WEB：一种基于网络嵌入的互联网借贷欺诈预测方法

王成[1,2,3]，舒鹏飞[1,2]
1. 同济大学计算机科学与技术系，上海 201804；
2. 嵌入式系统与服务计算教育部重点实验室，上海 201804；
3. 上海智能科学与技术研究院，上海 200092

摘要
基于关联图谱的互联网借贷欺诈预测方法限制了特征的挖掘效率、挖掘深度以及特征的可复用性、可表达性。针对此问题，引入网络嵌入技术，在保留欺诈特征的前提下，将网络中的节点嵌入低维的向量空间，利用向量对网络中的结构和语义信息进行表达；提出了基于周期性时间窗口的网络更新方法和决策批处理方法来提升网络嵌入在精准性和实时性方面的性能。实验表明，网络嵌入技术能够自动有效地学习网络中隐含的关联关系与特征；通过将传统方法和网络嵌入方法相结合，欺诈预测性能得到了显著提升。

关键词
关联图谱；互联网借贷；网络嵌入；反欺诈；风险防控

中图分类号：TP181　　文献标识码：A　　doi: 10.11959/j.issn.2096-0271.2019052

WEB: a fraud prediction method of Internet lending using network embedding

WANG Cheng[1,2,3], SHU Pengfei[1,2]
1. Department of Computer Science, Tongji University, Shanghai 201804, China
2. The Key Lab of Embedded System and Service Computing Ministry of Education, Shanghai 201804, China
3. Shanghai Institute of Intelligent Science and Technology, Shanghai 200092, China

Abstract
Internet lending fraud prediction method based on association graph limits the mining efficiency and depth of features, as well as the reusability and expressibility of features. To solve this problem, the network embedding technology was introduced, and the structure and semantic information in the network by using the vector was expressed. The network update method based on periodic time window and decision batch method were proposed to improve the performance of network embedding in the two business requirements of accuracy and real-time. The experiment shows that the network embedding technology can automatically and effectively learn the implicit relationship and characteristics of the network. By combining the traditional method and the network embedding method, the fraud prediction performance has been significantly improved.

Key words
association graph, internet lending, network embedding, anti-fraud, risk management

1 引言

互联网借贷平台的规范化发展对社会经济的进步起着积极的推动作用，而互联网借贷欺诈已成为阻碍其发展的重要消极因素。欺诈者向借贷平台提供通过非法途径获取的他人信息或者伪造的虚假个人信息，达到骗贷的目的。通常，借贷平台很难立即发现欺诈的发生，只有到还款日用户未能按时还款，借贷平台才能发现欺诈的发生，但此时造成的损失通常已无法挽回。每年互联网借贷欺诈都给金融平台造成了巨大的经济损失。金融借贷平台急需建立有效的欺诈风险预测机制，以求能够对用户的借贷申请进行欺诈预测，并以此作为发放贷款的依据。

图1是互联网借贷的流程，在用户获得准入以后，借贷平台就会启动欺诈预测机制。目前，金融平台常用的方法是建立黑名单机制和第三方征信的方式[1]。黑名单机制是指金融平台会对某些曾经发生过借贷逾期未还的用户建立黑名单，当在黑名单中的用户再次申请借贷时，发生欺诈的风险就会过高。但是黑名单机制只能应对曾经申请过互联网借贷的用户，对于新的用户无法进行预测。利用第三方征信的方式也是目前广泛应用的方式，金融平台通过委托第三方征信机构对申请贷款的用户进行信用评估，将贷款发放给信用良好的借贷申请用户。但是网络贷款的申请数量众多，且通常为小额的贷款申请，利用第三方征信的方式花费的时间成本和人力成本过高，而且对于那些盗用他人信息进行互联网借贷的情况通常很难进行判断。

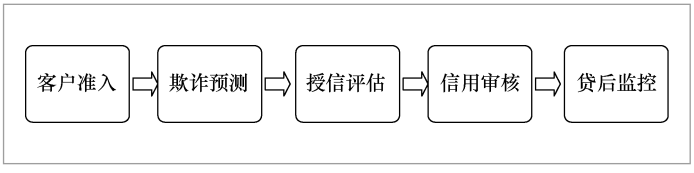


图1 互联网借贷流程

近年来，随着机器学习和数据挖掘技术的发展，越来越多的机器学习方法被应用到了金融反欺诈的领域。支持向量机（support vector machine，SVM）、朴素贝叶斯（naive Bayes）以及随机森林（random forest）等机器学习模型已经在金融反欺诈领域得到广泛应用[2-3]。但是使用这些方法的前提是找出有用的数据特征，这样才能训练出有效的机器学习模型。这需要研究人员具备一定的专家经验，并且基于传统机器学习的方法通常更关注显性的欺诈特征[4]。随着知识图谱和图数据库技术的不断发展，基于知识图谱的反欺诈技术吸引了越来越多研究者的关注[5]。基于知识图谱的方法能够有效地挖掘出网络中潜在的欺诈特征，Cao B等人[6]提出了一种基于异质信息网络的群体欺诈检测的方法。该方法基于知识图谱的视角揭示可疑交易之间的关系，即交易间的依赖关系。通过捕获常见的欺诈交易行为来检测可疑交易，这些欺诈交易行为在单独进行考虑时不会被视为可疑行为。他们提出的HitFraud方法可以检测出那些在独立检测下无法识别的欺诈交易。Mao R等人[7]提出了一种新的货币流通网络欺诈交易识别的方法。从“僵尸”账户和“崩溃”网络的角度对支付宝的资金流网络进行分析，能够有效地识别出资金流网络上超过99.3%的欺诈交易。McGlohon M等人[8]提出了一种基于网络链路分析的风险评估方法，这项工作建立在信念传播算法的基础上，用于检测在线交易中的合谋欺诈，但是该方法需要网络分析人员具有一定的领域知识和网络链路分析的背景知识。

欺诈者通常利用非法获得的他人信息向借贷平台申请网络贷款，且通常是团

伙作案，这些欺诈团伙提供的个人信息通常存在一些关联性。针对以上问题，本文将关联图谱应用到了互联网借贷反欺诈场景中，通过构建不同借贷申请之间的关联网络，利用关联图谱表达不同借贷申请之间的关联关系。传统基于关联图谱分析的方式需要研究人员掌握一定的行业背景和网络分析的知识背景，通过人工分析网络结构和特征，挖掘出网络中潜在的欺诈风险。这种基于人工网络分析的方法需要耗费大量的人力和物力。并且，随着数据网络规模不断扩大，传统的网络分析算法复杂度较高，需要消耗大量的计算资源。为此，本文提出了一种称为WEB（windowing-embedding-batching）的互联网借贷反欺诈方法。该方法将关联图谱和网络嵌入技术[9]相结合，创新性地应用到了互联网借贷反欺诈领域，利用网络嵌入技术自动进行网络表征学习，将网络中的所有实体都映射到低维的向量空间，利用向量表达网络中的所有信息，并且大规模网络在向量空间中形成的表征可以有效地降低复杂度。本文中的网络是一个动态更新的关系网络，随着借贷申请的增加，网络的规模不断扩大，网络结构发生改变，导致每次更新都需要重新学习节点的向量表示。网络嵌入技术在动态网络实时嵌入上存在不足，针对互联网借贷对实时性的低要求，本文提出了基于周期性网络更新的方法和互联网借贷批处理的方法，从动态网络更新和风险批处理两个方面克服网络嵌入的不足。

