ICDM 2022 大规模电商图上的风险商品检测——三个火枪手队

刘奔
武汉大学计算机学院
2981125675@qq.com

彭淼
武汉大学计算机学院
376755744@qq.com

徐文杰
武汉大学计算机学院
jaysaligia@foxmail.com

摘要—由于图结构数据的丰富关系信息，基于图神经网络的风险检测已经引起了学术界和工业界的广泛关注。ICDM 2022 举办了大规模电商图上的风险商品检测挑战赛，面向真实场景中的图数据进行风险商品检测。这篇报告介绍了我们队伍的解决方案，最终在复赛阶段获得第六名的评测成绩。首先，我们介绍比赛数据存在的挑战，这制约了模型在最终评测上的表现。然后，针对评测任务存在的挑战，我们分别介绍在我们模型中所使用的基于关系类型的采样器和基于梯度扰动的对抗训练策略两个模块。最终，在评测数据集上进行的实验表现出我们的方案的优越性，我们的方案在 session1 取得了 0.934 的 AP 分数，在 session2 取得了 0.916 的 AP 分数，消融实验也证明了我们每个模块的有效性。

***Index Terms*—风险商品检测, 图神经网络, ICDM Cup 2022**

I. Introduction

我们首先讨论队伍在比赛阶段所经历的挑战和方法背后的动机。随后详细描述所采用的模型的每个组成部分。

通过对赛事数据分析可以发现，该评测任务存在两个突出的问题，一是电商图是一个大规模的异质图，我们需要通过 mini-batch 的方式进行训练；二是我们所面临的真实场景下的电商图存在严重的数据不平衡问题，正负样本的数量比例超过 10。现有的基于 GNN 的方法表达能力仅限于低通滤波器，它强化低频信号（更加平滑的信号），从而抑制了高频信号（更加振荡的信号）[1]，容易受到类别不平衡问题的影响，尤其是在少数但更重要的类别，即风险商品检测上表现不佳。因此，如何设计好的标签平衡采样器选择节点和边构建子图进行小批量训练是我们面临的第一大挑战。其次，电商图是高度动态的，不断遇到新商品上架或下架，因此需要我们的模型是能够适应 inductive 场景，这点在 ICDM Cup 2022 的赛制说明中也有体现，session2 的数据是一个新图，图上的节点和 session1 的图节点没有对应关系。此外，由于电商图数据存在大量的噪声，往往会导致下游评测表现不佳。因此，如何让模型对新的图结构数据进行归纳学习，并产生更加鲁棒的节点嵌入以适应存在噪声的真实场景是我们面临的另外一大挑战。

针对上述两大挑战，我们队伍基于 GraphSage [2] 的采样方式设计了一个新的子图采样器以解决类别不平衡问题。同时为了保证模型是能够处理 inductive 场景，我们的模型同大部分 Inductive Graph Networks 一般，不会显式的去为每一个节点维护一个 embedding，而是希望能够利用 GNN 的 Message-Passing 范式，学习到子图采样器和节点邻居特征聚合器以泛化到未知的节点上。在采样到子图后，我们采用 R-GCN [3] 作为编码器。尽管一些异质图嵌入或者知识图谱嵌入 [4]–[6] 模型似乎能够学习到更有效的嵌入表示，然而在随后的实验评测中，R-GCN 取得了最优的效果。最后，为了学习到更加鲁棒的节点表示以适应充满噪声数据的场景，我们队伍受到 FLAG [7] 启发，在训练过程中，采用基于梯度的对抗性扰动来迭代增强节点特征，使模型对输入数据的微小波动不发生变化。

我们的模型在 session2 的表现是远远优于 session1（从排名上的角度）证明了我们的模型是鲁棒的，能够有效适应存在噪声且 inductive 设定的真实场景。

II. OUR APPROACH

我们团队所提出的方法主要分为三个部分，基于关系类型的子图采样器，R-GCN 编码器和基于梯度扰动

的对抗训练策略。

A. 基于关系类型的子图采样器

由于电商图是一个类别极度不平衡的大规模异质图，我们队伍受到之前重采样方法 [8] 的启发，考虑从节点的类别标签和节点的 one-hop 关系类型两个角度去设计采样器。但是考虑到商品图的 schema，商品之间的拓扑关联较为稀疏且为了适应测试阶段的 inductive 设定，我们放弃了从节点的类别标签设计采样器，决定采用基于 one-hop 关系类型的采样方式。具体对于一个 target 节点，为了保证节点的邻域信息均衡，我们对其每种关系类型的邻域有放回的采样相同数目的节点，然后迭代 K 次以获得一个子图。相较于 GraphSage 的随机采样方式，我们通过节点的关系类型来指导采样，使得采样出的子图邻域语义更均衡。通过这样的采样方式，可以有效构建 mini-batch 训练大规模的商品图。

