

一种基于图卷积神经网络的网络小贷反欺诈方案

毛巧儿^{1,2} 刘晓强¹ 李柏岩¹ 蔡立志² 胡芸²

¹(东华大学计算机科学与技术学院 上海 201620)

²(上海市计算机软件评测重点实验室 上海 201112)

摘要 针对网络小额贷款团伙欺诈的现象,提出一种基于图卷积神经网络的网络小贷反欺诈方案。根据信贷领域知识自顶向下定义知识图谱,通过电话联系等数据搭建用户关系网络;对数据进行预处理,获取欺诈风险特征;将关系网络的邻接矩阵及特征作为图卷积网络的输入,聚合二阶邻居的特征传播计算未知标签节点的违约概率。实验表明,与 DeepWalk 模型结合逻辑回归、XGBoost、GBDT 分类器相比,该方法在 KS 值上分别提高 0.214、0.168、0.076,提高了正负样本区分度,能够有效识别团伙欺诈。

关键词 图神经网络 反欺诈 网络小贷 知识图谱

中图分类号 TP391

文献标志码 A

DOI:10.3969/j.issn.1000-386x.2024.05.014

AN ANTI-FRAUD SCHEME BASED ON GRAPH CONVOLUTIONAL NETWORK FOR NETWORK MICRO-FINANCE

Mao Qiaoer^{1,2} Liu Xiaoqiang¹ Li Boyan¹ Cai Lizhi² Hu Yun²

¹(College of Computer Science and Technology, Donghua University, Shanghai 201620, China)

²(Shanghai Key Laboratory of Computer Software Testing and Evaluating, Shanghai 201112, China)

Abstract Aiming at the phenomenon of network micro-finance gang fraud, this paper proposes an anti-fraud scheme based on graph convolutional network for network micro-finance. According to the knowledge of credit field, the knowledge graph was defined by the top-down method, and the user network was built by the user call logs. The data was preprocessed to obtain the features of fraud risk. The adjacency matrix and features of the relational network were used as the input of graph convolutional network, and the feature propagation of the second-order neighbors was aggregated to calculate the default probability of the unlabeled node. Experimental results show that compared with the DeepWalk model combined with logistic regression, XGBoost, GBDT classifier, the KS value of our method is improved by 0.214, 0.168, 0.076 respectively, which distinguishes between positive and negative samples better, and effectively identifies fraud gang.

Keywords Graph convolutional network Anti-fraud Network micro-finance Knowledge graph

0 引言

随着互联网的普及,尤其是移动互联网技术的快速发展,网络小贷作为一种贷款新形式出现。用户在移动终端 App 上申请小额贷款,网络小贷公司通过评估用户信用来审核借贷资格。网络小贷不受

地域限制,客户可以随时随地完成贷款申请,审核成本较低,灵活性高,这些优点迅速吸引了众多市场用户。

面对大量的贷款申请,采用人工审核的方式难以完成快速审核的要求,机器审核能够快速筛选出不符合审核要求的用户,有效缓解了审核压力。然而,一些欺诈团体利用了机审的特点,采用了形式多变的作案

手段,致使网络小贷公司蒙受了巨额损失。网络小贷欺诈形式大致分为两类:个人欺诈和团伙欺诈。个人欺诈是指盗用他人身份信息申请贷款,特异性强。团伙欺诈是指多人联合进行欺诈,危害性大。本文主要针对团伙欺诈进行研究。

团伙检测研究受到学术界以及工业界的关注。学者多采用数据挖掘、社交网络分析、机器学习等方式。早在2005年Chau等^[1]研究用户交易行为图的过程中发现了欺诈同盟的现象,文献[2-3]利用Kore值与中心加权算法、矩阵相似度计算与秩排序和变化算法等数据挖掘方法计算团伙欺诈,文献[4-6]利用Louvain算法等社会网络分析算法对欺诈团伙进行检测。文献[7]采用了机器学习异常检测算法对团伙化网络进行侦测。近几年,图表示学习在欺诈检测领域的应用成为当前研究的热点之一,例如Liang等^[8]采用基于Node Embedding和图神经网络算法解决运费险团伙欺诈问题。

