基于图神经网络的电商欺诈检测

汇报人：彭浩
penghao@buaa.edu.cn

https://penghao-bdsc.github.io/

网络空间安全学院
School of Cyber Science and Technology
大数据科学与脑机智能高精尖中心
Beijing Advanced Innovation Center for Big Data and Brain Computing

彭浩，北京航空航天大学，网络空间安全学院、北京市大数据科学与脑机智能高精尖创新中心，讲师，博士生导师。近五年发表IEEE TKDE、TPDS、TNNLS、TII、ACM TOIS、TKDD、WWW、SIGIR、AAAI、IJCAI等论文60余篇，主持国家自然科学基金、国家重点研发子课题等项目9项。

主要研究方向：网络数据挖掘、深度学习、强化学习；

科研获奖：ESI高被引论文2篇（TKDE2019、TITS2019），学术会议最具影响力论文3篇（WWW2018、CIKM2019、CIKM2020），学术会议最佳论文提名奖2篇（ICDM2021、KBCOM2018），2018年中国电子学会技术发明一等奖、2020年中国人工智能学会优秀博士学位论文奖。


中国电子学会科学技术奖

获奖证书

为表彰中国电子学会科学技术奖获得者，特颁发此证书。

项目名称：网络空间大数据的行为融合分析方法与技术

奖　种：技术发明

奖励等级：一等奖

获 奖 人：彭 浩

证 书 号：KJ2018-F1-07-R06

二〇一八年十一月


证书 编号：B66-P202005

2020年度中国人工智能学会优秀博士学位论文

证 书

彭 浩

经中国人工智能学会优秀博士学位论文评审委员会评审，您的论文《社交网络数据表示学习与事件挖掘技术研究》被授予中国人工智能学会优秀博士学位论文奖。

特颁此证。

中国人工智能学会

二〇二〇年十一月十四日

Misbehaviors on the Web

- **Fraud:**
  - a misrepresentation of a fact, made from one person to another, with knowledge of its falsity and for the purpose of inducing the other to act.

Social Network

- Fake Reviews
- Social Bots
- Misinformation
- Disinformation
- Fake Accounts
- Social Sybils
- Link Advertising

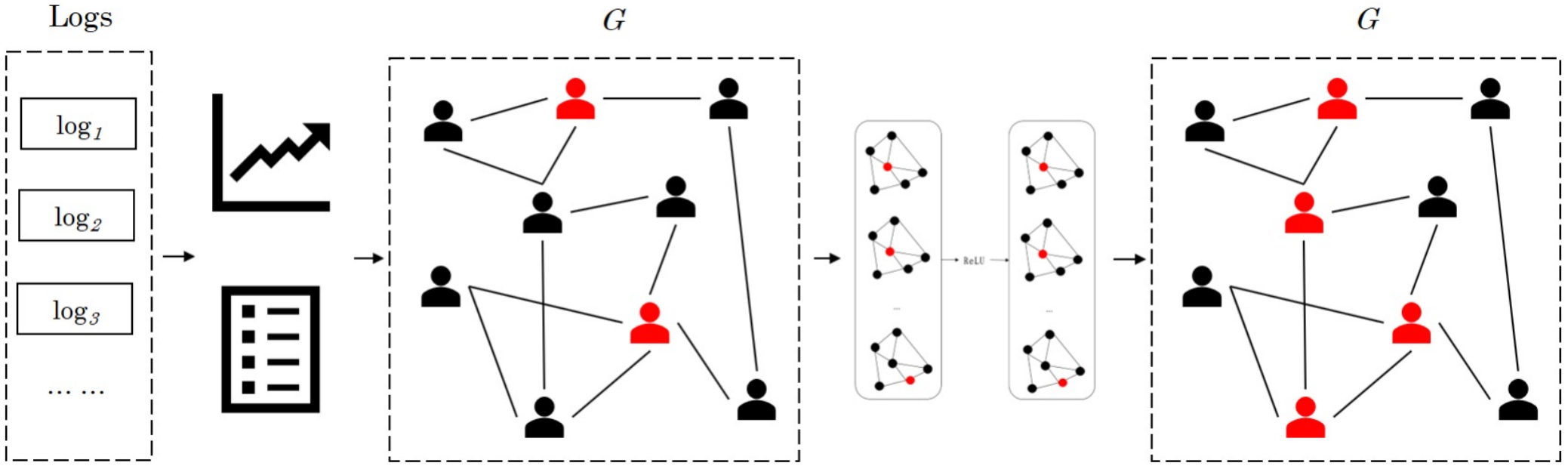
Finance

- Insurance Fraud
- Loan Defaulter
- Money Laundering
- Malicious Account
- Transaction Fraud
- Cash-out User
- Bitcoin Fraud

Others

- Advertisement
- Mobile Apps
- Ecommerce
- Crowdturfing
- Fake Clicks
- Game
- Account Takeover

GNN-based Fraud Detection

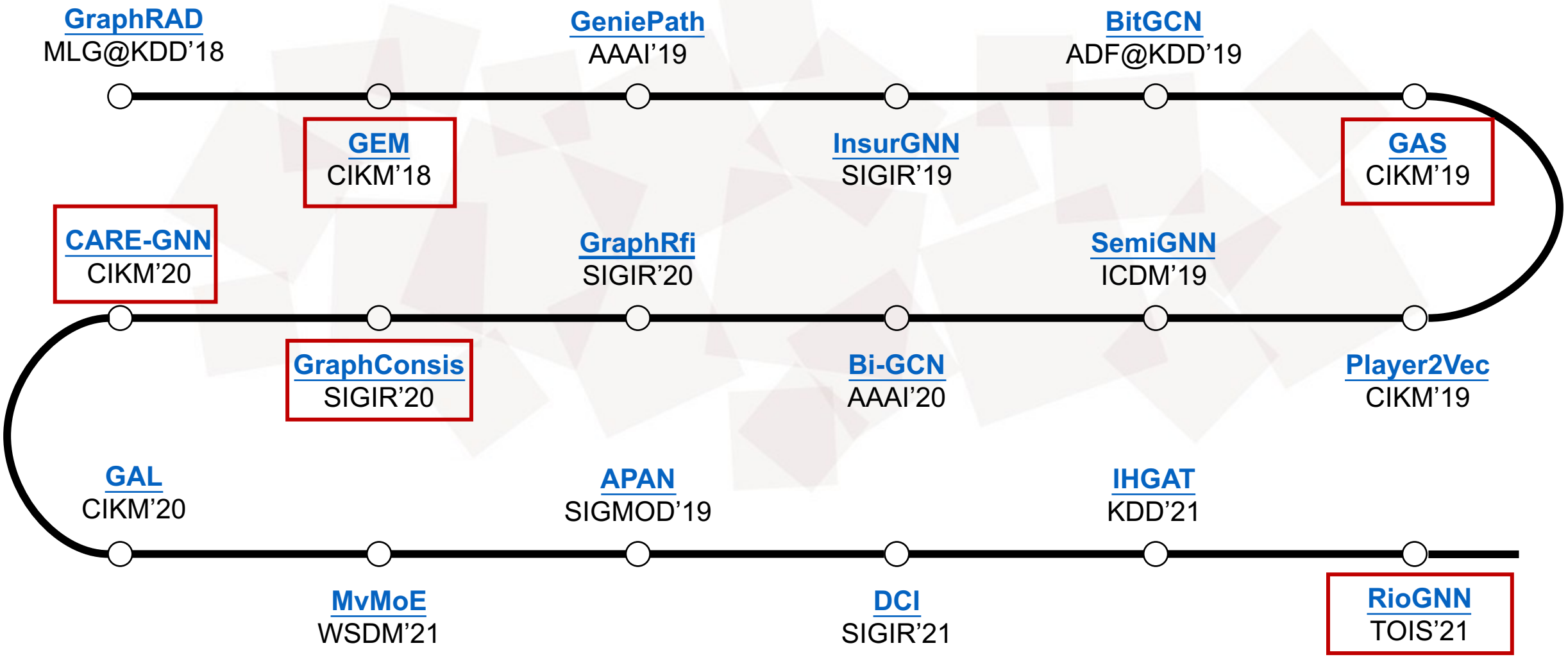


(1) Graph Construction. (2) Training GNN on the Graph. (3) Classifying Unlabeled Nodes.

Key idea: the connected nodes are similar (homophily assumption)

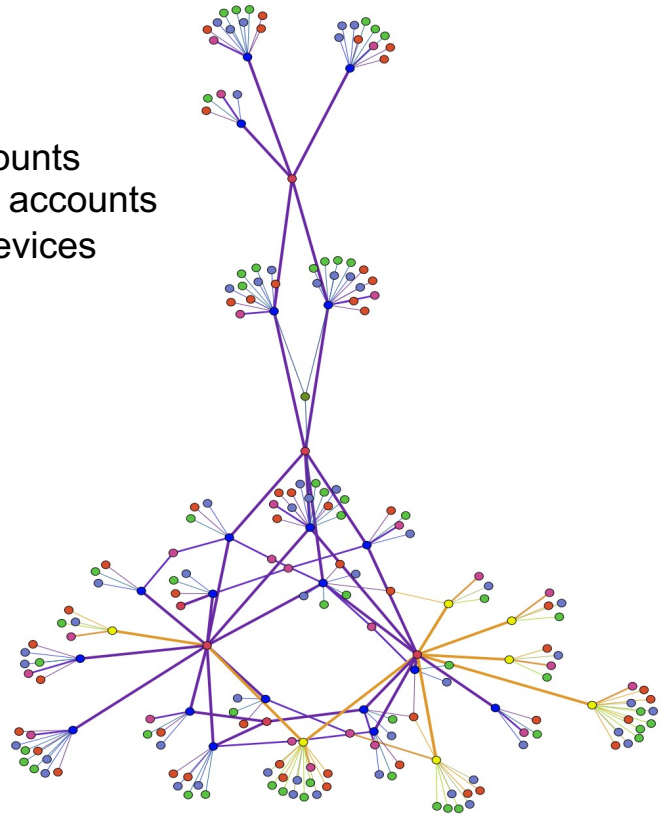
Image from Jianyu Wang et. al. 2019. FdGars: Fraudster Detection via Graph Convolutional Networks in Online App Review System. WWW 2019.

