	0.9187	0.9306	0.9243	0.9200
7	0.9632	0.9183	0.9505	0.9334	0.9409
8	0.9674	0.9276	0.9553	0.9407	0.9460
9	0.9666	0.9241	0.9583	0.9398	0.9333
10	0.9643	0.9196	0.9541	0.9356	0.9287

从表 7 可以看出,当 $K=8$ 时,模型的各项检测指标均达到最佳表现,表明此时图结构能够有效刻画交易主体之间的潜在行为关联。当 K 值进一步增大时,模型性能呈现下降趋势,这可能是由于过大的邻居范围引入了无关的噪声边,导致图结构的表达能力受到影响。而当 K 值较小时,图结构过于稀疏,节点间的潜在联系不能充分挖掘,导致模型性能有所下降。

进一步与表 6 对比可以发现,无论 K 值的选择如何变化,AM-GAML 模型在不同参数设置下的绝大部分指标得分均优于基线模型。例如,即使在模型性能相对较低的 $K=3$ 和 $K=6$ 时,AM-GAML 的关键指标仍明显优于基线模型,显

示出其在资产管理行业反洗钱检测任务中的稳健性。

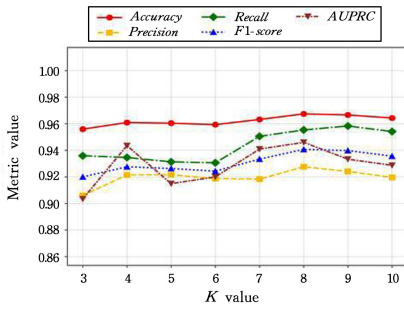


图5 参数 K 对 AM-GAML 性能的影响

Fig. 5 Impact of parameter K on AM-GAML performance

2) 序列长度 L 的敏感性分析

在时序特征工程模块中,交易序列的长度 L 决定了模型可利用的历史交易信息量。为系统评估序列长度 L 对 AM-GAML 性能的影响,本研究在保持其他参数不变的前提下,设置不同的序列长度进行实验。如图 6 所示,当采用较短序列长度(如 100 或 512)时,由于无法充分覆盖客户的完整交易行为,模型性能出现一定程度的下降,但仍优于基准模型。总体来看,尽管模型性能随序列长度变化略有波动,但 AM-GAML 框架在各参数设置下展现出良好的稳健性,保持了较为稳定且优越的识别效果。

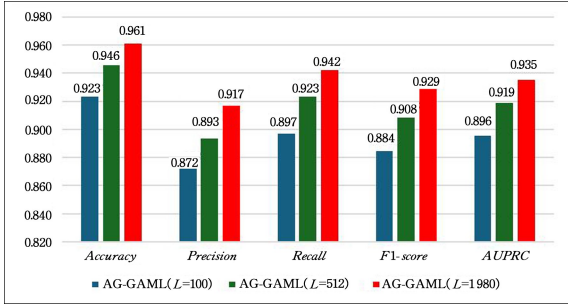


图6 参数 L 对 AM-GAML 性能的影响

Fig. 6 Impact of parameter L on AM-GAML performance

4.5.4 模型实时性分析

在资产管理行业中,反洗钱检测不仅需要识别复杂的可疑交易模式,还要高效处理大规模数据以满足周期性检测需求。为评估 AM-GAML 在反洗钱任务中的实时性表现,实验测量了不同参数 K 下的图构建时间、训练时间及单批预测延迟,结果如表 8 所列。

模型的运行效率可从 3 个方面进行分析。首先,生成一次完整交易网络图所需的时间约为 30 s,其中主要开销来自时序嵌入生成,后续图结构生成模块耗时较少,因此在不同 K 值下图构建时间基本保持一致。该结果表明,图构建过程整体耗时处于可接受范围,适合在周期性批量任务中执行。其次,在图学习建模阶段,模型在已构建的网络上进行参数训练。实验结果显示,训练时间在不同 K 值下稳定在 1.5~1.9 s 之间。由于该过程为离线操作,且耗时较短,因此不会影响周期性检测任务的效率。最后,在预测阶段,模型对单批数据的推理延迟约为 1.7 ms,呈现毫秒级响应能力,能够高效满足大规模交易网络的处理要求。

