文章编号:1671-6833(2022)02-0007-08

社交网络中协同舆论欺诈检测方法应用研究

吴小燕[1], 刘 强[1], 朱成璋[2]

(1.国防科技大学 计算机学院,湖南 长沙 410005; 2.军事科学院 战争研究院,北京 100091)

摘 要: 为了能够使网络空间提供更加可靠的信息,欺诈检测变得越来越重要,但现有的方法在检测欺诈用户时仅考虑了用户评论之间评论相同商品时形成的静态密集子图,而忽略了用户自身在评论时的异常行为,从而导致准确性较低,在实践中往往需要进一步手动验证检测结果的可靠性。针对此问题,提出了一种协同舆论欺诈检测(CPOFD)方法,该方法使用一种新的度量,即对比可疑度。该度量主要包括拓扑连接的信息,使得 CPOFD 方法能够通过拓扑连接、时间戳以及评分等信息有效检测欺诈者的异常行为,以更为聚合的方式检测欺诈群体。该度量强调了欺诈者和正常用户的动态对比,使得算法能够在拓扑连接、时间戳以及评分方面更为有效地检测欺诈者的异常行为。同时,CPOFD 方法结合基于密度子图的聚类算法和决策树分类算法将社交网络中用户进行有效分组,且在聚簇分类时使用模拟退火算法进行剪枝优化,能更加简洁快速地寻找近似最优解,时间复杂度与欺诈者数量呈线性关系,具有较高的可扩展性。基于 Yelp 数据集的实验结果表明:CPOFD 方法对欺诈舆论检测的准确度大多数在 98%以上,验证了 CPOFD 方法的有效性。

关键词: 欺诈检测; 协同欺诈检测; 无监督欺诈检测; 行为识别; 社交网络安全

中图分类号: TP393 **文献标志码**: A **doi**:10.13705/j.issn.1671-6833.2022.02.010

0 引言

在大数据时代背景下,各种网络平台、网络应用爆发式增长,网络信息传播方式、广度、速度都是之前任何一个时代无法比拟的,网络传播环境的复杂度也前所未有。在这种环境下,随之而来的网络舆论欺诈事件也呈指数级增长。国际咨询公司 Gartner 曾预测:到 2020 年,互联网虚假信息将面临泛滥之势,基于人工智能的造假能力将远超虚假信息检测的能力[1]。舆论欺诈给人们生活带来极大的危害,影响人们的正常生活,而欺诈者使用舆论欺诈牟取暴利,也给国家利益造成巨大损失,因此,在网络空间中检测出舆论欺诈评论、欺诈用户和欺诈行为迫在眉睫。

当前欺诈审查检测上的研究主要集中在分析用户和审查对应项目的行为和社会关系[2]。Hooi 等[3]提出通过物体度数的反对数来加权边缘的可疑性,以找出可疑度最大的最紧密子网络。Beutel 等[4]通过 CrossSpot 算法,采用泊松模型估计块的可疑性。Shehnepoor 等[5]提出了 NetSpam 框架,该框架将检测过程映射到网络中的分类问题,易于执行。但是,这些方法忽略了协作操纵的复杂性,协作欺诈者可能并非异常并且规模较小等问题。为解决上述问题,更先进的方法是为欺诈用户行为建模,显示出更好的性能[2]。但是,该方法需要搜集每个用户大量历史数据,当面对冷启动问题(即新用户刚刚发布新评论)时,由于缺少新用户的历史信息,可能无法提取行为特征。Lovisotto 等[6]研究了欺诈审查检测中的冷启动问题,该方法通过考虑用户、项目和评论之间的相关性来处理冷启动问题。You 等[7]通过将实体之间的关系与实体属性合并在一起,进一步解决了此类问题。一些研究者[8-11]通过将实体交互和用户社会关系融入到图中,进行了更深入的研究。

采用这些方法可能会出现 2 个问题:①如 Mukherjee 等[12]所述,仅使用评论本身是无效的,并且容易受到伪装的影响;②需要高质量的标记数据,这在现实生活中确实很难获得[13]。因此,

收稿日期:2021-08-12;**修订日期**:2021-10-18

基金项目:国家自然科学基金资助项目(61703539);国家重点研发计划项目(2018YFB0204301);湖南省自然科学基金资助项目(2018JJ3611)

通信作者:朱成璋(1990—),男,湖南湘潭人,军事科学院助理研究员,博士,主要从事人工智能、数据科学、高性能仿真等研究,E-mail:kevin.zhu.chine@ hotmail.com。