本文提出一种基于图卷积神经网络的网络小贷反欺诈方案。针对团伙欺诈的关系网络特点,研究构建用户通话关系,形成网络小贷知识图谱,通过图卷积神经网络的标签传播,计算某个未知节点的欺诈概率,从而达到有效识别团伙欺诈的目的。

本文的主要贡献如下:

1) 挖掘和构建用户与用户之间的关联,建立网络小贷知识图谱,构造用户通话网络,帮助识别异常欺诈用户。

2) 提出一种基于图卷积神经网络的网络小贷反欺诈方法,采用半监督学习模式,即使数据集存在未知标签的数据,也能够计算节点欺诈概率。

实验和应用表明,本文方案识别效果优于基于DeepWalk的逻辑回归、XGBoost、GBDT模型。

1 反欺诈方案整体框架

网络小贷反欺诈方案包括知识图谱构建、特征矩阵处理、图卷积神经网络欺诈分类等流程,如图1所示。系统首先根据信贷领域知识和现有数据集定义网络小贷概念图谱,利用团伙欺诈的特性构建用户通话关联网络,生成网络小贷知识图谱存储于图数据库;对每个实体的特征信息处理形成图卷积神经网络所需的特征矩阵;在图卷积神经网络中输入知识图谱整体邻接矩阵和特征矩阵,输出各节点的欺诈概率。

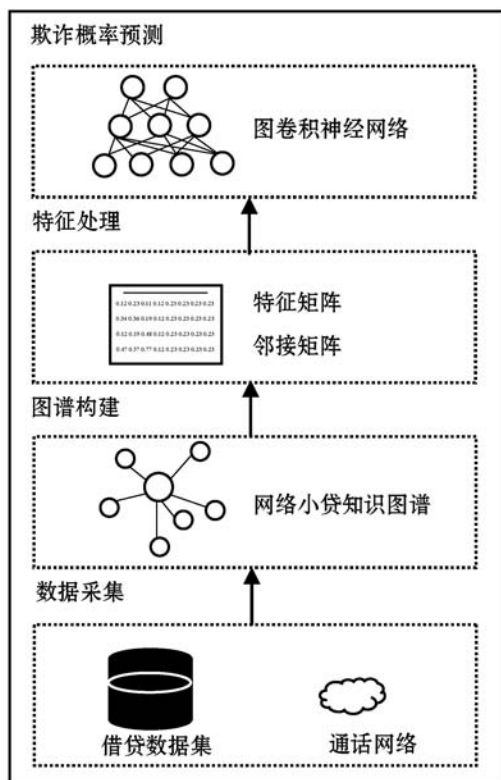


图1 网络小贷反欺诈方案处理流程

2 反欺诈方案技术实现

2.1 网络小贷知识图谱

在反欺诈过程中,如果单一地以用户数据为每个用户的全部特征,可能会丢失一些重要但不明显的信息,当欺诈团伙利用一些看似可信的用户特征时,风控引擎的判断就会受到影响。用户关系网络可以传递除了用户本身数据之外的信息,帮助发现异常的用户联系。知识图谱本质是连接实体间关系的图,即揭示实体之间关系的语义网络^[9],由实体与关系组成。基于知识图谱的反欺诈手段能够将孤立信息联结起来,通过知识推理发现更多知识。

结合知识图谱和信贷领域知识,本文以用户为核心设计网络小贷知识图谱。一个完整的知识图谱包含了大量的实体与关系,其中许多较次要的内容不仅占据了大量的存储空间,而且还会影响模型欺诈检测的准确度。针对团伙欺诈检测特性,这里仅选取知识图谱的一些关键实体与关系,展示核心关系网络,如图2所示。文中保留了用户实体、贷款实体、手机号码实体。用户实体包含固有属性,例如就业年限;信用属性,例如不良征信记录数;行为属性,例如过去12个月信用查询数;贷款实体包括申请贷款时的信息,例如借款金额等。手机号码实体例如近一周通话次数较以往是否增多等属性。

