利用加权用户关系图的谱分析探测大规模电子商务水军团体

韩忠明 杨 珂 谭旭升
(北京工商大学计算机与信息工程学院 北京 100048)

摘 要 电子商务水军的识别已成为众多网络水军识别领域中较为突出的研究问题.已有电子商务水军识别研究多关注网络水军自身属性和行为特征,以发现隐藏其中的网络水军行为模式.电子商务服务急速扩张刺激以获取经济利益为目的的大规模水军傀儡账号泛滥,水军逐渐形成团体规模.大规模水军泛滥使得单独网络水军的行为更加趋向正常用户,团体内部成员间不具有明显相似性,基于特征模式识别的研究方法无法很好地发现该类电子商务水军.文中定义电子商务用户的加权用户关系图模型,分析其谱特征定位用户关系图中的异常关系结构,从而找出隐藏其后的大规模电商水军团体,并提出一种基于用户关系图模型定位大规模电商水军团体的算法.文中在两个国内外最具代表性的电子商务平台(淘宝、亚马逊)数据集上进行了大量实验,并评估了算法的不同参数定位电商水军团体的能力.实验结果表明文中提出的加权用户关系图异常结构能够很好地定位隐藏较深的大规模电子商务网络水军团体,且加权用户关系图定位电子商务网络水军团体的能力优于非加权用户关系图.

关键词 水军;水军团体;团体检测;用户关系图;异常结构发现;社交网络
中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2017.00939

Analyzing Spectrum Features of Weight User Relation Graph to Identify Large Spammer Groups in Online Shopping Websites

HAN Zhong-Ming YANG Ke TAN Xu-Sheng
(*School of Computer and Information Engineering, Beijing Technology & Business University, Beijing* 100048)

Abstract With rising popularity, the identification of online shopping websites spammers has become one of the hottest topics in the wide field of spammer detection. The existing works in detection of online shopping websites spammers usually focus on the behavior patterns of spammers. When most spammers start functioning as many large spammer groups to game the detection system, the individual member of the large group tends to act like a normal user. The behavior pattern discovery of spammers cannot effectively detect these large spammer groups. This paper proposes a novel angle to this problem by modeling the weight relation network of online shopping websites users. An algorithm called User Relation Graph Spectrum-based Spammer Group Detection (URGSSGD) is also proposed to detect the signal network of large spammer group in the user relation network by analyzing its spectrum features. Experiments on two typical real-life review datasets, which comprise Amazon and Taobao review dataset, demonstrate the effectiveness of proposed model which outperforms the existing methods to identify large spammer groups. Also this paper proves the weight user relation network performs well than the unweight user relation network on detecting large spammer groups in online shopping websites.

Keywords spammers; spammer group; group detection; user relation graph; anomaly structure detection; social networks

收稿日期:2014-08-19;在线出版日期:2015-06-22.本课题得到国家自然科学基金(61170112)和教育部人文社会科学研究青年基金(13YJC860006)资助.**韩忠明**,男,1972 年生,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为互联网数据挖掘、模式识别等.E-mail:hanzm@th.btbu.edu.cn.**杨 珂**,女,1990 年生,硕士研究生,主要研究方向为互联网信息挖掘、网络水军识别.**谭旭升**,1989 年生,硕士研究生,主要研究方向为互联网数据挖掘、社团发现.

1 引 言

电子商务是较早发展的新兴网络商业模式,在传统零售业被大部分信息化的同时,网络购物成为Web2.0网络服务中的主要部分.辅助用户购买决策的电子商务信息成为网络水军的主要危害目标.当用户考虑购买某件产品时,用户会浏览该产品的已买用户评论,并根据其评论趋势决定其购买意向.网络水军即通过操纵软件机器人或傀儡账号在互联网中制造、传播虚假意见和垃圾信息等的网络垃圾意见产生者的总称.现有网络环境催生了大量网络水军,其行为特点主要包括大规模团体行动,数量庞大,行为区别于正常用户[1]等.在商业利益的驱动下,电子商务网络水军利用虚假评论鼓吹或诋毁目标产品,形成对目标产品舆论导向控制,从而影响用户对产品真实质量的判断,导致用户购买不真实产品,从而损害用户的切身经济利益[2].电子商务网络水军(简称电商水军)大规模利用水军傀儡账号,在进行虚假评论或购买时分批操控其手中的傀儡账号,使得该类傀儡水军用户在其行为属性上更加趋向于正常用户,基于网络水军行为属性特征模式发现的研究方法无法很好地检测该类电商水军,这也使得对其的识别研究日益复杂[3].因与用户切身经济利益紧密相关,电子商务领域的网络水军识别研究较社交领域等其他领域网络水军识别研究更为迫切.

本文通过分析电子商务用户形成稳定用户关系且大规模电商水军团体进行虚假点评等水军行为时造成异常用户关系结构的特点,发现该类电商水军关系结构不易受网络水军行为属性多变性的影响,对电商水军的识别贡献较为稳定.因此,本文定义电子商务用户的加权用户关系图,分析其邻接矩阵的谱特征,从而定位其异常关系结构,挖掘其背后潜藏的大规模电商水军团体.在此基础上,本文提出一种基于用户关系图谱特征定位电商水军团体的算法,并在国内外两大代表性电子商务实验数据集上对其进行了测试及不同参数下的算法评估.此外,本文对于加权用户关系图与非加权用户关系图对大规模电商水军团体的定位能力进行了对比实验,发现加权用户关系图能够更好地找出隐藏的电商水军团体.

2 相关研究工作

电子商务领域网络水军识别研究具有极高的应用价值,一直是近几年研究的热点.按照其识别体系不同,又可将电子商务网络水军识别研究分为监督识别和非监督识别.电子商务网络水军监督识别方法主要包括依据评论内容特征的识别方法,如文献[4-7]所采用的方法.非监督识别方法按照识别特征不同可分为5类,其识别特征主要包括个人网络水军特征[2,8]、网络水军团体特征[3,9]、时间序列特征[10]、评论模式特征(评分偏差[5]、评论突发性[11])、行为分布特征[12].传统电子商务领域网络水军识别方法主要依据评论内容的相似性和其语言特征来发现虚假评论者[8,13-14].例如,通过分析评论文本与正常用户评论的偏离发现网络水军发布的虚假评论[15].这是由于为影响和改变用户的购买决定,电商水军需对目标商品发表背离正常用户的评价.Mukherjee等人[16]分析了电子商务网络水军的各种行为,认为网络水军与正常用户具有极为不同的行为分布,其多具有评论集中突发性、评论极端性、发布早期产品评论等特点,并利用电子商务领域网络水军可疑度作为隐性变量构建了贝叶斯识别模型.该文利用用户和其发表的评论特征构建分类器,利用上述水军行为特点将其与普通用户区分,并首次利用评论自身语言特征客观验证识别结果,辅以人工评价,更好地验证了网络水军识别准确性.该方法提高了电子商务网络水军识别评价的准确性,为电子商务网络水军识别结果评价提供了新的研究思路.

电子商务网络水军与目标产品和商店形成了一些特定关系.由于网络水军总是宣传其雇主的目标商品或商店,因此对于目标产品的选择并不具备随机性.Wang等人[8]首次在电子商务网络水军识别中引入复杂关系模型,对网络水军、其产生的评论、目标商店间的关系建模,分析节点间交互行为,以定位水军危害源头,并识别出可疑评论者.此外,Wang等人在文献[17]中使用图模型来表达网络水军可疑度、水军发布的评论质量以及评论所在商店的评分这三者之间的相互影响关系.其方法与PageRank中计算节点与边相互影响关系的方法相似,通过学习训练数据,迭代得到水军可疑度.该文利用图模型对网络水军间关系建模,很好地利用网络水军间关系特征来识别,具有很好的可推广性.

电商水军傀儡账号的泛滥使得水军逐渐形成团体规模,水军团体通过操控大量水军傀儡账号对目标产品进行虚假评论,目的是为造成对目标产品的舆论导向控制.已有的电商水军团体识别研究多关

注团体水军行为特征，文献[9]中分析电商水军行为意图，利用电商水军团体共同评论目标产品以造成对其舆论导向的控制的特点，对亚马逊数据集上的大量电商水军进行了实验分析，发现亚马逊电商水军团体多具有团体内部成员行为聚集性、团体成员评论内容相似性、团体水军行为突发性、团体评论时间较早等特点. 该研究中对于网络水军团体的识别是以水军团体具有共同评论产品为前提的. 当前泛滥的大规模网络水军，为避免水军识别研究对其的检测，多通过分批操控水军傀儡账号来进行虚假评论，因此水军团体并不具有明显相似性，即不具有共同评论产品. 同时文献[3]提出水军团体通过较少的共同评论产品或共享一部分团体关键成员来避免对其的探测. 故上述两类研究方法并不能探测不具有共同评论产品或不共享团体成员的大规模电商水军团体. 对该类危害较大的大规模电商水军的探测问题正是本文提出的利用电商用户关系图谱特征探测电商水军团体算法所关注解决的电商水军探测问题.

文献[18]提出利用社交网络用户形成的用户关系网络探测社交网络中存在的垃圾链接攻击行为，该文献利用对于用户关系网络结构的谱分析发现用户关系网络中存在的噪声结构，即用户异常关系的形成，以定位社交网络中发生的垃圾链接攻击行为. 该文献利用社交网络用户行为关系具有稳定性的特点，发现因突发性的异常行为造成的用户关系网络异常结构. 该思路同样可适用于电子商务领域中. 电子商务领域中的用户对于目标产品的购买行为同样形成较为稳定的关系结构，大规模电商水军突发性的购买行为使得电子商务平台用户间的关系结构具有代表该类电商水军行为的异常结构，因此可以利用图模型异常探测的方法定位大规模电商水军团体.

文献[19]提出图邻接矩阵的谱特征能够很好地反映图的结构特点，并从理论上证明图邻接矩阵的谱特征能够捕捉网络结构中的微小噪声，从而定位图结构中的异常. 该文在真实论文作者关系网络上进行了实验验证，并在其他 5 个公开实验数据集上对其结论进行了验证. 该文为本文的研究工作提供了理论依据，利用大规模电商水军团体形成的不易隐藏的异常关系结构特征，挖掘出潜藏的大规模电商水军团体.

