一种社交网络Sybil用户检测方法

康 恺 张颖君 连一峰 刘玉岭
(中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

摘 要 对社交网络中广泛存在的"女巫攻击"(Sybil Attack)进行检测。通过对收集的近10万微博用户数据提取特征并进行分析,同时结合网络可信度,提出了社交网络Sybil用户检测方法。最后通过实验验证了该方法的有效性。

关键词 社交网络,女巫攻击,恶意用户检测
中图法分类号 TP393.0 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.039

Compound Approach for Sybil Users Detection in Social Networks

KANG Kai ZHANG Ying-jun LIAN Yi-feng LIU Yu-ling
(Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract We mainly focused on the detection of Sybil attack in social networks. By analyzing the collected 100000 data in social networks, we extracted the users' features, and combining the network reliability, we proposed a method to detect Sybil users. Finally, we conducted some experiments to validate the effective of our method.

Keywords Social networks, Sybil attack, Detection of malicious users

1 引言

以微博为代表的社交网络已成为网民获取和发布网络信息的重要途径之一,越来越多的公众人物或机构通过微博来发布或传播消息。中国互联网络发展状况统计报告显示,截止2013年6月底,我国微博网民规模为3.31亿,网民中微博使用率达到56.0%。社交网络满足了人们在碎片化的时间里通过强弱关系进行沟通的需求,因而拥有庞大的用户群体。为保障社交网络用户安全,研究社交网络的典型攻击方法是十分必要的。

常见的网络攻击方式,如钓鱼链接、跨站点脚本攻击、信息窃取、身份假冒等,藉由社交网络信息高效传播的特点,对网络安全构成重大威胁。除此之外,一种名为"女巫攻击"[1]的攻击方法需要引起我们的高度重视。这种攻击方式的特点是能对前述多种攻击方法提供强而有力的支持,成倍扩大其危害。在社交网络中,攻击者通过在网络中创建大量的虚假用户(Sybils)的方法,提升在整个系统中受其控制的用户比例,以此来提高自身的影响力。这类似于基于僵尸网络的攻击方法,不同之处在于Sybil Attack控制的是自身创建的虚假用户,不像僵尸网络那样需要对实体机进行控制,因而更加易于实施并难以被防范。本文重点对此类典型攻击方法及其防范工作进行研究。

目前对于社交网络Sybil Attack进行检测的方法大致分为两类,一类是利用网络拓扑结构进行检测,此类方法检测的准确性和效率不高;另一类是利用用户特征进行检测,这一类方法大多从恶意行为入手,缺乏对Sybil用户特征的分析,因此不能有效识别Sybil用户。为解决上述问题,本文提出了一种社交网络Sybil用户检测方法,该方法通过提取社交网络用户特征,并结合网络可信度进行检测。

本文第2节将对社交网络Sybil用户检测的相关工作进行介绍;第3节介绍社交网络用户特征提取与分析;第4节对社交网络Sybil用户判别方法进行介绍;第5节是实验验证;最后对本文进行总结。

2 相关工作

目前对于社交网络中Sybil Attack的检测方法大致可分为两类:一类是基于网络拓扑结构图对Sybil用户进行检测;另一类着重关注用户行为的分析,通过分析社交网络中用户的好友数、粉丝数等属性特征来对恶意用户进行辨析。

(1)基于网络拓扑结构的检测方法

基于网络拓扑结构的检测方法大致可分为两类,一类是基于非集中式网络结构的,另一类是基于集中式网络结构的。

基于非集中式网络拓扑结构的检测方法是指网络中不存在核心服务器或是核心服务器数据不可得,因而需要从网络节点个体出发进行探索。最早出现的这类方法是由Haifeng Yu等人提出的SybilGuard[2],该方法设计了一种基于fast-

到稿日期:2014-11-16 返修日期:2015-04-07 本文受国家自然科学基金(61303248,U1536106),北京市自然科学基金(4144089,4122085),国家863计划(2013AA01A214)资助。

康 恺(1988-),男,硕士生,主要研究方向为安全测评,E-mail:kangkai@tca.iscas.ac.cn;张颖君(1982-),女,博士,副研究员,主要研究方向为系统安全、安全测评;连一峰(1974-),男,博士,高级工程师,主要研究方向为安全测评;刘玉岭(1982-),男,博士,助理研究员,主要研究方向为安全测评。

mixing[3]假设的、使用随机路径探测的 Sybil Attack 检测方法。其中 fast-mixing 假设指的是：正常情况下，社交网络中的一个群体在经过一段时间(称为 mix time)之后，会逐渐与整个网络融合，不再有那么鲜明的群体特征。而 Sybil 用户由于难以与正常用户建立联系，故 Sybil 群体不具有 fast-mixing 的特点，整个网络可以比较明显地划分为正常用户和 Sybil 用户这两个群体。在 SybilGuard 基础之上，逐步出现了更加优化的 SybilLimit[4] 和 GateKeeper[5] 等。此类方法能较快判定某一节点是否为 Sybil 节点，但在实际大型社交网络中对 Sybil 群体进行辨别时的效率较低。