上述方法准确性较低,在实践中往往需要进一步通过手工验证的方式来检验结果的可靠性。因此,对这些方法进行改进十分必要,本文提出了一种协同舆论欺诈检测(collaborative public opinion fraud detection,CPOFD)方法,该方法基于密度子图的聚类算法与决策树分类算法,将用户、商户、评分、时间戳为元组构成二部图,划分数据集,使用贪婪算法得到不同欺诈者团体。该方法在很大程度上保留了数据之间的完整关系,通过用户可疑性变化来进行贪婪选择,较高效地完成了欺诈检测。

1 面向异构欺诈者群体的舆论欺诈检测方法

1.1 基本定义

本文的目标是找到作用于宿节点 $B \subset V$ 的可疑源节点 $A \subset V$ 的锁步行为。这基本上可以通过密度来测量源节点 A 与宿节点 B 的总啮合。本文算法指标允许进行多种方法的密度度量。但是,由于平均程度度量标准一般包含太多节点,因此本文将 $D(A,B)$ 表示的度量用作算法的基础,定义为

$$D(A,B)=\frac{\sum_{v_i\in B} f_A(v_i)}{|A|+|B|}。\tag{1}$$

式中:$f_A(v_i)$ 为源节点 A 到宿节点 v_i 的总边沿频率,也可以看作 A 在 v_i 上的锁步。

$$f_A(v_i)=\sum_{(u_j,v_i)\in E\wedge u_j\in A}\sigma_{ji}\cdot e_{ji}。\tag{2}$$

式中:常数 σ_{ji} 为边的全局可疑度,如果未将额外的全局可疑度分配给节点对 (u_j,v_i),则 σ_{ji} 等于1;e_{ji} 为邻接矩阵 $\boldsymbol{M}$ 的元素,即节点对 (u_j,v_i) 之间的边缘频率。

为了最大化 $D(A,B)$,可疑源节点 A 和宿节点 B 是相互依赖的,因此,引入对比可疑度:在给定可疑源节点 A 的情况下,对比可疑度 $P(v_i\in B|A)$ 定义为属于 B(可疑对象集)的宿节点 v_i 的条件似然。

对比可疑度的直观思想:在大多数情况下,需要判断当前选择的可疑用户 A 对于对象的可疑性。例如,如果该用户相连对象中有许多非 A 中的用户,则该用户显得非常可疑。如果某用户的相连对象中有一些可疑用户,则该用户更加可疑。物体的突发与降落主要由 A 引起,因此,这种可疑度对 A 中用户与非 A 中用户或整个用户之间进行对比。引入对比可疑度以及突发与降落的情况是一种新的尝试。在详细描述该检测算法之前,首先给出一些基本的符号解释和定义。

定义1 对比可疑度。给定一个有向图 $G=(U,W,E)$,U 为用户节点集;W 为商户节点集;E 为用户对象之间的特征(评分或者是时间戳)。令 $A\subseteq U$ 为用户的子集,$B\subseteq W$ 为商户的子集,$S=A\cup B$,$P=U\cup W$。本文用 g 表示算法优化的密度度量,f 表示可疑度,则:

$$g(S)=\frac{f(S)}{|S|};\tag{3}$$

$$f(S)=f_v(S)+f_e(S)=\sum_{i\in S}a_i+\sum_{i,j\in S\wedge(i,j)\in\varepsilon}c_{ij};\tag{4}$$

$$E[D(A,B)]=\frac{1}{|A|+\sum_{k\in V}P(v_k|A)}\sum_{i\in V}f(v_i)P(v_i|A)。\tag{5}$$

定义2 突发与降落。根据文献[6]中"Sleeping Beauty"的定义,本文借鉴该文献中一种无参数测量方法,使用从起点到爆发点的辅助直线距离最大化的点来确定唤醒点,唤醒点之后是突发,爆发点之后是降落。

定义3 优先级树。优先级树是包含 $n(n\geqslant 1)$ 个节点且满足下列条件的有限集合:

(1) 优先级树中的每一个节点都由1个 $N(N\geqslant 1)$ 元组组成;