3　用户关系图模型谱分析

图 G 的结构特征与其邻接矩阵 $\boldsymbol{A}$ 的代数性质有着不可分割的关系，如邻接矩阵 $\boldsymbol{A}$ 的特征值包含了图中是否含有环及其直径的信息. 连通图中的最大度数，团数，分支数都与邻接矩阵的主特征有关，即邻接矩阵的最大特征值[20]. 进一步可推知电商水军关系图 G 的邻接矩阵 $\boldsymbol{A}$ 的特征值包含了该图 G 的大部分属性，也包含其中存在的异常结构信息.

在此基础上，将电商水军间的关系抽象为由 n 个用户及其之间 m 条关系组成的加权无向对称连通图 G. 分析现有电子商务平台中用户评论信息并结合领域专家经验，本文认为若电子商务平台用户 i 与用户 j 共同评论了 3 个及以上的共同产品，则用户 i 与用户 j 之间具有关系，其关系上的权值为其共同评论的产品数[9]. 因网络水军多通过大规模虚假评论行为意图操控目标产品舆论导向，其评论行为较正常用户更为频繁，且其多针对相同的目标产品集合以最大程度施加影响. 对于用户关系权重阈值即代表用户关系的共同评论数的选取，本文结合评论数据分析和现有研究，通过筛选共同评论 3 个及 3 个以上共同产品的用户，最大程度避免正常用户因相似购买习惯导致的目标产品交集，同时经过对比不同用户关系权重，验证用户关系权重阈值的选择.

为更好地分析电商水军间的用户关系网络，我们同样对电商水军关系进行了非加权用户关系图(Unweight User Relation Graph，UURG)建模，方法与加权用户关系图(Weight User Relation Graph，WURG)相同，但其关系不具有权值. 其中 $\boldsymbol{A}_{n\times n}$ 表示该用户关系图 G 的邻接矩阵. 即若用户 i 与用户 j 之间存在关系，则邻接矩阵元素 $a_{ij}=1$，否则 $a_{ij}=0$.

表 1 显示了本文在两个实验数据集即亚马逊和淘宝电子商务平台用户评论数据集中预处理用户关系以建立加权用户关系图的过程. 采用亚马逊和淘宝数据集(数据集构建详见 5.1 节)中所有商品所涉及评论作为初始评论数据集，按照表 1 所示步骤进行过滤，得到最终评论数据集作为本文的实验数据集. 通过深入分析两个电商数据集上用户的行为特点，本文采用不同的过滤参数建立加权用户关系图. 这是因为本文采用的亚马逊实验数据集来自于亚马

逊平台中的电子产品类别下的用户评论数据，其包括的产品和用户数量较多，每个产品评论数相对较少，形成的用户关系对较多，因此对其进行了进一步的过滤，以筛选合适的用户关系建立其加权用户关系图.对于亚马逊实验数据集，本文最终得到 5243 个用户及其 37747 条关系以形成用户关系图.而本文使用的淘宝实验数据集来自于淘宝电子产品类别中热门手机的用户评论数据，该实验数据集中产品和用户数目相对亚马逊实验数据集较少，但每个产品的评论数较多，因此采用低于亚马逊实验数据集的过滤阈值对其产品进行过滤并形成最终的用户关系对.对于淘宝实验数据集，本文最终得到 2743 个用户及其 23745 条关系以建立加权用户关系图.

表 1 亚马逊和淘宝实验数据集上的用户关系预处理过程

用户关系预处理	预处理步骤	输出数据统计
亚马逊实验数据集（总产品数：36197）	筛选具有两个评论者以上的产品	10911 个产品
	筛选只包含出现次数超过 3 次的评论者的产品	7361 个产品
	得到产品的所有用户关系对	467496 条用户关系
	筛选出现次数超过 2 的用户关系对，建立用户关系图	37747 条用户关系
淘宝实验数据集（总产品数：2908）	筛选具有两个评论者以上的产品	2709 个产品
	筛选只包含出现次数超过 2 次的评论者的产品	862 个产品
	得到产品的所有用户关系对，建立用户关系图	23745 条用户关系

上述预处理过程筛选出用以建立用户关系图的所有用户.本文目的为发现大部分隐藏于电子商务热门产品中的大规模网络水军团体，经过上述评论数据筛选过程，保证了建立用户关系图的所有用户为热门产品中的活跃用户.同时上述过程保证了最大程度过滤正常用户因相同的购买兴趣造成的用户关系积累.同时，为验证用户关系权重阈值的选取即代表用户关系的共同评论数的选取，本文对不同关系权重阈值下的用户关系矩阵进行了统计分析.表 2 显示了不同关系权重阈值下预处理后的用户关系矩阵统计信息.

如表 2 所示，可以发现在经过热门产品筛选的数据预处理过程后，剩余用户关系中采用用户关系权重阈值为 3 即代表用户关系的共同评论产品数为 3 时，能够保证大部分用户关系，并发现在此基础上的异常密集用户关系.若采用 4 个或 4 个以上用户共同评论产品数会导致用户关系数锐减且用户关系过分密集，较难发现因水军频繁交互导致的用户关系图中的异常密集关系，且其不能覆盖热门产品中

表 2 不同用户关系权重阈值下用户关系矩阵统计信息

当前阈值下用户关系数统计		用户关系权重阈值 3	4	5	6
亚马逊实验数据集（总用户数：5243）	用户数	1602	591	130	96
	用户关系总数	37747	3210	674	112
	权重为 1 的用户关系数	33663	674	112	47
	权重为 2 的用户关系数	3210	112	47	9
	权重为 3 的用户关系数	674	47	26	6
	权重为 4 及以上的用户关系数	112	26	9	0
淘宝实验数据集（总用户数：2572）	用户数	844	233	55	0
	用户关系总数	23745	2329	85	0
	权重为 1 的用户关系数	21323	85	8	0
	权重为 2 的用户关系数	2329	8	0	0
	权重为 3 的用户关系数	85	0	0	0
	权重为 4 及以上的用户关系数	8	0	0	0

的大部分评论用户.经过热门产品筛选后的用户大多数皆为较为活跃的可疑用户，过高的用户关系权重阈值会使得因此构建的用户关系图无法覆盖大部分可疑用户，对于热门产品中大量存在的网络水军团体相对召回率较低.因此本文通过筛选共同评论 3 个及 3 个以上共同产品的用户，以最大程度避免正常用户因相似购买习惯导致的目标产品交集，同时保证最大程度检测可疑水军用户.

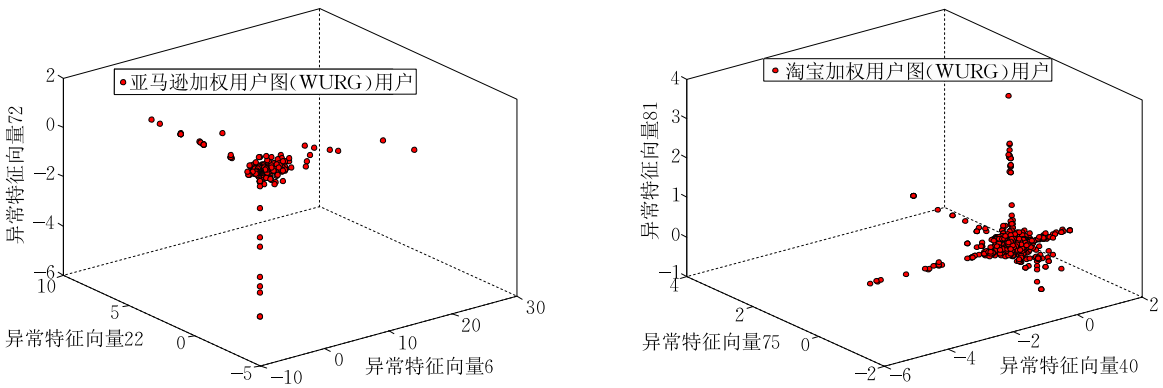
在此基础上，对上述预处理过程形成的加权用户关系图进行谱空间的特征分析.λ_i 表示邻接矩阵 $\boldsymbol{A}$ 的第 i 大的特征值，x_i 为其对应的特征向量，其中 $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$.对其邻接矩阵 $\boldsymbol{A}$ 进行谱分解，$\boldsymbol{A}=\sum_j \lambda_i \boldsymbol{x}_j \boldsymbol{x}_j^{\mathrm{T}}$.其中 x_{ju} 表示第 u 个特征向量 $\boldsymbol{x}_j$，特征向量 $\boldsymbol{x}_j$ 可表示为列向量 $(x_{j1}, x_{j2}, \cdots, x_{jn})^{\mathrm{T}}$.行向量 $(x_{1u}, x_{2u}, \cdots, x_{nu})$ 表示节点 u 在 n 维谱空间中的坐标.

文献[21]证明 ER 图的邻接矩阵所有主特征值 ξ 服从非对称的正态分布，并得出其估值为 $\hat{\xi}_1 = np$.次特征值（即除主特征值之外，最大的特征值）具有其上限 $\xi_2 \leq 2\sqrt{np(1-p)} + O(n^{1/3}\log n)$.

由图的谱分析可知除主特征值和其特征向量包含了图的大部分结构信息外，其他特征值及其对应的特征向量均代表了图中存在的噪声信息[18].且用户关系图 G 的邻接矩阵 $\boldsymbol{A}$ 的特征值具有一定的分布趋势，且其对应的特征向量具有相似的分布.