B. R-GCN 编码器

在采样得到子图后，我们采用 R-GCN 编码器作为节点的聚合器，具体的在聚合邻居节点的信息时按照边的类型进行分类，根据边类型的不同进行相应的转换，其中每个节点的信息更新共享参数，并行计算：

$$\mathbf{h}_i^{k+1} = \sigma\Big(\sum_{r\in R}\sum_{j\in N_i^r}\frac{1}{c_{i,r}}\mathbf{W}_r^{(k)}\mathbf{h}_j^{(k)} + \mathbf{W}_0^{(k)}\mathbf{h}_i^{(k)}\Big) \tag{1}$$

其中，$h_i^{(k)}, h_j^{(k)}$ 分别表示节点 i, j 在第 k 层的节点表示；N_i^r 表示节点 i 的关系为 r 的邻居节点集合；$c_{i,r}$ 是一个正则化常量；$\mathbf{W}^{(l)}$ 是线性转换函数，将同类型边的邻居节点使用同一个参数矩阵进行转换。

C. 基于梯度扰动的对抗训练策略

为了更好的适应存在噪声数据的真实场景，避免由于小的噪声导致检测失败，我们队伍考虑通过基于特征的数据增强方法来提高模型的鲁棒性。在该次测评中，节点的初始特征是通过预训练模型获得的，因此常用的手工设计的数据增强手段（如扰动节点、边等）是不适用于本次测评的。受到 FLAG [7] 启发，对抗扰动被认为是一种数据依赖的正则化，有助于推广到分布外样本，同时考虑到标签节点样本的稀缺性，我们采用对抗扰动策略作为输入特征增强的方法。

对抗训练通过生成对抗性数据点然后将它们注入到训练数据中，通常可以概括为如下的最大最小化公式：

$$\min_{\boldsymbol{\theta}} E_{(x,y)\sim\mathcal{D}}\left[\max_{\|\boldsymbol{\delta}\|_p\leq\epsilon} L\left(f_{\boldsymbol{\theta}}(x+\boldsymbol{\delta}), y\right)\right] \tag{2}$$

其中，$\mathcal{D}$ 为数据分布，y 为标签，$\|\cdot\|_p$ 为 l_p 范数距离度量，ϵ 为扰动界，L 为目标函数。扰动量 δ 动态更新。

我们的目标就是寻找合适的扰动，使得模型有更强的鲁棒性，PGD [9] 通过多次迭代的方式让扰动 δ 的方向沿着梯度提升的方向，沿着梯度提升意味着让最大化损失的增大，具体的：

$$\boldsymbol{\delta}_{t+1} = \Pi_{\|\delta\|_\infty\leq\epsilon}\left(\boldsymbol{\delta}_t + \alpha\cdot\operatorname{sign}\left(\nabla_\delta L\left(f_{\boldsymbol{\theta}}\left(x+\boldsymbol{\delta}_t\right), y\right)\right)\right) \tag{3}$$

上述迭代过程循环执行 M 次来制造最坏情况下的噪声，然后使用 δ_M 对输入特征进行扰动并在此基础上优化模型权值实现训练过程。

FLAG 在 PGD 的基础上，首先对 δ_M 的生成过程进行优化，PGD 的训练过程导致 M 次 δ_M 的生成迭代后模型只训练一次，因此 FLAG 在生成 δ_M 的过程中同时执行模型参数的更新，实现参数与扰动更新并行计算尽可能不需要额外的成本。同时为了利用多尺度特征增强对模型参数 θ 进行优化的思想，不同于 PGD 的单尺度扰动 δ_M，我们的节点特征被注入多尺度的干扰噪声 $\delta_{1:M}$，因此训练过程增强了数据增强的多样性，最终模型参数更新的方式为：

$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i - \frac{\tau}{M}\sum_{t=1}^{M}\nabla_{\boldsymbol{\theta}} L\left(f_{\boldsymbol{\theta}}\left(x+\boldsymbol{\delta_t}\right), y\right) \tag{4}$$

