一种基于图神经网络的电信诈骗识别方法*

张杰俊[1]，唐颖淳[1]，季述郧[2]，李静林[2]
（1.中国电信股份有限公司上海分公司，上海 200041；
2.北京邮电大学 网络与交换技术国家重点实验室，北京 100876）

摘　要： 通信技术的普及给人们带来便捷的同时，电信欺诈行为也急剧增加。由于诈骗行为特征、号码类型等与正常业务具有极高相似性，传统基于统计的电信欺诈检测方法难于筛选。提出将用户通信关系转换为一组拓扑特征，建立通信社交有向图，将具有统计特征的顶点表示用户，具有关系特征的边表示他们之间的活动。在通信社交图基础上，通过图卷积模块捕获用户的通信行为规律和通信社交关系特征，通过池化读出机制聚合通信社交网络的潜在特征，以识别电信欺诈行为。真实通信历史数据验证表明了该方法的有效性。

关键词： 欺诈检测；通信社交网络；图神经网络；行为分类
中图分类号： TP18；F626　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.200976

中文引用格式： 张杰俊，唐颖淳，季述郧，等. 一种基于图神经网络的电信诈骗识别方法[J].电子技术应用，2021，47(6)：25-29，34.
英文引用格式： Zhang Jiejun，Tang Yingchun，Ji Shuyun，et al. A telecom fraud identification method based on graph neural network[J]. Application of Electronic Technique，2021，47(6)：25-29，34.

A telecom fraud identification method based on graph neural network

Zhang Jiejun[1]，Tang Yingchun[1]，Ji Shuyun[2]，Li Jinglin[2]
（1.China Telecom Corporation Limited Shanghai Branch，Shanghai 200041，China；
2.State Key Laboratory of Networking and Switching Technology，Beijing University of Posts and Telecommunications，Beijing 100876，China）

Abstract： While communication technology brings convenience to people，telecom fraud also increases sharply. Traditional detection methods are mainly based on data mining and statistical learning of history data. However，due to the high similarity between fraud behavior and normal business，traditional statistical methods are difficult to screen. This paper proposes to transform user communication relationship into a set of topological features and establish communication social directed graph，where vertices with statistical characteristics represent users and edges with relational characteristics represent activities between them. On the basis of the communication social graph，the potential characteristics of the communication social network are learned through the graph neural network，and the information characteristics of multiple nodes are aggregated through pooling readout mechanism，in order to identify the telecom fraud users. The validation of real communication history data shows the effectiveness of this method.
Key words： fraud detection；communication social network；graph neural networks；behavior classification

0 引言

随着信息社会的发展，电信欺诈高发，但由于通信关系的复杂性和不确定性，电信欺诈检测成为了一个十分困难的问题。

传统电信欺诈检测技术主要基于用户属性和通话记录来获得用户行为样本，再通过 SVM、LGB 等机器学习方法学习行为特征[1-2]。这些方法主要使用短时间的行为统计进行分类，往往会出现时间尺度特征不足的问题。同时，由于用户通话行为的复杂性，以固定窗口的统计特征作为诈骗电话的统计依据[3-4]，容易受到长期行为变化影响，分类效果差。

由于通信是一种社交行为，通信社交网络包含丰富的关系信息，通过社交网络能成功捕获用户的相关性，如两个人的社交网络重叠程度与其联系强度相关，即彼此认识的普通用户可能会有共同好友[5-6]。而电信诈骗分子并不了解用户社交特征，电信诈骗号码与被骗号码之间难以存在共享社交节点。同时不同用户的社交关系存在不同的节点数量、节点度数、节点 k-core 值、Page Rank 得分等[7-8]，使得其社交网络拓扑并不相同。基于这一思路，可以利用通信社交网络分析方法进行诈骗

* 基金项目：国家自然科学基金资助项目(61472338)

检测[9]。

本文提出了基于图神经网络(Graph Neural Network, GNN)的通信社交检测方法。该方法建立了一种端到端学习 GNN 模型,该模型基于游走采样和节点融合策略动态构建计算图,之后通过节点卷积算子和关系边卷积算子的混合算法基于计算图实现图卷积(Graph Convolution Network, GCN)[10]进行信息融合,最后引入均值池化读出机制,聚合来自不同节点范围的信息,并最终实现分类表示。该模型将用户行为特征和社交关系特征结合在一起,以识别欺诈行为。通过上海市真实电信数据集实验验证,相比于传统方法,基于 GNN 的通信社交检测模型可以提高电信诈骗识别的检出率。