本文提出的WEB方法通过在某金融平台的互联网借贷数据的实验表明，利用网络嵌入技术进行互联网借贷反欺诈的效果接近于传统的网络分析的方法，但其具备不需要人工花费大量时间进行网络分析的重要优势。通过将2种方法结合，能够有效地提高互联网借贷欺诈风险预测的能力。实验表明，利用网络嵌入的方法能够挖掘出传统网络分析方法无法获得的有效特征。

2 相关工作

2.1 传统网络分析技术在反欺诈领域的应用

近年来，基于网络分析的方法在网络欺诈检测领域得到不断发展。

将传统机器学习模型与网络分析技术相结合的欺诈检测方法越来越受到关注。在Veronique V V等人[10]提出的方法中，根据交易数据构建用户交易行为的关联图谱，并使用RFM（recency-frequency-monetary）方法提取基本的网络特征，最后利用这些特征训练逻辑回归、随机森林和神经网络模型。实验表明，通过将网络特征与随机森林模型相结合，能够识别高达98%的信用卡欺诈交易。LIANG C等人[11]提出了一种图神经网络的方法解决运费险欺诈性骗保问题。通过构建索赔人之间的设备共享网络，开发了一个基于图形学习算法的自动欺诈检测解决方案，将欺诈者从普通客户中分离出来，并发现有组织的欺诈者群体。该方法在阿里巴巴平台上有效地阻止了80%以上的欺诈性保险索赔案例。

在进行欺诈检测时，记录的标签有时是不充分的，半监督的学习方法能够很好地解决标签不充分的问题。Li Y等人[12]将图挖掘技术和半监督方法相结合，并将其应用在拥有少量标签的数据集上。实验证明，该方法能够在京东的线上欺诈套现场景中取得很好的效果。基于标签传播的算法是网络欺诈检测中常用的方法，Libichot B等人[13]提出了一种基于网络欺诈传播的

半监督检测算法，从而识别信用卡欺诈交易。通过一组有限的、已确认的欺诈交易，根据网络传播欺诈的影响，判断其他未确认的交易是否为欺诈交易，从而给其他没标签的数据打上标签。LU P等人[14]提出了一种基于标签传播社区检测算法（label propagation algorithm，LPA）的欺诈电话分析方法，通过将呼叫内容数据转换成复杂的网络，并将LPA应用在此复杂网络上生成欺诈社区。通过生成网络的详细分析，提取社区的详细信息。结果表明，该方法有助于快速识别诈骗电话。基于聚类和社区发现的无监督算法能够有效地应对群体欺诈问题，Ganggopadhyay A等人[15]提出了一种通过人际网络挖掘欺诈社区的方法。通过构建人际关系网络，对网络中的社区结构进行分析，能够有效地挖掘网络中的欺诈团伙，实验证明了该方法在大型人际网络中的有效性。Kim J等人[16]将神经网络模型与聚类模型相结合，提出了一种基于层次聚类的深度神经网络方法，该方法将自动编码器预先训练的层次聚类的异常特征作为深度神经网络的初始权值来检测各种欺诈行为。

在基于传统网络分析的欺诈检测方法中，重点主要集中在寻找适合业务场景的网络特征，并且随着网络规模的不断扩大，网络中“边”的存在给网络处理和分析带来极大挑战，使得网络分析算法是迭代或组合爆炸的，导致复杂的网络分析算法无法应用于大型的网络结构。因此如今的网络规模已经使得任何相对复杂的分析算法都不可能在实际中被大规模地应用。

2.2 网络表征学习

网络表征学习的目标是为网络中的每一个节点学习一个特征表达，这种特征表达通常为低维的向量空间。给定一个网络$G=(V, E)$，对于网络中的每一个节点v，都能学习出一个d维的向量空间，其中$d<<|V|$，对于整个网络，就生成了一个向量矩阵$X\in R^{|V|\times d}$，这个矩阵能够获取网络中不同节点之间的结构和语义联系[17]。

将大规模的网络在向量空间中进行表征可以有效地降低复杂度，不仅可以非常容易地进行分布式并行计算，同时还可以应用前沿的机器学习算法对网络数据进行学习和分析。目前，常用的网络表征模型主要有以下3种。

（1）基于矩阵分解的模型

邻接矩阵通常用来表示网络的拓扑结构，其中每一行和每一列可以代表一个节点，矩阵的值代表节点之间的关系。可以简单地用行向量或列向量作为节点的向量表示，但形成的矩阵空间巨大。矩阵分解的方法以学习原始矩阵的低秩空间为目标，可以将网络嵌入一个低维的向量空间。在一系列矩阵分解模型中，奇异值分解（singular value decomposition，SVD）[18]、非负矩阵分解（no-negative matrix factorization，NME）[19]被广泛地应用于网络嵌入中。

（2）基于随机游走的模型

在进行网络嵌入时，保留网络结构是基本要求。受Word2Vec模型[20]的启发，Perozzi B等人[21]提出了基于随机游走和skip-gram模型[22]结合的DeepWalk模型，利用随机游走的方式获取网络的局部结构信息，并利用skip-gram模型对网络进行嵌入学习，以获得节点的向量表示。Tang J等人[23]在DeepWalk的基础上进行了改进，在一阶邻居相似性的基础上加上二阶邻居相似性，从而学习到对大规模稀疏网络有更好的区分能力的节点表示。

（3）基于深度神经网络的模型

网络嵌入是将原始网络空间转化为低维向量空间，内在的问题是学习这2个

空间之间的映射函数。有些方法（如矩阵分解）的前提假设是认为映射函数是线性的。然而，网络的形成过程复杂且高度非线性，因此线性函数可能不足以将原始网络映射到嵌入空间。如果要寻找一个有效的非线性函数学习模型，深层神经网络无疑是有用的选择。结构化深度网络嵌入（structural deep network embedding，SDNE）[24]和堆叠降噪自编码器（stacked denoising auto encoder，SDAE）[25]是具有代表性的基于深度学习模型的网络嵌入方法。

3 方法设计

本节主要介绍利用网络嵌入技术进行互联网借贷反欺诈的方法研究，主要包括关联网络的构建和风险预测方法的研究。

3.1 关联网络构建

用户的历史借贷记录$S_n=\{(x_1,y_1,t_1),(x_2,y_2,t_2),\cdots,(x_n,y_n,t_n)\}$是一个按时间排列的序列，其中$x_i\in R^m(i=1,2,\cdots,n)$是在$t_i$时刻产生的借贷记录，有$m$个不同的特征，通常包括申请人信息、电话、地址等。$y_i\in\{0,1\}(i=1,2,\cdots,n)$是记录$x_i$的标签，1表示该笔借贷是欺诈借贷，0表示该笔借贷是正常借贷。对于在t_{n+1}时刻产生的一条新的申请记录x_{n+1}，笔者的目的是预测借贷申请x_{n+1}的欺诈概率risk(x_{n+1})。

$$\text{risk}(x_{n+1})=P(y_{n+1}=1|X=\{x_1,\cdots,x_n,x_{n+1}\};Y=\{y_1,\cdots,y_n\}) \quad (1)$$