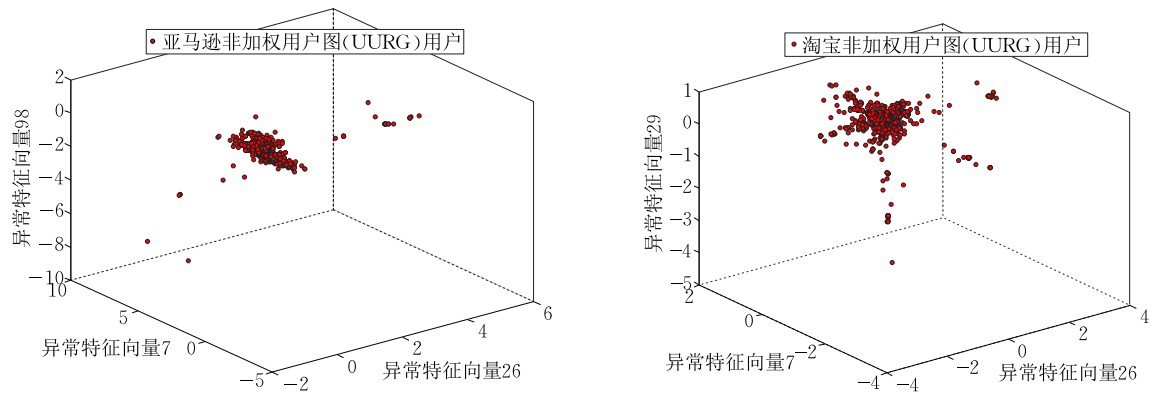
本文对两个实验数据集即淘宝和亚马逊电子商务平台用户评论数据分别建立加权和非加权用户关系图，并使用 Lancoz 算法计算其特征值和特征向量.为验证特征向量区分数据集中异常用户的能力，选取由 Lancoz 算法计算出的部分特征向量，将表 1 构造出的实验数据集中的用户在其上进行映射，结

果如图 1 和图 2 所示. 本文称该类能够区分实验数据集中异常用户的特征向量为典型异常特征向量. 该类典型异常特征向量即用户关系图矩阵所有特征向量中具有一定异常的特征向量. 若所有特征向量呈正态分布,则其中不满足整体分布的特征向量即属于典型异常特征向量. 目标即找到一种方式合理的表征特征向量的分布,以找到其中不满足于其分布的异常特征向量. 本文选取特征向量的峰度值和 L1 范数这两个较为普适的统计指标作为度量其分布的方法. 利用特征向量的 L1 范数和峰度值分布特点,发现其中不满足分布的异常特征向量. 图 1 和图 2 分别显示了两个实验数据集上加权用户关系图(WURG)和非加权用户关系图(UURG)邻接矩阵典型异常特征向量上的电商用户分布. 图中 X,Y,Z 轴分别为该实验数据集上的典型异常特征向量. 该类典型异常特征向量能够度量原用户关系图中电商水军团体造成的异常用户关系结构,即本文研究发现的主要目标.



(a) 亚马逊　　(b) 淘宝

图 1　亚马逊(a)和淘宝(b)加权用户关系图(WURG)邻接矩阵典型异常特征向量上的用户分布



(a) 亚马逊　　(b) 淘宝

图 2　亚马逊(a)和淘宝(b)非加权用户关系图(UURG)邻接矩阵典型异常特征向量上的用户分布

从图 1 和图 2 可以发现,两个实验数据集的特征向量中存在一些异常点不服从特征向量整体分布. 我们认为该类异常特征向量捕捉了用户关系图 G 中的异常结构,即大规模电商水军团体形成的异常用户关系结构[18].

4　基于用户关系图谱特征定位电商水军团体

根据上文可知,图邻接矩阵异常特征向量可反映图的异常结构. 本文分别利用特征向量的 L1 范数[22]和图邻接矩阵的峰度值 Kurtosis[19]度量用户关系图邻接矩阵的特征向量分布,以定位其中的异常噪声结构.

图 3 和图 4 分别显示了本文两个实验数据集中加权用户关系图(WURG)和非加权用户关系图(UURG)邻接矩阵排序前 100 位特征向量的 L1 范数和峰度值(Kurtosis)分布. 图中 X 轴为排序后的相应特征向量,Y 轴为其相应峰度值或 L1 范数值.

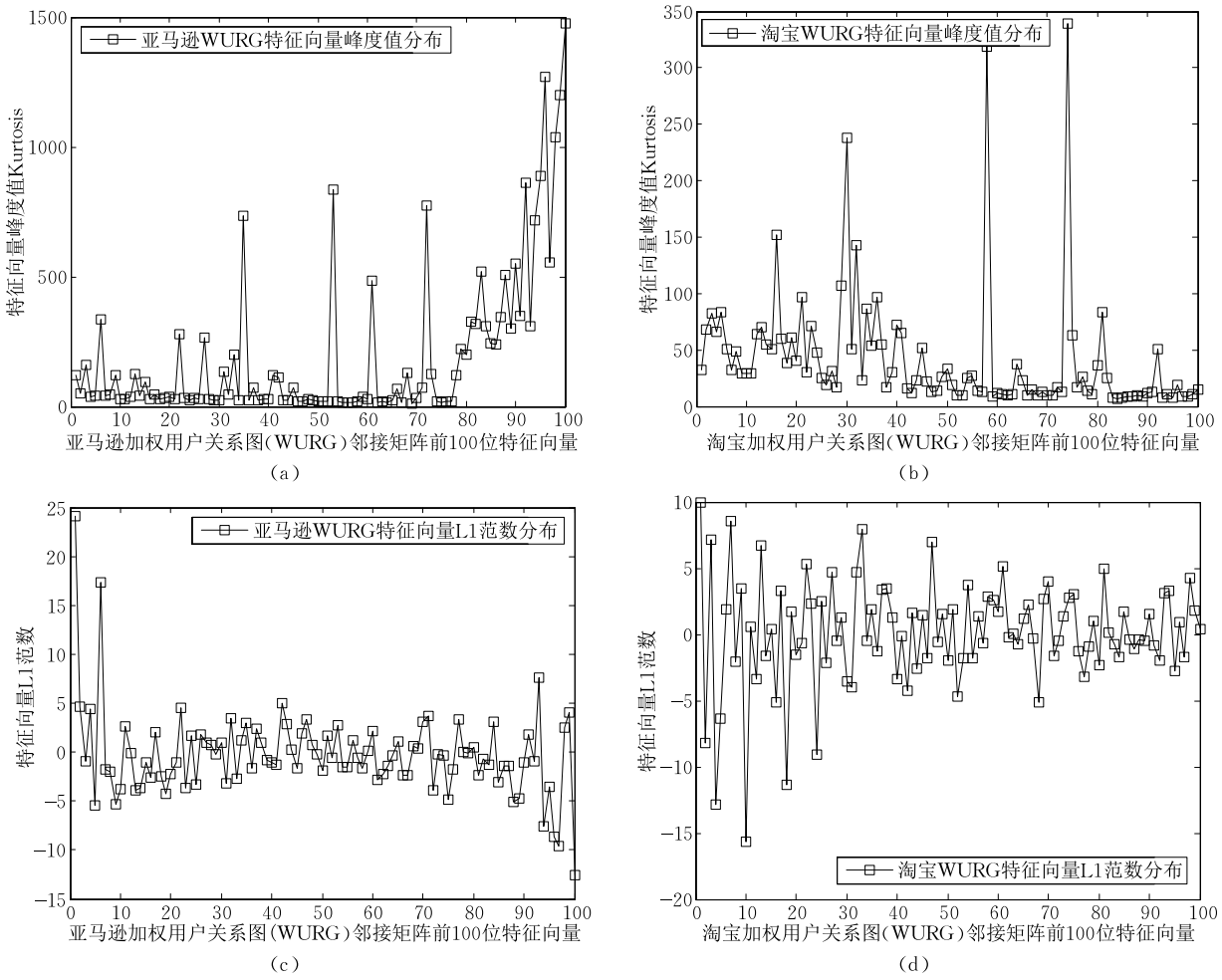


图 3 亚马逊(a)、(c)和淘宝(b)、(d)加权用户关系图(WURG)邻接矩阵排序前 100 特征向量峰度值(Kurtosis)(a)、(b)和 L1 范数(c)、(d)分布

分析图 3 和图 4 中用户关系图的 L1 范数和峰度值分布,发现峰度值在两个实验数据上的统计出的异常特征向量数目较多,即分布中异常点较多,其能够在保持特征向量整体趋势的基础上更加细粒度地发现异常特征向量.

本文分别统计分析了峰度值和 L1 范数检测出的典型异常特征向量.将峰度值和 L1 范数检测出的典型异常特征向量投影于源用户关系图中,发现峰度值表征出的典型异常特征向量对应的源用户关系图中异常用户团体信息,其行为特征具有明显的水军趋向性.表3显示了由峰度值和L1范数表征出的典型异常特征向量对应异常用户的评论特征统计均值.由表 3 可以发现,峰度值在两个实验数据集中检测出的典型异常特征向量所定位的可疑水军用户较多,即该类可疑水军用户具有评论数较多,且评论内容多具有较高重复性,评论时间间隔较短等电商水军行为特点[9].

表 3 峰度值与 L1 范数表征的异常特征向量检测用户对比

实验数据集		检测出的典型异常特征向量定位真实用户评论统计信息对比		
		评论数量/条	评论内容相似性(重复率)/%	评论时间间隔/天
亚马逊实验数据集	峰度值 Kurtosis	7.5	73.2	13.2
	L1 范数	5.1	51.5	24.3
淘宝实验数据集	峰度值 Kurtosis	8.4	67.5	17.3
	L1 范数	6.2	54.5	15.2

如上所述,该类由特征向量峰度值统计出的典型异常特征向量能够更好地表征源用户关系图中的异常结构.因此本文使用特征向量峰度值来统计特征向量的分布情况,以此定位不符合分布的特征向量.特征向量的峰度计算方法如下:

$$\kappa(x_j)=\frac{n\sum_{i=1}^{n}(x_j(i)-\bar{x}_j)^4}{\left(\sum_{i=1}^{n}(x_j(i)-\bar{x}_j)^2\right)^2} \tag{1}$$

其中,$\bar{x}_j=\frac{1}{n}\sum_{i=1}^{n}x_j(i)$.