1 基于图神经网络的电信诈骗识别算法设计

GNN 的核心思想是从局部图邻域迭代聚合特征信息[11]。局部图中的边表示两个节点之间的依赖关系,并通过周围的状态来更新节点的状态,从而能够解决通信社交关系拓扑的挖掘和基于节点间相关性强弱的迭代更新问题。

1.1 图神经网络模型架构

基于 GNN 的通信社交行为检测模型结构如图 1 所示。模型划分为三部分:(1)图构建模块;(2)图卷积层;(3)均值池化(Mean-pooling)读出机制。

输入有向图 G 为一对 (V, E),其中 V 表示具有用户特征 $x_v \in \mathbf{R}^{d_v}$ 的有限节点集合(例如,用户属性、用户呼叫数量等),E 表示用户交互的一组边,边特征为 $e_{vw} \in \mathbf{R}^{d_e}$(例如,通话次数、通话时长、呼叫类型等),$d_v$ 表示节点特征数,d_e 表示关系边特征数。

首先,GNN 为每个用户构造计算图,然后将其映射到卷积层的输入。图卷积层由几个节点卷积算子和边卷积算子组成,它们对用户之间的交互进行建模并提取不同范围的融合信息。然后,均值池化读出机制会利用多范围节点信息,并逐步进行全局的图迭代更新(Graph Embedding)。最后,将 GNN 输出与分类器结合起来,用于最终的欺诈预测。

1.2 图构建模块

为了处理大规模通信社交网络,本文提出一种基于相对关系强度的短步游走策略来对计算图进行采样,有效减轻了无效节点对模型训练的影响。

计算图的构建流程如图 2 所示。

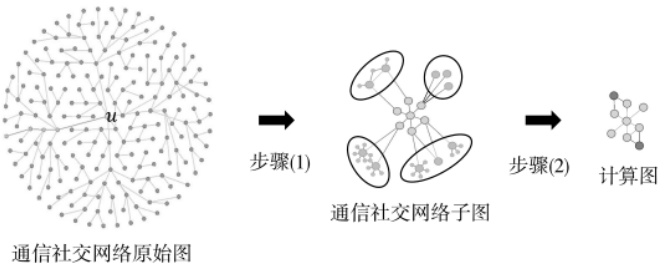


图 2 计算图的生成过程

该流程分为两个步骤:

(1)针对通信社交网络原始图,对源节点 u,通过固定长度 l 游走策略生成用户通信社交网络子图。方法是,从源节点 u 开始以固定步长 l 进行游走,并保留游走过程中的节点。为了保留相对较强的社交关系,游走根据亲密关系采样 k-hops$(2 \leqslant k \leqslant l)$邻居。

(2)针对通信社交网络子图,合并用户的 k-hops 邻居簇,生成用户节点 u 的最终计算子图。为了降低计算复杂度,该策略保留了源节点及其直接邻居,合并了 k-hops 邻居并删除度为一的合并节点。