A History of GNN Fraud Detection (80+Papers)



GEM (CIKM'18)

Blue: normal accounts
Yellow: malicious accounts
Other: different devices

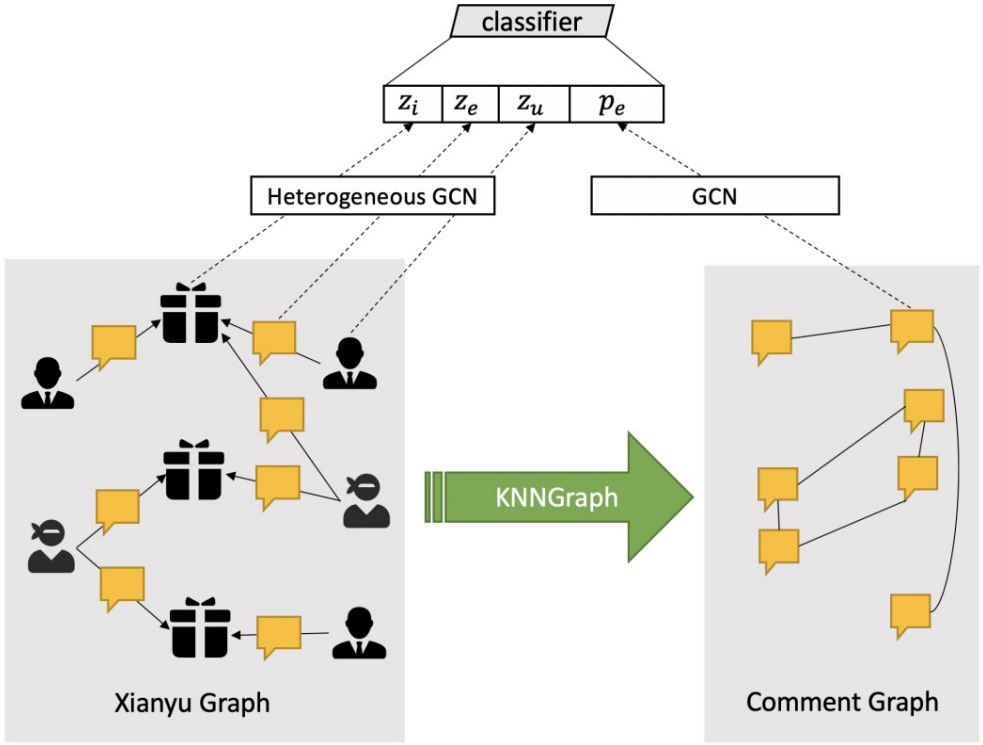


Account-Device Heterogeneous Graph

- Task: malicious accounts detection in Alipay.
- **The first paper leveraging the heterogeneous graph for fraud detection.**
- Device types include UMID, MAC address, IMSI, APDID (Alipay Fingerprint).
- Using attention mechanism to learn importance of different sub-graphs.
- Insight: Device Aggregation, Activity Aggregation

Ziqi Liu, et. al. 2018. Heterogenous graph Neural Network for Malicious Account Detection. CIKM 2018.

GAS (CIKM'19)



User-Comment-Product Graph
+
Comment-Comment Graph

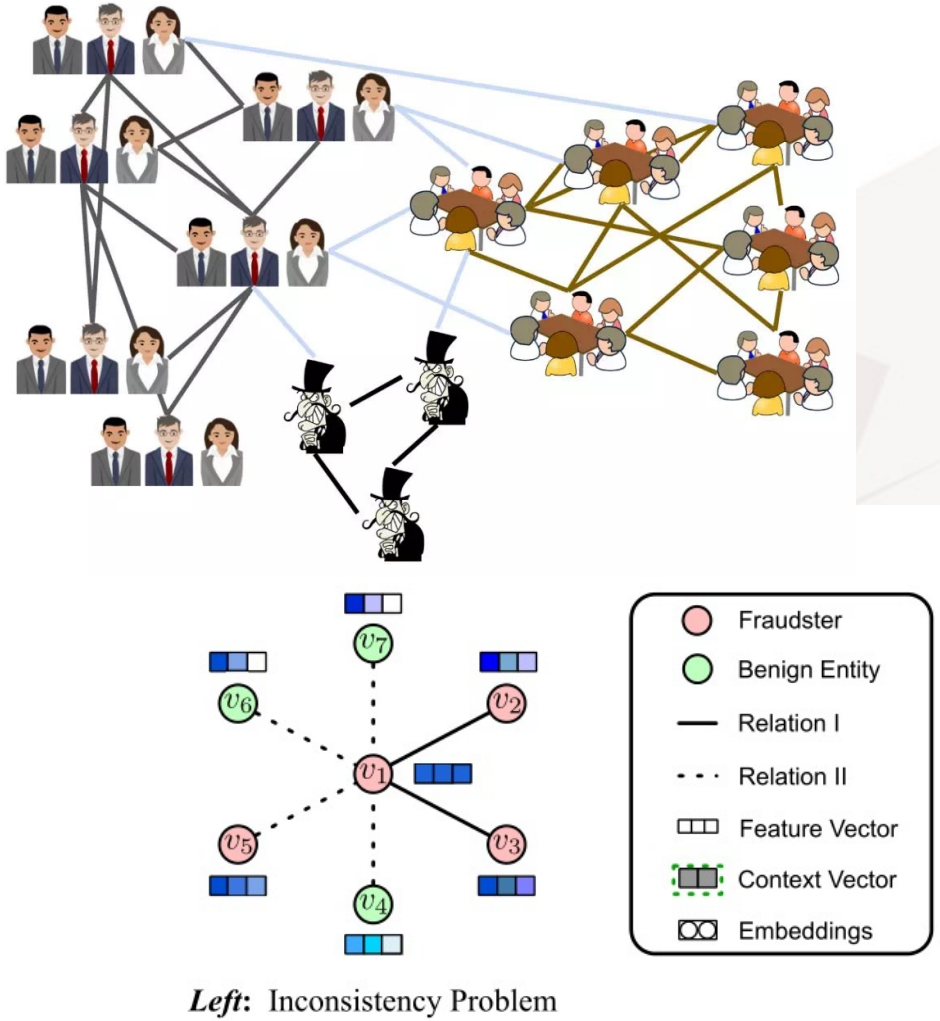
- Task: spam review detection on the Xianyu Platform.
- CIKM'19 Industrial Track Best Paper.
- **Novel graph construction approach. Encoding each heterogeneous entity separately.**
- Verifying a sampling approach for graph construction.

Ao Li, et. al. 2019. Spam Review Detection with Graph Convlutional Networks. CIKM 2019.

CONTENTS

- Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. Zhiwei Liu, Yingtong Dou, Philip S. Yu, Yutong Deng, Hao Peng. ACM SIGIR 2020.
- Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. Yingtong Dou, Zhiwei Liu, Li Sun, Yutong Deng, Hao Peng, Philip S. Yu. ACM CIKM 2020.
- Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. Hao Peng, Ruitong Zhang, Yingtong Dou, Renyu Yang, Jingyi Zhang, Philip S. Yu. ACM TOIS 2021.

研究背景01：图神经网络在欺诈检测领域的应用



***Left*: Inconsistency Problem**

欺诈节点特征

- 上下文不一致 → 连接良性实体
- 功能不一致 → 同一用户 连接不同评论
- 关系不一致 → 多种类型关系

Zhiwei Liu, et. al. 2020. Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. SIGIR 2020.