基于集中式网络结构的检测方法是指网络中存在一个核心服务器，在检测过程中可以从核心服务器上获取整个网络中的各类统计信息(通常称为“全局知识”，Global Knowledge)，使用这些信息可以有效增强检测效果。其中，SRNC[6] 围绕一种典型的全局知识“边介数”(betweeness)进行了探索，对边介数的分析可以有效划分出 Sybil 群体，但是会误把一对有大量邻居的节点对之间的边也当作可疑边。SybilDefender[7] 仍然是在随机路径探测的基础之上设计的，该方法不依赖过多的假设，在实际网络中的效果更好，但在获取一些重要参数时仍需依赖全局知识。

(2)基于社交网络用户特征的恶意用户检测方法

社交网络特征较多，根据不同需求，分析方法也较多。D. boyd[8] 和 C. Honeycut 等人[9] 针对 Twitter 中的转发“@”功能进行了研究，分析了用户之间的交流互动、行为模式等。L. Blige 等人[10] 研究了在社交网络中假冒身份的攻击方法，得出这样一个结论：攻击者在使用假冒身份混入正常用户好友圈后，非常容易窃取用户的私密信息，并进一步骗取其朋友的信任。这份研究所描述的其实是一种比较典型的 Sybil 攻击方法，非常有效地表明了 Sybil 攻击在社交网络中的危害性。不过他们的研究仅限于验证攻击产生的影响，未对其抵御方法进行探讨。S. Ghosh 等人[11] 在 Twitter 上对已知的恶意用户进行了跟踪，对其行为进行分析，研究发现 Twitter 上存在一个巨大的恶意用户群体(spam-farm)，这表明恶意用户之间会互相协作，形成一个群体，以规避安全检测。

B. Krishnamurthy[12] 等人收集了 10 万个 Twitter 用户的数据进行分析，使用粉丝/关注比(follower-to-following)作为指标对恶意用户进行划分，取得了不错的划分成果，不过这种基于单一指标的划分方法的准确性尚有提高空间；Z. Chu[13] 等人分析了 50 万 Twitter 用户，归纳分析了多个属性作为用户群体划分的依据，其中包括关注数、粉丝数、注册时间、发文方式等，在此基础之上使用了基于朴素贝叶斯模型的线性判别分析，能较为有效地对不同种类的用户进行划分。谈磊[14] 提出的基于复合分类模型的社交网络恶意用户识别方法是在机器学习基础上，分析用户的恶意链接发布数、粉丝与关注数、粉丝/关注比、注册时间、发文方式等属性，根据属性之间的相关程度，分别使用贝叶斯算法和 KNN 分类算法对用户进行分类，划分出恶意用户群体。这些基于用户特征的恶意用户检测方法缺乏针对 Sybil 用户特征的分析。因此本文将结合用户特征和网络可信度提出一种针对社交网络 Sybil 用户的检测方法。

3 Sybil 特征提取与分析

本节将对社交网络用户特征进行分析。首先需要获取两类用户数据集用于对比分析，一类是 Sybil 用户数据，一类是正常用户数据。从在新浪微博上收集的信息中剔除一些对分类指导意义不大的指标，如所在地、昵称等，重点分析下文中的指标。