本文分析了两个实验数据集中特征向量峰度值和其对应特征值的分布情况,发现两个实验数据集

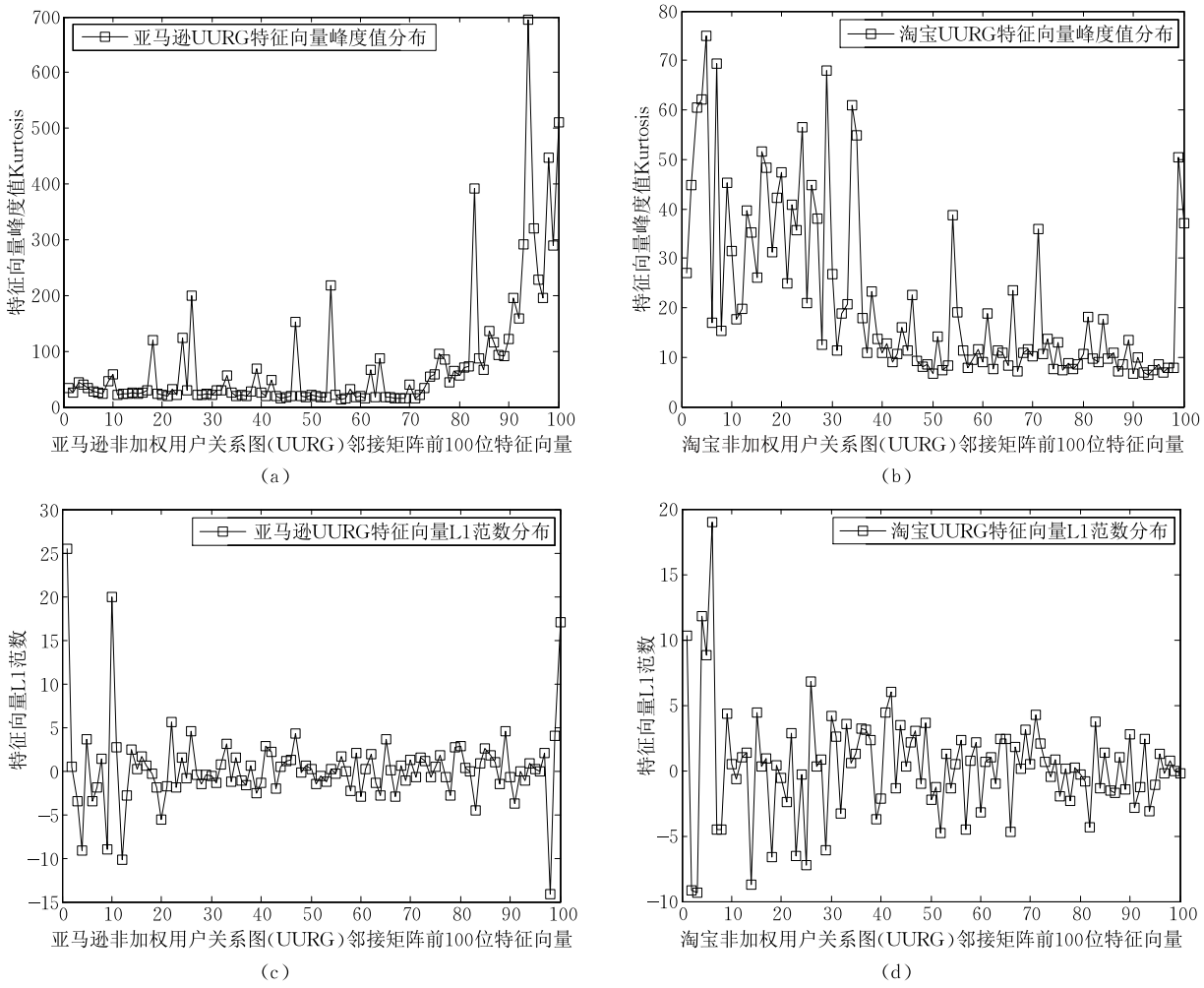


图 4　亚马逊(a)、(c)和淘宝(b)、(d)非加权用户关系图(UURG)邻接矩阵排序前 100 特征向量峰度值(Kurtosis)(a)、(b)和 L1 范数(c)、(d)分布

中特征向量峰度值和其特征值都趋近于正态分布，如上文第 2 部分所述特征向量与特征值分布相似. 因此本文定义 URGSSGD 算法定位用户关系图的异常特征向量，进而挖掘其捕捉到的大规模电商水军团体.

算法 1. URGSSGD：基于用户关系图谱特征定位大规模电商水军团体算法(User Relation Graph Spectrum-based Spammer Group Detection).

输入：User Relation Graph Adjacency Matrix $\boldsymbol{A}_{n\times n}$，Parameter l,k,c,γ,γ_{sg}

输出：*Spammer GroupSG*

1. Calculate eigenvectors x_i and eigenvalues λ_i using Lancoz Algorithm eigen-decompose $\boldsymbol{A}_{n\times n}$;
2. FOR $i=1\rightarrow l$ DO
3. Calculate kurtosis of x_i: $\kappa(x_i)$;
4. END FOR
5. FOR $i=1\rightarrow l$ DO
6. Calculate the set of x_j such that $\lambda_j=\left(\lambda_i\left(1-\sqrt{\frac{k}{c^2(l-k)}}\right),\lambda_i\left(1+\sqrt{\frac{k}{c^2(l-k)}}\right)\right)$;
7. Calculate the meanmand standard derivation σ for the kurtosis values of x_j find in last step;
8. IF $\kappa(x_i)>m+\gamma\sigma$ THEN
9. Output $x_{s,s\in[1,g]}$;
10. END IF
11. END FOR
12. FOR $s=1\rightarrow g$ DO
13. FOR $s=1\rightarrow g$ DO
14. FOR $i=1\rightarrow n$ DO
15. Calculate $M_{si}=\frac{\boldsymbol{A}(n,i).x_s}{|x_s|}$;
16. END FOR
17. END FOR
18. Calculate the meanmand standard derivation σ for the vector M_s;
19. FOR $i=1\rightarrow n$ DO
20. IF $m-\gamma_{sg}\sigma<M_{si}<m+\gamma_{sg}\sigma$ THEN
21. Add M_{si} to SG_s;

22. END IF
23. END FOR
24. Output SG_s;
25. END FOR

算法 1 中检测图邻接矩阵异常特征向量具体通过以下方式进行.使用特征向量峰度值度量特征向量分布.对于每一个特征向量,算法第 6 步计算其邻域大小.对于当前特征向量邻域中的所有特征向量,算法第 7 步计算其均值和方差.若当前特征向量的峰度值大于置信度外(算法第 8 步),则当前特征向量属于典型异常特征向量.

其中参数 n 代表邻接矩阵大小,即用户关系图节点数即用户数量.参数 l 代表实验中采用 Lancoz 算法求得的排序前 l 位特征值及其对应的特征向量进行用户关系图异常结构的定位.参数 k 和 c 代表调节当前特征向量邻居特征向量范围的参数[22].参数 γ 代表调节标准正态分布中的置信区间参数,用于判断当前用户关系图特征向量是否满足该正态分布,γ_{sg} 与 γ 相同,用于判断当前电商水军是否满足正态分布时的调节置信区间参数.对于本文采用的两个实验数据集,分别进行大量实验评估不同参数在不同用户关系图模型中定位大规模电商水军团体的能力,该部分将在 4.2 节实验参数评估部分进行详述.

利用上述 URGSSGD 算法本文在两个实验数据集不同用户关系图模型上发现了多个大规模电商水军团体.因正常用户不具有高度相似的目标产品交集且评论频率较低,采用表 1 所构造的用户评论数据集能够最大程度避免正常用户因相似购买兴趣导致的目标产品交集.典型异常特征向量即特定维度下电子商务网络水军区别于其他正常用户的异常分布,电商水军在该维度下具有相似区别于正常用户的异常特征.

图 5 显示了 URGSSGD 算法在本文两个实验数据集上定位的用户关系图异常特征向量所捕捉到的多个大规模电商水军团体.图中 X,Y 轴为 URGSSGD 算法在本文两个实验数据集上定位的用户关系图异常特征向量,图中每个点代表实验数据集中用户在异常特征向量上的分布.

5 实验与评价

5.1 实验设置

为了客观评估 URGSSGD 算法的效果,本文使用两个实验数据集:淘宝数据集和亚马逊数据集.淘宝实验数据集来源于大型电子商务平台淘宝网,本文抽取了淘宝部分热门手机商品的用户评论信息.其包括约 3000 个产品,102 498 个用户的 10 万条评论信息.对该数据集按照表 1 所示步骤进行了预处理,得到其中评论数超过 3 次的 862 个产品及其涉及的 2573 个用户和其产品评论信息作为实验数据.亚马逊实验数据集来自于网络公开数据集,文献[1,4,8]中曾使用.其包括了 32 075 个产品和 313 120 个用户的 404 637 条评论数据.因亚马逊实验数据集较大,本文选取了其中电子产品评论数据集作为实验初始数据集,以最大程度与淘宝平台中相应的电子产品评论数据集对应.同样按照表 1 所示步骤对其进行了预处理,得到了 5245 个用户及其产品评论信息作为实验数据.实验数据的统计信息如表 4 所示.

表 4 实验数据集统计信息

实验数据集	用户数量	关系数量	产品数量	评论数量
亚马逊数据集	5243	37747	7361	224039
淘宝数据集	2572	23745	862	7396

5.2 参数评估

为了准确地度量 URGSSGD 算法定位大规模电商水军团体的能力,本文分别设置两组实验,即加权用户关系图 WURG 模型和非加权用户关系图 UURG 模型下 URGSSGD 算法的实验.同时为验证不同算法参数在不同用户关系图模型下的效果,本文对每个参数进行了不同模型设置下的评估.如上文所述,URGSSGD 算法参数包括 l,k,c,γ,γ_{sg}.参数 k 和 c 调节当前特征向量邻居特征向量范围的参数,其中 k 值的变化对于邻居特征向量范围变化影响较为明显,在固定其他参数的条件下,对其进行不同值的测试,进而确定其最优值.本文将参数 k 的取值范围设为 $k\in[1,40]$,其在两个实验数据集上的测试结果如图 6 所示.同时本文发现参数 c 对于确定邻居特征向量范围的贡献度并不大,因此,根据文献[19]定理 4,本文算法在不同用户关系图模型中运行将时参数 c 置为 $\sqrt{3}/2$.参数 l 代表实验中采用 Lancoz 算法求得的排序前 l 位特征值及其对应的特征向量,本实验中将其值设为 100.结合上文所述,图邻接矩阵排序较前的特征值包含其大部分结构信息,实验选取排序前 100 位的特征值及其特征向量对其中存在的异常特征向量进行探测.参数 γ 代表调节标准正态分布中的置信区间参数,用于判