研究背景02：欺诈者伪装

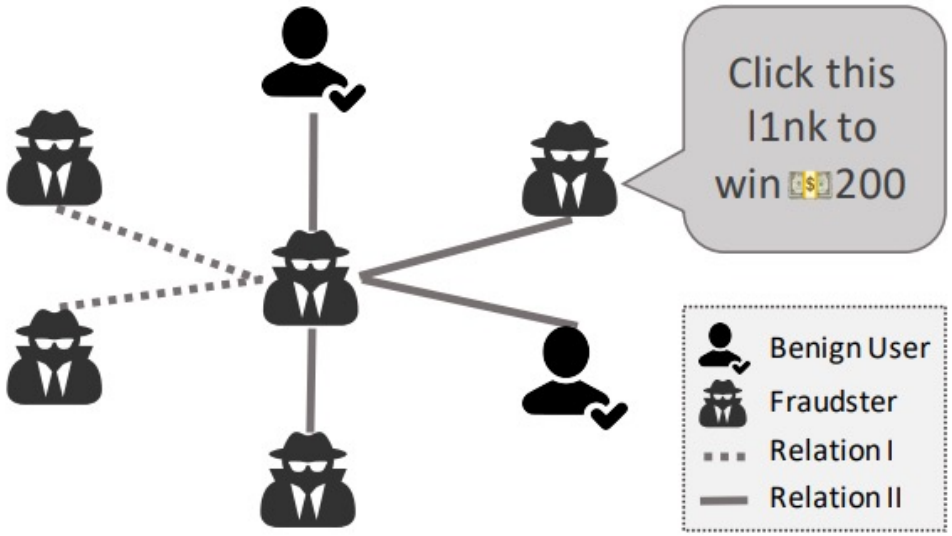


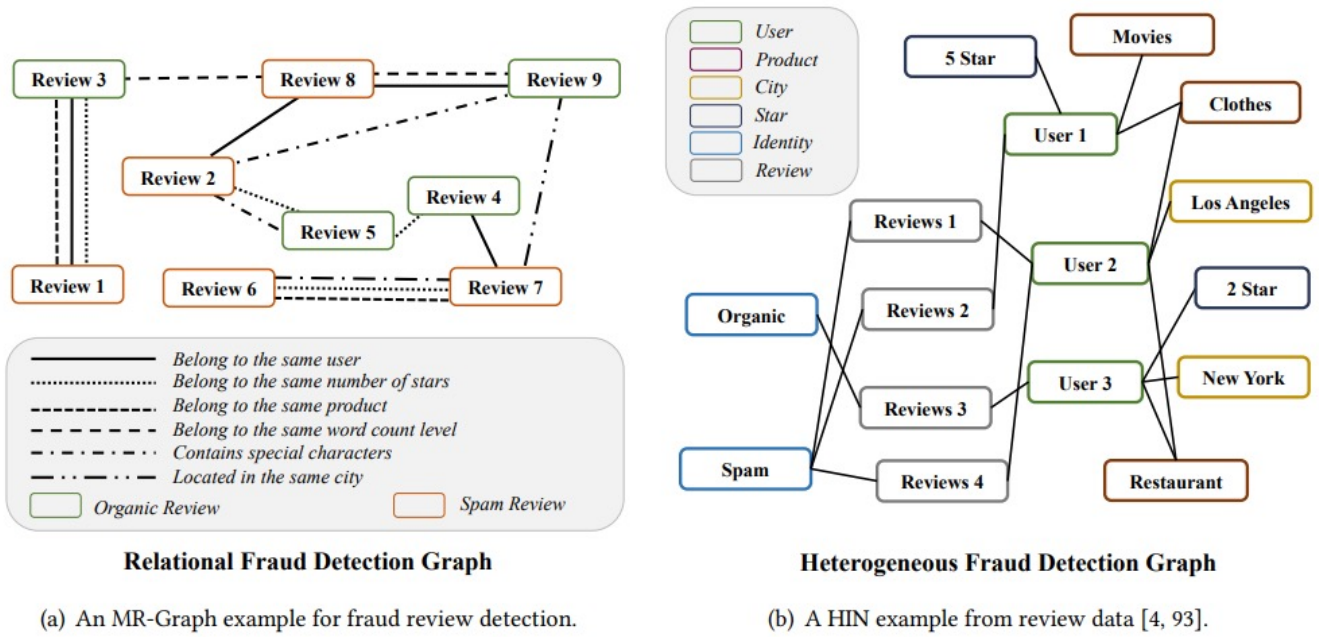
Figure 1: Two types of fraudster camouflage. (1) Feature camouflage: fraudsters add special characters to the text and make it delusive for feature-based spam detectors. (2) Relation camouflage: center fraudster connects to many benign entities under Relation II to attenuate its suspiciousness.

欺诈节点伪装

- 特征伪装：添加特殊字符
- 关系伪装：连接良性实体

Yingtong Dou, et. al. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. CIKM 2020.

研究背景03：垃圾邮件审查检测



Relational Fraud Detection Graph

(a) An MR-Graph example for fraud review detection.

Heterogeneous Fraud Detection Graph

(b) A HIN example from review data [4, 93].

Fig. 1. Graph Modeling in Fraud Review Detection.

垃圾评论检测痛点

- 行为伪装
  - 添加特殊字符
  - 模拟良性行为
- 无效评论
  - 同一用户不同产品的评论
- 复杂关系
  - 多种行为映射关系
- 计算效率
  - 快计算

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

2.研究思路

1 缓解图神经网络应用于欺诈检测不一致性问题

2 强化的图神经网络欺诈检测器对抗伪装欺诈者

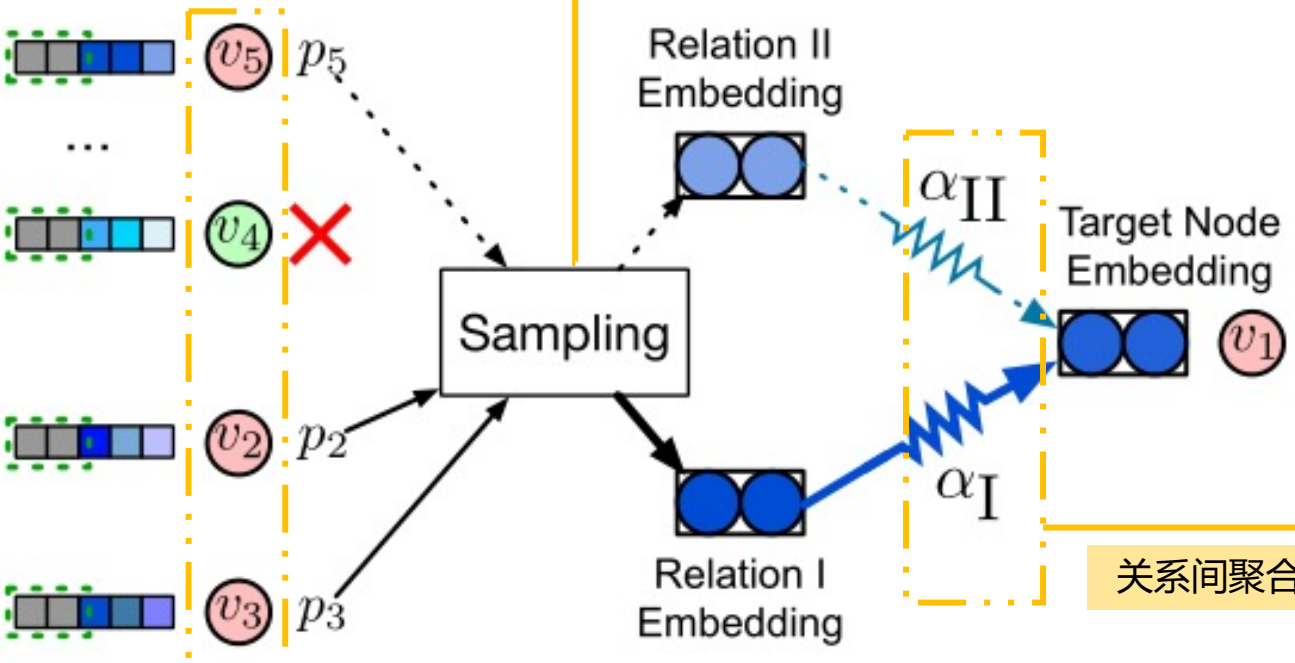
3 强化的邻域选择稳定聚合的多关系图神经网络

研究工作1.GraphConsis框架

非等概率邻居采样

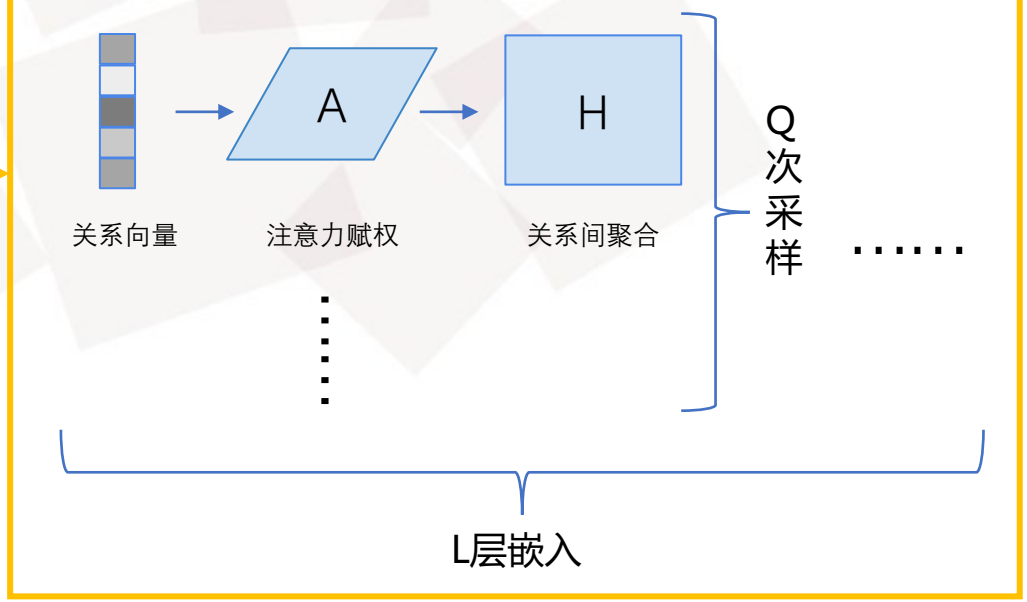
相似性得分 $s^{(l)}(u,v) = \exp\left(-\left\|\mathbf{h}_u^{(l)} - \mathbf{h}_v^{(l)}\right\|_2^2\right)$