笔者利用动态网络分析的方法进行欺诈预测。给定一个t_n时刻的交易序列S_n，构建一个对应的关系网络$G_n=(V,E,W,T_n)$，即$\varnothing:S_n\rightarrow G_n$，其中$V$是网络中的节点，$E$是网络中的边，$W$是边的权重，$T_n$是$t_n$时刻网络中节点的时间戳序列。在时序网络$G_n$中，每个节点对应$S_n$的一条记录$\varphi:X\rightarrow V$，$v_i\in V$表示申请记录$x_i$在网络中的表示，节点的时间戳$t_i\in T_n$。给定两笔借贷记录$x_i$和$x_j$，统计两条记录相同的特征个数count($i,j$)。如果count($i,j$)>0，则在网络中节点$v_i$和节点$v_j$之间存在一条边，即$e_{ij}\in E$，且边$e_{ij}$的权重$w_{ij}$=count($i,j$)，则问题转化为：

$$\text{risk}(x_{n+1})=P(y_{n+1}=1|G_{n+1}=(V,E,W,T_{n+1});Y=\{y_1,\cdots,y_n\}) \quad (2)$$

图2（a）是基于**表1**的借贷记录构建的关系网络。**表1**中有5笔不同的借贷记录，分别对应网络中的5个节点，每条记录有5个不同的特征（编号、时间、借贷人姓名、住址、公司），这些特征可能是申请人的真实信息，也可能是虚假信息。其中，记录x_1和x_2有1个相同的特征（公司），即count(1,2)=1，则在网络中节点v_1和v_2之间存在一条边，且边的权重w_{12}=1。

3.2 风险预测方法

本节从序列窗口化（sequence windowing）、网络嵌入法（networking embedding）和预测批处理（prediction batching）3个部分介绍WEB方法。在第一部分中，本文提出了一种基于周期性滑动窗口的动态网络更新方法，既能实时地对网络进行更新，又能在特定时间删除网络中冗余的节点和边。第二部分介绍将借贷关系网络进行向量化嵌入的方法，解决

表1 历史申请记录示例

编号	时间	姓名	公司	住址
x_1	t_1	Bob	C1	Addr1
x_2	t_2	Jack	C1	Addr2
x_3	t_3	Sandy	C2	Addr3
x_4	t_4	Bob	C2	Addr1
x_5	t_5	Tim	C3	Addr2

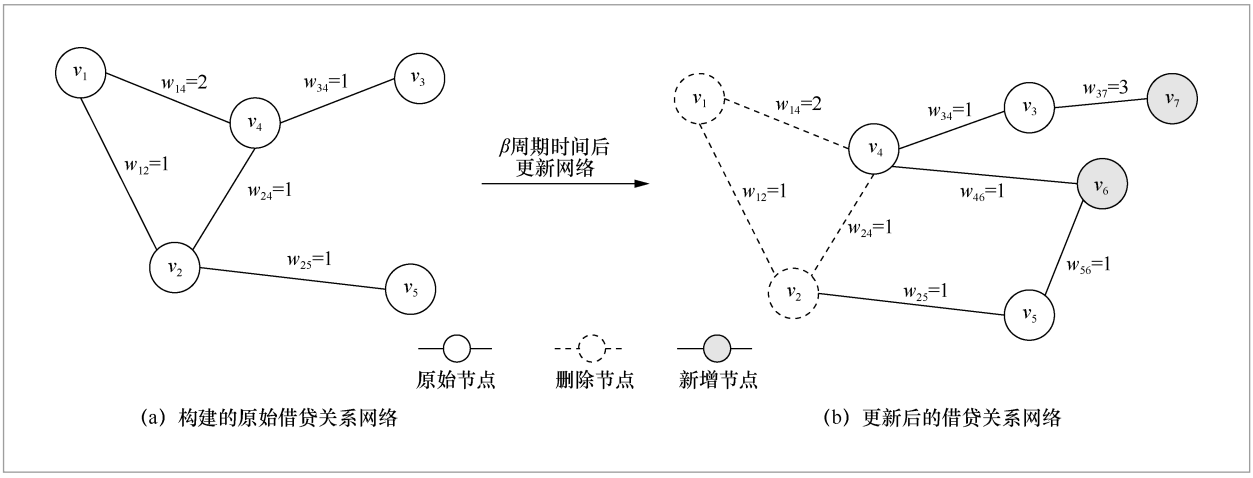


图 2 借贷关系网络构建与更新

了传统特征工程方法对专家经验的依赖性。第三部分针对网络嵌入在实时性上的不足，提出了一种借贷申请批处理的方法。

（1）序列窗口化

给定一个t时刻的关系网络$G_t=(V,E,W,T_t)$，在此后的时间里，每产生一条记录，都需要在网络中添加一个新的节点，并计算该节点与网络中其他所有节点之间的关系。随着时间的不断增长，网络中的节点和边的数量不断增加，网络规模不断增大。在进行互联网借贷欺诈预测时，数据存在一定的时效性，相关联的欺诈借贷通常聚集在一定的时间周期内。在对庞大的网络进行网络嵌入时，会学习到很多不必要的关联信息，并且会增加网络嵌入学习的复杂度，减小网络嵌入的效率。

本文提出了一种基于周期性滑动窗口的网络更新方式，设置一个固定大小为α的时间窗口和一个滑动周期β。在t时刻只保存时间戳$t_i\in[t-\alpha,t]$的节点，将时间戳小于$t-\alpha$的节点和相关联的边从网络中删除。从t时刻之后的时间β内，在任意$t+j(0\leqslant j<\beta)$时刻产生1条新的记录x_{t+j}，在网络中添加1个新的节点v_{t+j}，并计算与该时刻之前的网络G_{t+j-1}中所有节点之间的关系，生成相应的边，更新后的网络为G_{t+j}，此时网络中任意一个节点的时间戳$t_i\in[t-\alpha,t+j]$。在$t+\beta$时刻，即$j=\beta$，滑动时间窗口，删除网络中时间戳小于$t+\beta-\alpha$的节点和其相连的边，生成$t+\beta$时刻的网络$G_{t+\beta}$。在网络$G_{t+\beta}$中，任意一个节点的时间戳$t_i\in[t+\beta-\alpha,t+\beta]$。因此在$t$之后的$\beta$时间内，任意时刻$t+j$网络中的节点为：

$$V=\begin{cases}\{v_{t-\alpha},v_{t-\alpha+1},\cdots,v_{t-\alpha+j}\},0\leqslant j<\beta\\ \{v_{t+\beta-\alpha},v_{t+\beta-\alpha+1},\cdots,v_{t+\beta}\},j=\beta\end{cases}\quad(3)$$

图2（b）是在**表1**构建的原始网络上增加**表2**的记录x_6和x_7更新后的网络。在初始关系网络中，添加节点v_6和v_7，并生成相应的边与边上的权重。设置滑动周期$\beta=t_7-t_5$，则在t_7时刻滑动时间窗口，时间窗口的大小$a<t_7-t_2$，则节点v_1和v_2在t_7时刻从关系网络中被删除，与其相关的边也被删除，**图2（b）**中虚线的点和边即删除的节点和边。