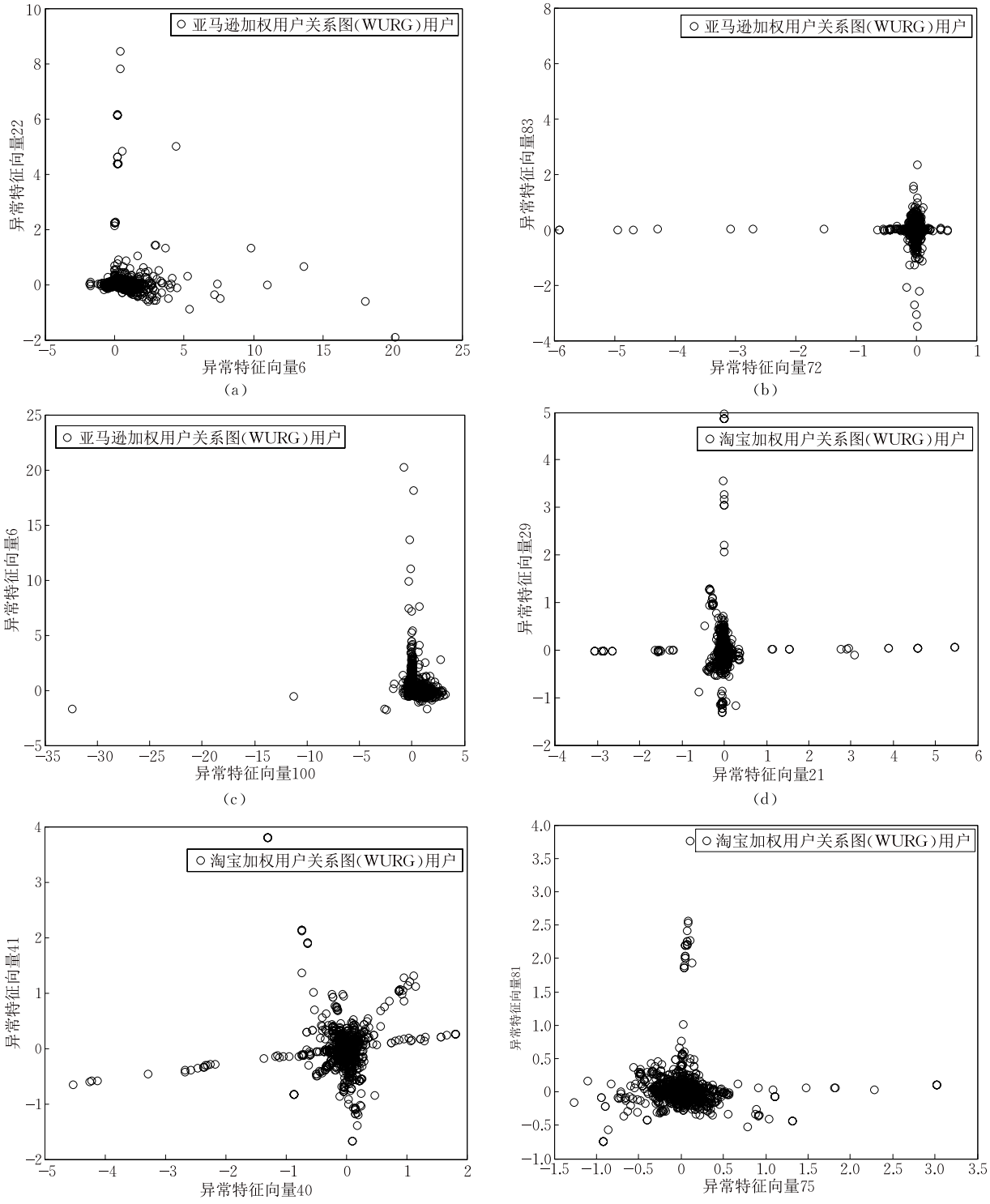


图 5　亚马逊(a)、(b)、(c)和淘宝(d)、(e)、(f)加权用户关系图(WURG)邻接矩阵上异常特征向量捕捉到的电商水军团体

断当前用户关系图特征向量是否满足该正态分布.根据统计学理论，γ 取值为 1.96 时，均值偏移 γ 单位代表该正态分布 95%的置信区间，因此在本文实验中将参数 γ 的取值范围设为 $\gamma\in[0.1,2]$. 本文发现 γ 参数不同的取值对于定位用户关系图模型中的异常特征向量影响较大，同样采用固定其他参数的方式，对参数 γ 的不同取值对于不同实验数据集不同用户关系图模型中 URGSSGD 算法运行的效果进行评估，评估结果如图 7 所示. 与 γ 相似，参数 γ_{sg} 用于判断当前电商水军团体是否满足正态分布时的置信区间范围参数，采用与评估参数 γ 相似的方法，本文对其进行了不同值的评估.

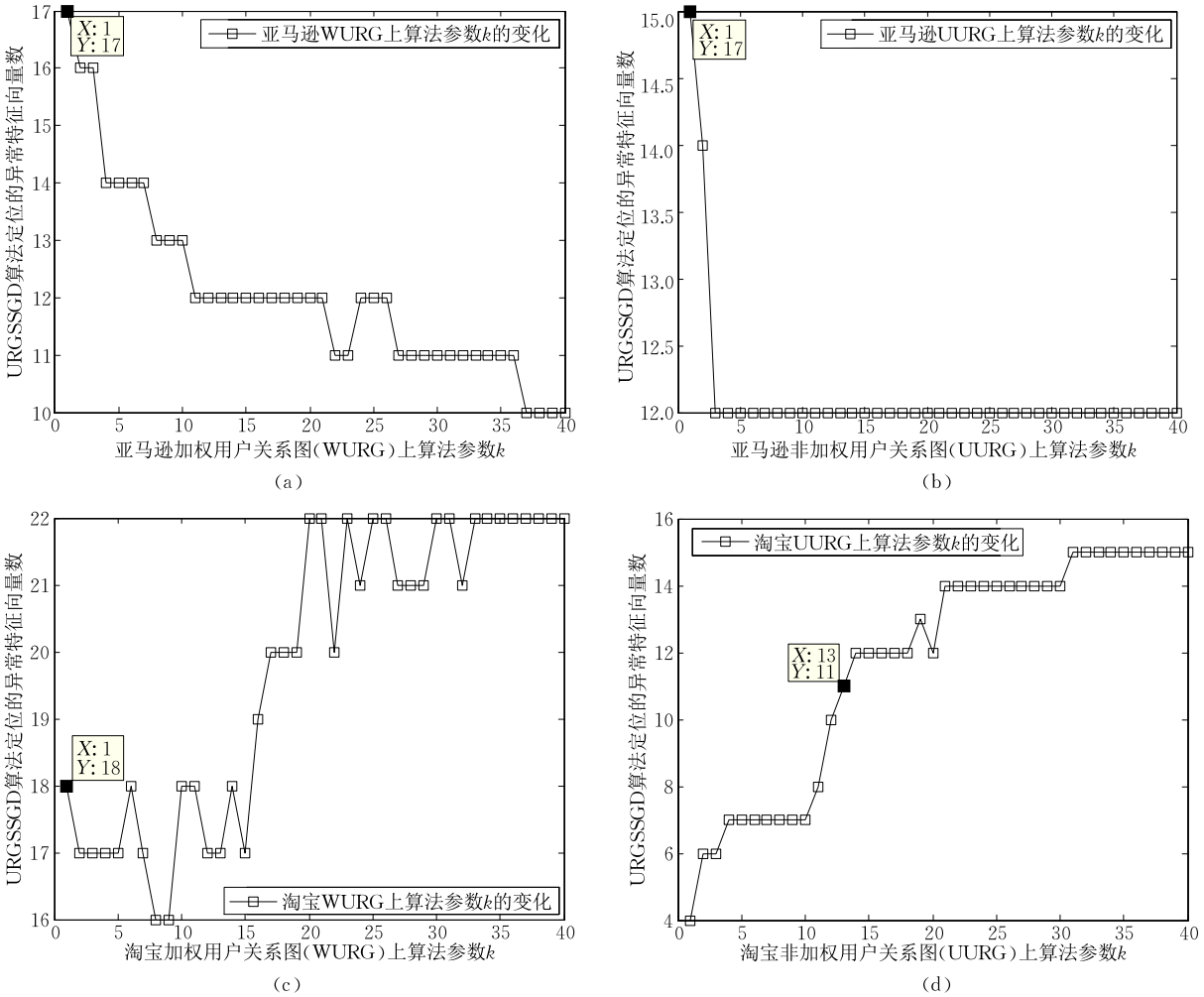


图 6 URGSSGD 算法参数 k 在亚马逊(a)、(b)和淘宝(c)、(d)加权用户关系图(WURG)(a)、(c)和非加权用户关系图(UURG)(b)、(d)模型上的评估

图 6 和图 7 显示了 URGSSGD 算法中对于定位大规模电商水军团体能力影响较大的参数 k 和 γ 在本文两个实验数据集上 WURG 和 UURG 模型上的运行结果. 图中 X 轴为当前参数的取值,Y 轴为当前参数下 URGSSGD 算法定位的异常特征向量数目. 图中标注点代表当前实验数据集用户关系图模型下参数的最优值.

为计算 URGSSGD 算法在不同实验数据集上不同用户关系图模型中各个参数的最优值,通过评估不同参数设置下 URGSSGD 算法定位的异常特征向量能力,即定位大规模电商水军团体的能力,来确定不同实验数据集中不同用户关系图模型的最优参数. 若当前参数能够较为全面地定位用户关系图中的异常程度较高的特征向量且能够避免过拟合现象,则当前参数设置优于其他参数. 图 8 中正方形代表当前参数在当前数据集模型下定位的异常特征向量. 曲线代表其源分布即用户关系图特征向量的峰度值分布. 从图 8 中可以发现,算法当前参数下定位的异常特征向量(正方形)几乎全面覆盖了其分布的峰值(曲线峰值),即偏离源分布的异常点.

通过对 URGSSGD 算法参数的大量实验和人工检验,确定了 URGSSGD 算法在本文两个实验数据集上不同用户关系图模型中的最优参数设置,表 5 显示了该最优参数集的详细信息. 同时表 6 显示了本文所有实验设置下 URGSSGD 算法的输出信息.