过滤阈值 $p^{(l)}(u;v) = s^{(l)}(u,v) / \sum_{u \in \tilde{\mathcal{N}}_v} s^{(l)}(u,v)$

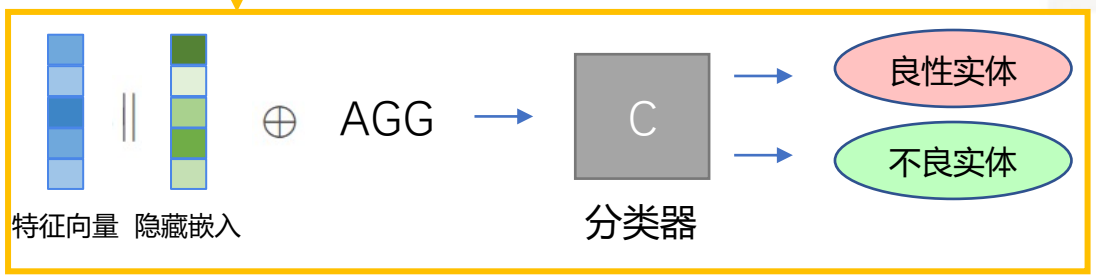


***Right*: Proposed GraphConsis Model**

关系间聚合



过滤不良实体



Zhiwei Liu, et. al. 2020. Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. SIGIR 2020.

实验结果

针对邻居采样的对照

更高密度更接近实际的异构图

更复杂的图构建方式

Table 1: The statistics of different graphs.

	Graph	#Nodes	#Edges	$\gamma^{(f)}$	$\gamma^{(c)}$
Others	Cora	2,708	5,278	0.72	0.81
	PPI	14,755	225,270	0.48	0.98
	Reddit	232,965	11,606,919	0.70	0.63
Ours	*R-U-R*	45,954	98,630	0.83	0.90
	R-T-R	45,954	1,147,232	0.79	0.05
	R-S-R	45,954	6,805,486	0.77	0.05
	Yelp-ALL	45,954	7,693,958	0.77	0.07

Table 2: Experiment results under different training %.

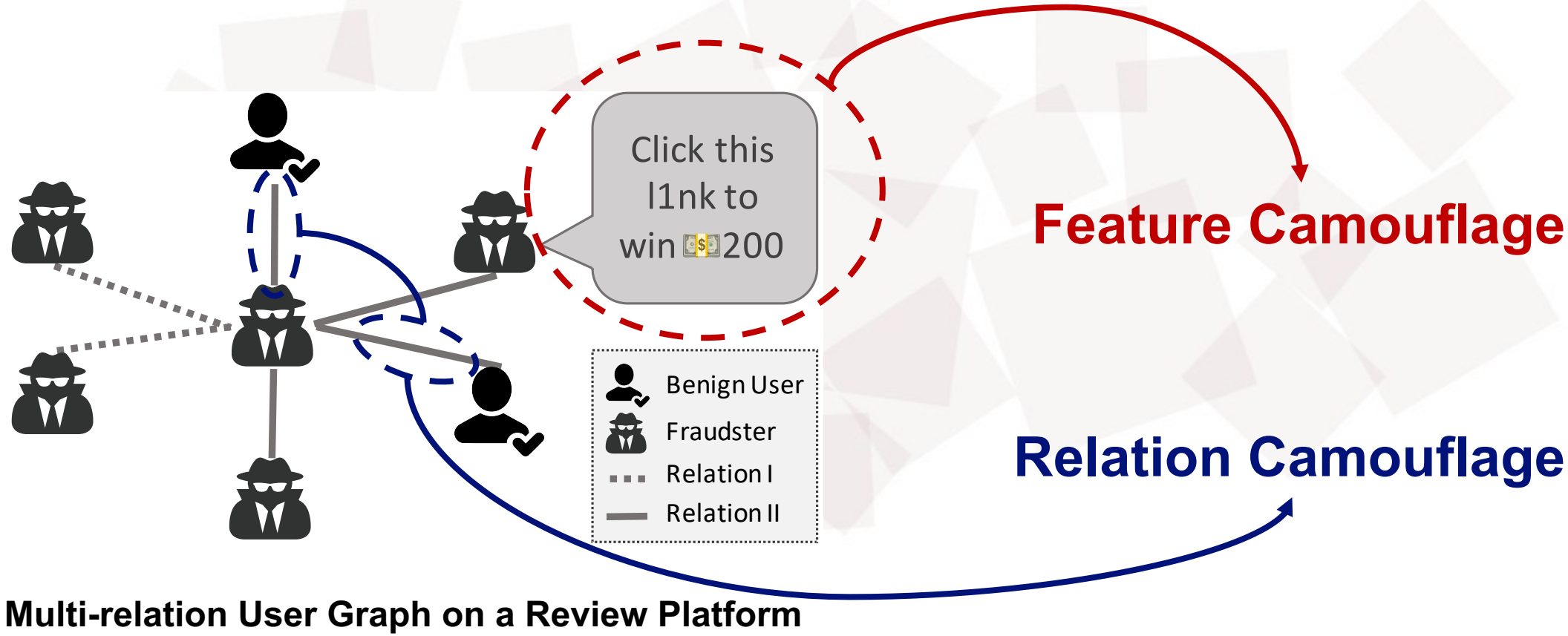
Method	40%		60%		80%	
	F1	AUC	F1	AUC	F1	AUC
LR	0.4647	**0.6140**	0.4640	0.6239	0.4644	0.6746
GraphSAGE	0.4956	0.5081	0.5127	0.5165	0.5158	0.5169
FdGars	0.4603	0.5505	0.4600	0.5468	0.4603	0.5470
Player2Vec	0.4608	0.5426	0.4608	0.5697	0.4608	0.5403
GraphConsis	**0.5656**	0.5911	**0.5888**	**0.6613**	**0.5776**	**0.7428**

AUC的高得分证明了过滤不良实体的必要性

针对缓解特征不一致的对照

Zhiwei Liu, et. al. 2020. Alleviating the Inconsistency Problem of Applying Graph Neural Network to Fraud Detection. SIGIR 2020.

研究工作2. CARE-GNN模型



Multi-relation User Graph on a Review Platform

Yingtong Dou, et. al. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. CIKM 2020.

研究工作2. CARE-GNN模型

- 改进
- 使用强化学习选择过滤阈值
- 根据过滤阈值聚合不同关系

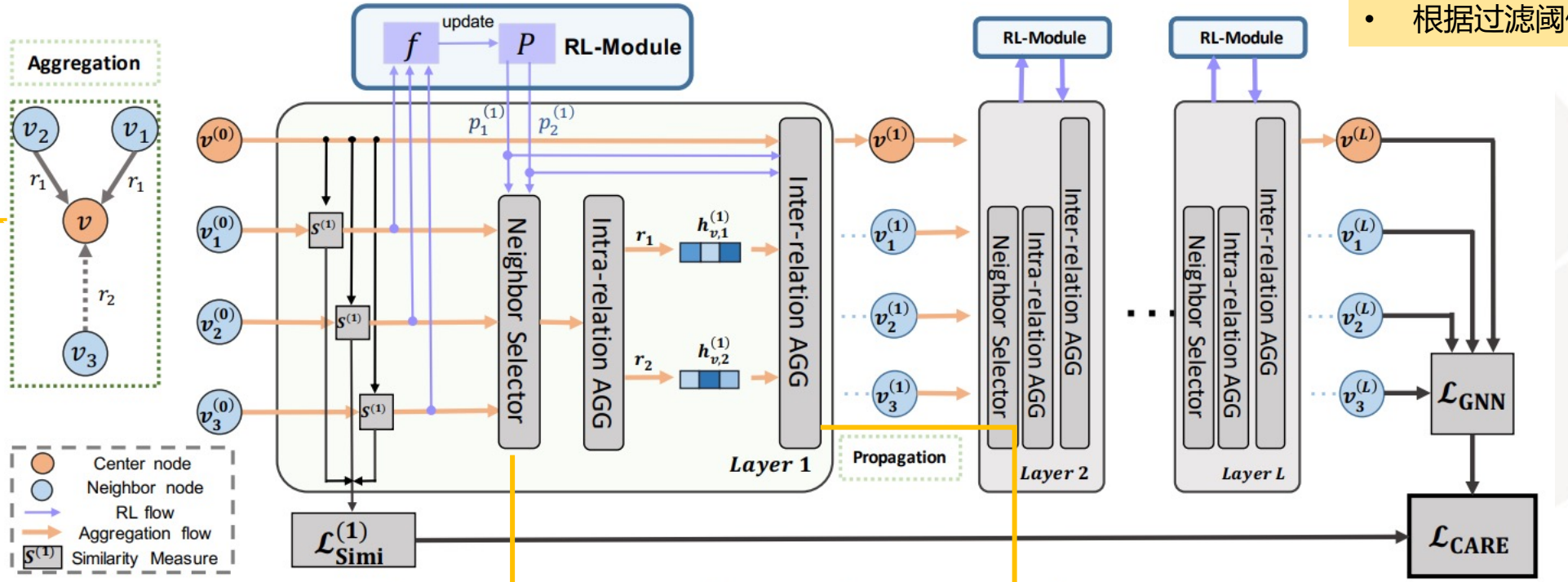


Figure 2: The aggregation process of proposed CARE-GNN at the training phase.

$$\mathcal{L}_{\text{CARE}} = \mathcal{L}_{\text{GNN}} + \lambda_1 \mathcal{L}_{\text{Simi}}^{(1)} + \lambda_2 ||\Theta||_2,$$

- MLP单层节点标签预测
- 交叉熵定义损失函数
- 快速筛选相似邻居

- 强化学习指导的邻居选择器
- 自动选择过滤阈值而非视为超参数
- Top-p采样保留最相关的邻居

- 强化学习指导的过滤阈值作为权重
- 聚合来自不同关系的信息
- 综合考虑中心嵌入与邻居嵌入

Yingtong Dou, et. al. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. CIKM 2020.