3.1 用户特征提取

对于一个具体用户 x，可以定义其 10 个指标$\{F1,F2,W,Res,Coms,Favs,M,Acts,VIP,P\}$：

$F1(x)\in N$，其中 $F1$ 为用户 x 的关注数，N 为自然数；

$F2(x)\in N$，其中 $F2$ 为用户 x 的粉丝数；

$W(x)\in N$，其中 W 为用户 x 的微博数；

$Res(x)\in R^+$，其中 Res 为用户 x 的微博平均被转发数＝用户微博被转发数/用户微博数，R^+ 为正实数；

$Coms(x)\in R^+$，其中 $Coms$ 为用户 x 的微博平均被评论数＝用户微博被评论数/用户微博数；

$Favs(x)\in R^+$，其中 $Favs$ 为用户 x 的微博平均被赞数＝用户微博被赞数/用户微博数；

$M(x)\in N$，其中 M 为用户 x 的勋章数；

$Acts(x)\in N$，其中 $Acts$ 为用户 x 的活跃天数；

$VIP(x)\in\{0,1\}$，其中 VIP 表示用户是否为 VIP 用户，“1”表示是，“0”表示否；

$P(x)\in N$，其中 P 表示用户 x 的相片数。

由于特征指标之间存在一定相关性，因此可以将其结合起来提高区分度，生成新的指标。例如，由于每个用户活跃的时间长短差异很大，只通过微博数量来衡量用户的活跃程度是不准确的，因此，通过定义每活跃日微博数来取代微博数以衡量不同用户的活跃程度。同样，一个用户的粉丝数和关注数也会随着时间发生变化，注册时间长的用户一般粉丝/关注数量都会比刚注册的用户粉丝/关注数量多很多，因此设计粉丝-关注比来衡量一个用户在社交网络中受欢迎的程度，这种受欢迎程度对于正常用户和 Sybil 用户存在很大的不同。具体定义如下。

定义 1 每活跃日微博数 WAD，$WAD(x)=W(x)/Acts(x)$，$WAD\in R^+$。其中 $W(x)$ 为用户的微博数，$Acts(x)$ 为用户活跃天数。

考虑到 Sybil 用户倾向于在某一时段内集中发送消息，$WAD(x)$ 将比原有的两个指标拥有更高的区分度。

定义 2 粉丝-关注比 FF 是指粉丝和关注的用户数的比值，表示为 $FF(x)=F2(x)/F1(x)\in R^+$。其中 $F2(x)$ 是指用户 x 的粉丝数，$F1(x)$ 是用户 x 的关注用户数。

考虑到单一使用关注数或粉丝数不容易区分正常用户和 Sybil 用户，使用粉丝-关注比作为指标，这样能够抓住 Sybil 用户倾向于关注其他用户的特点，有效地对 Sybil 用户进行区分。

因此，用 2 个新指标替换掉原来的 4 个旧指标，得到 8 元组$\{WAD,FF,M,P,VIP,Res,Coms,Favs\}$

3.2 用户特征分析

通过对收集的 10 万微博用户数据(包含正常用户和 Sybil 用户)进行对比分析，得出如下结果。

(1)每活跃日微博数 $WAD(x)$

如前文所述，每活跃日微博数综合了 Sybil 用户倾向于发送大量微博且难以维持高活跃状态的两类特征，可以比较有效地对 Sybil 用户进行区分。如图 1 所示，正常用户每活跃日微博数通常在 8 以下，且更多分布在小于 2 的区域里；而 Sybil 用户每活跃日微博数通常大于 8。从图 1 中可以直观看出这一指标区分度较高。

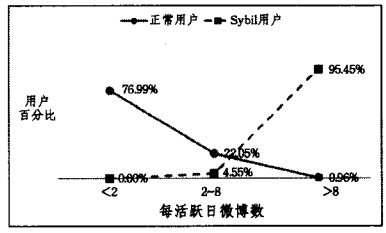

图 1　每活跃日微博数

(2)粉丝-关注比 $FF(x)$

粉丝-关注比是一个较为常见的用于区分恶意用户的指标，这一指标对 Sybil 用户的区分度较高，如图 2 所示。Sybil 用户的 FF 值大多小于 1/3；而正常用户的这一指标接近正态分布，多数分布在 2/3 至 4/3 之间，与预期相符。

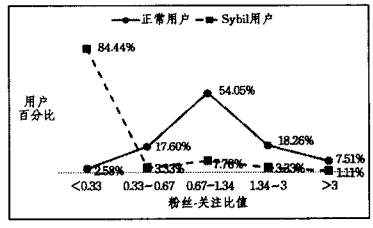

图 2　粉丝-关注比

(3)勋章数 $M(x)$

新浪微博中的“勋章”系统有着这样的设计：微博用户需要首先具备一些特定条件，如有 100 个粉丝、一条微博有 9 条以上评论等，微博系统会向用户发送一条可申请相应勋章的消息，用户需要手动点击消息以领取勋章。Sybil 用户一方面由于目的单一，难以达成申领各种勋章的条件；一方面又不太关注勋章信息，难以像正常用户一般处理勋章通知信息并完成申领。因此 Sybil 用户的勋章数通常较少。如图 3 所示，大部分 Sybil 用户只有 1 个勋章，而正常用户的勋章数通常会比较多。

