基于行为特征分析的微博恶意用户识别

夏崇欢 李华康 孙国梓

(南京邮电大学计算机学院软件学院 南京 210003)

摘 要 近年来,社交网络数据挖掘作为物理网络空间数据挖掘的一大热点,目前在用户行为分析、兴趣识别、产品推荐等方面都取得了令人可喜的成果。随着社交网络商业契机的到来,出现了很多恶意用户及恶意行为,给数据挖掘的效果产生了极大的影响。基于此,提出基于用户行为特征分析的恶意用户识别方法,该方法引入主成分分析方法对微博网络用户行为数据进行挖掘,对各维度特征的权重进行排序,选取前六维主成分特征可以有效识别恶意用户,主成分特征之间拟合出的新特征也能提升系统的识别性能。实验结果表明,引入的方法对微博用户特征进行了有效的排序,很好地识别出了微博社交网络中的恶意用户,为其他方向的社交网络数据挖掘提供了良好的数据清洗技术。

关键词 恶意用户,机器学习,微博,主成分分析法(PCA),特征提取

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.12.017

Microblogging Malicious User Identification Based on Behavior Characteristic Analysis

XIA Chong-huan LI Hua-kang SUN Guo-zi

(School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract In recent years, as a hotspot in data mining of physical network, social network data mining has made gratifying achievements in the current user behavior analysis, interest recognition and product recommendation. With the advent of social networking business opportunities, many malicious users and malicious behaviors have also emerged, which have a great impact on the effectiveness of data mining. A malicious user identification method based on user behavior feature analysis was proposed. This method uses the principal component analysis(PCA) to mine the user behavior data in microblogging network, and ranks the weight of each feature. It can effectively identify malicious users with first six-dimensional principal component features. The new features fitted by the principal component features are used to improve the recognition performance of the system. The experimental results show that the proposed method can effectively sort the microblogging user features and identify the malicious users in the microblogging social network, which provides a good data cleaning technique for social network data mining in other directions.

Keywords Malicious users, Machine learning, Microblogging, Principal component analysis(PCA), Feature extraction

1 引言

微博凭借其信息来源广、传播速度快、时效性强以及交互性好等特点,吸引了数以亿计的用户[1],而这些用户中存在恶意用户[2]。微博的恶意用户行为包括:发布有害链接(指向钓鱼网站和恶意网站的链接)、过度的关注行为(为了引起注意进行大量关注和取消关注的行为)、滥用@提醒功能骚扰其他用户、高频且重复发布微博、发布与微博内容无关的URL、单时间节点大量发布微博。恶意用户由于受自动化软件控制,软件设计灵活,其使用的语言不再是简单词汇的重复,而是带有较强的主观性、原创性与独特性的语言。这些特点使得恶意用户的仿真度较高,极易被人误认为是普通用户。如何识别并清除恶意用户对互联网的高效、良性发展有重要作用!

社交网络反恶意行为的技术可以分为恶意用户识别、交互以及排名权限。识别是指利用各种信息和特征来判断检测恶意行为和恶意用户,这种反恶意行为技术最常见;在恶意用户识别中,研究者从恶意用户内容行为特征和用户关系特征2个方面来进行恶意用户的挖掘。而在恶意用户内容行为特征提取工作中,研究者用一些简单的经验特征(粉丝数低、微博数低),或者利用原始特征通过拟合函数构造出一些新的用

到稿日期:2017-11-29 返修日期:2018-03-31 本文受国家自然科学基金青年项目(61502247),公安部重点实验室开放课题(2015DSJSYS001),江苏省高校自然科学研究面上项目(14KJB520028)资助。

夏崇欢(1991-),男,硕士生,主要研究方向为信息安全、大数据应用;**李华康**(1982-),男,博士,讲师,CCF会员,主要研究方向为智慧城市、大数据应用、互联网安全;**孙国梓**(1972-),男,博士,教授,CCF高级会员,主要研究方向为网络空间安全、电子数据取证,E-mail:sun@njupt.edu.cn(通信作者)。