实验结果

数据集特点
- 巨量真实节点
- 复杂异构关系
- 多种实体行为
- 较低欺诈比例

Table 2: Dataset and graph statistics.

	#Nodes (Fraud%)	Relation	#Edges	Avg. Feature Similarity	Avg. Label Similarity
Yelp	45,954 (14.5%)	*R-U-R*	49,315	0.83	0.90
		R-T-R	573,616	0.79	0.05
		R-S-R	3,402,743	0.77	0.05
		ALL	3,846,979	0.77	0.07
Amazon	11,944 (9.5%)	*U-P-U*	175,608	0.61	0.19
		U-S-U	3,566,479	0.64	0.04
		U-V-U	1,036,737	0.71	0.03
		ALL	4,398,392	0.65	0.05

包含对酒店和餐馆的良性实体评论与垃圾评论

包含对乐器的良性实体评论与垃圾评论

Table 3: Fraud detection performance (%) on two datasets under different percentage of training data.

	Metric	Train%	GCN	GAT	RGCN	Graph-SAGE	Genie-Path	Player-2Vec	Semi-GNN	Graph-Consis	CARE-*Att*	CARE-*Weight*	CARE-*Mean*	CARE-GNN
Yelp	AUC	5%	54.98	56.23	50.21	53.82	56.33	51.03	53.73	61.58	66.08	71.10	69.83	**71.26**
		10%	50.94	55.45	55.12	54.20	56.29	50.15	51.68	62.07	70.21	71.02	71.85	**73.31**
		20%	53.15	57.69	55.05	56.12	57.32	51.56	51.55	62.31	73.26	74.32	73.32	**74.45**
		40%	52.47	56.24	53.38	54.00	55.91	53.65	51.58	62.07	74.98	74.42	74.77	**75.70**
	Recall	5%	53.12	54.68	50.38	54.25	52.33	50.00	52.28	62.60	63.52	66.64	**68.09**	67.53
		10%	51.10	52.34	51.75	52.23	54.35	50.00	52.57	62.08	67.38	68.35	**68.92**	67.77
		20%	53.87	53.20	50.92	52.69	54.84	50.00	52.16	62.35	68.34	69.07	**69.48**	68.60
		40%	50.81	54.52	50.43	52.86	50.94	50.00	50.59	62.08	71.13	70.22	69.25	**71.92**
Amazon	AUC	5%	74.44	73.89	75.12	70.71	71.56	76.86	70.25	85.46	89.49	89.36	89.35	**89.54**
		10%	75.25	74.55	74.13	73.97	72.23	75.73	76.21	85.29	**89.58**	89.37	89.43	89.44
		20%	75.13	72.10	75.58	73.97	71.89	74.55	73.98	85.50	89.58	**89.68**	89.34	89.45
		40%	74.34	75.16	74.68	75.27	72.65	56.94	70.35	85.50	89.70	89.69	89.52	**89.73**
	Recall	5%	65.54	63.22	64.23	69.09	65.56	50.00	63.29	85.49	88.22	88.31	88.02	**88.34**
		10%	67.81	65.84	67.22	69.36	66.63	50.00	63.32	85.38	87.87	**88.36**	88.12	88.29
		20%	66.15	67.13	65.08	70.30	65.08	50.00	61.28	85.59	88.40	**88.60**	88.00	88.27
		40%	67.45	65.51	67.68	70.16	65.41	50.00	62.89	85.53	88.41	88.45	88.22	**88.48**

半监督学习快速训练模型

动态调整阈值强泛化能力

Yingtong Dou, et. al. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. CIKM 2020.

强化学习有效性解释

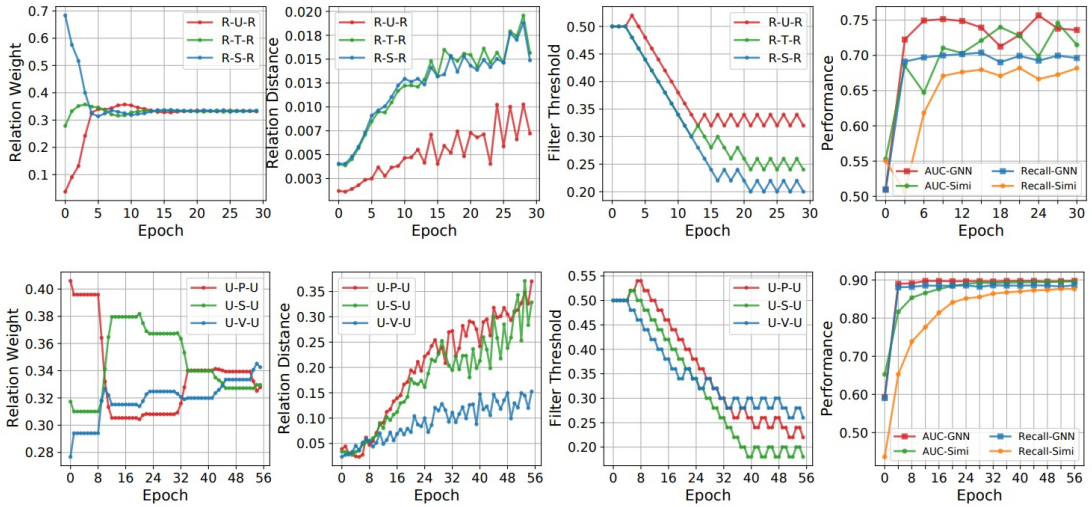


Figure 3: The training process and testing performance of CARE-*Weight* on Yelp (upper) and Amazon (lower) dataset.

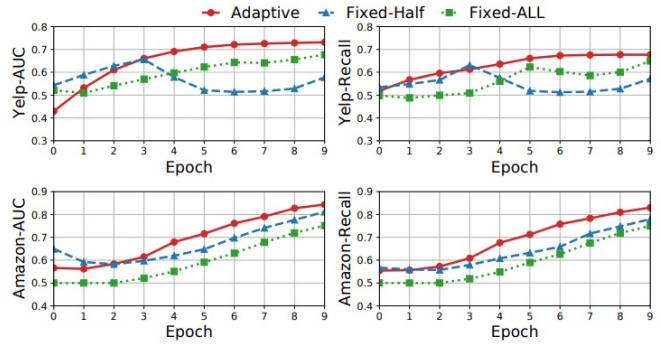


Figure 4: The testing AUC and Recall for CARE-GNN with different neighbor filtering methods during training.