(2) 优先级树的更新是根据对比可疑度的动态变化来更新的。

1.2 突发与降落

突发与降落是舆论欺诈检测产生巨大偏差的重要原因之一。在大多数实际设置中,通常都可以使用创建边缘的时间戳来表示加入图的时间节点,然而对于转发数相同的两用户子组来说,其可疑性是不一定相同的(大概率是一定不相同的),因此,本文将时间属性包含在算法框架中,以定义对比可疑度。图1是数据集 Yelp_Zip 中时间属性与节点边缘数图,从图1可以发现,不同时间点用户评论数相差较大。图2为截取图1中曲线最后一小部分来对突发和降落特征进行分析,但是本文实验中使用的是总体情况中的突发和降落。

将连接到宿节点 v 的边的时间戳列表表示为 T_v。为了简化表示,在讨论单个给定接收器节点 v 时,使用不带下标的 T。T 的时间序列表示为 $\{(t_0,c_0),(t_1,c_1),\cdots,(t_e,c_e)\}$,即 T 的直方图。c_i 是时间段 $[t_i-\Delta t/2,t_i+\Delta t/2]$ 中的时间戳数,其中 Δt 为直方图时间宽度。当 T 增加时,本文的算法可以低成本更新时间序列。

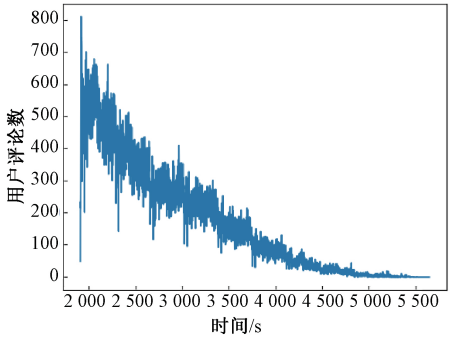

图 1　用户评论数与时间的关系

Figure 1　Relationship between the number of user comments and time

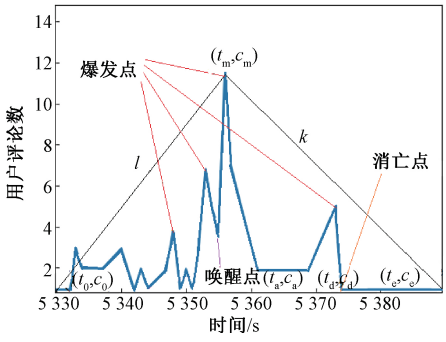

图 2　检测突发与降落

Figure 2　Detection of temporal bursts and drops

为了考虑突发和降落模式,需要确定突发的起点和时间序列 T 下降的终点。设最大爆发点为 (t_m,c_m),最大值为 c_m。图 2 显示了来自数据集 Zip 中某一部分消息的时间序列 T,从左下角 (t_0,c_0) 到 (t_m,c_m) 作辅助直线 l,最大的唤醒点 (t_m,c_m) 定义为时间序列 T 上使距离最大化的点。唤醒点 (t_a,c_a) 满足:

$$t_a = \arg\max_{(c,t)\in\tau,t<t_m} \frac{|(c_m-c_0)t-(t_m-t_0)c+t_mc_0-c_mt_0|}{\sqrt{(c_m-c_0)^2+(t_m-t_0)^2}}。\tag{6}$$

仅找到一个突发的唤醒点是不够的,因为可能会出现多个突发。因此,应考虑子突发点和相关的唤醒点。故本文在总算法框架中增加一种递归算法 MultiBurst。为此,找到唤醒点和爆发点后,爆发意识的对比可疑度满足 $P(v_i \mid A) \propto q(\varphi_i)$。

$$\varphi_i = \frac{\Phi(T_A)}{\Phi(T_U)};\tag{7}$$

$$\Phi(T) = \sum_{(t_a,t_m)} \Delta c_{am} \cdot s_{am} \sum_{t\in T} 1,\quad t\in[t_a,t_m]。\tag{8}$$

式中:φ_i 为 A 中源节点的参与率。T_A 为从 A 到接收节点 v_i 的时间序列。在此根据当前脉冲串的陡峭程度使用 s_{am} 作为权重。值得注意的是,MultiBurst算法仅需要执行一次。通过预处理唤醒点和突发点,计算宿节点 v 的对比可疑度的复杂度 $O(d_v)$,其中 d_v 表示宿节点 v 的度,因此,整个宿节点的复杂度为 $O(|E|)$。