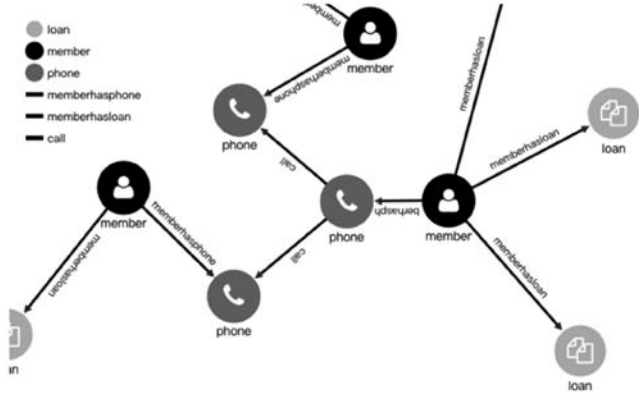


图2 网络小贷知识图谱

2.2 特征处理

通过对知识图谱的实体属性进行抽取获得特征矩阵。特征处理需要将节点的所有属性根据属性类型的不同分别处理,然后合并为一个整体特征矩阵。处理步骤为:1) 根据实体以及实体的属性信息组成图数据库查询语句,查询获取每个实体的属性。2) 根据配置文件对各个实体属性类型的描述,分别处理各个实体属性。针对分类变量进行缺失值处理、One-Hot 编码等操作,对维度较高的数据采用 PCA 降维。针对连续变量进行缺失值处理,对其标准化等。3) 由于知识图谱存在多个异构实体,需要将不同实体特征拼接成一个特征矩阵,没有对应特征维度的实体则在该特征维度上简单填充随机数。

文中特征处理之后,特征矩阵包含贷款特征、用户特征、通话特征三类。图谱的邻接矩阵通过配置文件获得所有关系类型,包含用户申请贷款、用户拥有手机号、电话联系等多种关系,查询获取知识图谱所有关系并保存为 CSV 格式,需要应用邻接矩阵时,可通过 python 的 networkx 包加载。

2.3 图卷积神经网络

近年来,图神经网络已经成为了深度学习领域的热点,在图表示学习上表现突出。图卷积神经网络(Graph Convolutional Network)解决了 CNN 无法处理非欧几里得结构的卷积问题,通过逐层聚合所有邻居信息,更新节点特征以达到预测节点标签的目的。将一个 N 个节点构成的无向图记为 $G = (V, E)$, $V = \{v_i\}_1^N$, 为点集, $E \in \mathbf{R}^{N \times N}$ 为边集,如果点 v_i 和 v_j 有关系,则 $e_{ij} = 1$, 否则 $e_{ij} = 0$ 。卷积神经网络分为两类:基于空域的图卷积神经网络^[10]和基于谱域的图卷积神经网络^[11]。谱域的图卷积通过图傅里叶变换,将数据从空域转换到谱域,在谱域完成卷积之后,通过图傅里叶反变换将卷积结果转换到空域,转换公式为:

$$g_\theta * x = \mathcal{F}^{-1} \{ \mathcal{F}(f) * \mathcal{F}(g) \} \quad (1)$$

式中: g_θ 为图过滤器; x 为图信号; $*$ 表示卷积; \mathcal{F} 为图傅里叶变换; \mathcal{F}^{-1} 为图傅里叶反变换。频域图卷积涉及拉普拉斯矩阵的谱分解,拉普拉斯矩阵的特征向量 U 为傅里叶变换的基函数,而拉普拉斯矩阵的特征值 ψ 类似频率的概念,谱分解表示为:

$$g_\theta * x = U g(\psi) U^T * x \quad (2)$$

式中: $g(\psi)$ 表示卷积核。由于图中所有节点都需要参与矩阵分解,卷积核太大将导致计算非常复杂,GCN 采用一阶切比雪夫多项式代替谱域的卷积核,表示为:

$$g_\theta * x \approx \theta(\tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}}) * x \quad (3)$$