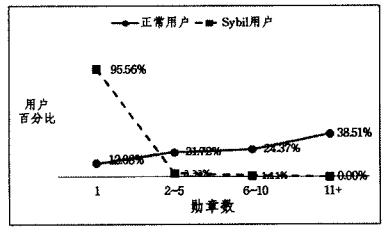

图 3　勋章数

(4)相片数 $P(x)$

新浪微博的相册会把用户所有的头像、原创微博图片等都收集起来存放，因此这里收集到的相片数指的是用户在微博中使用过的各类图片总数。Sybil 用户基本不会更换头像，因此头像相册相片数很少。大部分 Sybil 用户发送的原创微博都不复杂，不含图片，所以微博图片相册中的相片数也很少；部分 Sybil 用户会推送广告等带图片的微博，他们的相片数稍多。如图 4 所示，正常用户的相片数整体呈现正态分布，在 51～200 区间最多，而 Sybil 用户的相片数通常较少，多数在 10 张以下。

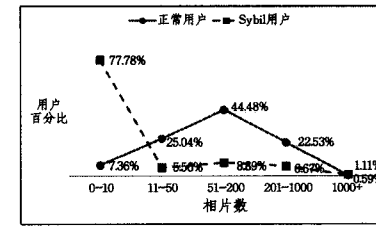

图 4　相片数

(5)会员信息 $VIP(x)$

新浪微博允许普通用户通过充值或是参加特定活动的方式成为微博会员。虽然对大部分用户来说，无需使用微博会员功能即可满足自身应用需求，但是微博会员提供的指定用户屏蔽、微博等级加速、关注人数无上限等功能还是吸引了大批用户。Sybil 用户一方面不需要微博会员带来的各种高级功能，一方面也基本不会向微博充值，因此几乎没有会员。在当前样本集中，正常用户的会员比例为 3%，略低于实际网络中的会员比例；而 Sybil 用户集的会员比例为 0%。

(6)微博平均被评论数 $Coms(x)$

一般来说，Sybil 用户不像正常用户那样有较为频繁的交流互动，因此其微博被评论的数量不如正常用户多。如图 5 所示，正常用户近半数有 1～5 条平均被评论数，而 Sybil 用户的平均被评论数几乎为 0。

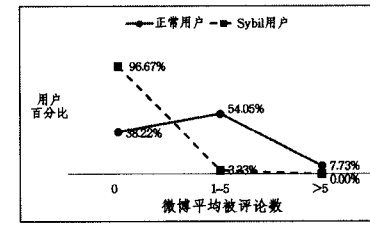

图 5　微博平均被评论数

(7)微博平均被转发数 $Res(x)$

与“微博平均被评论数”类似，本指标考察用户微博被转发的次数。如图 6 所示，整体上符合预期，Sybil 用户较正常用户的平均被转发数少。然而从图中也可看出，本指标的区分度要明显低于“微博平均被评论数”，而且两个指标之间有一定相关性，下文分析中将剔除此指标。

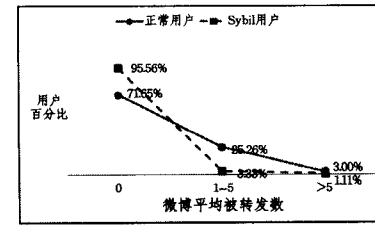

图 6　微博平均被转发数

(8)微博平均被赞数 $Favs(x)$

本指标关注用户微博被赞的次数，具体计算方法与“微博平均被评论数”类似。“赞”在微博中相对于评论和转发来讲，

是一个相对不太常用的功能，大部分用户得到的赞数都较少。在现有正常用户样本集中，平均被赞数不小于 1 的用户占 17%；而在 Sybil 样本集中，所有样本平均被赞数接近于 0。因而这一指标也有较高区分度，可以认为平均被赞数不小于 1 的用户有非常大的几率是正常用户。

通过上述分析，针对社交网络用户特征，采用七元组 $\{WAD, FF, M, P, VIP, Coms, Favs\}$ 进行描述，用户特征将作为 Sybil 用户检测的重要组成部分。

4 社交网络 Sybil 用户检测方法

为了更好地检测 Sybil 用户，本文将从用户特征(S)和网络可信度(F)两个角度进行综合判定。其中网络可信度 F 是指从网络关注角度对 Sybil 用户进行分析，本文主要指关注 Sybil 用户中正常用户和 Sybil 用户占的比例大小。