户特征。相对于传统手工查找恶意用户的方法,这种方法简单高效,但提取出的此类特征对于分类精确率的贡献度和有效率还有待考证。

本文从恶意用户的行为特征提取角度出发,引入主成分分析算法对恶意用户的特征进行权重排序,提炼出用户的主成分特征。少数几个互不相关的主成分特征保留了用户特征的主要信息,实现了对数据的压缩和冗余数据的去除;再通过累积分布函数图,分析并验证了基于主成分分析方法提炼出的主成分特征对于恶意用户识别的优劣性。最后,基于决策树传统分类算法进行实验。实验结果表明,基于主成分分析方法提取的主成分特征以及主成分特征之间的拟合构造出的新特征,对恶意用户识别工作具有良好的效果。

本文第 2 节从相关领域介绍国内外现有的研究成果;第 3 节介绍如何利用主成分分析方法进行恶意用户特征提取;第 4 节详细分析基于提取出的主成分特征对于恶意用户识别的优劣性;第 5 节利用传统分类算法进行实验结果分析;最后总结全文并展望未来。

2 相关工作

一些研究者从恶意用户的行为内容特征提取入手进行研究。Chu 等[3]提出了一种通过构造信息熵,利用随机森林算法进行恶意用户判别的方法,其模型构建复杂、计算量大。文献[4]主要对微博内容进行了研究,在 Twitter 的恶意用户识别过程中,利用 E-mail、短信息、Web 等其他媒体中的用户文档,与 Twitter 中的文档共同组成跨媒体知识库模型,对 Twitter 中的恶意用户进行识别。Wang[5]提出了"用户权威度""含 URL 的微博比例"以及"微博重复率"等内容特征,将恶意用户的检测转化为机器学习的分类问题。Zheng 等[6]同样建立内容和行为特征集合,用分类算法对新浪微博中的恶意用户进行识别。张锡英等[7]提出了基于微博用户行为的恶意用户检测方法,相对于针对微博用户静态特征的方法,准确率有较大提升。Chu 等[8]分析了 50 万个 Twitter 用户的账号信息、发帖行为以及博文内容,并构建了一个分类系统用以计算该用户被划分为真实用户、机器人以及半机器人的概率。文献[9]利用恶意用户在短时间内重复垃圾信息的行为特点,从重发发布行为和微博内容两个方面建模,对新浪微博中的恶意用户进行识别。Mccord 等[10]利用用户与博文特征设计分类器区分正常用户与恶意用户。Antonakaki 等研究了故意滥用热门话题和其他微博用户的特征,提出了一个垃圾用户和垃圾内容的简易分类器[11]。Perveen 等提出了基于情感内容的垃圾用户检测模型,着重分析了微博文本中的情感词项、符号、表情等[12]。Fu 等[13]提出了谨慎度的概念,对相关的行为特征值进行修正,有效解决了恶意用户相互关注的问题。

另一些研究者考虑到微博的社交属性,将用户关系特征引入到恶意用户识别问题中。Moh 等[14]利用了 Twitter 用户的关注关系,通过信任传播机制来发现虚假用户。Becchetti 等[15]首次针对大规模无向图,给出了节点局部三角形数量近似统计方法,同时在 WEB SPAM-UK2006 数据集上统计了正常网站与垃圾网站局部三角形数量的分布情况,表明正常网站和垃圾网站的局部三角形数量分布存在差异性。文献[16]先后对微博中的用户关系特征和主题特征进行了建模,并在统一的模型中将两者无缝地结合在一起,达到了较好的识别结果。Zhang 等[17]提出将发布相同 Twitter 的用户联系起来以构建一个关系图并分析其密度。

更多的研究者将用户行为内容特征与用户关系特征相结合来对恶意用户进行识别。Benevenuto 等[18]对 Twitter 中的大量数据集进行分析,采用人工识别的方法建立标签集划分恶意用户和正常用户,并寻找标签集中用户的特征,建立内容属性和用户行为属性两个集合,利用分类算法对恶意用户进行识别,调整两个数据集的权重以提高分类效果。Hu 等[19]对微博中的用户关系特征和主题特征进行建模,并在统一的模型中将两者无缝地结合,利用 Nesterov 的方法[20]解决优化问题,并将该方法用于 Twitter 中的恶意用户识别,达到了较好的识别结果。刘勘等[21]提取了行为模式、微博内容、用户关系和发布平台 4 个维度上的 8 个特征属性,机器用户识别准确率高达 96.7%。