1.3 图卷积模块

图卷积(GCN)可看作为一个图数据特征提取器,核

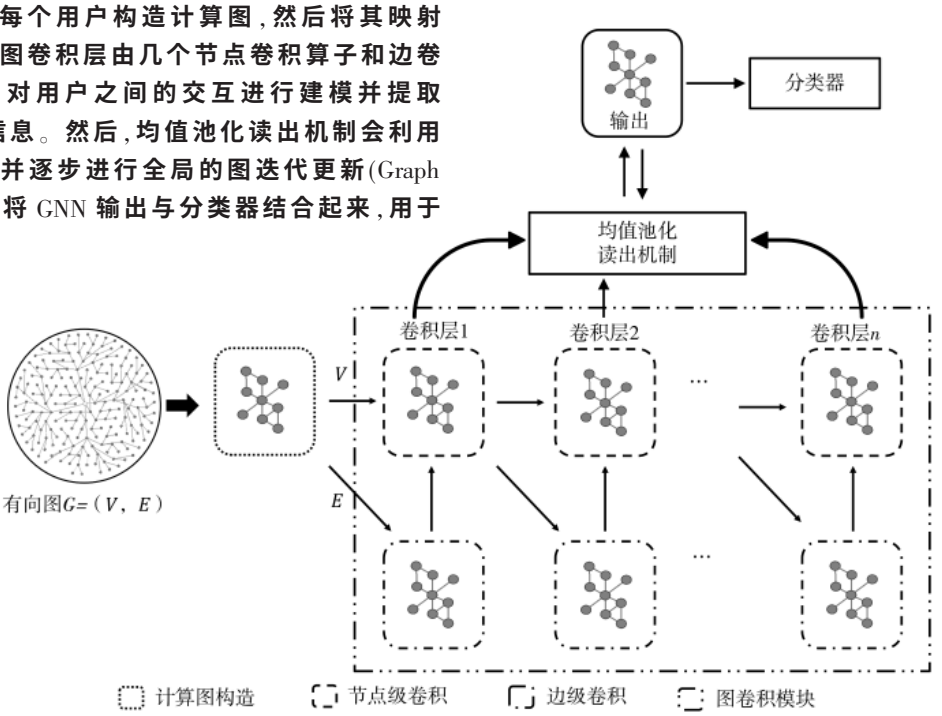


图 1 基于图的通信社交行为检测模型框架

心思想是利用边的信息对节点信息进行聚合并把邻居节点加和求平均，从而生成新的节点表示。基于拉普拉斯矩阵的谱分解，GCN 采用以下图卷积子：

$$X'=\hat{D}^{-1/2}\hat{A}\hat{D}^{-1/2}X\Theta \tag{1}$$

其中，X 表示节点初始特征向量，X' 表示节点更新后的状态向量，$\hat{A}=A+I$ 表示带自环的邻接矩阵 $\hat{D}_{ii}=\sum_{j=0}\hat{A}_{ij}$，并且 I 表示节点度数矩阵，Θ 为卷积子学习参数。

可以找到一个函数 $f(x)$ 作为节点卷积子，同时运用于当前节点和邻居节点。其中，可以通过一个可学习的参数来调整中心节点的权值 ε^k：

$$h_v^{(t)}=f_\Theta^{(t)}\left((1+\varepsilon^k)h_v^{(t-1)}+\sum_{u\in N(v)}h_u^{(t-1)}\right) \tag{2}$$

其中，$h_v^{(t)}$ 表示节点信息，$f_\Theta^{(t)}$ 可以使用多层感知机(MLPs)拟合，ε^k 用于调整中心节点的权值。

为了对通信社交网络的节点和关系边进行建模，需要堆叠多个卷积层以学习图中每个节点的内部隐藏表示，完成行为内容或社会关系的信息融合。

在传统图卷积中，领域消息传递阶段运行固定步长 T，并根据消息函数 M_t 和节点更新函数 U_t 进行节点学习。在当前时刻 t，根据当前节点状态 $h_v^{(t-1)}$、领域状态 $h_w^{(t-1)}$ 和关系信息 e_{vw}，计算消息 $m_v^{(t)}$ 并更新节点隐藏状态 $h_v^{(t)}$。在 GNN 中，为了聚合节点特征和关系边特征，更新了卷积函数，将其视为消息函数和更新函数的组合，以进行信息融合：

$$h_v^{(t)}=f_\Theta^{(t)}\left(h_v^{(t-1)}+\sum_{w\in N(v)}h_w^{(t-1)}g_\Theta^{(t)}(e_{vw})\right) \tag{3}$$

式中，$N(v)$ 表示图中节点 v 的邻居集，$f_\Theta^{(t)}$ 和 $g_\Theta^{(t)}$ 表示需要学习的函数。考虑到两个用户之间的复杂交互，选择使用神经网络 $g_\Theta^{(t)}$ 将边特征映射到节点特征，从而聚合来自邻域节点信息和边信息。在节点任务下，神经网络 $f_\Theta^{(t)}$ 可以表示为节点及其邻居的通用状态更新函数。

GNN 的图卷积模块结构如图 3 所示。GNN 的图卷积层通过 3 层堆叠而成，每一层参数共享，每个节点的邻居都进行一次卷积操作，并用卷积的结果更新该节点，然后经过激活函数 ReLU 完成节点隐藏状态的更新。

1.4 均值池化读出机制

局部图中较小的邻域范围表示局部依赖关系，较大的范围倾向于捕获更高阶的社交关系特征，不同范围的信息在正常网络和欺诈网络中的贡献均不相同。为了更好地利用多范围信息，获取最佳的图表示，本文提出图神经网络的均值池化读出机制，以对各节点隐藏状态的集合进行操作，并且这些节点隐藏状态排列是保持不变的。