社交网络 Sybil 用户的判别方法中，核心内容是为受测用户计算一个 Sybil 分值。

定义 3 Sybil 分值 $Rank$，$Rank=\alpha S+\beta F$。其中 S、F 分别为前文计算得出的用户特征和网络可信度，α、β 为加权参数(其中 $\alpha+\beta=1$)，用于调整两类分值的影响权重，最终计算得总评价 $Rank$ 值，其取值范围为[0,1]，越接近 0 则说明该用户为正常用户的可能性越大，而越接近 1 则说明该用户越可能为 Sybil 用户。

4.1 用户特征分析

参照 3.2 节内容，在原有的八元组中剔除掉区分度不高的“微博平均被转发数”项，使用七元组 $\{WAD, FF, M, P, VIP, Coms, Favs\}$ 设计判别算法，设计过程参考贝叶斯公式。

对于某特征 u，假设其取值分为 n 个区段，分别为 $a_1, a_2, \cdots, a_n$，Sybil 用户在这 n 个区段上分布的概率为 $p_1, p_2, \cdots, p_n$，正常用户在这 n 个区段上分布的概率为 $q_1, q_2, \cdots, q_n$，在整个网络中任一用户为 Sybil 的概率为 r。假设有一未知类型的用户，其属于两个类别的概率相同，现已知其特征 u 取值为 a_i，那么由贝叶斯公式计算该用户为 Sybil 用户的几率的方法如下：

假设事件 A 表示用户为 Sybil 用户，事件 B 表示用户的特征 u 取值为 a_i，则：

$$P(A)=r$$

$$P(B)=p_i*r+q_i*(1-r)$$

$$P(B|A)=p_i$$

$$P(A|B)=P(B|A)P(A)/P(B)=(p_i*r)/(p_i*r+q_i*(1-r)) \quad (1)$$

对于一个未知类型的用户，不失一般性，本文假定该用户是 Sybil 用户或正常用户的概率相等，于是根据式(1)，将 $r=0.5$ 代入，得：

$$P(A|B)=p_i/(p_i+q_i) \quad (2)$$

本文以式(2)为基础，依据图 1－图 6，各特征参数的计算结果如表 1 所列。

对于待测用户 x，收集其七元组 $\{WAD, FF, M, P, VIP, Coms, Favs\}$ 的数值，按照表 1 得出 7 项特征参考值 $S_1, \cdots, S_7$，假设各个特征对 Sybil 用户的影响近似相同，计算其平均数作为该用户特征值：

$$S=(S_1+S_2+\cdots+S_7)/7 \quad (3)$$

表 1 特征参数表

特征类别	值域分段	Sybil 指数
每活跃日微博数 WAD(x)	<2	0
	2～8	0.17
	>8	0.99
粉丝-关注比 FF(x)	<1/3	0.97
	1/3～2/3	0.16
	2/3～4/3	0.13
	4/3～3	0.15
	>3	0.13
勋章数 M(x)	0～1	0.89
	2～5	0.13
	6～10	0.04
	>11	0
相片数 P(x)	0～10	0.91
	11～50	0.18
	50～200	0.17
	201～1000	0.23
	>1000	0.35
会员信息 VIP(x)	是	0
	否	0.51
微博平均被评论数 Coms(x)	0	0.72
	1～5	0.09
	>5	0.00
微博平均被赞数 Favs(x)	0	0.57
	1～5	0.17
	>5	0.26

4.2 网络可信度

通过对粉丝链和关注链收集的两类共约 10 万个用户进行分析，发现 Sybil 用户关注的用户中 Sybil 用户比例较高，而正常用户很少会主动关注 Sybil 用户。

通过全面分析关注用户中 Sybil 用户所占的比例(见图 7)可以看出，正常用户与 Sybil 用户之间存在较大差异。选取 $x=0, 0.2, 0.4, 0.6, 0.8, 1$ 进行对比，如 $x=0.2$ 表示用户的关注中有 20%是疑似 Sybil 用户。从 $x=0.2$ 对应的用户百分比可以看出，正常用户约有 7%，Sybil 用户约有 22%，他们的关注中有 20%的疑似 Sybil 用户。由图 7 可以看出，正常用户基本不会关注 Sybil 用户，而 Sybil 用户之间会互相关注以提升彼此的粉丝数量。