因此,在国内外的研究中还未尝试运用一种方法,可以有效地对各维度特征的权重进行排序,选取前几维特征就能进行分类识别,实现对特征数据的压缩和冗余数据的去除,提高特征提取的效率,从而有效地进行分类识别。

3 基于 PCA 方法的微博用户特征提取

3.1 PCA 简介

本文应用的主成分分析方法是目前应用得最广泛的特征提取方法之一,它是统计学中分析数据的一种有效的方法。主成分分析被广泛地应用于图像分析、数据压缩、模式识别和数据挖掘等领域。如在人脸识别中,可利用 PCA 对人脸图像进行特征提取和特征选择,它的基本思想是提取出高维数据空间中的主要特征,使数据在一个低维的特征空间中被处理,同时保持原始数据的绝大部分信息,从而解决数据空间维数过高的瓶颈问题。主成分分析方法就是提取数据的主要元素,从数学的角度来说就是寻找一组最能表达数据之间关系的基向量。PCA 作为一种无参数、无监督的特征提取算法,理解简单,易于实现。

3.2 基于 PCA 提取微博用户的特征原理

本文通过建立蜜罐账户、微博爬虫、网络购买恶意用户粉丝 3 种方式,来得到用于分析特征的原始数据。微博用户的原始数据的特征中存在一系列特征向量:用户 ID、屏幕名、性别、地区、关注数、粉丝数、微博数、等级、教育程度、创建时间等。设在微博用户数据集中有 n 个用户,每个用户有 p 个原始特征,则有:

$$X=\begin{bmatrix} x_{11} & \cdots & x_{1p} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{np} \end{bmatrix}=[X_1 \ \cdots \ X_p]$$

其中,$X_i=(x_{1i},\cdots,x_{ni})^{\mathrm{T}}, i=1,\cdots,p$。矩阵的一列代表 n 个不同的微博用户的某一维特征向量。

用 PCA 进行处理得到的第一个微博用户的新特征可以表示为 $y_i=Xw_i^{\mathrm{T}}$。微博用户新特征提取过程可以描述为当

微博用户原始数据投影到特征空间后，首先通过寻找正交变换向量 w_1，使 $y_1=Xw_1^{\mathrm{T}}$ 具有最大的方差，称 y_1 为新的用户特征的第一主分量(PC_1)；接着通过寻找正交变换向量 w_2，使 $y_2=Xw_2^{\mathrm{T}}$ 具有次大的方差，且 y_1 与 y_2 不相关，将 y_2 称为新的用户特征的第二主分量(PC_2)；以此类推，直到找到所有的新的用户特征主分量$\{y_i \mid i=1,2,\cdots,p\}$。

3.3　微博用户主成分特征的提取过程

根据数学理论，本文可以采取如下步骤来实现对微博用户的新特征的提取，从而实现对微博原始用户数据特征的降维。

首先建立一个微博用户-特征矩阵：

$$A=\begin{bmatrix} x_{11} & \cdots & x_{1p} \\ \vdots & \ddots & \vdots \\ x_{n1} & \cdots & x_{np} \end{bmatrix}$$

矩阵的一行代表一个微博用户的原始特征向量，矩阵的一列代表 n 个不同的微博用户的特征值。

根据 PCA 基本理论，首先计算矩阵 A 的协方差矩阵 R_A 的特征值，把得到的 R_A 的特征值按从大到小的顺序排列为 $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_p \geqslant 0$，相应的特征向量为 $e^1, e^2, \cdots, e^p$，有下列变化：

$$Y=AW^{\mathrm{T}}$$

其中，$W=[e^1,e^2,\cdots,e^p]$被称为正交变换矩阵，它将原来的矩阵 A 转换为 p 维正交矩阵 Y，此矩阵可以保留原始微博用户特征更多的信息。

实际上，少数几个新的用户特征主分量就可以满足提炼用户特征选择的需求，即令正交变换向量$\{w_i \mid i=1,2,\cdots,p\}$构成的正交变换矩阵 $W=[e^1,e^2,\cdots,e^p]$中的下标 $q \leqslant p$，输出新的用户特征主分量 $Y=(y_1,y_2,\cdots,y_q)$。这几个少数互不相关的主分量已经保留了新的用户特征的主要信息，实现了对数据的压缩和冗余数据的去除。