式中: \tilde{D} 表示有自连接的邻接矩阵的度矩阵; \tilde{A} 表示有自连接的邻接矩阵。

GCN 层的前向传播公式为:

$$H^l = \sigma(\tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}} H^{l-1} W^l) \quad (4)$$

由于 GCN 层数过多容易产生过度平滑的问题^[12], 因此采用两层图卷积神经网络:

$$Z = \text{softmax}(\tilde{A} \text{ReLU}(\tilde{A} X W^{(1)}) W^{(2)}) \quad (5)$$

式中: $\tilde{A} = \tilde{D}^{-\frac{1}{2}} \tilde{A} \tilde{D}^{-\frac{1}{2}}$ 。

本文通过网络小贷知识图谱将欺诈分类问题转化为图表示学习的节点分类问题。将图谱的拓扑信息以及实体的特征矩阵输入到 GCN, 根据 GCN 的原理,每一层都做如下操作:根据邻接矩阵,将节点的特征矩阵 H 变换之后传播至邻居节点;节点聚集所有邻居节点传递的特征矩阵以及自身上一层的特征矩阵;将聚集的特征矩阵做非线性变换的处理从而得到该层特征矩阵。GCN 按照已知欺诈标签节点的图卷积结果计算损失函数,调整每一层的 W 权重系数,提升模型预测效果。在节点特征逐层传播的过程中,未知标签节点获取了已知标签节点的特征传播,从而得到未知标签的欺诈概率。

3 实验与结果

3.1 数据集

本研究项目数据集来源于上海某网络小贷公司,由于保密要求,采用了公开数据集 LendClub 的贷款数据进行实验,并根据文献[13-14]提及的团伙欺诈的特点以及项目采集特征,模拟了用户通话网络及通话特征。

本文首先从美国借贷公司 LendingClub 的公开数据集中随机抽取了 1 000 条数据,正常借贷记录有 836 条,违约记录为 164 条,比例趋近于 5:1。其中借贷特征共有 45 个,如表 1 所示。

表 1 借贷特征描述(部分)

特征	描述
grade	信用证指定的贷款等级
emp_length	就业年限
home_ownership	借款人在注册过程中提供的房屋所有权状态
annual_inc	借款人在注册过程中提供的自我报告的年收入
delinq_2yrs	过去 2 年中借款人的信用档案中逾期 30 天以上的逾期欠款的次数
earliest_cr_line	借款人最早报告的信贷额度开放的月份
inq_last_6mths	最近 6 个月的查询数量(不包括汽车和抵押贷款查询)
purpose	贷款目的
loan_amnt	贷款金额

其次构造了虚拟用户通话网络。由于用户通话网络能够很好地反映社交网络^[9],因此本文在构造用户社交网络时优先选择了通话网络。文献[13]认为违约用户在通话行为方面,申请前一周比往常与好友的通话次数更多,同时在通话网络中的度和 PageRank 值较正常用户高,即与网络中的更多用户联系更加紧密;文献[14]提及电信欺诈涉案人员之间的通话次数多且多发生在凌晨。文献[15]描绘了核心成员驱动、扁平化组织结构的犯罪网络,团伙欺诈的角色分为核心成员、中介人、边缘成员,通过三个人即可互相联系的小世界等特征。

本数据集欺诈团伙的核心人物有 1 至 3 人,由每次生成欺诈团伙时的随机数决定。每个核心人物分别发展随机多个中介人,除了中介人以外,将剩余的欺诈用户划分到当前的三个团伙中。除了欺诈团伙成员,其他用户也随机选择多个用户作为自己的联系人。