实际上,突然下降也是欺诈行为的主要模式,因为在完成攻击后,欺诈者通常会迅速停止活动。为了利用突然下降的可疑模式,本文将消亡点定义为下降的终点。消亡点就是图中突增点之后以时间为横轴的线陡降并逐渐趋于零的临界点。由于图 2 只是选取了某段时间,所以消亡点不是特别明确。从最高点 (t_m,c_m) 到其后一点 (t_e,c_e) 绘制了另一条辅助直线,可以通过使到该直线的距离最大的点来找到消亡点 (t_d,c_d)。因此,这里可以通过爆发点和消亡点之间的绝对斜率值 $s_{bd}=(c_m-c_d)/(t_d-t_m)$ 发现“突然下降”。由于在波动的时间序列 T 中可能会有多次下降,因此选择幅度最大的下降为消亡点。为了找到最大跌落,还需要运用递归算法,算法步骤如下:

步骤 1　根据定义找到最大点 (t_m,c_m) 和相应的消亡点 (t_d,c_d);

步骤 2　计算当前的下降斜率 s_{bd},并且下降量 $\Delta c_{bd}=c_m-c_d$;

步骤 3　递归求出 T 的左右部分的下降斜率和下降量。

该算法返回递归求出的最大下降量 Δc_{bd} 及其下降斜率 s_{bd},使用加权下降斜率作为式(2)中的整体可疑度,以测量下降可疑度,即

$$\sigma = \Delta c_{bd} \cdot s_{bd}。\tag{9}$$

2　基于密度子图的聚类模型

一般的基于密度子图的聚类算法思想:首先随机选取一个序列,按照给定长度 w 将其分割成单个的子序列,从这些子序列中随机选取一个作为候选体,放入候选体集,再从剩余序列中找出与候选体集中所有候选体最相近的实例,放入候选体集。每次只增加一个实例[14]。基于密度子图的聚类算法先是建立最小生成树,构建聚类层次结构,压缩聚类树后提取簇。每个聚类都有一个密度最大的点作为聚类中心,每个聚类中心吸引并连接周围的较低密度点,且不同的聚类中心点相距较远。将每个集群的密度分为几个子集,根据该子集获得可以合并或分离的集群,并获得不同密度的集群,即完成聚类。为了实现该思想,本算法首先计算每个节点的密度(同时计算其附近

ε 内的点数),然后计算每个点到密度更高的最近点的距离。如此一来,每个点均有 2 个属性值,一个是本身的密度值,另一个是它与密度更高的最近点之间的距离值。对于这 2 个属性,可以生成一个 2D 图(决策图),然后图中的一些点可以代表不同聚类的中心,最后,可以将聚类中心与其附近具有相似性的点相连。这样,所有共享一个聚类中心的集群都属于一个簇,而远离集群并且密度较低的点就是异常点。由于此方法是基于相对值的,因此可以找到具有不同密度的聚类。每个集群中心点均为该集群中的最大密度的点,如果一个集群的密度分布相同或一个集群具有多个高密度点,它将把某些集群分为几个子集群。由于一般的基于密度的聚类算法要求用户指定聚类数,因此必须不断尝试在实际操作中进行调整,这大大增加了工作量,所以本文结合层次聚类算法的思想,将所有数据簇中最为相似的 2 个簇合并,依次迭代,最后生成一个较为良好的聚类树。

同时,本文使用密度比估计来解决基于密度聚类算法无法找到不同密度的簇的问题。密度比的基本思想是计算每个点的密度与附近密度的比值,然后用密度比找到核心关键点。基于此思想,还可以根据原始数据的密度分布对其进行归一化,即高密度区域被扩大而低密度区域继续缩小。使用这种方法,用户必须通过定义邻域范围来计算密度比:

$$D=\sum_{i=1}^{m}d(G_i)=\sum_{i=1}^{m}\frac{L(V_i,V_i)-L(V_i,\bar{V}_i)}{|V_i|}。\quad(10)$$

式中:$d(G_i)$ 表示与用户 i 相连的二部图的密度比;L 表示区域密度。

式(10)主要是通过计算某簇域不同点密度与其一相邻簇域各点密度之比,将其相加得到总密度比。若该簇域与其邻域密度比不相同,则可以先划分该簇域各个邻域为不同簇域。

本文将密度模块化函数与层次聚类相结合来发现社交网络。首先是使用层次聚类的思想,将所有不同点看成是一个簇,然后通过计算密度相似性,使用递归算法合并这些原子簇,同时若发现密度过于相似,用密度比估计指标来判断子簇是否可以合并,这样就将二部图中对象划分成了多个集群。从某个节点子图出发,通过贪心算法,选择能使 ΔD 值最大化的子集群进行合并,得到簇。可是包含单个结点的子图中密度不是相近的,这将使得 ΔD 难以计算。所以将密度相近且有边相连的子图合并,如果他们能够使得 D 增大,则说明这 2 个子图是可以合并的。