表 8 AM-GAML 在不同 K 值下的运行时间分析

Table 8 Runtime analysis of AM-GAML under different K values

K 值	边数	图构建时间/s	训练时间/s	单批预测延迟/ms
3	11 736		1.5674	1.7581
4	15 648		1.5784	1.7665
5	19 560		1.8465	1.7660
6	23 472	30.43	1.8524	1.7708
7	27 384		1.8565	1.7611
8	31 296		1.8604	1.7719
9	35 208		1.8637	1.7731
10	39 120		1.8689	1.7832

综上所述,本方法在周期性扫描任务中能够高效完成资产管理高频交易场景下的反洗钱检测。同时,实验结果显示,模型预测延迟随图规模变化较小,具备良好的可扩展性与实际应用前景。

结束语 资产管理行业的客户交易缺乏显性资金流路径,且行为差异显著,给反洗钱建模带来了独特挑战。针对资产管理场景,本文提出了一种基于时序图神经网络的反洗钱检测框架(AM-GAML)。总体而言,该框架融合时序模型与图神经网络,构建了统一的时间-结构联合嵌入表示,重建交易实体间的潜在交互关系,有效捕捉了复杂的洗钱行为模式。同时,设计了一种新颖的图生成机制,在缺乏显性交易路径的情况下,揭示客户之间的隐式关系,显著提升了模型对洗钱客户的检测能力。实验结果表明,AM-GAML 在真实交易环境下的各项检测指标均显著优于多个先进方法。此外,模型在训练效率和稳定性方面也表现出色,验证了其在资产管理行业反洗钱场景中的适用性。

未来研究将重点从以下几个方向深入:首先,在实时处理优化方面,将开发基于滑动窗口的增量式图更新算法,研究模型轻量化技术,并考虑延迟时间等关键性能指标;其次,在算法改进方面,将优化模型结构设计,探索时序注意力机制等方法来提升实时检测效率;此外,在应用扩展方面,将探索跨机构联合建模方案,以开展实际场景的验证,并应对更复杂的资金跨平台流动场景。这些改进将进一步提升框架的实时检测能力,更好地满足资产管理行业反洗钱的实际应用需求。

参考文献

- [1] CHEN Z, VAN KHOA L D, TEOH E N, et al. Machine learning techniques for anti-money laundering(AML) solutions in suspicious transaction detection: A review[J]. Knowledge and Information Systems, 2018, 57: 245-285.
- [2] NICHOLLS J, KUPPA A, LE-KHAC N A. Financial cyber-crime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape[J]. IEEE Access, 2021, 9: 163965-163986.
- [3] ZHANG Y, TRUBEY P. Machine learning and sampling scheme: An empirical study of money laundering detection[J]. Computational Economics, 2019, 54(3): 1043-1063.
- [4] JULLUM M, LØLAND A, HUSEBY R B, et al. Detecting money laundering transactions with machine learning[J]. Journal of Money Laundering Control, 2020, 23(1): 173-186.
- [5] QIN Z P, ZHOU Y T, LI Z. Bank transaction fraud detection method based on graph neural network[J]. Computer Science, 2024, 51(S2): 921-928.
- [6] LIU X, WANG X G. Probabilistic graphical model based ap-