自适应滤波优越性

邻居选择的必要性

不同关系的区分度

滤波阈值的稳定性

模型综合表现对比

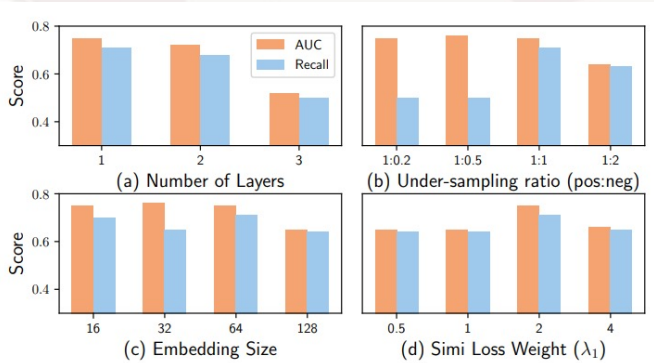
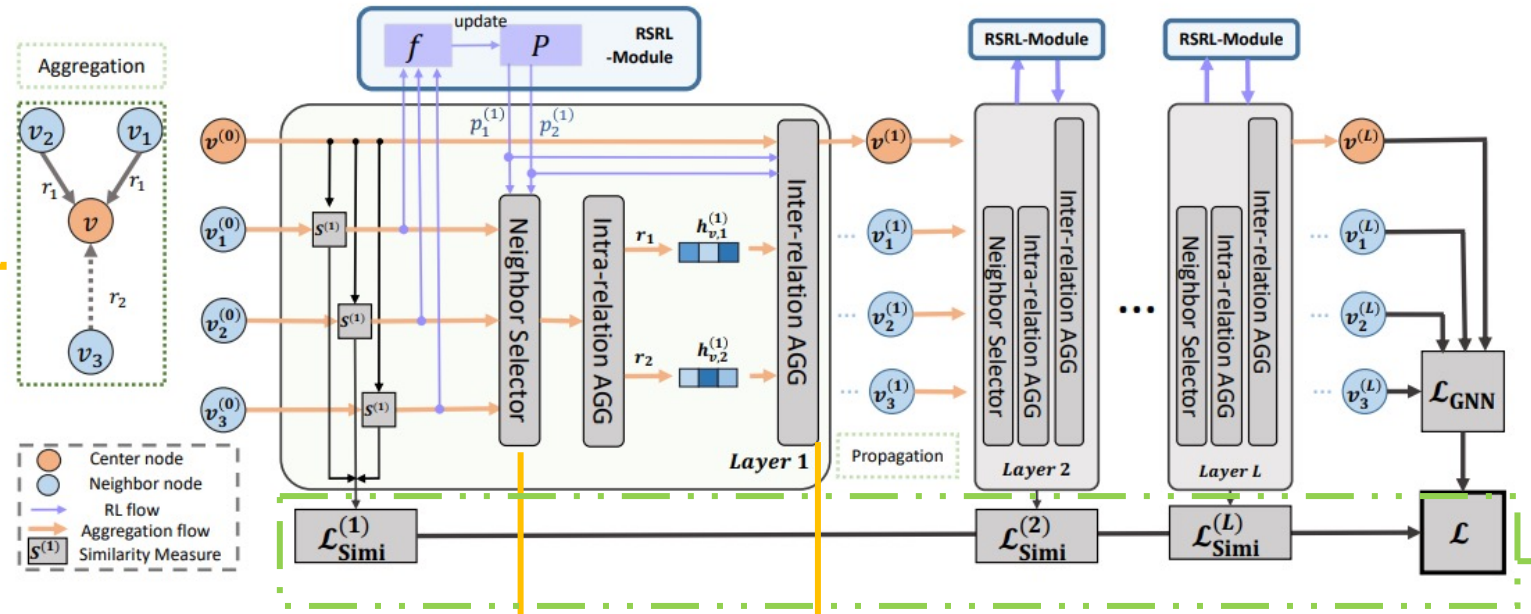


Figure 5: Parameter Sensitivity. For each parameter configuration, only the best results among 30 epochs are recorded.

参数灵敏度分析
- 训练层数
- 欠采样比例
- 嵌入规模
- 相似损失权重

Yingtong Dou, et. al. 2020. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. CIKM 2020.

研究工作3.RIOGNN框架



改进
- 泛化能力更强的RSRL框架
- 计算效率更优的RSRL框架

$$\mathcal{L}_{\text{RIOGNN}} = \mathcal{L}_{GNN} + \lambda_l \sum_{l=1}^{L} \mathcal{L}_{Simi}^{(l)} + \lambda_* ||\Theta||_2,$$

- GNN节点分类损失函数
- 相似性度量损失函数

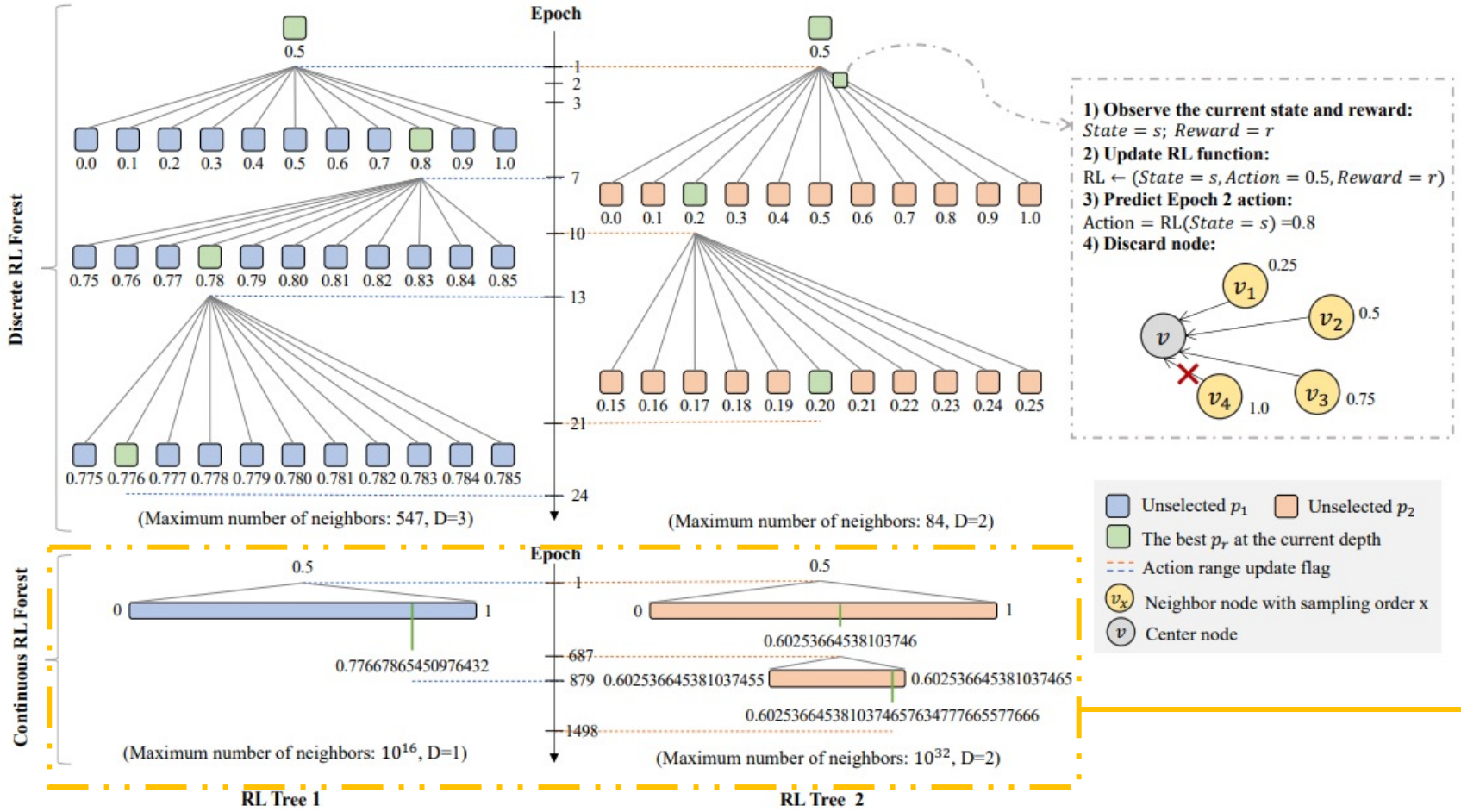
- 标签感知相似性度量
- 交叉熵定义损失函数
- GNN半监督过滤邻居

- RSRL框架指引邻居选择器
- 自动选择过滤阈值而非视为超参数
- Top-p采样保留最相关的邻居

- 强化学习指导的过滤阈值作为权重
- 聚合来自不同关系的信息
- 综合考虑中心嵌入与邻居嵌入

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

相似性感知自适应邻居选择器



RSRL框架要点

- 递归选择更高精度阈值
- 连续动作空间离散化
- 标签感知距离度量作为状态
- 节点相似度视为奖励

离散&连续空间下强化学习滤波阈值自适应选择

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

欺诈检测任务应用

准确性分析

Models	Yelp								Amazon							
	AUC				Recall				AUC				Recall			
	5%	10%	20%	40%	5%	10%	20%	40%	5%	10%	20%	40%	5%	10%	20%	40%
GCN	54.98	50.94	53.15	52.47	53.12	51.10	53.87	50.81	74.44	75.25	75.13	74.34	65.54	67.81	66.15	67.45
GAT	56.23	55.45	57.69	56.24	54.68	52.34	53.20	54.52	73.89	74.55	72.10	72.16	63.22	65.84	67.13	65.51
GraphSAGE	53.82	54.20	56.12	54.00	54.25	52.23	52.69	52.86	70.71	73.97	73.97	75.27	69.09	69.36	70.30	70.16
RGCN	50.21	55.12	55.05	53.38	50.38	51.75	50.92	50.43	75.12	74.13	75.58	74.68	64.23	67.22	65.08	67.68
GeniePath	56.33	56.29	57.32	55.91	52.33	54.35	54.84	50.94	71.56	72.23	71.89	72.65	65.56	66.63	65.08	65.41
Player2Vec	51.03	50.15	51.56	53.65	50.00	50.00	50.00	50.00	76.86	75.73	74.55	56.94	50.00	50.00	50.00	50.00
SemiGNN	53.73	51.68	51.55	51.58	52.28	52.57	52.16	50.59	70.25	76.21	73.98	70.35	63.29	63.32	61.28	62.89
GraphConsis	61.58	62.07	62.31	62.07	62.60	62.08	62.35	62.08	85.46	85.29	85.50	85.50	85.49	85.38	85.59	85.53
GAS	54.43	52.58	52.51	52.60	53.40	53.26	53.37	51.61	71.40	77.49	74.51	71.03	64.31	64.57	62.08	63.74
FdGars	61.77	62.15	62.81	62.66	62.83	62.16	62.73	62.40	85.58	85.41	85.88	85.81	85.83	85.73	85.84	85.93
GraphNAS^H	52.93	54.69	56.73	54.46	52.40	54.15	55.69	56.16	71.01	72.48	73.52	76.05	69.17	69.48	70.35	70.16
GraphNAS	53.26	55.31	57.15	55.59	53.69	55.47	56.04	57.00	72.41	73.04	73.58	76.25	70.36	70.53	71.73	71.88
Policy-GNN^H	54.04	55.73	59.30	60.60	53.08	55.35	58.75	59.99	72.20	73.30	74.11	77.20	70.10	71.20	73.08	74.44
Policy-GNN	55.75	56.29	60.01	61.52	54.15	56.16	58.95	60.33	73.69	74.06	75.29	78.85	71.34	72.46	74.55	76.70
CARE-GNN	71.26	73.31	74.45	75.70	67.53	67.77	68.60	71.92	89.54	89.44	89.45	89.73	88.34	88.29	88.27	88.48
RioGNN	**81.97**	**83.72**	**82.31**	**83.54**	**75.33**	**75.78**	**75.51**	**76.19**	**95.44**	**95.41**	**95.63**	**96.19**	**90.17**	**89.48**	**89.51**	**89.82**

Table 4. Fraud Detection results (%) compared to the baselines.