4　恶意用户的行为特征分析

基于上述 PCA 的特征提取后，根据主成分分析提取特征的理论原理，本文最终选择出前 6 个主成分特征：关注数(PCA_1)、粉丝数(PCA_2)、微博数(PCA_3)、关注数是否过千(PCA_4)、微博内容是否大量重复(PCA_5)、是否间隔特定时间发博(PCA_6)。利用指标函数来拟合人气指数、关注指数、微博受众指数这 3 个新的特征。接下来，本文使用 Python 绘制累积分布函数图(CDF)，并对所选特征进行分析，以验证所选的 9 个特征能否用来进行恶意用户的识别。在本节描绘的 CDF 图中，X 轴表示特征值的量值，Y 轴表示低于某个值的用户比例，比如，某一点在 X 轴上对应的值为 m，在 Y 轴上对应的值为 n，则该点表示特征值在 $0\sim m$ 之间的用户占总用户的 $n\%$。

本文采用人工方式对抓取到的数据集进行标注，选出正常用户 1200 位、恶意用户 300 位作为实验的专家样本，其中恶意用户记标为 1，正常用户标记为 0，利用 CDF 图对专家样本集进行所选特征的分析。

4.1　PCA 主成分特征分析

用户粉丝数与关注数代表用户的社交关系。恶意用户没有社交关系，理论上其粉丝数为 0。普通用户粉丝数的分布范围较广，个体差异大。恶意用户粉丝数主要集中在 100～200 的狭小区间，个体差异小。此外，恶意用户以提高其他用户粉丝量为目的，自身关注数必然较高，恶意用户想引起更多正常用户对自己的关注，以便扩散和传播自身恶意行为。关注数和粉丝数的 CDF 图如图 1 和图 2 所示。图中两条曲线在特征同等量值时所占比例存在明显区别，代表用户的粉丝数和关注数这两个特征在恶意用户和正常用户之间有较好的区分度，适用于识别恶意用户。

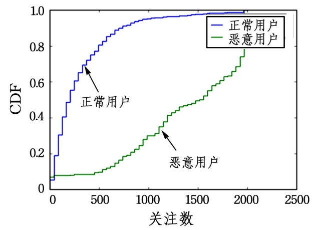

图 1　关注数 CDF 图

Fig. 1　CDF of number of attention

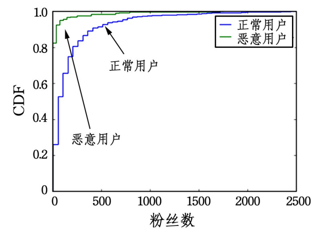

图 2　粉丝数 CDF 图

Fig. 2　CDF of number of fans

早期的恶意用户并不会发送微博，但为了逃避新浪微博的封杀，恶意用户开始升级。现有的新型恶意用户通过软件不定期更新并发送大量微博，而且其微博数远远超过大多数普通用户的微博数。微博数的 CDF 图如图 3 所示，图中两条曲线在特征同等量值时所占比例存在明显区别，代表用户的微博数这个特征在恶意用户和正常用户之间有较好的区分度，适合用于恶意用户的识别。

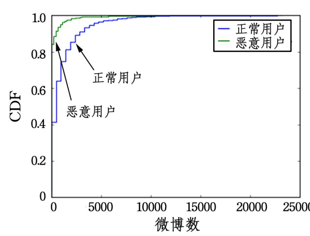

图 3　微博数 CDF

Fig. 3　CDF of number of microblogging

此外，每一个正常用户的关注角度和范围一般来说是有限的。关注数是否过千也可以作为特征选项，用于进行恶意用户识别。相比于正常用户，大部分恶意用户存在连续重复发布相同内容的微博的问题，以求更大力度地宣传和传播。微博内容是否大量重复这一项也可以作为特征选项，用于识别恶意用户。正常用户的微博主页不定时发布一些微博内容，这比较符合正常的发博规律，即时间的无规律性，是否间

隔特定时间发博这一项也可以作为特征选项用于恶意用户的识别。因为这3类特征数值为离散性,所以不做CDF图分析。

4.2 指标函数拟合新特征分析

除去上述6个主成分特征,本文利用指标函数拟合出了人气指数来更好地反映用户社交关系的组成,其定义为:

$$人气指数=\frac{粉丝数}{粉丝数+关注数}$$

普通用户与恶意用户的人气指数对比如图4所示。由图4可以看出,普通用户的粉丝数与关注数较为接近,反映了现实生活中"对等"的社交关系,而恶意用户的关注数远远大于其粉丝数,偏离了实际的社交关系网络。