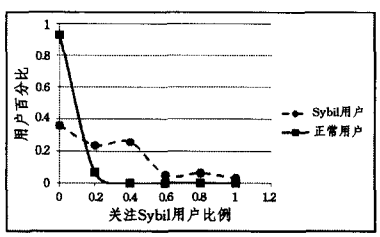

图 7 关注 Sybil 用户比例分布

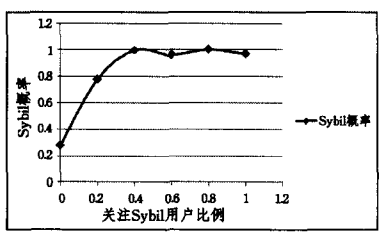

图 8 关注 Sybil 比例-Sybil 概率分析

为了更详细地观察关注 Sybil 用户的概率分布，将图 7 中的特征点进行计算，使用贝叶斯公式计算每一处的参考值，如 $x=0.2$ 时，$y=22\%/(22\%+7\%)=0.76$。将所得的 6 个点作散点图，并用平滑曲线相连，如图 8 所示。由于选取样本存

在一定偶然性，导致曲线中段并不太平滑，因此需要设计合适的函数对曲线进行拟合，以方便进一步的分析计算。

由图 8 可知，在 x 取值于[0，0.4]区间时的增长速度较快，而在[0.4，1]区间上基本保持定值，因此对曲线进行分段拟合：

a)$x\in[0,0.4]$

此段上的 3 个特征点(x,y)为(0，0.28)，(0.2，0.76)，(0.4，0.99)。先将(x,y)的值域由[0，0.4]，[0.28，0.99]均变换为[0，1]，设变换后坐标为(x',y')，那么

$x'=x/0.4$

$y'=(y-0.28)/(0.99-0.28)$

原先的 3 个特征点变为(0，0)，(0.5，0.7)，(1，1)。观察曲线走势，曲线呈单调递增趋势，二阶导数小于 0，因此可寻找形如 $y=xk(0<k<1)$ 的指数函数进行拟合。经实验，$k=1/2$ 时拟合效果较好，即有 $y'=(x')1/2$，代入 x,y 得：

$y=0.71(x/0.4)0.5+0.28$

b)$x\in[0.4,1]$

此段上的 y 值只在很小范围内波动，因此使用简单的定值 y 进行拟合，取 $y=0.99$。

综合以上两部分，得到基于关注 Sybil 用户比例的 Sybil 概率分析式：

$$y=\begin{cases}0.71(x/0.4)^{0.5}+0.28, & 0\leqslant x<0.4\\ 0.99 & 0.4\leqslant x\leqslant 1\end{cases} \tag{4}$$

拟合对比图如图 9 所示，拟合效果良好，且与前文推论预期一致。式(4)用于计算网络可信度 F。

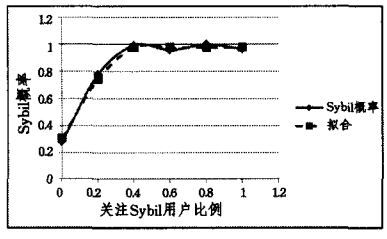

图 9　关注 Sybil 比例-Sybil 概率拟合

5　实验结果与分析

由于当前工作中使用的社交网络用户特征大多是针对恶意用户进行检测，缺乏专门对 Sybil 用户的检测，因此，本文提出一种社交网络 Sybil 用户检测方法，并将通过实验验证该方法的有效性。本文使用 977 个正常用户和 432 个 Sybil 用户进行实验，为了计算 α 和 β 不同取值对最终检测的影响，定义误检率进行描述。Sybil 用户检测的漏报率是指没有识别出的 Sybil 用户数量与 Sybil 用户总数的比值。误报率是指错误识别的正常用户数量与正常用户总数的比值。下面将进行具体说明。对不同的 $\alpha:\beta$，误报率和漏报率的计算结果如表 2 所列。

表 2　误报率和漏报率对比

$\alpha:\beta$	漏报率	误报率	$\alpha:\beta$	漏报率	误报率
1:3	13.60%	14.20%	7:1	3.84%	3.74%
1:2	9.11%	14.96%	8:1	3.68%	3.83%
1:1	6.58%	11.75%	9:1	3.77%	3.90%
2:1	6.03%	7.00%	10:1	3.78%	3.94%
3:1	4.80%	5.12%	11:1	3.79%	3.99%
4:1	3.99%	4.51%	12:1	3.78%	4.04%
5:1	4.23%	3.82%	13:1	3.80%	4.11%
6:1	4.07%	3.76%	14:1	3.79%	4.22%

从表 2 中可以看出，取 $\alpha:\beta=8:1$ 可以得到最优解。实验中选取 $\alpha:\beta$ 为 8:1，对 Sybil 分值以间隔 0.01 进行分析，得出对正常用户和 Sybil 用户在该分值下的概率。由于篇幅有限，表 3 仅列出部分结果。