- proach for bank telecommunication fraud detection[J]. *Computer Science*, 2018, 45(7): 122-128, 134.
- [7] CHENG D, YE Y, XIANG S, et al. Anti-money laundering by group-aware deep graph learning [J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023, 35(12): 12444-12457.
- [8] LIANG Y, WU W, LIANG R, et al. A plug-and-play data-driven approach for anti-money laundering in bitcoin[J]. *Expert Systems with Applications*, 2025, 266: 126072.
- [9] LORENZ J, SILVA M I, APARÍCIO D, et al. Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity [C] // *Proceedings of the First ACM International Conference on AI in Finance*. 2020: 1-8.
- [10] LIU L, LI X, LAN T, et al. A survey on anti-money laundering techniques in blockchain systems[J]. *Strategic Study of Chinese Academy of Engineering*, 2025, 27(2): 287-303.
- [11] LIU K Y, YU T T. An improved support-vector network model for anti-money laundering[C]//2011 Fifth International Conference on Management of E-Commerce and E-Government. IEEE, 2011: 193-196.
- [12] BAKRY A N, ALSHARKAWY A S, FARAG M S, et al. Combating financial crimes with unsupervised learning techniques: Clustering and dimensionality reduction for anti-Money Laundering[J]. *arXiv:2403.00777*, 2024.
- [13] TATULLI M P, PALADINI T, D'ONGHIA M, et al. HAMILLET: A transformer based approach for money laundering detection[C]//International Symposium on Cyber Security, Cryptology, and Machine Learning. Springer, 2023: 234-250.
- [14] JENSEN R I T, IOSIFIDIS A. Qualifying and raising anti-money laundering alarms with deep learning[J]. *Expert Systems with Applications*, 2023, 214: 119037.
- [15] CARDOSO M, SALEIRO P, BIZARRO P. Laundrograph: Self-supervised graph representation learning for anti-money laundering[C]//Proceedings of the Third ACM International Conference on AI in Finance. 2022: 130-138.
- [16] EDDIN A N, BONO J, APARÍCIO D, et al. Anti-money laundering alert optimization using machine learning with graphs[J]. *arXiv:2112.07508*, 2021.
- [17] LI X, CHEN L. Graph anomaly detection with domain-Agnostic pre-training and few-shot adaptation[C]//2024 IEEE 40th International Conference on Data Engineering (ICDE). IEEE, 2024: 2667-2680.
- [18] WEBER M, DOMENICONI G, CHEN J, et al. Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics[J]. *arXiv:1908.02591*, 2019.
- [19] SCHOTT P A. Reference guide to anti-money laundering and combating the financing of terrorism [M]. Washington, DC: World Bank Publications, 2006.
- [20] FORCE F A T. Risk-based approach guidance for the banking sector[R/OL]. Paris: FATF, 2014: 48. [https:// www. fatf-gafi. org/](https://www.fatf-gafi.org/).
- [21] VAN DUYN P C, SOUDIJN M R. Crime-money in the financial system-What we fear and what we know[M] // *Transnational Criminology Manual: Volume 2*. Nijmegen: Wolf Legal Publishers, 2010.
- [22] HEIDARINIA N, HAROUNABADI A, SADEGHZADEH M. An intelligent anti-money laundering method for detecting risky users in the banking systems[J]. *International Journal of Computer Applications*, 2014, 97(22): 35-39.
- [23] EL-BANNA M M, KHAFAGY M H, EL KADI H M. Smurf detector: a detection technique of criminal entities involved in money laundering[C]//2020 International Conference on Innovative Trends in Communication and Computer Engineering(IT-CE). 2020: 64-71.
- [24] CAI T, LUO S, XU K, et al. Graphnorm: A principled approach to accelerating graph neural network training[C]//International Conference on Machine Learning. 2021: 1204-1215.
- [25] BRODY S, ALON U, YAHAV E. How attentive are graph attention networks? [J]. *arXiv:2105.14491*, 2021.
- [26] HAMILTON W, YING Z, LESKOVEC J. Inductive representation learning on large graphs[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017: 1025-1035.
- [27] HE K, ZHANG X, REN S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2016: 770-778.
- [28] XU K, LI C, TIAN Y, et al. Representation learning on graphs with jumping knowledge networks[C]//International Conference on Machine Learning. 2018: 5453-5462.
- [29] CORTES C, VAPNIK V. Support-vector networks[J]. *Machine Learning*, 1995, 20: 273-297.
- [30] FRIEDMAN J H. Greedy function approximation: a gradient boosting machine[J]. *Annals of Statistics*, 2001, 29(5): 1189-1232.
- [31] CHEN T, GUESTRIN C. Xgboost: A scalable tree boosting system[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016: 785-794.
- [32] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. *Neural Computation*, 1997, 9(8): 1735-1780.
- [33] VELICKOVIC P, CUCURULL G, CASANOVA A, et al. Graph attention networks[J]. *Stat*, 2017, 1050(20): 10-48550.
- [34] HU Z, DONG Y, WANG K, et al. Heterogeneous graph transformer[C]//Proceedings of the Web Conference. 2020: 2704-2710.
- [35] SCHLICHTKRULL M, KIPF T N, BLOEM P, et al. Modeling relational data with graph convolutional networks[C]//European Semantic Web Conference. 2018: 593-607.
- [36] FU X, ZHANG J, MENG Z, et al. Magnn: Metapath aggregated graph neural network for heterogeneous graph embedding[C]//Proceedings of the Web Conference. 2020: 2331-2341.



XU Xin, born in 1983, Ph.D, associate professor, is a member of CCF (No. J2031M). His main research interest is financial data analysis.



ZHANG Xiaorong, born in 1994, Ph.D, assistant professor. Her main research interest is data mining.