相对地,还引入了关注指数,以进一步反映用户信息行为特征,其定义为:

$$关注指数=\frac{关注数}{关注数+粉丝数}$$

如图5所示,恶意用户一般会大量地关注其他用户,导致其关注数远多于粉丝数,因此恶意用户的关注指数高于普通用户。

图4和图5中,两条曲线在特征同等量值时所占比例存在明显区别,代表人气指数和关注指数这两个拟合特征在恶意用户和正常用户之间有较好的区分度,适合用于恶意用户的识别。

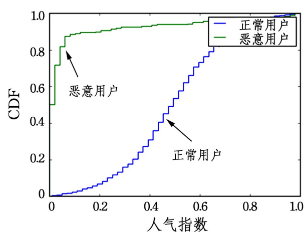

图4 人气指数CDF图

Fig.4 Weibo popularity index CDF

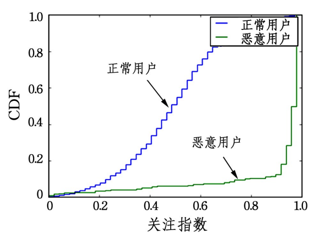

图5 关注指数CDF图

Fig.5 Weibo attention index CDF

本文引入微博受众指数来表明用户微博受众关系特征,其定义如下:

$$微博受众指数=\frac{微博数}{粉丝数}$$

普通用户与恶意用户的微博受众对比如图6所示。由图6可以看出,普通用户的微博数与粉丝数较为接近,客观地反映了普通用户现实生活中较平衡的发博习惯,而恶意用户为了扩大更多的信息传播,发博数远远多于其粉丝数,偏离了实际的社交发博习惯。

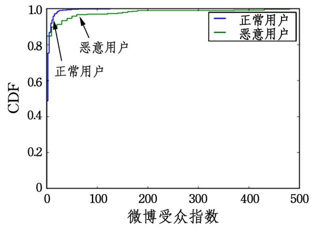

图6 微博受众指数CDF图

Fig.6 Weibo audience index CDF

图6中,两条曲线在特征同等量值时所占比例存在明显区别,代表拟合出的这个特征在恶意用户和正常用户之间有较好的区分度,适合用于恶意用户的识别。

5 基于行为特征的恶意用户识别系统

5.1 构造实验数据集

1)本文注册了30个蜜罐账户,成功吸引了300位粉丝。

2)本文经过爬虫程序的筛选,一共过滤得到了1667个恶意用户嫌疑人。

3)本文向6家网店购买了"粉丝服务"和"推广服务",一共获得了大约8000左右的恶意用户。

采用人工方式对抓取到的数据集进行标注,选出正常用户1200位、恶意用户300位作为实验的专家样本,其中恶意用户标记为1,正常用户标记为0。随机选取其中的20%作为测试样本,剩余的80%作为训练样本。

5.2 基于决策树算法的恶意用户识别

决策树(Decision Tree)属于多级决策系统。根节点是输入的整个微博用户专家样本数据集,分类规则由基于PCA方法提取出的主成分向量特征和拟合新特征等不同的特征确定,随着树的不断增长,用户数据集也被成功划分为正常用户或者恶意用户。先用80%的训练样本 X 进行分类器的训练,最后用20%的测试样本 Y 对分类器进行分类效果测试,本文微博用户分类生成决策树的一般过程是:

1)将基于PCA方法提取到的主成分特征和拟合函数新特征作为分支的特征集合 *feature_list*。树节点 t 与训练集 X 的特定子集 X_t 相关,X_{tN} 表示分类决策后判断为正常用户的子集,X_{tY} 是分类决策后判断为恶意用户的子集,且满足:

$$X_{tN}\cap X_{tY}=\varnothing$$

$$X_{tN}\cup X_{tY}=X_t$$

2)采用用户分支准则(Splitting Criterion),每一次划分的目的是使新子集中的用户比划分之前更"纯",即使原子集中能成功分类为正常用户和恶意用户的数目更多,"节点不纯度"记为 $I(t)$:

$$I(t)=\sum_{i=1}^{M}P(w_i|t)\log_2 P(w_i|t)$$

其中,$P(w_i|t)$ 表示节点 t 处属于 w_i 类的用户数占总用户的频度。其中,w_1 为正常用户,w_2 为恶意用户。在一次分支过程中,假设 N_{tY} 个用户被判断为恶意用户,并将其分到 X_{tY} 中,N_{tN} 个用户被判断为正常用户,并将其分到 X_{tN} 中,节点不纯度减少量为:

$$\Delta I(t)=I(t)-\frac{N_{tY}}{N_t}I(t_Y)-\frac{N_{tN}}{N_t}I(t_N)$$

其中，$I(t_Y)$和 $I(t_N)$代表节点 t_Y 和节点 t_N 的不纯度。

3)采用用户停止分支准则控制树的增长，若节点的分支被声明为叶子节点，则分支停止。停止分支依据两个判断准则：准则一是采取阈值 T，若全部可能的分支的 $\Delta I(t)$的最大值 $\Delta I(t)_{\max}<T$，则分支结束；准则二是当子集 X_t 足够小或 X_t 是纯的，即用户都能被分类，则停止分支。

4)确定类的用户分配规则，为每一个终止的节点指定所属的类，采取多数规则，使叶子节点 t 所属的类是 X_t 数目最多的类，即将叶子节点标记为 w_i，其中：

$$j=\arg\max_i P(w_i|t)$$

为了验证本文所引入的 PCA 方法能有效地将用户各维度行为特征的权重进行排序，相对于随机的原始特征组合，可以直接选取排在前列的主成分向量特征进行有效分类，对恶意用户的识别具有更好的效果。本文设置了 3 种特征选择场景进行实验，每一种实验场景的不同点在于选取的实验特征。

实验 1　随机地选取了原始微博用户数据中的 6 个特征进行实验，并将其作为分类器的输入特征，正常用户一共有 200 位，有 25 位被错判为恶意用户，恶意用户一共有 100 位，有 30 位被错判为正常用户。

实验 2　选取基于 PCA 提取出的前六维主特征，包括：关注数(PCA_1)、粉丝数(PCA_2)、微博数(PCA_3)、关注是否过千(PCA_4)、微博内容是否大量重复(PCA_5)、是否间隔特定时间发博(PCA_6)等。将选取的 6 个主特征作为分类器的输入特征，正常用户一共有 218 位，其中有 10 位被错判为恶意用户，恶意用户一共有 82 位，其中有 9 位被错判为正常用户。

实验 3　选取了基于 PCA 提取出的主成分特征以及主成分特征之间拟合构造出的新特征，总共九维向量特征，包括：关注数(PCA_1)、粉丝数(PCA_2)、微博数(PCA_3)、关注是否过千(PCA_4)、微博内容是否大量重复(PCA_5)、是否间隔特定时间发博(PCA_6)、人气指数、关注指数、微博受众指数。将这 9 个特征作为分类器的输入特征，正常用户一共有 233 位，其中有 9 位被错判为恶意用户，恶意用户一共有 67 位，其中有 5 位被错判为正常用户。

5.3　实验结果分析

通过分类器实验得到了每一种实验情况下的混淆矩阵图，并进一步计算出了每一种情况下的准确率和召回率，如表 1 所列。

表 1　各维度特征下决策树分类器的性能指标

Table 1　Performance indicators of decision tree classifiers under various dimensional characteristics

	性能指标	测试结果/%
随机原始六维特征	准确率	81.67
	召回率	70.00
PCA_1-PCA_6	准确率	93.67
	召回率	89.02
PCA_1-PCA_6 加上拟合特征	准确率	95.33
	召回率	92.54

结果显示，相比于随机组合的原始用户的六维特征通过 PCA 算法提取出的六维主成分特征的准确率和召回率的结果更好，而在增加主成分特征通过指标函数拟合出新特征后，准确率和召回率也均有所上升。基于以上实验数据结果可以说明，利用微博用户原始特征随机组合下的实验效果不能得到保证，而基于 PCA 提取出的主特征向量，有效地将微博用户各维度行为特征的权重进行了排序，可以直接选取排在前列的主成分向量特征进行分类实验，准确率和召回率有较好的结果。此外，增加利用主成分特征之间的指标函数拟合出的新特征，对提升系统的识别性能也有一定的效果。