为了更好地模拟通话数据,混淆了欺诈团伙与正常用户的边界,其中欺诈成员与随机多个正常用户联系,由于不是所有的违约用户都属于欺诈性质的违约。欺诈团伙总人数设置为 1/2 的违约用户。考虑到不是所有的通话数据都能被采集到,将所有用户的通话网络随机抹除掉一定数量的边。在通话特征的构造中,也适当地混淆了欺诈用户与正常用户的区别,例如 30% 的欺诈用户的通话特征表现为正常。

3.2 实验设置

将邻接矩阵以及特征矩阵输入至 GCN 模型。经过一次图卷积聚合了一阶邻居的特征,其中激活函数采用 ReLU 函数,隐藏层神经元个数为 16 个,第二层激活函数为 softmax 函数,再经过一次图卷积聚合了二

阶邻居节点特征,输出的是节点的欺诈概率,维度为 2 维的欺诈类别。

本文 GCN 模型学习率为 0.01,迭代次数 200 次,损失函数采用交叉熵损失函数。模型训练使用了 Early Stopping、dropout 等技术防止模型过拟合。

3.3 结果与讨论

实验将数据集切割为训练集、验证集、测试集,比例为 6:2:2,实验结果与基于 DeepWalk 嵌入的逻辑回归、XGBoost、GBDT 模型对比。对比实验首先对网络结构进行嵌入,将嵌入数据与本身属性特征合并输入至 LR、XGBoost、GBDT 等分类器。DeepWalk 嵌入维度为 100 维,将迭代训练次数同样设置为 200 次,多次对比的实验结果如表 2 所示。

表 2 模型 KS 值比较

模型	KS 值	AUC
GCN	0.465	0.76
DeepWalk + LR	0.251	0.62
DeepWalk + XGBoost	0.297	0.68
DeepWalk + GBDT	0.389	0.69

4 结 语

知识图谱是网络小贷反欺诈的关键技术之一。本文从用户实体出发搭建网络小贷知识图谱探索了团伙欺诈,采用基于 GCN 的网络小贷反欺诈方案利用用户的社交网络,通过特征的逐层聚合传播,挖掘用户之间的潜在关联。与 DeepWalk 图表示学习技术相比,GCN 能够更加精准地分辨异常社区。在团伙欺诈的识别中,相较于 DeepWalk 结合 LR、XGBoost、GBDT 分类模型,KS 值分别高出 0.214、0.168、0.076。但是 GCN 模型要求邻接结构是固定的,这意味着每次新增一个节点时,就需要重新训练 GCN 模型,在节点数量逐渐增多的情况下,这一点将会大大影响欺诈检测的时效性,需要进一步探索解决这个问题。

参 考 文 献

- [1] Chau D H, Faloutsos C. Fraud detection in electronic auction[EB/OL]. [2021-03-15]. <https://sil0.tips/download/fraud-detection-in-electronic-auction>.
- [2] Wang J C, Chiu C. Recommending trusted online auction sellers using social network analysis[J]. Expert System with Applications, 2008, 34(3):1666-1679.

借鉴 Inception 架构造了多尺度卷积神经网络结构在计算量不显著提升的前提下增加了神经网络的宽度,减少了对神经网络深度的要求。

4 结 语

本文在低过采样下对多种数字调制信号在一个解调模型下解调进行研究。本文利用了多尺度网络结构构建并联合一维卷积层提取低维时序序列中的幅度相位特征,全连接层处理提取出来的特征,设计了适应于低过采样倍数的数字信号解调器,并验证了解调器对 BPSK、4QAM、8QAM、16QAM 四种数字调制信号在高斯和瑞利衰落信道下解调的误码性能。相较于已有深度学习解调方法,本文方法在保证解调性能同时,降低了网络的复杂度,减少了对采样倍数的要求。另外本文方法所需过采样倍数与传统解调器相同,理论上能直接嵌入到现代通信系统当中,具有一定的实际应用价值。