表 3　正常用户的分值 *Rank* 计算结果

Sybil 分值	正常用户	Sybil 用户	Sybil 分值	正常用户	Sybil 用户
0	0	0	0.5	0.6%	0.9%
0.1	0.1%	0	0.6	0	3%
0.2	2.7%	0	0.7	0	4.8%
0.3	4.3%	0	0.8	0	0.6%
0.4	1.6%	0.2%	0.9	0	0
0.48	0.7%	0.7%	1.0	0	0

使用 R 语言[15]对两类用户的 100 个 Sybil 分值原始数据进行正态拟合，拟合结果如图 10 所示，正常用户概率密度峰值于 $x=0.30$ 时取得，Sybil 用户概率密度峰值于 $x=0.65$ 时取得；交点位于 $x=0.47$ 至 $x=0.48$ 之间。由此可见，正常用户大致分布于 Sybil 分值小于 0.48 的区域内，而 Sybil 用户大致分布于 Sybil 分值大于 0.48 的区域内，且二者之间存在较为明显的分划，与预期一致。为了验证所提方法的有效性，随机检查了 71 个用户，人工确认发现有 13 个 Sybil 用户；工具检出 11 个，漏报率 15.4%；58 个正常用户有 5 个被误检，误报率 9%。

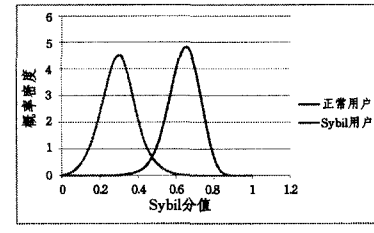

图 10　正常用户与 Sybil 用户分值分析

结束语　本文提出了一种社交网络 Sybil 用户检测方法。该方法对收集的近 10 万新浪微博用户进行分析，并提取了用于检测的特征元素，通过这些特征元素，针对正常用户和 Sybil 用户进行了用户特征分析和网络可信度分析，进而构建了社交网络 Sybil 用户判别公式，实现了 Sybil 用户的检测。最后通过实验验证了本文方法的有效性。

参 考 文 献

[1] Douceur J. The Sybil attack [M]// Lecture Notes in Computer Science 2429，2002：251-260

[2] Yu H，Kaminsky M，Gibbons P B，et al. SybilGuard：Defending Against Sybil Attacks via Social Networks [J]. IEEE/ACM Transactions on Networking，2008，16(3)：576-589

[3] Yu H，Gibbons P B，Kaminsky M，et al. Sybillimit：A near-optimal social network defense against sybil attacks [C] // IEEE Symposium on Security and Privacy. Oakland，2008：3-17

[4] Tran N，Li J，Subramanian L，et al. Optimal sybil-resilient node admission control[C]//IEEE INFOCOM. Shanghai，2011：3218-3226

[5] Danezis G，Mit P. Sybilinfer：Detecting sybil nodes using social networks[C]//NDSS. 2009

[6] Xu L，Chainan S，Takizawa H，et al. Resisting Sybil attack by social network and network clustering[C]//10th Annual International Symposium on Applications and the Internet. Seoul，2010：15-21

[7] Wei W, Xu F, Tan C C, et al. Sybil Defender: Defend Against Sybil Attacks in Large Social Networks[C]// IEEE INFOCOM. 2012:1951-1959

[8] Golder S, Lotan G. Tweet, tweet, retweet: Conversational aspects of retweeting on Twitter[C]// 2010 43rd Hawaii International Conference on System Sicences(HICSS). 2010:1-10

[9] Honeycutt C, Herring S C. Beyond microblogging: Conversation and collaboration via Twitter[C]// 42nd Hawaii International Conference on System Sciences, 2009(HICSS'09). IEEE, 2009: 1-10

[10] Bilge L, Strufe T, Balzarotti D, et al. All your contacts are belong to us: Automated identity theft attacks on social networks [C]// Proceedings of the 18th International Conference on World Wide Web(WWW'09). 2009:551-560

[11] Ghosh S, Korlam G, Ganguly N. Spammers' Networks within Online Social Networks: A Case-Study on Twitter[C]// Proceedings of the 20th International Conference Companion on World Wide Web(WWW'11). 2011:41-42

[12] Krishnamurthy B, Gill P, Arlitt M. A few chirps about twitter [C]// Proceedings of the First Workshop on Online Social Networks(WOSN'08). 2008:19-24

[13] Chu Z, Gianvecchio S, Wang H, et al. Who is tweeting on Twitter: human, bot, or cyborg? [C]// Proceedings of the 26th Annual Computer Security Applications Conference(ACSAC'10). 2010:21-30