结束语　本文提出了一种基于微博用户行为特征分析的恶意用户识别方法，该方法利用主成分分析法对微博网络用户行为数据进行挖掘，将各维度特征的权重进行排序，直接选取前六维主成分向量具有较好的分类效果，且引入主成分特征之间的指标函数拟合出的新特征以提升系统的识别性能。实验表明，通过 PCA 方法提取出的前几维主成分特征向量，以及增加主成分特征之间拟合出的新特征，均能有效地识别出微博恶意用户，从而有助于提升微博网络的其他应用，如基于可信关系的好友推荐等网络扩散研究等。由于收集到的样本质量和数量存在局限性，对基于 PCA 提取特征向量有所影响，接下来需要多考虑这方面的样本收集改进，争取提炼出更有效的主成分向量特征；此外，本文所提炼出的特征没有考虑时间维度对特征的影响，在目前的微博环境下，对于更高级别的恶意用户识别存在较大的问题，接下来的工作考虑根据时间维度的动态提炼出更适合的识别特征。

参 考 文 献

[1] WANG Y L,ZHANG M. Summary of the Current Research Status of Weibo in China [J]. Library Science Research,2014 (12):2-8.(in Chinese)
王莹莉，张敏. 国内微博研究现状综述[J]. 图书馆学研究，2014 (12):2-8.

[2] Wikipedia:Spamming[EB/OL]. [2017-03-25]. http://en.wikipedia.org/wiki/Spamming.

[3] CHU Z,GIANVECCHIO S,WANG H N,et al. Detecting Automation of Twitter Accounts:ARE you a human,bot,or cyborg? [J]. IEEE Transactions on Dependable and Secure Computing, 2012,9(6):811-824.

[4] ZHU X,TANG J,LIU H. Leveraging knowledge across media for spammer detection in microbiogging[C]// Proceedings of the 37th International ACM SIGIR Conference on Research & Development in Information Retrieval. ACM,2014:547-556.

[5] WANG A H. Don't follow me:Spam detection in Twitter[C]// Secrypt 2010-Proceedings of the International Conference on Security and Cryptography. 2010:1-10.

[6] ZHENG X,ZENG Z,CHEN Z,et al. Detecting spammers on social networks[J]. Neurocomputing,2015,159(C):27-34.

[7] ZHANG X Y,CHE X,TIAN X Y. A Malicious User Identification Method Based on Weibo User Behavior [J]. Natural Science Journal of Heilongjiang University,2014,10(1):250-254.(in Chinese)
张锡英，车鑫，田宪允. 一种基于微博用户行为的恶意用户识别方法[J]. 黑龙江大学自然科学学报，2014,10(1):250-254.

[8] CHU Z,GIANVECCHIO S,WANG H,et al. Who is tweeting on twitter:human,bot,or cyborg? [C]// Twenty-Sixth Computer Security Applications Conference. 2011:21-30.

[9] LI G C. Weibo spam user behavior modeling and screening [D]. Beijing:Beijing University of Posts and Telecommunications,2014.(in Chinese)
李冠辰.微博垃圾用户行为建模和甄别[D].北京:北京邮电大学,2014.

[10] MCCORD M,CHUAH M. Spam detection on twitter using traditional classifiers [C]// International Conference on Autonomic and Trusted Computing. 2011:175-186.

[11] ANTONAKAKI D,POLAKIS I,ATHANASOPOULOS E,et al. Social Network Analysis and Mining[J]. International Journal of Advanced Computer Science & Applications,2016,6(1):48.

[12] PERVEEN N,MISSEN M S,RASOOL Q,et al. Sentiment Based Twitter Spam Detection[J]. International Journal of Advanced Computer Science & Applications,2016,7(7):568-573.

[13] FU H,XIE X,RUI Y. Leveraging Careful Microblog Users for Spammer Detection[C]// Proceedings of the 24th International Conference on World Wide Web Companion. International World Wide Web Conferences Steering Committee,2015:419-429.

[14] MOH T S,MURMANN A J. Can you judge a man by his friends?-enhancing spammer detection on the twitter microblogging platform using friends and followers [M]// Information Systems,Technology and Management. Springer Berlin Heidelberg,2010:210-220.

[15] BECCHETTI L,BOLDI P,CASTILLO C,et al. Efficient semi-streaming algorithms for local triangle counting in massive graphs[C]// Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2008:16-24.