参 考 文 献

- [1] Li M, Zhong H, Li M. Neural network demodulator for frequency shift keying[C]//International Conference on Computer Science and Software Engineering, 2008.
- [2] Amini M, Balarastaghi E. Universal neural network demodulator for software defined radio[J]. International Journal of Machine Learning and Computing, 2011, 1(3):305 - 310.
- [3] Ahmed N, Aziz M. Neural network demodulator for quadrature amplitude modulation[J]. International Journal of Advanced studies in Computers, Science and Engineering, 2016, 5:10 - 14.
- [4] Meng F, Wu L. Demodulator based on deep belief networks in communication system[C]//International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE). IEEE, 2017.
- [5] Fang L, Wu L. Deep learning detection method for signal demodulation in short range multipath channel[C]//International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE), IEEE, 2017.
- [6] Lin X, Liu R, Hu W, et al. A deep convolutional network demodulator for mixed signals with different modulation types [C]//2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing (DASC). IEEE, 2017.
- [7] Wu T. CNN and RNN-based deep learning methods for digital signal demodulation[C]//Proceedings of the 2019 International Conference on Image, Video and Signal Processing (IVSP). IEEE, 2019.
- [8] Wang H. Deep learning for signal demodulation in physical layer wireless communications: Prototype platform, open dataset, and analytics[J]. IEEE Access, 2019, 7:30792 - 30801.
- [9] Szegedy C. Going deeper with convolutions[C]//2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), IEEE, 2015.
- [10] 弗朗索瓦·肖莱. Python 深度学习[M]. 张亮译. 北京:人民邮电出版社, 2018.
- ~~~~~
- (上接第 95 页)
- [3] 喻伟,冯根福,张文珺. 机动车辆保险欺诈检测系统及团伙识别研究[J]. 保险研究, 2017(2):63 - 73.
- [4] Palshikar G K, Apte M. Collusion set detection using graph clustering[J]. Data Mining Knowledge Discovery, 2008, 16:135 - 164.
- [5] 杨烁. 基于图的车险欺诈可视化分析系统的设计与实现[D]. 北京:北京邮电大学, 2019.
- [6] 范倬瑜. 基于图数据库 Neo4j 的信用卡反欺诈系统的设计与实现[D]. 杭州:浙江工业大学, 2020.
- [7] 孙权,汤韬,郑建宾,等. 金融交易数据驱动的图谱网络智能化欺诈侦测[J]. 应用科学学报, 2020, 38(5):713 - 723.
- [8] Liang C, Liu Z Q, Liu B, et al. Uncovering insurance fraud conspiracy with network learning[EB]. arXiv:2002.12789, 2020.
- [9] 刘峤,李杨,段宏,等. 知识图谱构建技术综述[J]. 计算机研究与发展, 2016, 53(3):582 - 600.
- [10] Knyazev B, Lin X, Amer M R, et al. Image classification with hierarchical multigraph networks [EB]. arXiv:1907.09000, 2019.
- [11] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks[C]//International Conference on Learning Representations, 2017:2197 - 2208.
- [12] Li G H, Muller M, Thabet A, et al. DeepGCNs: Can GCNs go as deep as CNNs? [C]//IEEE International Conference on Computer Vision, 2019:9267 - 9276.
- [13] Yang Y, Xu Y H, Wang C P, et al. Understanding default behavior in online lending [C]//28th ACM International Conference on Information and Knowledge Management, 2019:2043 - 2052.
- [14] 凡友荣,杨涛,孔华锋,等. 基于知识图谱的电信欺诈团伙特征挖掘方法[J]. 计算机应用与软件, 2019, 36(11):182 - 187.
- [15] 周志涛,鲍灵佳. 社会网络分析在团伙诈骗犯罪侦查中的应用[J]. 江西警察学院学报, 2014(3):39 - 44.