（2）网络嵌入法

给定一个由借贷申请构成的关系网络$G=(V,E,W)$，提取出网络中重要的特征对

于互联网借贷反欺诈是非常重要的。在本文中，利用网络嵌入技术将所有的网络节点嵌入低维的向量空间，获得的向量能够表达网络中节点之间的关系。

在自然语言处理中，给定一个语料库，利用Word2vec算法，能够将网络中的每一个单词映射到一个低维向量空间。受此启发，利用skip-gram模型学习网络中节点与局部邻居节点之间的结构相似性，将网络中的每个节点映射到一个低维的向量空间。基于局部结构相似性，skip-gram模型的目标是最大化以下概率：

$$J=\underset{\theta}{\operatorname{argmax}}\frac{1}{|V|}\prod_{v\in V}\prod_{c\in N(v)}p(c|v;\theta)=\underset{\theta}{\operatorname{argmax}}\frac{1}{|V|}\sum_{v\in V}\sum_{c\in N(v)}\ln p(c|v;\theta) \quad (4)$$

其中，$N(v)$是节点v在网络中局部邻居集合，可包括节点的一阶邻居、二阶邻居或其他多阶邻居；$p(c|v;\theta)$表示在给定节点v的情况下，节点c是节点v的邻居节点的条件概率。在基本的skip-gram模型中，概率$p(c|v;\theta)$可以通过softmax函数定义：

$$p(c|v;\theta)=\frac{\exp(X_c\cdot X_v)}{\sum_{u\in V}\exp(X_u\cdot X_v)} \quad (5)$$

其中，X_v是节点v的向量表示。

在本文中，通过训练skip-gram模型将关系网络中的每个节点嵌入一个d维的向量空间，即每条借贷记录都可以得到一个d维的向量表示。

skip-gram模型训练时输入的是多个节点对，在利用skip-gram模型进行向量学习之前，需要获取每个节点与其局部邻居节点的节点对。在本文中，输入skip-gram模型中的就是借贷记录节点对。

对于网络中的一个借贷记录节点v，将其作为游走的首节点，然后从节点v随机走到其任一邻居节点c_1，然后从c_1随机游走到c_1的任一邻居节点c_2，以此类推。设置一个随机游走的长度l，当从v随机游走的序列

表2 新增申请记录

编号	时间	姓名	公司	住址
x_6	t_6	Lucy	C3	Addr1
x_7	t_7	Sandy	C2	Addr3

长度等于l时，停止游走，那么从节点v通过随机游走就可以得到一个借贷记录节点序列$S=vc_1c_2\cdots c_l$。重复此过程，依次选取网络中的每个节点作为随机游走的首节点，这样完成了以网络中每个节点作为游走首节点的过程后就得到了$|V|$条长度为l的随机游走序列。为了增加样本的个数，随机游走的过程可以重复多次，设置一个重复游走的次数r。通过重复r次以网络中每个节点作为游走首节点的随机游走过程后，笔者得到了$r|V|$条随机游走的节点序列，这些序列也可以看作多条申请记录序列。

为了获得交易记录节点对(v,u)，设置局部邻居节点范围大小h，并设置一个大小为$2h+1$的滑动窗口，利用这个滑动窗口在每条游走的借贷记录节点序列上进行滑动，每滑动一次，就获得了一个窗口序列$\{v_{i-h},\cdots,v_{i-1},v_i,v_{i+1},\cdots,v_{i+h}\}$，将中间节点$v_i$作为中心节点，将其前面$h$个节点和后面$h$个节点看作节点$v_i$的局部邻居节点，这样每滑动一次就可以获得$2h$个节点对$\{(v_i,v_{i-h}),\cdots,(v_i,v_{i-1}),(v_i,v_{i+1}),\cdots,(v_i,v_{i+h})\}$，通过固定大小的滑动窗口在每条游走序列上进行滑动，就得到了训练skip-gram模型的样本集合。

在本文中，笔者采用nod2vec[26]中随机游走的方式，该方法设置两个控制参数p和q，假设之前一步刚刚从节点v_i游走到节点v_j，当前正游走在节点v_j上，现在节点v_j不是随机选择一个邻居进行游走，而是根据游走转移概率π_{jk}游走到下一个节点v_k，设置$\pi_{jk}=\mu(i,k)\cdot w_{jk}$，其中$w_{jk}$是节点$v_j$和节点$v_k$

之间边的权重，$\mu(i,k)$ 可表示为：

$$\mu(i,k)=\begin{cases}\frac{1}{p}, d_{ik}=0\\ 1, d_{ik}=1\\ \frac{1}{q}, d_{ik}=2\end{cases} \quad (6)$$

其中，d_{ik}表示节点v_i和v_k间的最短距离，只能属于{0,1,2}，参数p,q相当于调节深度优先和宽度优先搜索的程度。从节点v_i游走到节点v_j后，应该再从节点v_j游走到其某一个邻居节点v_k，当p过小时，从节点v_j随机游走再次返回节点到v_i的概率会变大，即v_k=v_i的概率会增加，如果v_k=v_i，则下一次又会从v_i随机游走到一个邻居节点，这类似于网络中的广度搜索；当q的值过小时，从节点v_i游走到节点v_j后，再从v_j游走到一个不等于v_i的邻居节点v_k的概率会增加，这类似于网络中的深度优先搜索。在本文中的随机游走过程中，其随机转移概率是由边的权重和网络搜索参数共同决定的。

（3）预测批处理

不同于在线支付等网络欺诈检测对实时性的要求，互联网借贷通常存在一定的审核期。同时，利用网络嵌入技术，很难实现实时的欺诈风险预测（即每有一笔新的借贷申请就立即判断是否为欺诈申请），而且这种实时的欺诈检测也是不必要的。在本文中，笔者提出了一种借贷申请批处理的方法。

设置一个批处理的时间$\delta(\delta<<\alpha)$，每隔δ时间，对此期间产生的所有借贷申请进行欺诈预测。在t时刻对当前所有的借贷记录进行了处理，在此后的δ时间内，每产生一条新的记录，只更新借贷关系网络，不进行网络嵌入和欺诈预测的工作。在$t+\delta$时刻的关系网络为$G_{t+\delta}$，此时网络中的节点V分为两部分，一部分是从t时刻到$t+\delta$时刻之间生成的节点集合V_{test}，对于任意的节点$v_i \in V_{\text{test}}$，其时间戳$t_i \in [t,t+\delta]$。另一部分的节点集合是$V_{\text{train}}=V \setminus V_{\text{test}}$，假设关系网络最近一次进行周期性滑动窗口更新的时间为t_k，则对于任意节点$v_i \in V_{\text{train}}$，其时间戳$t_i \in [t_k-\alpha,t]$。

在$t+\delta$时刻，将此时的关系网络$G_{t+\delta}$输入网络嵌入模型中，对于任一节点$v \in V$会得到其对应的向量表示。将V_{train}中节点的向量和其对应的记录标签输入分类器模型中，训练一个分类器模型。模型训练完成后，将V_{test}中节点的向量输入训练好的分类器模型中，对于任一节点$v_i \in V_{\text{test}}$，模型会输出其对应的借贷记录x_i的欺诈风险值。设置一个欺诈风险阈值threshold，高于这个阈值的申请记录就可以看作欺诈借贷，拒绝给此类申请提供借贷服务，低于threshold的记录就可以看作正常的借贷申请，欺诈风险较小。