当生成干扰项时，基于梯度累计的模型参数更新实时完成，在 mini-batch 上通过积累梯度节省了一次向后传递，并节省了额外的 GPU 内存，产生了具有更大范围大小的扰动以增加数据增强结果的多样性和质量。

III. Experiment

在评测数据集上进行的实验表现出我们的方案的优越性。具体的，在 session1 中我们采用 ICDM Cup 2022 所提供的 baseline[1]划分训练集、验证集，在 session2 我们利用 session1 所提供的图数据作为训练集。最终，我们的方案在 session1 取得了 0.934 的 AP 分数（排名第 27），在 session2 取得了 0.916 的 AP 分

[1]https://git.openi.org.cn/GAMMALab/icdm_graph_competition

数（排名第 6）。接下来，将列出详细参数设置以及消融实验证明我们方案中每个模块的有效性。

A. 超参设置

我们的模型基于 PyG[2]和 FLAG[3]实现，同时列出了在 session1 和 session2 训练的时候的超参设置如表I。

表 I
在不同 SESSION 的超参设置

Hyper-Parameters	session1	session2
dim_size	256	256
num_bases_rgcn	8	8
num_samples_each_r	150	150
layers	3	3
learning rate	0.001	0.001
batch_size	200	200

B. 编码器选择

尽管学术界中有许多新颖有效的异质图编码器，但是我们队伍最终采用 RGCN 作为子图编码器。我们队伍在模型选择的时候进行了一系列的备选模型实验对比，考虑的备选模型包括 GraphSage [10], ChebConv [11], ResGatedGraph [6], GraphTransformer [12], HGT [4], EGConv [13], GAT [5]，RGAT [14]，和 FiLMConv [15]。所有的模型都是基于 PyG 实现，超参采用 PyG 推荐的最优超参。值得注意的是，在模型备选实验的时候，我们并没有采用我们队伍上面提到的采样方法和对抗训练策略，采样及训练策略按照 ICDM Cup 2022 所提供的 baseline 的方式。最终在 session1 提供的数据集上的模型选择实验结果如表II。通过备选模型实验结果可以看出，RGCN 在该评测场景中效果更优异，可能的原因在于 RGCN 对不同关系下的邻域信息分别编码，相较于其余模型能够更好的聚合该电商图的异质信息。

C. 消融实验

为了进一步的验证我们的方案中各个模块的有效性，我们做了较为详细的消融实验。首先，我们验证我们所设计的基于关系类型的采样器的效果，我们将其扩展到了 GAT，GraphSage，ResGated，代替原有的采样方法，在 session1 的数据上进行验证，具体实验效果如

[2]https://www.pyg.org
[3]https://github.com/devnkong/FLAG

表 II
备选模型实验对比–SESSION1 的验证集的 AP 指标

备选模型	AP Metric
GraphSage	94.27
ChebConv	94.34
GraphTransformer	91.70
EGConv	92.26
GAT	79.48
RGAT	93.43
ResGatedGraph	94.50
FiLM	94.37
HGT	94.60
RGCN	**95.42**

表III。从实验结果中我们可以发现，我们所设计的采样器大幅度的提升原有模型的效果，说明了我们的数据存在邻域信息不平衡的问题，通过基于关系类型的采样方法可以在一定程度上缓解这个问题。此外，我们设计了

表 III
采用基于关系类型的采样器–SESSION1 的验证集的 AP 指标

模型	AP Metric
GraphSage+S	95.14 (**0.87** ↑)
GAT+S	90.41 (**10.93** ↑)
ResGatedGraph+S	95.58 (**1.08** ↑)

两个变体模型 RGCN+S(仅采用我们设计的 Sampler) 和 RGCN+F（仅采用对抗训练策略 FLAG），并展示出了两个变体模型和我们的方案在 session1 中的验证集上的 ap 指标的表现。同时为了进一步体现我们方案的有效性，我们列出了 early stopping 后的每个 epoch 下的结果，具体的信息如表IV。从实验结果我们可以发现，无论是 RGCN+S 还是 RGCN+F 整体表现都是优于 RGCN 的，而且当两个模块都使用的时候，模型结果达到最优，这说明了我们所采用的基于关系类型的采样器和基于梯度扰动的对抗训练策略对最终的风险检测任务是有效果的。我们队伍最终选择在第 7 个 Epoch 的模型，在 Session2 上的最优评测结果为 AP 0.915781。