2 实验与分析

2.1 实验数据集

实验数据集采用上海市的真实呼叫记录，包含从 2019 年 5 月 10 日~2019 年 6 月 23 日的全部用户呼叫记录，用户之间可能存在多个通信事件。数据集的数据样本统计信息如表 1 所示。

表 1 数据样本统计

性质	数量
用户总数|V|	54 973 350
关系总数|ε|	525 150 320
单边数	307 511 138
节点最大度数	664 266
被标记为诈骗总数	20 163(占总数的 0.04%)

针对这一数据集，首先进行数据预处理，主要进行 Z 分数归一化。之后对数据集按时间顺序进行划分，其中

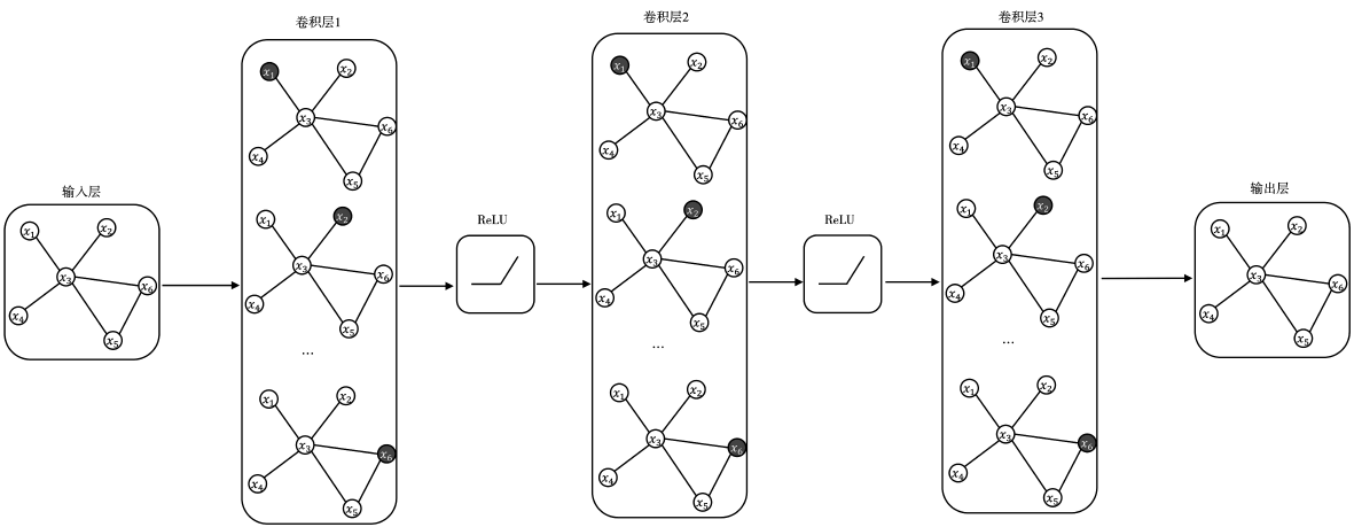


图 3 3 层 GNN 示意图

70%数据用于训练，10%数据用于验证，20%数据用于测试。

2.2 实验设置

针对数据集，选取 8 种用于构建计算图的用户特征，如表 2 所示。

表 2 用户特征

特征	描述
Call_count	通话次数
Total_calltime	总通话总时长
Max_calltime	最大通话时长
Min_calltime	最小通话时长
Max_start	最后通话时间
Min_start	最早通话时间
Fail_call_count	通话失败次数

对于每个用户的采样计算图，实验将最大游走长度 l 设置为 3。同时将每个卷积模型的卷积层数设置为 3，将节点隐藏状态维数和均值池化维数都设置为 16，并将均值池化函数应用于特征融合。最后的分类器采用两层 MLPs。

实验使用 Adam 优化器将模型训练 300 个 epochs，以使平均绝对误差（MAE）最小化。初始学习率设为 0.001，batch 大小设为 32。

实验采用的各种算法对比模型包括：

(1)SVM：使用包含社交网络结构信息的用户节点呼叫统计特征作为模型的输入信息。

(2)LGB(LightGBM)：使用包含社交网络结构信息的用户节点呼叫统计特征作为模型的输入信息。

(3)ANN：浅层人工神经网络，采用两层感知器进行分类[12]。使用包含社交网络结构信息的用户节点特征作为模型的输入信息。

(4)GCN：图卷积网络是基于图结构数据的半监督学习[10]。其模型中的边权重是通过用户之间的亲密关系计算得到，再根据权重构造边缘卷积算子完成对边缘特征评估，之后通过加权平均的方式更新节点状态。