WEB算法的描述如下。

输入：借贷申请流S，上次周期性窗口滑动时间t_u，上次批处理时间t_p。

输出：S中每一笔借贷申请是否为欺诈（0或1）。

for each $x_i \in S$

更新关系网络$v_i \Leftarrow x_i$，$G_i \Leftarrow G_{i-1}$；

if $t_u+\alpha=t_i$ then

滑动时间窗口，删除网络中时间戳小于$t_i+\beta-\alpha$的节点和对应的边；

for each $v_j \in G_i$

$t_j \in [t_i+\beta-\alpha,t_i]$；

end for

$t_u=t_i$

end if

if $t_p+\delta=t_i$ then

利用随机游走和skip-gram学习网络G_i中每个节点的向量表示；

划分出训练集V_{train}和批处理测试集V_{test}；

for each $v_j \in V_{\text{train}}$

$t_j \in [t_u+\beta-\alpha,t_p]$；

end for

for each $v_j \in V_{test}$

$t_j \in [t_p, t_i]$;

end for

利用V_{train}中节点的向量表示和标签训练一个分类器模型;

将V_{test}输入分类器中进行批预测，输出每条借贷申请的欺诈风险值集合;

for each $r \in R$

if $r \geqslant threshold$ then

该条借贷申请为欺诈申请;

return 1;

else

该条借贷为正常借贷申请;

return 0;

end if

end for

$t_p = t_i$;

end if

end for

输出借贷申请流S中每条申请是否为欺诈申请;

4 系统架构

图3所示是本文提出的WEB系统的架构，它主要包括3个主要的部分。

(1)网络更新

在当前t时刻，需要根据用户的历史记录S_t构建一个借贷关系网络G_t，该网络能够显性地反映不同记录之间的关系。在此后的β时间内，每产生一条新的记录，在网络中添加一个新的节点和与该节点相关的边。在β时间后，滑动大小α的时间窗口，删除时间戳小于$t+\beta-\alpha$的节点和与其相关的边。利用基于周期性滑动窗口的网络更新方法既能使得最新的记录实时地更新到网络中，又能在特定时刻删除一部分不必要的网络元素。在实际业务中，通常将时间窗口的大小设置为6个月，滑动周期的大小设置为15天。

(2)网络嵌入

为了摆脱专家经验和传统网络分析方

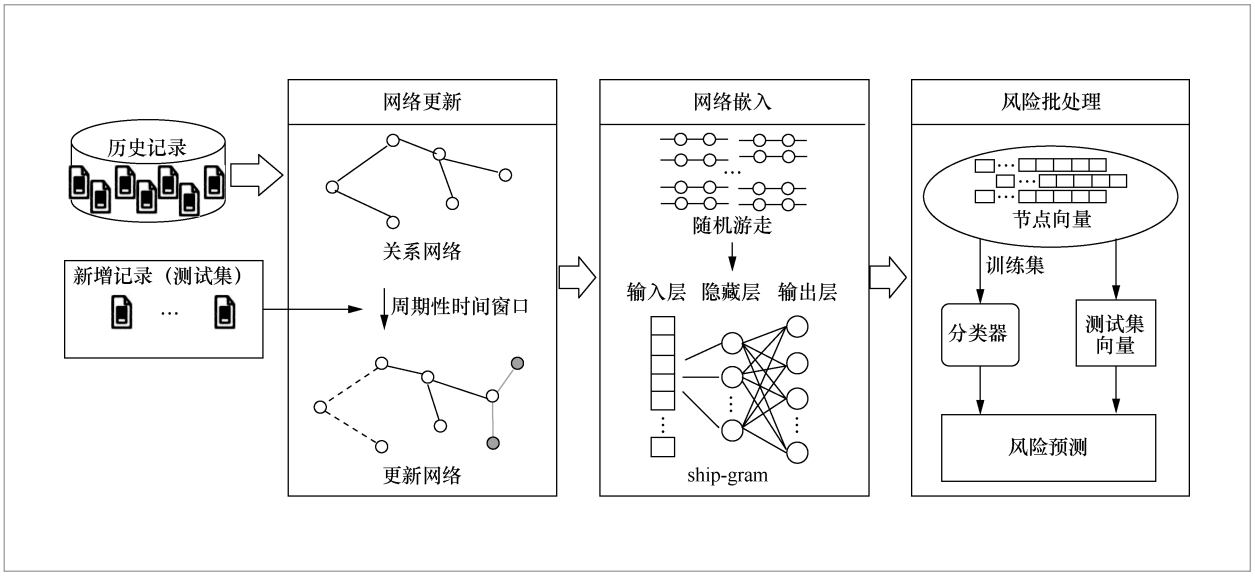


图 3 WEB 系统架构

法的弊端，本文利用网络嵌入的方法提取出借贷网络中隐含的关联特征。利用带权重的随机游走方式和skip-gram模型能够将每条申请记录嵌入低维的向量空间中，利用向量空间统一地表示每条申请记录。向量空间能够隐含地表示网络中的关系与特征，不需要进行传统网络分析中的大量特征工程的工作。

（3）风险批处理

历史的申请记录通常是有标签的，笔者对历史交易记录的向量进行建模，训练一个分类器模型就可以对新产生的借贷申请进行风险预测。每次在批处理时间间隔δ后，将当前的关系网络输入skip-gram模型中，学习每个节点的向量表示，然后利用δ时间间隔之前的节点和记录标签训练一个分类器模型，并对δ期间的借贷记录进行风险预测。在实际业务中，根据不同平台对实时性的要求，批处理时间通常是不同的，考虑到网络欺诈借贷的聚集性，δ通常设置为3天。

5 实验结果与分析

5.1 数据描述

实验数据集是从某金融借贷平台收集的1 516 995条互联网借贷数据，时间跨度为2015年1月1日到2017年7月31日。按时间顺序对数据集进行划分，将2017年7月1日之前的数据作为训练集，将2017年7月1日至31日的数据作为测试集。利用2017年7月1日之前的所有记录建立一个原始的关系网络，原始关系网络中有1 467 690个节点，即2017年7月1日之前一共有1 467 690条借贷申请记录，其中只有280 574条记录有真实的标签（0为正常，1为欺诈），超过80%的样本没有标签。在有标签的样本中只有14 574条为欺诈样本，占总样本的比例小于1%。为了便于存储大规模的网络结构，本工作使用Neo4j数据库存储构建的关系网络。

5.2 评价指标与阈值选择

一般来说，评价二元分类器性能的指标有很多，如AUC值（OC曲线下面积）、F-measure度量等。然而，这些指标不能直接反映模型的影响，特别是在数据不平衡的情况下。考虑到实际使用情况，笔者使用精确率、召回率和打扰率作为评估指标，定义如下：$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}}$，$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}}$，$\text{FPR}=\frac{\text{FP}}{\text{TN}+\text{FP}}$，其中，TP、FP、TN和FN分别表示真阳率、假阳率、真阴率和假阴率。

在欺诈检测场景中，目标不仅是检测更多的欺诈借贷，而且要减少误检测的数量。由于分类模型通常输出欺诈交易的风险概率，因此需要设置一个阈值来确定是否发生欺诈。阈值实际上提供了精确率和召回率之间的权衡，对于不同的阈值，精确率、召回率和打扰率都会发生变化，并且对于不同的分类器，阈值可能是不同的。

在本文中，笔者使用KS值作为选择阈值的原则。假设测试集中共有n个测试样本，经过模型判别后每个样本都会输出一个风险概率值，将n个风险值从小到大排列为$\hat{Y}=\{\hat{y}_1,\hat{y}_2,\cdots,\hat{y}_n\}$，依次选择$\hat{Y}$中的值作为阈值，并计算不同阈值下的召回率和打扰率为：

$$\widehat{\text{Recall}}=\{\text{Recall}_1,\text{Recall}_2,\cdots,\text{Recall}_n\} \quad (7)$$

$$\widehat{\text{FPR}}=\{\text{FPR}_1,\text{FPR}_2,\cdots,\text{FPR}_n\} \quad (8)$$