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

欺诈检测任务应用

- 多层GNN效果更优
- 多深度结构的快速准确收敛
- 过滤阈值作为关系间权重的优越性

Table 5. Fraud Detection classification results (%) compared to RioGNN variants.

Models	Yelp		Amazon	
	AUC	Recall	AUC	Recall
RioGNN $_{2l}$	76.01	63.15	91.28	72.46
BIO-GNN	78.67	71.21	95.47	88.35
ROO-GNN	**83.59**	**75.56**	95.58	89.22
RIO-Att	78.65	71.69	93.97	83.78
RIO-Weight	80.40	72.83	**96.25**	**89.61**
RIO-Mean	77.84	71.43	94.57	89.47
RioGNN	83.54	75.55	96.19	88.66

RSRL框架要点

- 递归选择更高精度阈值
- 连续动作空间离散化
- 标签感知距离度量作为状态
- 节点相似度视为奖励
- 连续三次相同动作终止迭代

Table 6. Fraud detection clustering results (%) compared to RioGNN variants.

Dataset	Metric	RioGNN $_{2l}$	BIO-GNN	ROO-GNN	RIO-Att	RIO-Weight	RIO-Mean	RioGNN
Yelp	NMI	3.18	9.36	**12.39**	9.80	12.05	8.39	12.22
	ARI	6.12	11.84	**16.61**	11.88	15.88	8.80	16.45
Amazon	NMI	58.87	59.83	57.81	55.76	58.76	58.72	**61.26**
	ARI	76.53	77.38	76.09	76.54	76.73	76.51	**78.40**

- RIOGNN在密集数据集上的显著优势

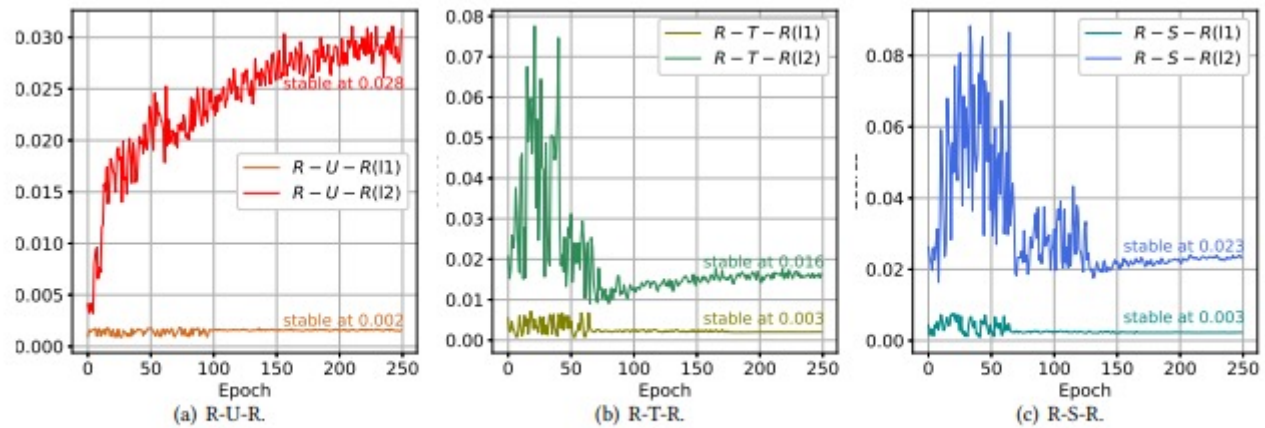
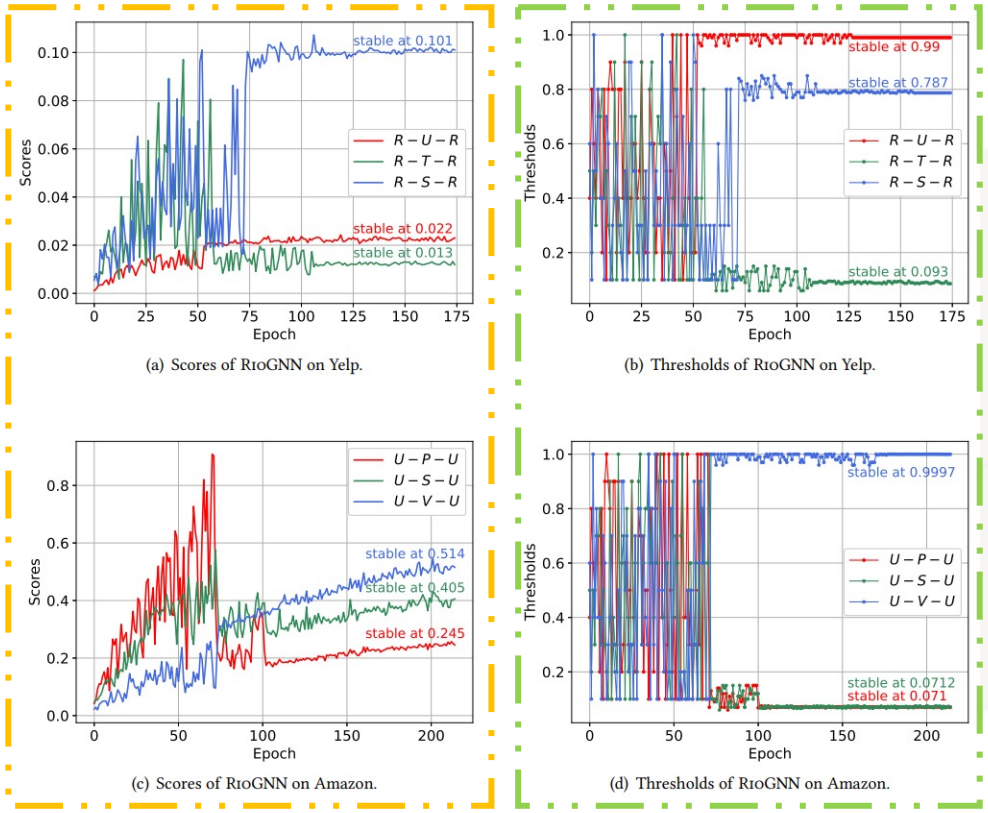


Fig. 7. Scores of Multi-Layer RioGNN on Yelp.

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

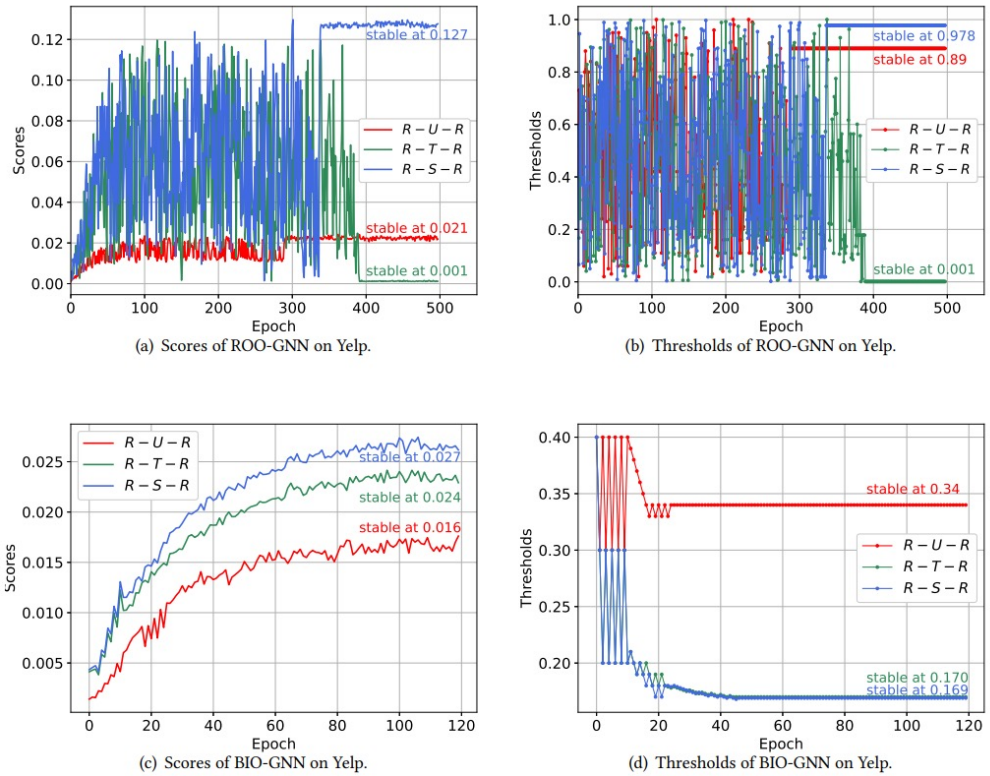
欺诈检测任务应用



(a) Scores of RioGNN on Yelp. (b) Thresholds of RioGNN on Yelp.