(5)GIN：图同构网络(Graph Isomorphism Network)是一种消息传递网络 (Message Passing Neural Network，MPNN)[11]。GIN 通过一个可学习的参数来调整中心节点的权值，再根据权值构造节点卷积算子完成节点状态更新[13]。

(6)GNN：本文构建的图神经网络。

2.3 样本分类结果与分析

实验采用正确率、精确率、召回率和 AUC 来评估电信诈骗识别的性能。

如表 3 所示，GNN 模型比其他模型具有更好的识别能力，并且 GNN 的 AUC 比传统机器学习模型 SVM 和LGB 分别提升了 8.23%和 7.57%，也比其他人工神经网络模型(ANN、GCN、GIN)分别实现了 5.35%、3.98%和 3.04%的 AUC 提升。实验结果表明，GNN 可以学习到通信社交网络更多的信息，同时，均值池化(mean-pooling)读出机制也比传统的池化(max-pooling)具有更好的效果[14]。

表 3 各模型的分类结果

模型名	正确率	精确率	召回率	AUC
SVM	0.868 5	0.881 6	0.829 0	0.865 9
LGB	0.869 6	0.824 4	0.914 9	0.872 5
ANN	0.889 3	0.885 2	0.903 4	0.894 7
GCN	0.920 4	0.840 1	0.976 8	0.908 4
GIN	0.922 8	0.889 8	0.945 9	0.917 8
GNN(max-pooling)	0.934 5	0.936 5	0.935 1	0.937 8
GNN(mean-pooling)	0.948 4	0.947 2	0.949 2	0.948 2

图卷积模块中，图卷积层数对识别性能的影响如图 4 所示。随着迭代次数的增长，相比第 1 层卷积和第 2 层卷积，第 3 层卷积实现了 2.2%和 1.45%AUC 的提升。因此，图卷积模块中较深的卷积层有益于电信诈骗的识别。