[16] HU X,TANG J,ZHANG Y,et al. Social spammer detection in microblogging[C]// Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence. AAAI Press,2013:2633-2639.

[17] ZHANG X,LI Z,ZHU S,et al. Detecting Spam and Promoting Campaigns in Twitter[J]. Acm Transactions on the Web,2016,10(1):4-8.

[18] BENEVENUTO F,MAGNO G,RODRIGUES T,et al. Detecting spammers on twitter [C]// International Joint Conference on Artificial Intelligence. 2010:1723-1728.

[19] HU X,TANG J,ZHANG Y,et al. Social spammer detection in microblogging [C]// International Joint Conference on Artificial Intelligence. 2013:1709-1714.

[20] NESTEROV Y. Introductory lectures on convex optimization [M]. IEEE Transactions on Dependable and Secure Computing,2007.

[21] LIU K,YUAN Y Y,LIU P. A Weibo Bot-users Indentification Model Based on Random Forest [J]. Acta Scientiarum Naturalium Universitatis Pekinensis,2015,10(2):10-13.(in Chinese)
刘勘,袁蕴英,刘萍.基于随机森林分类的微博机器用户识别研究[J].北京大学学报(自然科学版),2015,10(2):10-13.

(上接第 80 页)

[8] YI J,YANG S,CHA H. Multi-hop-based Monte Carlo Localization for Mobile Sensor Networks [C]// IEEE Communications Society Conference on Sensor,Mesh and Ad Hoc Communications and Networks. 2007:163-171.

[9] LI M,LUO T,XU H. Localization Algorithm Based on Anchor Node Select Model for Wireless Sensor Networks [J]. Chinese Journal of Sensors and Actuators,2011,24(2):264-268.(in Chinese)
李敏,罗挺,徐华.一种基于参考节点选择模型的无线传感器网络定位算法[J].传感技术学报,2011,24(2):264-268.

[10] QU Q,XIA Y. Node Localization of Wireless Sensor Network Based on IMCB Algorithm [J]. Computer Engineering,2014,40(7):42-46.(in Chinese)
曲强,夏勇.基于 IMCB 算法的无线传感器网络节点定位[J].计算机工程,2014,40(7):42-46.

[11] LIN S K,LI S Z,QIAO J Z,et al. Markov Location Prediction Based on User Mobile Behavior Similarity Clustering [J]. Journal of Northeastern University,2016,37(3):323-326.(in Chinese)
林树宽,李昇智,乔建忠,等.基于用户移动行为相似性聚类的 Markov 位置预测[J].东北大学学报,2016,37(3):323-326.

[12] HABIB S J,MARIMUTHU P N. Empirical analysis of query based data aggregation within WSN through Monte Carlo simulation[J]. International Journal of Pervasive Computing and Communications,2012,8(4):329-343.

[13] RAYMOND R,MORIMURA T,OSOGAMI T,et al. Map matching with hidden Markov model on sampled road network[C]// 2012 21st International Conference on Pattern Recognition (ICPR). IEEE,2012:2242-2245.

[14] QIAN W,STANLEY K G,OSGOOD N D. The impact of spatial resolution and representation on human mobility predictability [OL]. http://hdl. handle. net/10388/ETD-2012-11-835.

[15] LIAO L,FOX D,KAUTZ H. Location-based activity recognition using relational Markov networks[C]// Proceedings of the 18th International Conference on Neural Information Processing Systems(NIPS'05). 2005:787-794.

[16] BABU M V,RAMPRASAD A V. Discrete antithetic Markov Monte Carlo based power mapping localization algorithm for WSN[C]// 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). 2012:56-62.

[17] ZHENG J,WU C,CHEN Z. The Mobile Node Localization Algorithm Based on Monte Carlo[J]. Advanced Materials Research,2013,712-715:1847-1850.

[18] HU L,EVANS D. Localization for Mobile Sensor Networks [C]// Proceedings of the 10th Annual International Conference on Mobile Computing and Networking(MobiCom'04). 2004:45-57.

[19] ZHANG S T. Research on Localization for Wireless Sensor Networks [D]. Wuhan:Huazhong University of Science and Technology,2010.(in Chinese)
张松涛.无线传感器网络定位问题研究[D].武汉:华中科技大学,2010.