表 5 亚马逊和淘宝实验数据集上 URGSSGD 算法参数设置

最优参数集	加权用户关系图(WURG)	非加权用户关系图(UURG)
亚马逊实验数据集	$l=100$ $k=1$ $c=\sqrt{3}/2$ $\gamma=1.7$ $\gamma_{sg}=8$	$l=100$ $k=1$ $c=\sqrt{3}/2$ $\gamma=1.7$ $\gamma_{sg}=8$
淘宝实验数据集	$l=100$ $k=1$ $c=\sqrt{3}/2$ $\gamma=0.3$ $\gamma_{sg}=8$	$l=100$ $k=13$ $c=\sqrt{3}/2$ $\gamma=1.3$ $\gamma_{sg}=8$

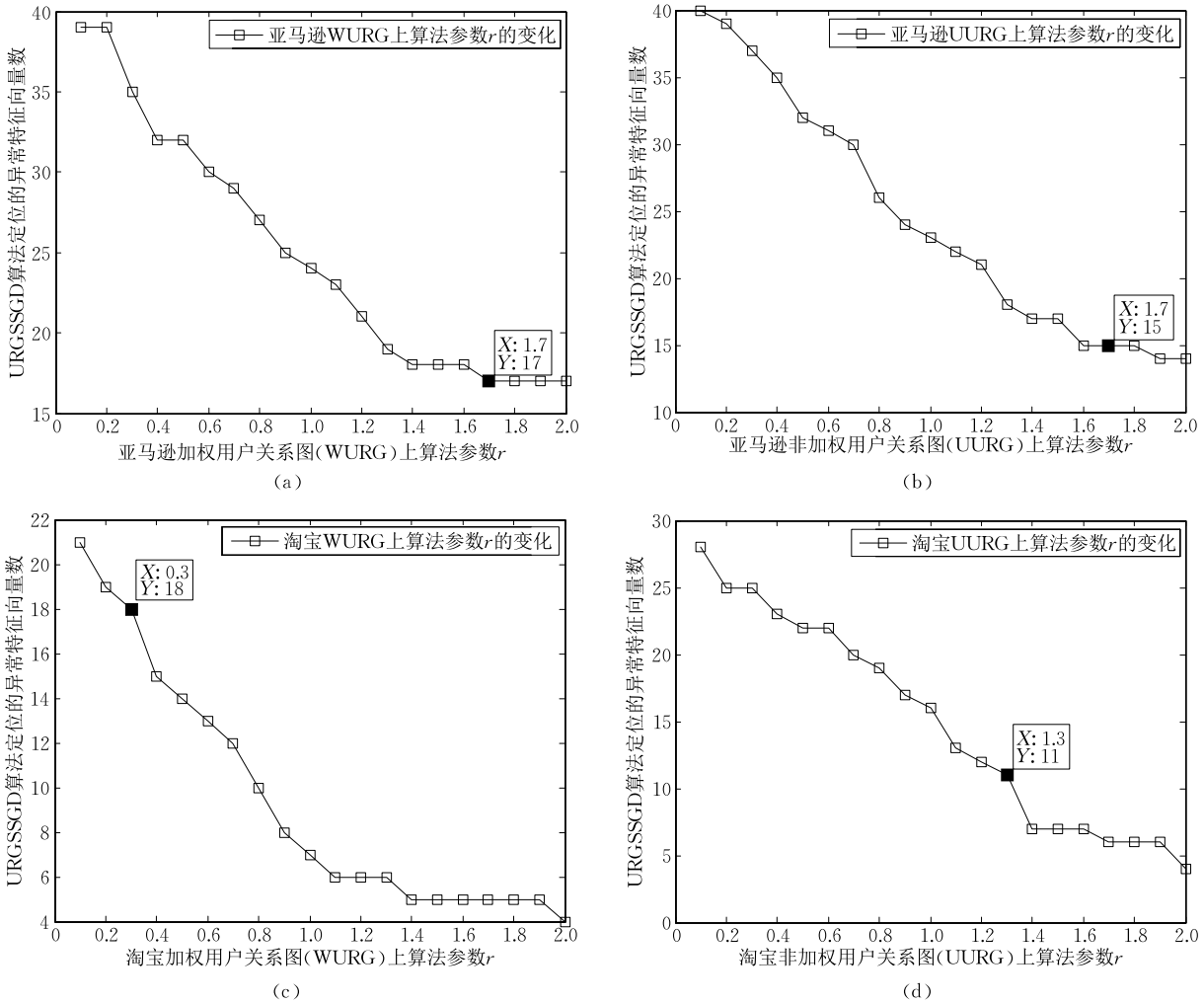


图 7　URGSSGD 算法参数 γ 在亚马逊(a)、(b)和淘宝(c)、(d)加权用户关系图(WURG)(a)、(c)和非加权用户关系图(UURG)(b)、(d)模型上的评估

表 6　亚马逊和淘宝实验数据集上 URGSSGD 算法在不同模型下的输出结果

URGSSGD 算法输出		输出用户总数	异常特征向量数	大规模电商水军团体数目
亚马逊数据集	WURG	95	17	6
	UURG	72	15	2
淘宝数据集	WURG	185	18	17
	UURG	194	11	9

5.3　实验结果评估

对于 URGSSGD 算法在不同实验数据集上发现的疑似水军用户，我们对其进行了人工标记，以评估算法定位电商水军团体的能力. 表 7 显示了 URGSSGD 算法在不同实验数据集上输出的水军数量.

表 7　亚马逊和淘宝实验数据集上 URGSSGD 算法在不同模型下输出水军结果

URGSSGD 算法输出水军数量(所占比例)	加权用户关系图(WURG)	非加权用户关系图(UURG)
亚马逊数据集	79(83.2%)	48(66.7%)
淘宝数据集	180(97.2%)	171(88.1%)

根据表 7 可知，URGSSGD 算法在亚马逊实验数据集 WURG 模型中发现 79 个水军用户，占所有输出用户的 83.2%，其在 UURG 模型中发现了 48 个水军用户，占所有输出用户的 66.7%；同时其在淘宝实验数据集 WURG 模型中定位了 180 个水军用户，占所有输出用户的 97.2%，在 UURG 模型中发现了 171 个水军用户，占所有输出用户的 88.1%.

分析上述实验结果，发现对于大规模电商水军团体的辨别，加权用户关系图模型能够定位更多的用户关系图异常特征向量，从而更加准确地定位数量较多的大规模电商水军团体. 这是因为电商平台用户关系权重的引入能够更加细粒度地度量用户间关系结构，从而更好地定位异常关系结构，挖掘大规模电商水军团体.

电商水军团体同时也是整个电商用户社团中区别于正常用户的用户团体，因此为了更好地衡量

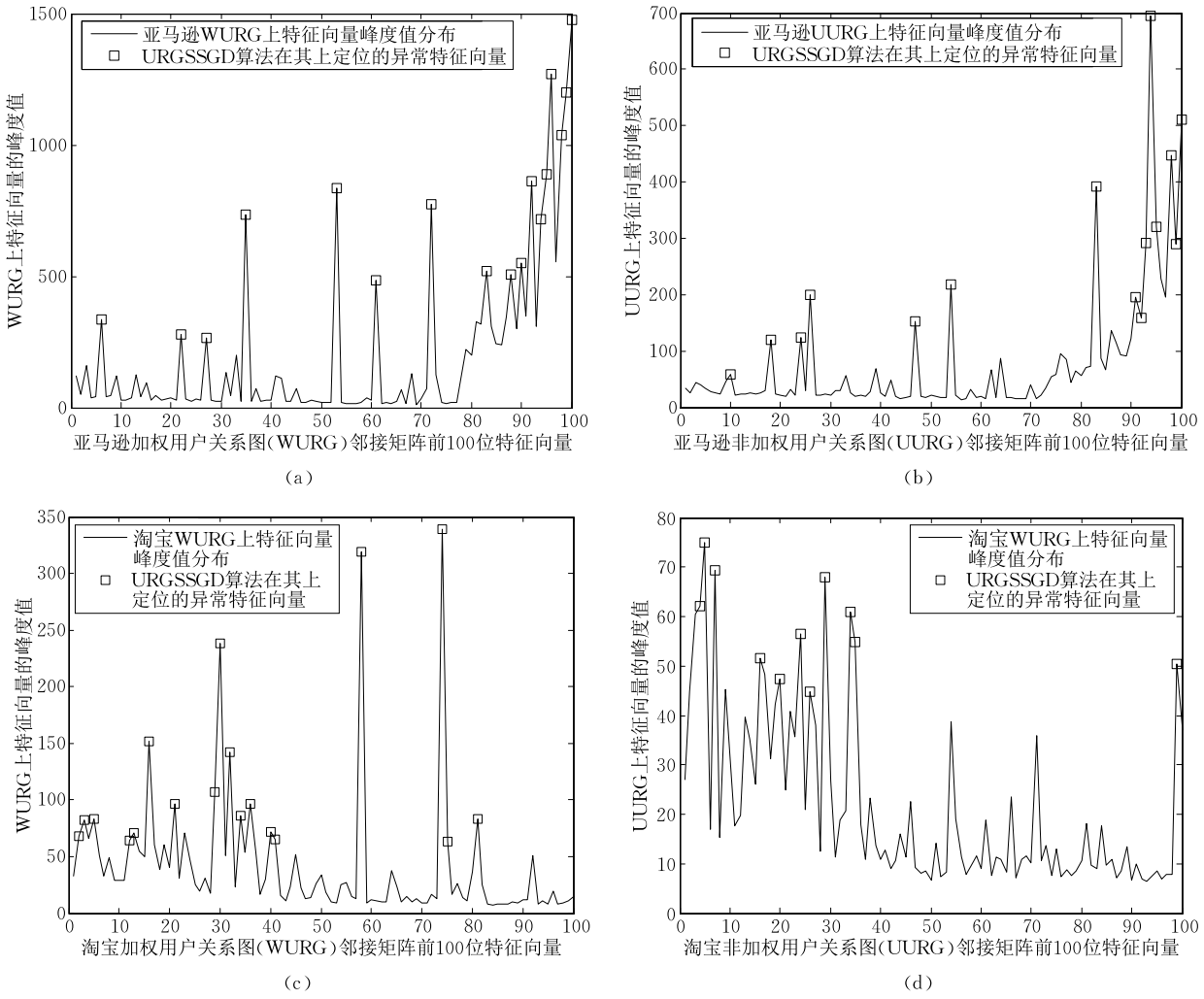


图 8 URGSSGD 算法最优参数在亚马逊(a)、(b)和淘宝(c)、(d)加权用户关系图(WURG)(a)、(c)和非加权用户关系图(UURG)(b)、(d)模型上定位的异常特征向量

URGSSGD 算法划分网络水军团体的能力,本文同时使用 Newman 算法对两个实验数据集中用户关系图进行划分,并对比人工标记结果,以衡量两个算法发现电商水军团体的能力. 表 8 显示了两个算法在不同实验数据集上输出的电商水军团体信息.

表 8 亚马逊和淘宝实验数据集上 URGSSGD 和 Newman 算法在 WURG 模型下的输出结果

算法输出		团体数	团体规模	准确率/%
亚马逊数据集	Newman	7	640	64.2
	URGSSGD	6	20	83.2
淘宝数据集	Newman	11	152	60.3
	URGSSGD	17	11	97.2

从表 8 可以看出 Newman 算法对于用户社团的划分粒度较大,即其划分出的社团规模较大,准确率较低. 相比之下,URGSSGD 发现的电商水军团体更加贴近其真实规模,且其准确率较高.