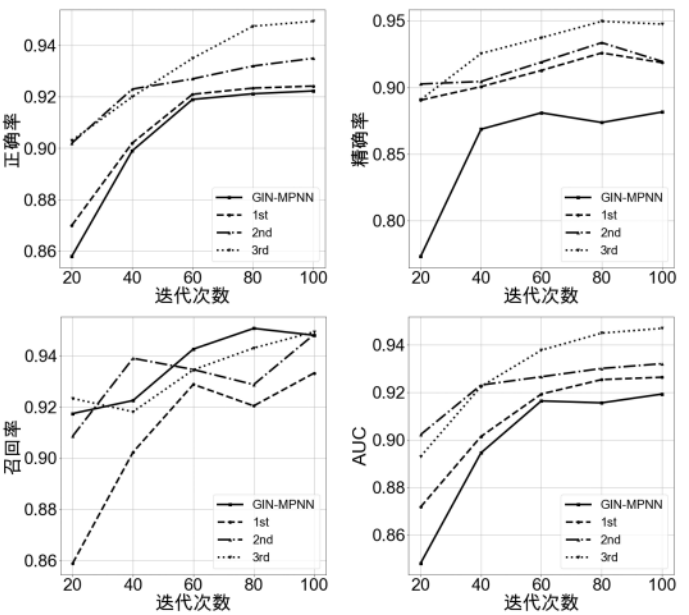


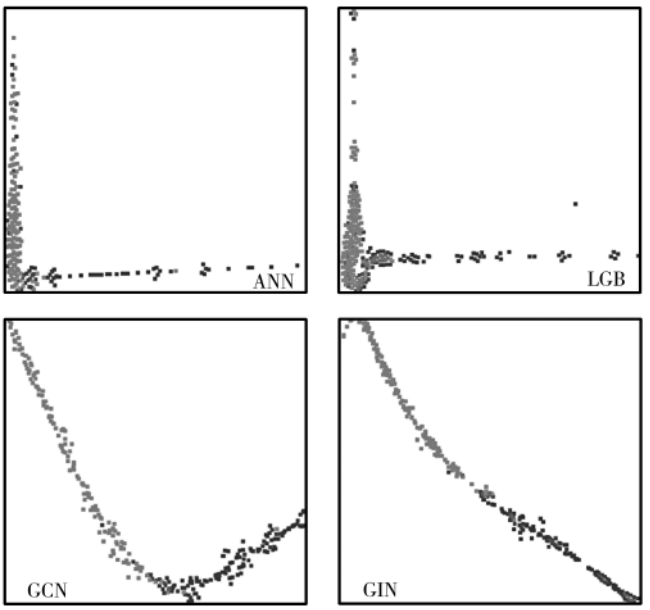
图 4 卷积层对模型性能的影响

对于不同模型的分类效果，本文使用 t-SNE(t-distributed Stochastic Neighbor Embedding)完成了高维图表示学习结果的降维和可视化[15]。

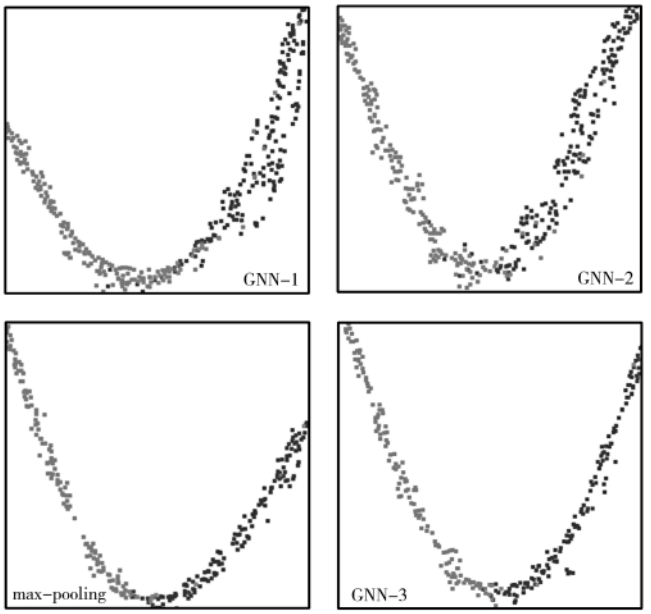
ANN、LGB、GCN、GIN 模型的可视化结果如图 5(a)所示，GNN 模型的可视化结果如图 5(b)所示。其中，灰色表示普通用户，黑色表示欺诈用户；GNN-1 为 1 层图卷积操作，GNN-2 为 2 层图卷积操作，GNN-3 为 3 层图卷积操作。GNN-1、GNN-2、GNN-3 使用均值池化操作，GNN Max-pooling 采用最大值池化操作。从可视化结果中可以看到，采用均值池化操作的 3 层 GNN 模型，其准确性始终高于其他方法。

3 结论

本文提出了一种基于图神经网络(GNN)的电信欺诈识别方法。这一方法基于短步游走采样和节点合并来构



(a)其他各模型



(b)GNN 模型

图 5 可视化结果

造计算图以适应大规模通信社交网络，通过融合通信社交信息的图同构算子和边卷积算子的混合体和过均值池化操作，有效地利用多范围信息对通信社交网络的特征进行学习。本文通过真实数据集对 GNN 模型进行了评估，与其他欺诈检测方法相比，图卷积方法能够适应大规模通信社交网络的检测，能满足电信欺诈检测的要求。未来的工作中，将进一步把图神经网络应用到现实系统中，以实现电信诈骗的实时拦截。

参考文献

[1] FARVARESH H，SEPEHRI M M.A data mining framework for detecting subscription fraud in telecommunication[J]. Engineering Applications of Artificial Intelligence，2011，24(1)：182-194.

[2] SAHARON R，MURAD U Z I，NEUMANN E，et al.Discovery of fraud rules for telecommunications—challenges and solutions[C].Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.ACM，1999：409-413.

[3] TANIGUCHI M，HAFT M，HOLLMEN J，et al.Fraud detection in communication networks using neural and probabilistic methods[C].Proceedings of the 1998 IEEE International Conference on Acoustics，Speech and Signal Processing，ICASSP'98(Cat.No.98CH36181).IEEE，1998.

[4] ESTÉVEZ P A，CLAUDIO M H，CLAUDIO A P.Subscription fraud prevention in telecommunications using fuzzy rules and neural networks[J].Expert Systems with Applications，2006，31(2)：337-344.