(c) Scores of RioGNN on Amazon. (d) Thresholds of RioGNN on Amazon.

Fig. 5. The training scores and thresholds of RioGNN on Yelp and Amazon.



(a) Scores of ROO-GNN on Yelp. (b) Thresholds of ROO-GNN on Yelp.

(c) Scores of BIO-GNN on Yelp. (d) Thresholds of BIO-GNN on Yelp.

Fig. 6. The training scores and thresholds of RioGNN variants on Yelp.

奖励对照

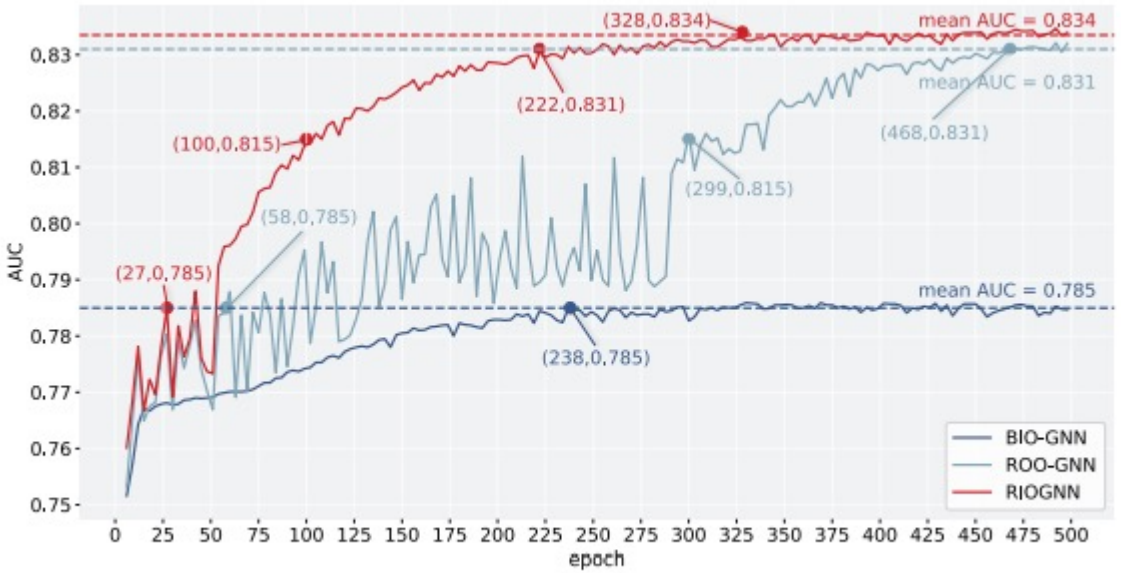
不同关系的重要性对照

RIOGNN变体对照（消融实验）

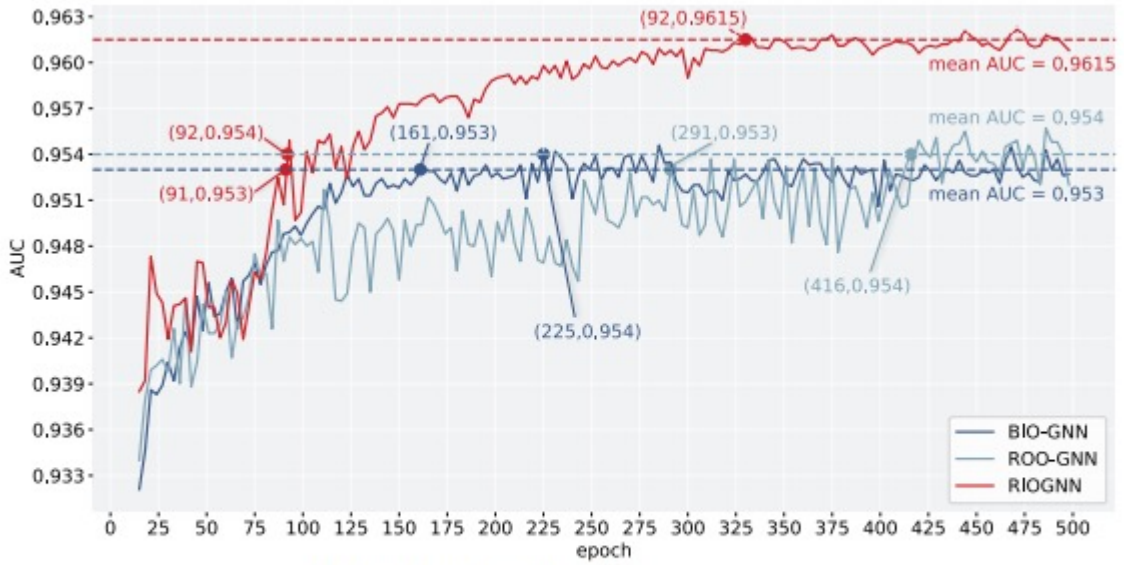
Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

欺诈检测任务应用

递归框架影响分析



(a) AUC of Rio-GNN, BIO-GNN and ROO-GNN on Yelp.



(b) AUC of RioGNN and RioGNN $_{No\ Recursion}$ on Amazon.

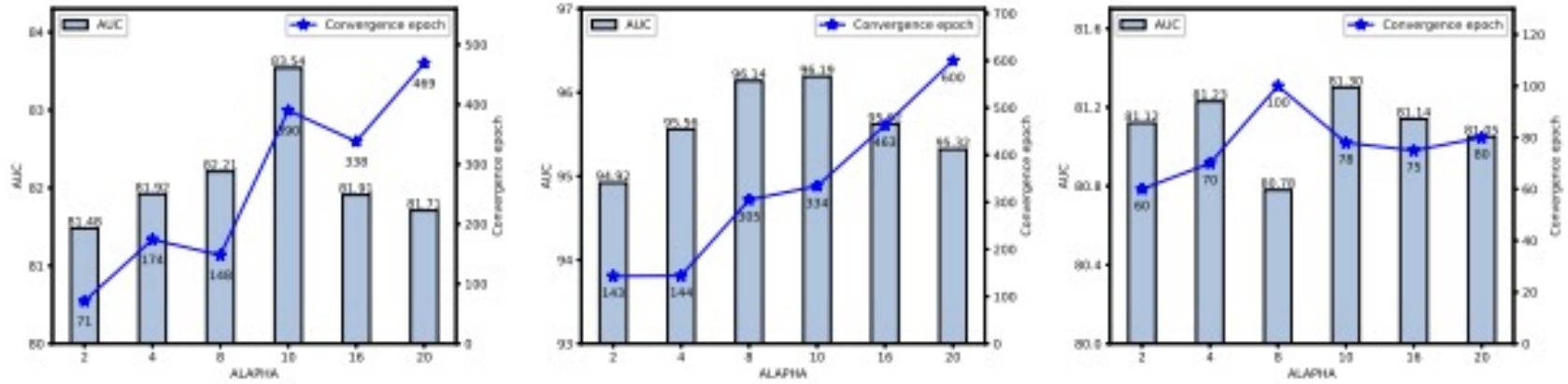
Fig. 8. The impact of recursive framework on computational efficiency.

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

RS RL框架通用性分析

Table 10. Results (%) compared to different RL algorithms and strengthening strategies.

	Methods	Yelp	Amazon	MIMIC-III
Discrete	AC [50]	83.54	**96.19**	81.36
	DQN [69]	84.08	95.13	80.96
	PPO [86]	80.52	94.99	80.98
Continuous	AC [50]	81.31	94.72	80.98
	DDPG [55]	83.80	95.39	81.17
	SAC [31]	80.42	94.76	80.87
	TD3 [23]	**84.18**	95.11	**81.51**



(a) Yelp. (b) Amazon. (c) MIMIC-III.

Fig. 11. Depth and Width for Different Task Scenarios.

Hao Peng, et. al. 2021. Reinforced Neighborhood Selection Guided Multi-Relational Graph Neural Networks. TOIS 2021.

未来工作

- 下一步希望能够完成的工作包括但不限于：

1. 采用多智能体 RL 算法，进一步使 RioGNN 能够自适应地识别每个节点的有意义的关系，而不是手动定义关系，以实现异构数据的自动表示学习。
2. 研究如何将我们的模型扩展到强动态图数据场景分析和应用任务。
3. 跨平台多语言的异常社交用户检测，联邦检测

谢谢各位老师和同学，敬请批评指正！

penghao@buaa.edu.cn
https://penghao-bdsc.github.io/

THANKS