则KS值为不同阈值下召回率和打扰率差值的最大值，可以表示为：

$$\text{KS}=\max(\text{Recall}_i-\text{FPR}_i),i=1,2,\cdots,n \quad (9)$$

则分类器的阈值可以表示为：

$$\text{threshold} = \hat{y}_i * I\left(\text{KS} = \left(\text{Recall}_i - \text{FPR}_i\right)\right), i = 1,2,\cdots,n \quad (10)$$

其中，$I(\cdot)$是指示函数（indicator function）。KS值可用于评估模型风险区分的能力，KS值越大，表示该模型能够更好地区分欺诈样本与正常样本。

5.3 分类器选择

利用网络嵌入技术可以将网络中的每个节点嵌入低维的向量空间，利用向量表达网络中的关联特征，在完成特征表征学习后，需要利用机器学习的分类器模型进行欺诈预测。为了选择适合WEB系统的分类器模型，在本节比较当前几种主流分类器的性能，包括XGBoost、随机森林、KNN、SVM以及逻辑回归（logistics regression）。参数设置为d=128，h=3，p=1，q=1，时间窗口α为6个月，滑动周期β为15天，批处理时间δ为3天。**图4**所示为不同分类器在精确率、召回率、打扰率和KS上的结果。

从**图4**可知，性能最好的是XGBoost，其精确率超过60%，召回率超过40%，KS值接近40%，而打扰率只有5%，精确率、召回率和KS值均大于其他分类器的测试结果，并且打扰率较其他分类器更小，这意味着利用XGBoost分类器在能发现更多欺诈借贷的同时，可打扰更少的正常借贷申请。随机森林的结果与XGBoost相差很小，其次是KNN，性能最差的是SVM和逻辑回归分类器。逻辑回归分类的打扰率接近10%，这表明会打扰到接近10%的正常借贷申请，导致KS值很小，模型的风险区分能力很小。根据实验的结果可知，将XGBoost作为WEB系统中的分类器模型能够实现更好的欺诈预测性能。

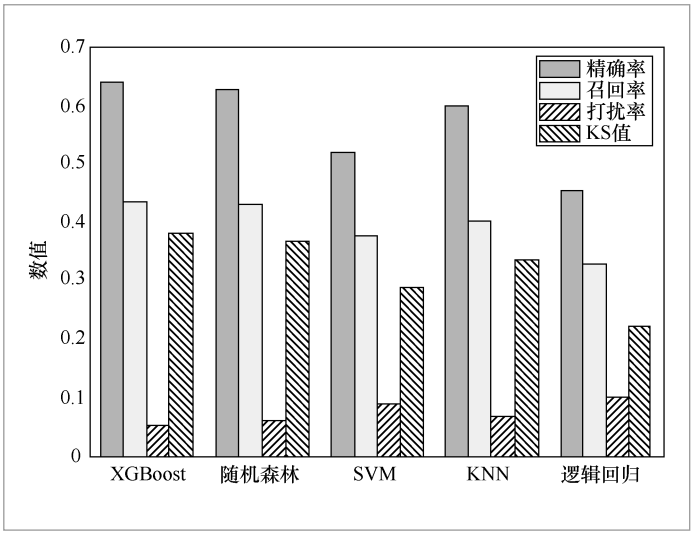


图 4 分类器性能比较

5.4 网络分析比较

在本节，将基于网络嵌入的方法和传统网络分析的方法进行比较，这2种方法都是将XGBoost作为基本的分类器模型。

- 传统网络分析：在利用传统的网络分析的方法中，需要从所有数据构建的大型网络中提取有效的网络特征。通过结合网络分析与专家经验，对于每条记录，提取15个有效的网络特征（如节点的一阶邻个数、二阶邻个数等），然后利用这些网络特征和记录标签训练一个XGBoost模型。当有一笔新的借贷申请产生时，更新关系网络，并从网络中提取该记录的15个特征，输入训练好的XGBoost模型中，模型可以得到当前记录的一个风险值。
- 网络嵌入：利用本文提出的网络嵌入方法进行互联网借贷欺诈检测。
- 网络嵌入+传统网络分析：将传统网络分析方法和网络嵌入方法提取的特征相结合，用于训练分类器模型，并对最新产生的借贷申请进行欺诈风险判断。

图5比较了两种方法在2017年7月的数

据集上的测试结果，网络嵌入方法检测性能接近于传统网络分析的方法。虽然传统网络分析的方法能够检测出更多的欺诈样本，但是也打扰了更多的正常借贷申请；并且网络嵌入技术只利用了小型的同质网络就达到了很好的效果，而基于传统网络分析的方法是在大型的关系网络中进行分析的，需要消耗很大的存储与计算资源，算法复杂度较高。

通过将2种方法结合，召回率和KS值得到了大幅的提高，见**表3**。两者结合的召回率比传统网络分析的方法提高了约8%，比网络嵌入的方法提高了13%；KS 值比传统网络分析的方法提高了5%，比网络嵌入的方法提高了接近10%。这意味着通过结合，可以检测出更多的欺诈样本，并且训练的模型能够更好地区分正常样本与欺诈样本。

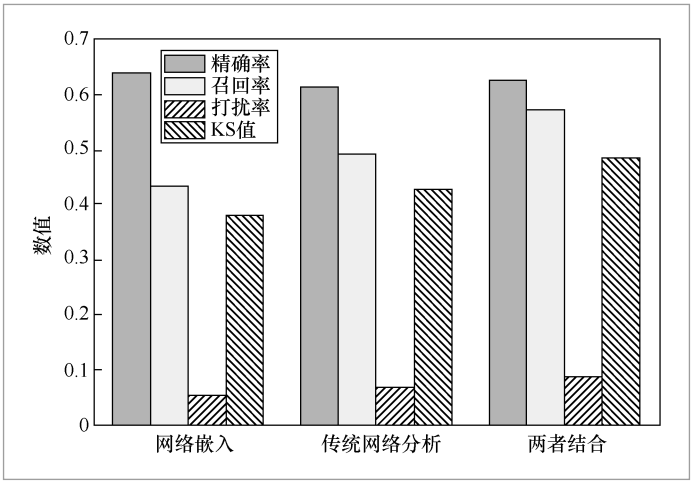


图 5　网络嵌入与传统网络分析方法的比较结果

表 3　3 种欺诈风险预测方法的比较结果

检测方法	精确率	召回率	打扰率	KS值
网络嵌入	0.638 2	0.434 2	0.053 9	0.380 2
传统网络分析	0.614 3	0.495 4	0.068	0.426 9
两者结合	0.623 6	0.570 5	0.086 1	0.484 4