[5] Liu Shenghua，HOOI B，FALOUTSOS C.Holoscope：topology-and-spike aware fraud detection[C].Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. ACM，2017.

[6] GRANOVETTER M S.The strength of weak ties[J].American Journal of Sociology，1973，78(6)：1360-1380.

[7] FAKHRAEI S，FOULDS J，SHASHANKA M，et al.Collective spammer detection in evolving multi-relational social networks[C].Proceedings of the 21th ACM Sigkdd International Conference on Knowledge Discovery and Data Mining.ACM，2015.

[8] Ying Xiaowei，Wu Xintao，BARBARÁ D.Spectrum based fraud detection in social networks[C].2011 IEEE 27th International Conference on Data Engineering.IEEE，2011.

[9] QIU J，TANG J，MA H，et al.Y.Deepinf：social influence prediction with deep learning[C].Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery & Data Mining.ACM，2018：2110-2119.

[10] KIPF T N，WELLING M.Semi-supervised classification with graph convolutional networks[C].International Conference on Learning Representations(ICLR) 2017，2017.

[11] GILMER J，SCHOENHOLZ S S，RILEY P F，et al.Neural message passing for quantum chemistry[C].Proceedings of the International Conference on Machine Learning，2017：1263-1272.

[12] BRUNA J，ZAREMBA W，SZLAM A，et al.Spectral networks and locally connected networks on graphs[C].Proceedings of the 3rd International Conference on Learning Representations，2014.

[13] Xu Keyulu，Hu Weihua，LESKOVEC J，et al.How powerful are graph neural networks?[J].arXiv preprint arXiv：1810.00826，2018.

(下转第 34 页)

《电子技术应用》http://www.chinaaet.com

[8] XIANG J,ZHU G.Joint face detection and facial expression recognition with MTCNN[C].IEEE Computer Society,2017:424-427.
[9] SCHROFF F,KALENICHENKO D,PHILBIN J.FaceNet:a unified embedding for face recognition and clustering[C].2015 IEEE Conference on Computer Vision and Pattern Recognition(CVPR),Boston,MA,2015:815-823.
[10] IANDOLA F N,Han Song,MOSKEWICZ M W,et al.SqueezeNet:AlexNet-level accuracy with 50x fewer parameters and<0.5 MB model size[J].arXiv preprint arXiv:1602.07360,2016.
[11] GAIKWAD A S,EL-SHARKAWY M.Pruning convolution neural network (squeezenet) using taylor expansion-based criterion[C].2018 IEEE International Symposium on Signal Processing and Information Technology(ISSPIT),Louisville,KY,USA,2018:1-5.
[12] DENG J,ZAFERIRIOU S.ArcFace for disguised face recognition[C].2019 IEEE/CVF International Conference on Computer Vision Workshop(ICCVW),Seoul,Korea(South),2019:485-493.
[13] JANG E,GU S,POOLE B.Categorical reparameterization with gumbel-softmax[J].arXiv Preprint arXiv:1611.01144,2016.
[14] 周光朕,杜姗姗,冯瑞,等.基于残差量化卷积神经网络的人脸识别方法[J].计算机系统应用,2018,27(8):39-45.
[15] 朱红,陈清华,刘国岁.一种高速神经网络HS-K-WTA的研究[J] 电子学报,2002,30(7):1020-1022.

(收稿日期:2020-09-30)

作者简介:
况朝青(1996-),通信作者,男,硕士研究生,主要研究方向:深度学习与计算机视觉,E-mail:2315650756@qq.com。
贺超(1990-),男,博士研究生,主要研究方向:光纤无线通信网络。
王均成(1996-),男,硕士研究生,主要研究方向:深度学习与计算机视觉。

扫码下载电子文档

(上接第29页)

[14] DUVENAUD D K,MACLAURIN D,IPARRAGUIRRE J,et al.Convolutional networks on graphs for learning molecular fingerprints[J].arXiv:1509.09292,2015.
[15] REX Y.Graph convolutional neural networks for web-scale recommender systems[C].Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining,2018.

(收稿日期:2020-10-06)

作者简介:
张杰俊(1971-),男,硕士,主要研究方向:电信网络ICT、云计算、人工智能技术。
唐颖淳(1975-),女,硕士,主要研究方向:电信领域人工智能技术。
季述郧(1996-),男,硕士,主要研究方向:机器学习与图神经网络。

扫码下载电子文档

版权声明