IV. Conclusion

在本报告中，我们首先讨论了我们队伍在比赛阶段经历的挑战和我们方法背后的动机，随后详细描述了我们所采用的模型的每个组成部分及背后理论，最后我们通过详细的实验和消融实验验证了我们方案中的每个

表 IV
消融实验分析–在 SESSION1 的验证集 AP 指标

Model	对抗训练策略 FLAG	基于关系类型的采样	epoch6	epoch7	epoch8	epoch9
RGCN	✗	✗	95.25	95.59	95.63	95.58
RGCN+F	✓	✗	95.29	95.68	95.76	95.64
RGCN+S	✗	✓	95.27	95.59	95.70	95.59
RGCN+S+F(Ours)	✓	✓	95.25	95.67	**95.82**	95.62

模块的有效性，证明了我们队伍所采用的基于关系类型的子图采样器和基于梯度扰度的对抗训练策略能够有效处理这种存在噪声、信息不平衡的大规模异质图，并且可以有效适应 inductive 场景。

参考文献

[1] Z. Chai, S. You, Y. Yang, S. Pu, J. Xu, H. Cai, and W. Jiang, "Can abnormality be detected by graph neural networks?" in *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI 2022, Vienna, Austria, 23-29 July 2022*. ijcai.org, 2022, pp. 1945–1951.

[2] W. L. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, 2017, pp. 1024–1034.

[3] M. S. Schlichtkrull, T. N. Kipf, P. Bloem, R. van den Berg, I. Titov, and M. Welling, "Modeling relational data with graph convolutional networks," in *The Semantic Web - 15th International Conference, ESWC 2018, Heraklion, Crete, Greece, June 3-7, 2018, Proceedings*, vol. 10843. Springer, 2018, pp. 593–607.

[4] Z. Hu, Y. Dong, K. Wang, and Y. Sun, "Heterogeneous graph transformer," in *WWW '20: The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*. ACM / IW3C2, 2020, pp. 2704–2710.

[5] P. Velickovic, G. Cucurull, A. Casanova, A. Romero, P. Liò, and Y. Bengio, "Graph attention networks," in *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*. OpenReview.net, 2018.

[6] X. Bresson and T. Laurent, "Residual gated graph convnets," *CoRR*, vol. abs/1711.07553, 2017.

[7] K. Kong, G. Li, M. Ding, Z. Wu, C. Zhu, B. Ghanem, G. Taylor, and T. Goldstein, "Robust optimization as data augmentation for large-scale graphs," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 60–69.

[8] Y. Liu, X. Ao, Z. Qin, J. Chi, J. Feng, H. Yang, and Q. He, "Pick and choose: A gnn-based imbalanced learning approach for fraud detection," in *WWW '21: The Web Conference 2021, Virtual Event / Ljubljana, Slovenia, April 19-23, 2021*. ACM / IW3C2, 2021, pp. 3168–3177.

[9] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," in *6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings*. OpenReview.net, 2018.

[10] W. L. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, December 4-9, 2017, Long Beach, CA, USA*, I. Guyon, U. von Luxburg, S. Bengio, H. M. Wallach, R. Fergus, S. V. N. Vishwanathan, and R. Garnett, Eds., 2017, pp. 1024–1034.

[11] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," in *Advances in Neural Information Processing Systems 29: Annual Conference on Neural Information Processing Systems 2016, December 5-10, 2016, Barcelona, Spain*, 2016, pp. 3837–3845.

[12] Y. Shi, Z. Huang, S. Feng, H. Zhong, W. Wang, and Y. Sun, "Masked label prediction: Unified message passing model for semi-supervised classification," in *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence, IJCAI 2021, Virtual Event / Montreal, Canada, 19-27 August 2021*. ijcai.org, 2021, pp. 1548–1554.

[13] S. A. Tailor, F. L. Opolka, P. Liò, and N. D. Lane, "Adaptive filters and aggregator fusion for efficient graph convolutions," *CoRR*, vol. abs/2104.01481, 2021.

[14] D. Busbridge, D. Sherburn, P. Cavallo, and N. Y. Hammerla, "Relational graph attention networks," *CoRR*, vol. abs/1904.05811, 2019.

[15] M. Brockschmidt, "Gnn-film: Graph neural networks with feature-wise linear modulation," in *Proceedings of the 37th International Conference on Machine Learning, ICML 2020, 13-18 July 2020, Virtual Event*, ser. Proceedings of Machine Learning Research, vol. 119. PMLR, 2020, pp. 1144–1152.