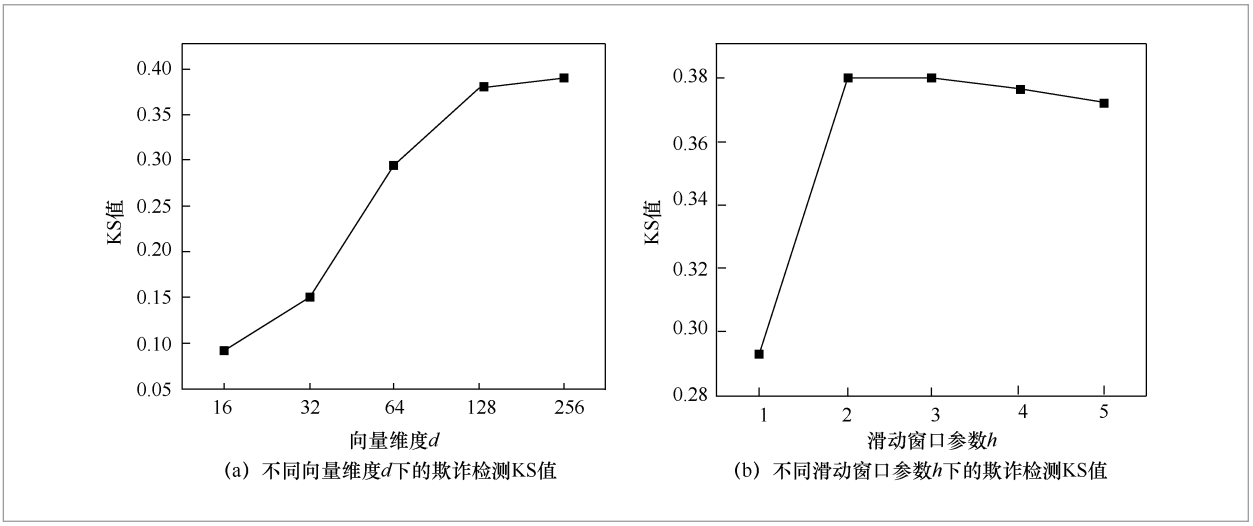
同时笔者发现，将传统网络分析与网络嵌入方法相结合，性能可比传统网络分析的性能有大幅提高，这证明了网络嵌入技术能够挖掘出传统网络分析方法无法提取的特征。通常，传统网络分析方法对网络中的显性特征比较敏感，而网络嵌入技术更能够挖掘出网络中的隐性关联特征。

5.5 参数分析

利用网络嵌入技术进行节点向量化表达时，主要的参数是设置向量的维度d和在随机游走序列上进行采样的滑动窗口参数h，**图6**表示不同参数下欺诈借贷检测的KS值。

利用网络嵌入技术进行节点向量表达时，向量的维度通常设置为2的整数次幂，在**图6（a）**中，设置了5个不同的向量维度，并比较它们的KS值。当向量维度过低时，通常很难对网络进行完整的表达；当向量维度过高时，通常会增加训练的复杂度。当d=16时，其KS值低于10%，无法有效地学习到网络中的关联关系；当d=256时，虽然KS的值比较高，但是与d=128时的KS值只有很小的差距。为了既能对网络进行完整的表达，又能降低网络嵌入的复杂度，在本文中，d=128是最好的选择。

利用网络嵌入技术，能够学习到网络的结构相似性。在本文中，利用网络嵌入技术可以学习到不同借贷申请之间的局部关联性，通过设置不同的滑动窗口参数h，能够学习到h阶邻居的关联关系。在**图6（b）**中，设置了5个不同的h值，并比较它们的KS值。从**图6（b）**可以看出，当h=2时，欺诈检测的性能最好，这说明欺诈借贷之间存在着一阶或二阶关联性（当h=2时能够学习到最多的二阶关联性），群体欺诈的聚集度较高。随着h值的增加，网络嵌入能够学



(a) 不同向量维度d下的欺诈检测KS值　(b) 不同滑动窗口参数h下的欺诈检测KS值

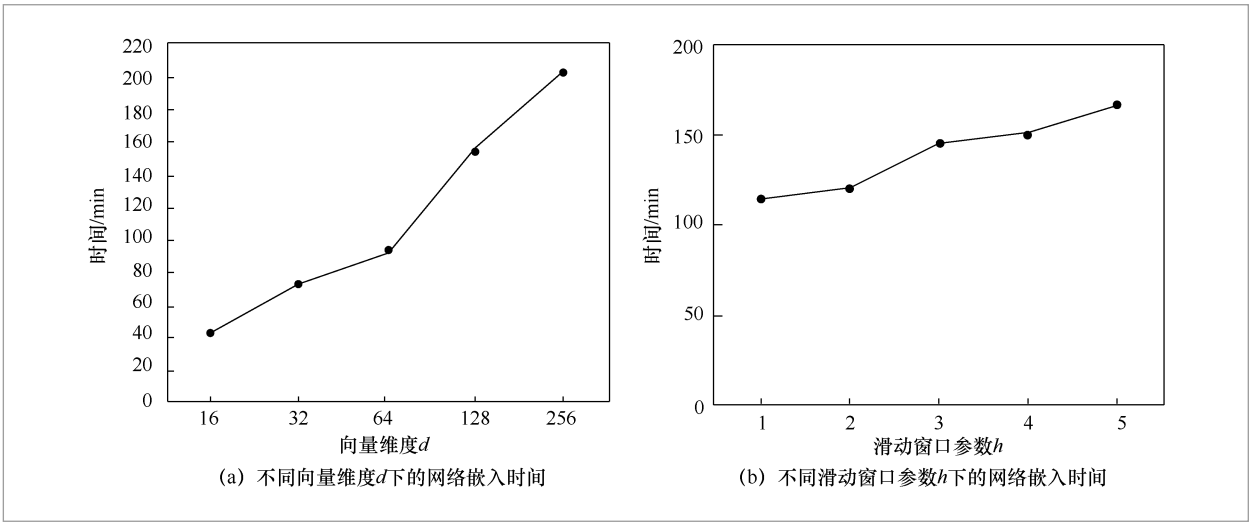
图 6　不同参数下欺诈借贷检测的 KS 值

习到更高阶的邻居相似性，但同时也会对欺诈检测造成干扰。

向量的维度大小和滑动窗口的参数不仅影响模型的性能，同时也影响网络嵌入模型的训练时间，图7(a)展示了在不同的向量维度下的网络嵌入的时间，可以看出，d的值加倍时，模型的训练时间增长得较快。图7(b)表示了不同的滑动窗口下的模型训练时间，可以看出，滑动窗口的大小对网络嵌入模型训练时间的影响较小。

6 结束语

关联图谱正逐渐成为一种主流的欺诈检测方法之一，它能够有效地表示不同实体间的关联关系。利用传统网络分析的方式对关联图谱进行特征提取时，需要研究



(a) 不同向量维度d下的网络嵌入时间　(b) 不同滑动窗口参数h下的网络嵌入时间

图 7　不同参数下的网络嵌入时间

人员具备一定的经验，并且在大规模的网络中，传统网络分析技术的算法复杂度较高。本文将网络嵌入技术创新性地应用到了互联网借贷欺诈风险预测的领域，给基于关联图谱的欺诈风险预测提供了新的启发。网络嵌入技术能够利用向量对网络进行表达，降低了网络复杂度。实验证明，该种方法能够有效地挖掘出网络中的隐性关联特征。

本文使用的是基于同质网络的嵌入技术，虽然在一定程度上可满足互联网借贷欺诈风险预测的任务，但丢失了网络中的很多信息，如边的类型等。利用异质网络结构可保留更多的网络信息，但其嵌入复杂度也随之大幅增加。在下一步工作中，笔者将着力于运用和设计异质网络嵌入技术，在保留更加全面的互联网借贷欺诈特征的前提下优化算法，以降低执行复杂度。

参考文献:

[1] SONG M, WANG J. An objective measurement of information value usingapplication traces in infomediary: A case study of credit reporting system in China[C]// The 20th International Conference on Information Quality(ICIQ2015), July 24, 2015, Cambridge, USA. [S.l.:s.n.], 2015.