[14] Tan Lei, Lian Yi-feng, Chen Kai. Malicious users identification in social network based on composite classification model[J]. Computer Applications and Software, 2012(12): 1-5(in Chinese)
谈磊,连一峰,陈恺. 基于复合分类模型的社交网络恶意用户识别方法[J]. 计算机应用与软件,2012(12):1-5

[15] R 语言[OL]. http://mirror.bjtu.edu.cn/cran/

(上接第 148 页)

结束语 本文提出了一种基于线性规划和二分图匹配的共享资源优化算法。hnRoM 算法将资源优化问题分解为 DU-CU 配对和时隙划分两个子问题。接着用线性规划的方法得到时隙划分子问题的最优解,根据时隙划分子问题的解构建二分图模型来求解 DU-CU 配对问题。二分图模型将端到端用户(DU)与蜂窝用户(CU)作为两个独立点集,将两者配对共享资源时的吞吐量之和作为边权值,通过权值修改,获取二分图最大权完美匹配,从而得到混合 D2D 蜂窝网络下的最优资源分配方案。仿真结果表明,hnRoM 算法能够保证接入所有 DU,在满足所有用户最小传输速率的前提下,最大化系统总的吞吐量。本文推荐的资源优化策略对理论研究和实际应用都具有探索和指导意义。

参 考 文 献

[1] Doppler K, Rinne M, Wijting C, et al. Device-to-device Communication as an underlay to LTE-advanced networks[J]. IEEE Communications Magazine, 2009, 47(12): 42-49

[2] Nasser N, Hasswa A, Hassanein H. Handoffs in fourth generation heterogeneous networks[J]. IEEE Communications Magazine, 2006, 44(10): 96-103

[3] Lee J, Gu J, Bae S J, et al. A session setup mechanism based on selective scanning for device-to-device communication in cellular networks[C]// 17th Asia Pacific Conference on Communications. Shanghai, China, 2011: 677-681

[4] Doppler K, Yu C H, Ribeiro C B, et al. Mode selection for device-to-device communication underlaying an LTE-advanced network[C]// IEEE Wireless Communications and Networking Conference. 2010: 1-6

[5] Phunchongharn P, Hossain E, Kim D I. Resource allocation for device-to-device communications underlaying LTE-advanced networks[J]. IEEE Wireless Communications, 2013, 31(9): 348-358

[6] Sun H, Sheng M, Wang X, et al. Resource allocation for maximizing the device-to-device communications underlaying LTE-Advanced networks[C]// IEEE International Conference on Communications. Dresden, 2013: 60-64

[7] Xu C, Song L, Han Z, et al. Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 348-358

[8] Lei L, Zhong Z, Lin C, et al. Operator controlled device-to-device communications in LTE-advanced networks[J]. IEEE Wireless Communications, 2012, 19(3): 96

[9] Yu C H, Doppler K, Ribeiro C B, et al. Resource sharing optimization for device-to-device communication underlaying cellular networks[J]. IEEE Transactions on Wireless Communications, 2011, 10(8): 2752-2763

[10] Min H, Seo W, Lee J, et al. Reliability improvement using receive mode selection in the device-to-device uplink period underlaying cellular networks[J]. IEEE Transactions on Wireless Communications, 2011, 10(2): 413-418

[11] Han J, Cui Q, Yang C, et al. Bipartite matching approach to optimal resource allocation in device to device underlaying cellular network[J]. Electronics Letters, 2014, 50(3): 212-214

[12] Plummer M D. Matching theory [M]. New York, American Mathematical Soc., 2009

[13] Sun F, Li V O K, Diao Z. Multi-objective optimized bipartite matching for resource allocation[C]// International Symposium on Communications and Information Technologies. 2007: 666-671

[14] Halabian H, Lambadaris I, Lung C H, et al. Throughput optimal relay selection in multiuser cooperative relaying networks[C]// IEEE military Communications Conference. 2010: 507-512

[15] Parveen N, Venkateswarlu D S, Bhandari B N. Implementation of OFDM based multi-relay multipair two-way communication network[C]// IEEE 2014 Eleventh International Conference on Wireless and Optical Communications Networks. 2014: 1-4

[16] Ng T C Y, Yu W. Joint optimization of relay strategies and resource allocations in cooperative cellular networks[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(2): 328-339

[17] Cai J, Shen X, Mark J W, et al. Semi-Distributed User Relaying Algorithm for Amplify-and-Forward Wireless Relay Networks [J]. IEEE Transactions on Wireless Communications, 2008, 7(4): 1348-1357