此外,本文将捕捉到的大规模电商水军团体进行了团体内部水军关系网络的建模. 其中将每个用户发布的评论总数作为其自身权值,并按照其权值将用户分为 3 类,分别为不活跃用户、中间用户、活跃用户. 活跃用户发布的评论数目超过 8 条,中间用户发布的评论数目在 3～5 条之间,不活跃用户发布的评论数目为 1～2 条. 存在于同一个电商水军团体中的用户之间均具有关系,利用用户间评论的相同产品数作为其关系权重. 按照其关系强度即关系权重的不同,将团体内用户间的关系分为 4 类,分别为强联系、中间联系、弱联系、无联系. 具有强联系的用户即具有超过 4 个的共同评论产品,具有中间联系的用户之间的共同评论产品数目为 2 个或 3 个,具有弱联系的用户的共同评论产品数为 1,用户间无联系则其具有的共同评论产品数为 0. 图 9 和图 10 显示了 URGSSGD 算法在亚马逊实验数据集和淘宝实验数据集中加权用户关系图(WURG)和非加权用户关系图(UURG)模型上定位的全部电商水

军团体.其中每个节点代表一个电商水军用户,其不同的形状特征代表了其自身权值.菱形节点代表活跃用户,三角形节点代表中间用户,椭圆形节点代表不活跃用户.图中用户间的关系,即两个节点间的连边线性宽度代表其不同关系强度.其中,具有强联系的用户连边为黑色粗曲线,具有中间联系的用户间的边为浅灰色粗线,具有弱联系的用户间连边为浅灰色细线、无联系的用户间连边为黑色虚线.

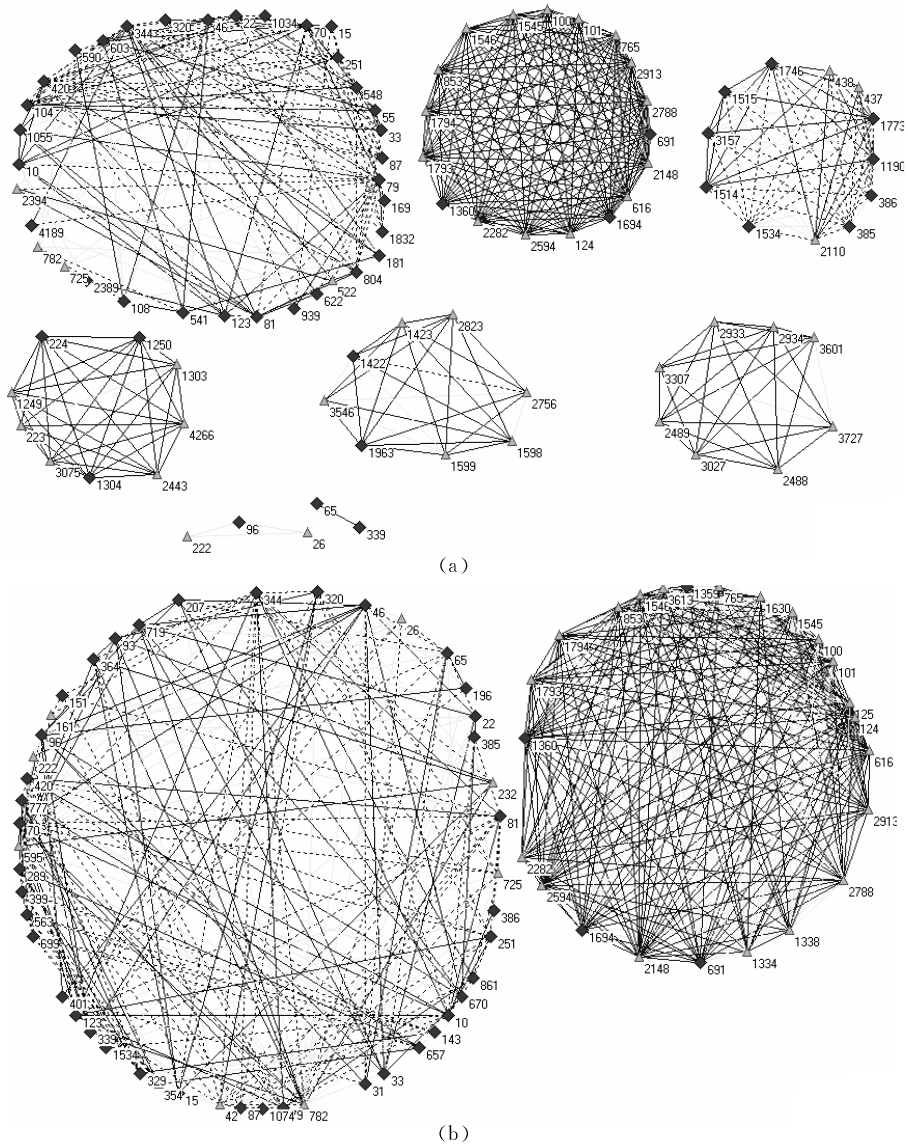


图 9　URGSSGD 在亚马逊加权用户关系图(WURG)(a)和非加权用户关系图(UURG)(b)模型中定位的大规模电商水军团体

分析图 9 和图 10,可以发现加权用户关系图(WURG)模型找出的大规模电商团体数目较多,且每个水军团体内部联系较为紧密,即团体内用户联系多为中间联系或强联系.这是因为加权用户关系图(WURG)模型能够更加细粒度地建模用户间的关系,定位微小的异常关系结构,从而发现更多的电商水军团体.综合上文所述,可以发现亚马逊实验数据集在加权用户关系图模型上定位的电商水军团体成员准确性较高,在加权用户关系图模型较为严格的用户关系筛选条件下,其定位大规模电商水军团体数目也较多.淘宝实验数据集上加权用户关系图模型输出的团体成员水军准确率也较高,其发现的大规模电商水军团体数目与非加权用户关系图模型发现的团体数目相差较小.

现有对于电商水军团体的识别多基于团体行为特征,该类团体行为特征以团体成员存在共同评论产品为前提.但现有电子商务平台中泛滥的多数电商水军团体为避免水军识别研究对其的检测,多通过分批操控大量电商水军傀儡账号的方式来避免水军团体内用户具有明显相似性.为验证本文提出的

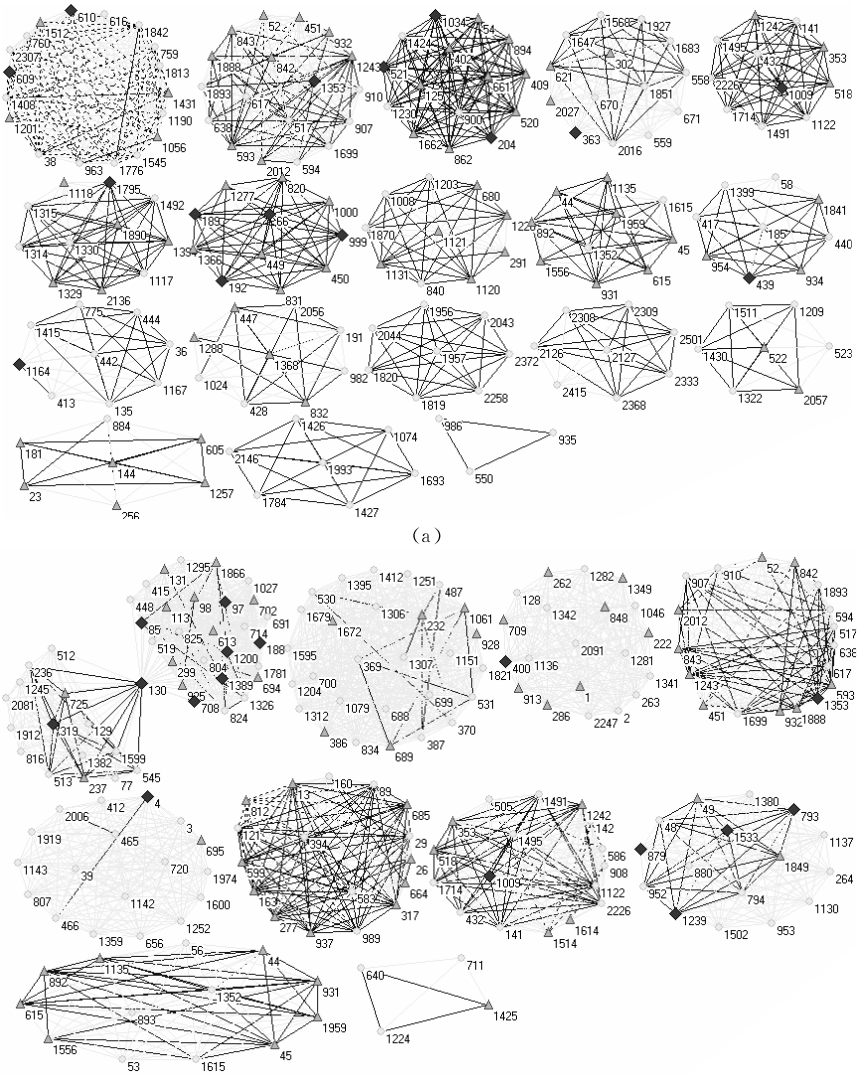


图 10 URGSSGD 在淘宝加权用户关系图(WURG)(a)和非加权用户关系图(UURG)(b)模型中定位的大规模电商水军团体

基于用户关系图谱特征发现大规模电子商务团体的算法对于该类不具有明显相似性的大规模电商水军团体的识别能力,实验通过对大规模电商水军团体建模时是否加入无联系用户关系进行比较分析.

图 11 分别显示了亚马逊和淘宝实验数据集上发现的某几个大规模电商水军团体在不考虑用户间明显相似性的情况下团体内部联系的对比.图中团体内部无联系成员较多(即用户间黑色虚线较多),即成员间不具有共同评论产品.该类团体在仅考虑团体内部成员行为特征相似性时,内部成员联系较弱,不易被发现.

综上所述,本文提出的 URGSSGD 算法在加权用户关系图(WURG)模型上能够捕捉该类不具有明显相似性的大规模电商水军团体内部成员间的联系,更好的定位该类容易被忽略危害较大的大规模电商水军团体.