[2] XIE S, YU P S. Next generation trustworthy fraud detection[C]// The 4th IEEE International Conference on Collaboration and Internet Computing, October 18-20, 2018, Pennsylvania, USA. Piscataway: IEEE Press, 2018: 279-282.

[3] XUAN S Y, LIU G J, LI Z C. Refined weighted random forest and its application to credit card fraud detection[C]// The 7th International Conference on Computational Data and Social Networks, December 18-20, 2018, Shanghai, China. Heidelberg: Springer, 2018: 343-355.

[4] BHATTACHARYYA S, JHA S, THARAKUNNEL K, et al. Data mining for credit card fraud: a comparative study[J]. Decision Support Systems, 2011, 50(3): 602-613.

[5] HOOI B, SHIN K, SONG H A, et al. Graph-based fraud detection in the face of camouflage[J]. ACM Transactions on Knowledge Discovery from Data, 2017, 11(4): 1-26.

[6] CAO B, MAO M, VIIDU S, et al. Hitfraud: a broad learning approachfor collective fraud detection in heterogeneous information networks[C]// The 2017 IEEE International Conference on Data Mining, November 18-21, 2017, New Orleans, USA. Piscataway: IEEE Press, 2017: 769-774.

[7] MAO R, LI Z, FU J. Fraud transaction recognition: a money flow network approach[C]// The 24th ACM International Conference on Informationand Knowledge Management, October 18-23, 2015, Melbourne, Australia. New York: ACM Press, 2015: 1871-1874.

[8] MCGLOHON M, BAY S, ANDERLE M G, et al. SNARE: a link analytic system for graph labelingand risk detection[C]// The 15th ACM SIGKDD International Conferenceon Knowledge Discovery and Data Mining, June 28-July 1, 2009, Paris, France. New York: ACM Press, 2009: 1265-1274.

[9] CUI P, WANG X, PEI J, et al. A survey on network embedding[J]. IEEE Transaction on Knowledge Data Engineering, 2019, 31(5): 833-852.

[10] VLASSELAER V V, BRAVO C, CAELEN O, et al. APATE: a novel approach for automated credit card transaction fraud detection using network-based extensions[J]. Decision Support Systems, 2015, 75: 38-48.

[11] LIANG C, LIU Z Q, LIU B, et al. Who

stole the postage? Fraud detection in return-freight insurance claims[C]// The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 19-23, 2018, London, UK. New York: ACM Press, 2018.

[12] LI Y, SUN Y H, CONTRACTOR N. Graph mining assisted semi-supervised learning for fraudulent cash-out detection[C]//The 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, July 31-August 3, 2017, Sydney, Australia. New York: ACM Press, 2017: 546-553.

[13] LEBICHOT B, BRAUN F, CAELEN O, et al. A graph-based, semi-supervised, credit card fraud detection system[C]// International Workshop on Complex Networks and their Applications, November 29 - December 1, 2017, Lyon, France. Heidelberg: Springer, 2017.

[14] LU P, LIN R H. Fraud phone calls analysis based on label propagation community detection algorithm[C]// 2018 IEEE World Congress on Services, July 2-7, 2018, San Francisco, USA. Piscataway: IEEE Press, 2018: 23-24.

[15] GANGOPADHYAY A, CHEN S. Health care fraud detection with community detection algorithms[C]// 2016 IEEE International Conference on Smart Computing, May 18-20, 2016, St. Louis, USA. Piscataway: IEEE Press, 2016.

[16] KIM J, KIM H J, KIM H. Fraud detection for job placement using hierarchical clusters-based deep neural networks[J]. Applied Intelligence, 2019, 49(8): 2842-2861.

[17] HAMILTON W L, YING R, LESKOVEC J. Representation learning on graphs: methods and applications[J]. IEEE Data Engineering Bulletin, 2017: 52-74.

[18] OU M, CUI P, PEI J, et al. Asymmetric transitivity preserving graph embedding[C]// The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 13-17, 2016, San Francisco, USA. New York: ACM Press, 2016: 672-681.

[19] WANG X, CUI P, WANG J, et al. Community preserving network embedding[C]// The 31st AAAI Conference on Artificial Intelligence, February 4-9, 2017, San Francisco, USA. Palo Alto: AAAI Press, 2017: 203-209.

[20] MIKOLOV T, CHEN K, CORRADO G, et al. Efficient estimation of word representationsin vector space[C]// The 1st International Conference on Learning Representations, May 2-4, 2013, Scottsdale, Arizona. [S.l.:s.n.], 2013.

[21] PEROZZI B, AL-RFOU R, SKIENA S. Deepwalk: online learning of social representations[C]// The 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 24-27, 2014, New York, USA. New York: ACM Press, 2014: 701-710.

[22] TANG L, LIU H. Uncovering cross-dimension group structures in multi-dimensional networks[C]// SDM workshop on Analysis of Dynamic, Networks International AAAI Conference on Connecting Corresponding Identities Across Communities, May 2, 2009, Calgary, Cananda. Palo Alto: AAAI Press, 2009.

[23] TANG J, QU M, WANG M Z, et al. LINE: large-scale information network embedding[C]// The 24th International Conference on World Wide Web, May 18-22, 2015, Florence, Italy. [S.l.:s.n.], 2015: 1067-1077.

[24] WANG D X, CUI P, ZHU W W. Structural deep network embedding[C]// The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 13-17, 2016, San Francisco, USA. New York: ACM Press, 2016: 1225-1234.

[25] CAO S S, LU W, XU Q K. Deep neural networks for learning graph representations[C]// The 30th AAAI Conference on Artificial Intelligence, February 12-17, 2016, Phoenix, Arizona.

Palo Alto: AAAI Press, 2016: 1145-1152.
[26] GROVER A, LESKOVEC J. Node2vec: scalable feature learning for networks[C]// The 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 13-17, 2016, San Francisco, USA. New York: ACM Press, 2016: 855-864.

作者简介

王成(1980-),男,同济大学计算机科学与技术系教授,主要研究方向为网络服务优化与安全、互联网金融反欺诈和网络空间异常事件检测研究。

舒鹏飞(1994-),男,同济大学计算机科学与技术系硕士生,主要研究方向为数据挖掘、机器学习和欺诈检测。

收稿日期: 2019-09-20
通信作者: 王成, cwang@tongji.edu.cn
基金项目: 国家自然科学基金资助项目(No.61972287, No.61571331);工业和信息化部工业互联网创新发展工程项目(No.[2018]282);霍英东教育基金会高等院校青年教师基金(No.151066);中央高校基本科研业务费专项资金资助项目(No. kx0137020181527);上海市青年拔尖人才开发计划

Foundation Items: The National Natural Science Foundation of China(No.61972287, No.61571331), The Major Project of Ministry of Industry and Information Technology of China(No.[2018]282), Fok Ying-Tong Education Foundation for Young Teachers in the Higher Education Institutions of China(No.151066), The Fundamental Research Funds for Central Universities (No.kx0137020181527), Municipal Human Resources Development Program for Outstanding Young Talents in Shanghai.