6 结论与总结

电子商务网络水军大量泛滥导致电商平台服务质量不断下降,妨害电子商务用户的切身经济利益,因此电子商务领域网络水军识别已成为网络水军识别研究中亟待解决的重点研究问题.如何在电商水军复杂多变导致高隐蔽性行为的条件下保证电商水军的识别效果是该研究领域重点关注的问题.本文分析电子商务平台水军团体行为特点后,发现电商水军团体间关系结构的不易隐藏性.定义加权用户关系图模型建模电子商务用户关系网络,提出基于用户关系图谱特征发现大规模电商水军团体算法,并评估了各个算法参数在不同用户关系图模型下的

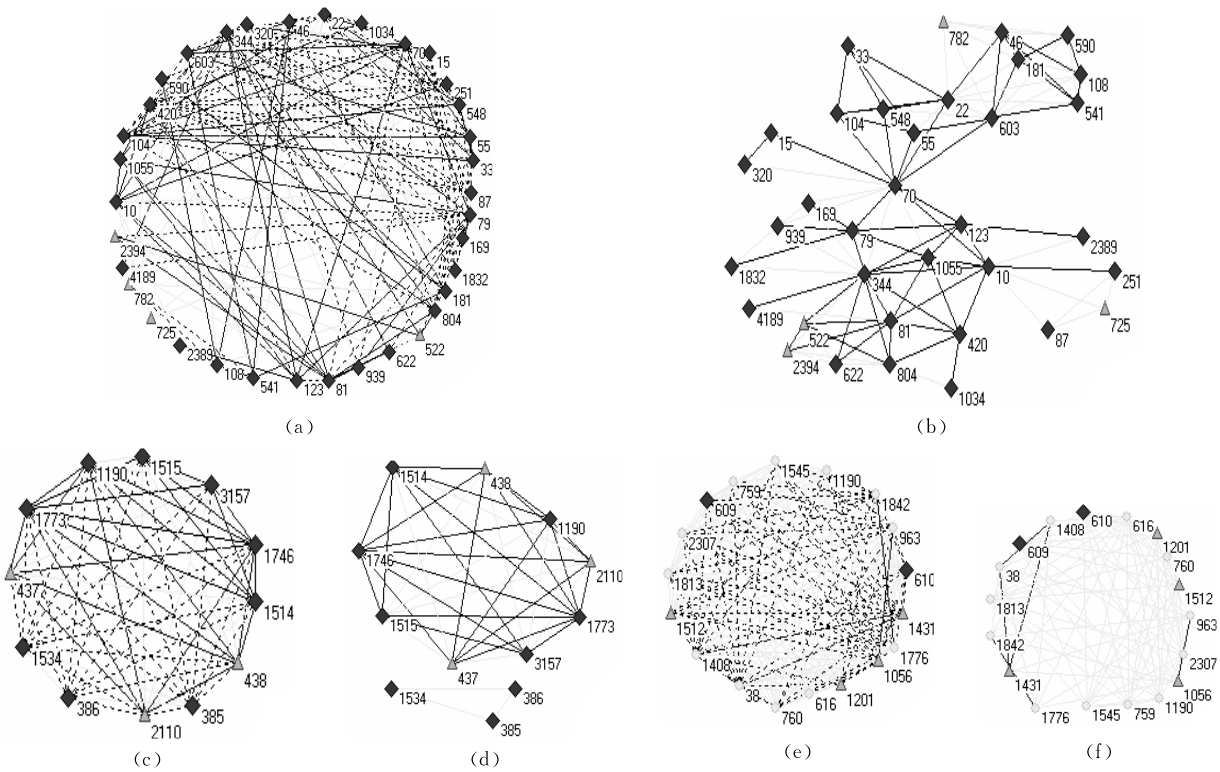


图 11　亚马逊(a)、(b)、(c)、(d)和淘宝(e)、(f)加权用户关系图(WURG)模型发现的大规模电商水军团体关系对比

识别能力.本文方法与已有电商水军识别研究角度不同,能够避免由于电商水军频繁更新用户信息或分批操控大量电商水军傀儡账号形成不具有明显相似性的大规模电商水军团体导致的水军特征模式识别瓶颈,从而保证较为准确地发现危害较大的大规模电商水军团体.此外,对比传统社团发现算法对电子商务用户的划分,本文方法能够更加真实准确地发现潜藏电商水军团体.如何更加准确高效地利用关系特征定位电商水军是本文下一步需要解决的问题.

致　谢　在此,我们向对本文的工作给予支持和建议的同行表示感谢!

参　考　文　献

[1] Mo Qian, Yang Ke. Overview of Web spammer detection. Journal of Software, 2014, 25(7): 1505-1526(in Chinese)
(莫倩, 杨珂. 网络水军识别研究. 软件学报, 2014, 25(7): 1505-1526)

[2] Lim E P, Nguyen V A, Jindal N, et al. Detecting product review spammers using rating behaviors//Proceedings of the 19th ACM International Conference on Information and Knowledge Management (CIKM 2010). Toronto, Canada, 2010: 939-948

[3] Xu C. Detecting collusive spammers in online review communities//Proceedings of the 6th Ph. D. Students Workshop on Information and Knowledge Management (PIKM 2013). San Francisco, USA, 2013: 33-40

[4] Li F, Huang M, Yang Y, Zhu X. Learning to identify review spam//Proceedings of the 22nd International Joint Conference on Artificial Intelligence (IJCAI 2011). Barcelona, Spain, 2011: 2488-2493

[5] Jindal N, Liu B, Lim E P. Finding unusual review patterns using unexpected rule//Proceedings of the 19th ACM International Conference on Information and Knowledge Management (CIKM 2010). Toronto, Canada, 2010: 1549-1552

[6] Ott M, Choi Y, Cardie C, Hancock J T. Finding deceptive opinion spam by any stretch of the imagination//Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, Vol. 1 (ACL HLT 2011). Portland, USA, 2011: 309-319

[7] Jindal N, Liu B. Opinion spam and analysis//Proceedings of the 2008 International Conference on Web Search and Data Mining (WSDM 2008). Palo Alto, USA, 2008: 219-230

[8] Wang G, Xie S, Liu B, Yu P S. Review graph based online store review spammer detection//Proceedings of the 11th International Conference on Data Mining (ICDM 2011). Vancouver, Canada, 2011: 1242-1247

[9] Mukherjee A, Liu B, Glance N. Spotting fake reviewer groups in consumer reviews//Proceedings of the 21st International Conference on World Wide Web (WWW 2012). Lyon, France, 2012: 191-200

[10] Xie S, Wang G, Lin S, Yu P S. Review spam detection via

temporal pattern discovery//Proceedings of the 18th ACM SIGKDD International Conference on Knowledge Discovery and Data mining (KDD 2012). Beijing, China, 2012: 823-831

[11] Fei G, Mukherjee A, Liu B, et al. Exploiting burstiness in reviews for review spammer detection//Proceedings of the 7th International AAAI Conference on Weblogs and Social Media (ICWSM 2013). Ann Arbor, USA, 2013: 175-184

[12] Feng S, Xing L, Gogar A, Choi Y. Distributional footprints of deceptive product reviews//Proceedings of the 6th International AAAI Conference on Weblogs and Social Media (ICWSM 2012). Dublin, Ireland, 2012: 98-105

[13] Gammereldin S E A, Mohamed E M. Analyzing and revealing spammer accounts in email social network: SUST mail case//Proceedings of the 4th International Conference on Information and Communication Technology. Karachi, Pakistan, 2011: 3-11

[14] Las-Casas P H B, Guedes D, Almeida J M, et al. SpaDeS: Detecting spammers at the source network. Computer Networks, 2012, 57(2): 526-539

[15] Song J, Lee S, Kim J. Spam filtering in Twitter using sender-receiver relationship//Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection (RAID 2011). Menlo Park, USA, 2011: 301-317

[16] Mukherjee A, Kumar A, Liu B, et al. Spotting opinion spammers using behavioral footprints//Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2013). Chicaho, USA 2013: 632-640

[17] Wang G, Xie S, Liu B, Yu P S. Identify online store review spammers via social review graph. ACM Transaction on Intelligent Systems and Technology, 2012, 3(4): 61

[18] Ying X, Wu X, Barbará D. Spectrum based fraud detection in social networks//Proceedings of the 27th International Conference on Data Engineering (ICDE 2011). Hannover, Germany, 2011: 912-923

[19] Wu L, Wu X, Lu A, et al. A spectral approach to detecting subtle anomalies in graphs. Journal of Intelligent Information Systems, 2013, 41(2): 313-337

[20] Seary A, Richards W. Spectral methods for analyzing and visualizing networks: An introduction//Breiger R, Carley K M, Pattison P eds. Dynamic Social Network Modeling and Analysis. Washington, USA: National Academies Press, 2003: 209-228

[21] Füredi Z, Komlós J. The eigenvalues of random symmetric matrices. Combinatorica, 1981, 1(3): 233-241

[22] Miller B, Bliss N, Wolfe P J. Subgraph detection using eigenvector L1 norms//Proceedings of the 23rd Advances in Neural Information Processing Systems. Vancouver, Canada, 2010: 1633-1641

HAN Zhong-Ming, born in 1972, Ph. D., associate professor. His current research interests include web data mining and pattern recognition.

YANG Ke, born in 1990, M. S. candidate. Her current research interests include web data mining and web spammers' detection.

TAN Xu-Sheng, born in 1989, M. S. candidate. His current research interests include web data mining and community detection.

Background

Web spammers' detection has already become one of the hottest topics in the web data mining field in these days. The main task of web spammers' detection is how to recognize the spammers' feature and behavior from big datasets in order to improve network environment and keep network clean. Nowadays, many works is focusing on improving the performance of web spammers' detection. The targeted domain of web spammers include social network, online shopping websites, email service and so on. The big challenge of web spammers' detection is there are more and more complex and hidden behaviors of web spammers when they campaign with the detection research. Also, many works are focusing on improving the detection evaluation. There are still many problems in the process of web spammers' detection and the accuracy of web spammers' detecting still need improve. However, there are a few researches in the Chinese web spammers' detection. While most spammers begin to function as many large spammer groups to game the detection system, the individual member of the large group tends to act like a normal user. The behavior pattern discovery of spammers cannot detect these large spammer groups. In our work, we propose a novel angle to this problem by modeling the weight relation network of online shopping websites users.

Our team has done a lot of work on the detection of web spammers. Our team has investigated the detection of Sina Weibo spammers. We found many kinds of spammer behaviors in social network Sina Weibo. All of our related work has provided the good foundation of web spammers' detection.

This work is supported by the National Natural Science Foundation of China under Grant No. 61170112. All its previous research results could speed our research. All in all, web spammers' detection could improve network environment and keep network clean. Its research result is very meaningful.