3 决策树分类算法优化

决策树学习通常会总结训练数据记录中的分类规则。与训练记录匹配的决策树会有很多(或没有),所需的决策树不与训练数据竞争,并且具有良好泛化能力[15]。从所有可能的决策树中选取最优决策树是一个 NP(non-deterministic polynomia)完全问题,所以现实中决策树学习算法通常采用启发式方法,近似求解最优化而不是一定要找到最优决策树。虽然这样得到的决策树是次优的,但是大大减少了工作量,使问题得到简化。决策树学习算法通常使用反向传播算法选择最佳资格,然后根据最佳资格分配训练数据。通过划分属性的位置并创建树的属性来完成此过程。

决策树学习算法总体上使用递归算法,递归地选择最优特征,然后根据最优特征划分训练数据。首先创建一个根节点,并将所有训练数据放在根节点上;然后选择最优特征,根据此特征将训练数据集分为几个子集。在正确分类的条件下,创建叶节点并将这些子集划分至相应的叶节点中。通常,如果存在无法正确分类的子集,则这些子集会重新选择特征,继续细分并创建相关节点,这些步骤将重复发生,直到能准确地对训练数据的所有子集进行分类或无法有效分类为止,每个训练集将被划分为叶节点,也就是说,存在明确的类时,创建决策树。

决策树学习算法包括特征选择、创建决策树以及决策树剪枝的过程。本文采用模拟退火算法(SA)作为决策树分类算法的优化算法,SA 理论上以概率 1 收敛于全局最优。SA 能有效地解决局部最优解的问题,其包含 2 个主要部分:Metropolis 算法和退火过程。Metropolis 算法相当于设置递归终止条件,是退火过程的基础。

SA 可以初步分解为 3 个部分:初始解、解空间和目标函数。这分别对应了物理中退火的 3 个过程,初始解相当于初始温度;求解空间过程相当于降温的过程;目标函数相当于最终温度。SA 是一种贪婪算法,只是它的搜索过程更为随机,其以 Metropolis 准则来判断是否接受一个非局部最优解,从而达到全局最优解。SA 与随机选择的初始值和初始解无关。

搜索解空间就是寻找最大化目标函数值的 0 和 1,使用模拟退火算法的随机搜索过程:开始仅搜索较小的子集,随机扰动 0 和 1,它们与“温度”

成比例,每次迭代“温度”降低,扰动边界减少。图 3 为使用模拟退火算法得到的一个对比可疑度值随集群大小变化图。随着迭代次数的增加,对比可疑度值逐渐趋于[0,5],亦即逐渐得到最优解的过程。

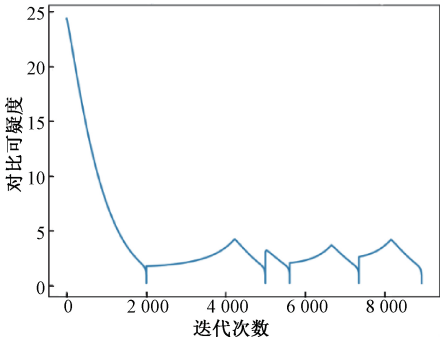

图 3　使用模拟退火曲线算法结果

Figure 3　Results of simulated annealing curve algorithm

4　实验与结果

在本实验中,仅考虑节点的时间序列波动中的多个有效脉冲串。唤醒和爆发点对保持不变,其高度差 Δc 至少为时间序列中最大高度差的 50%。大量研究表明,该性能对缩放 b 不敏感(b 为节点参与率与对比可疑度比率的缩放函数 b^{x-1} 的底数),并且在大于 32 时变得非常稳定。因此,在以下实验中选择 b = 32。本文实验在 64 位操作系统、Intel 2.4 GHz CPU、8 G 主存空间的主机上运行。

图 4 显示了 CPOFD 方法在 4 种注入伪装和没有伪装攻击的检测效果(评价指标为 F 值、召回率和 AUC),这 4 种伪装包括:①clique;②camo;③2 倍 camo;④biased camo。从图 4 中可以发现针对不同的伪装攻击,CPOFD 的检测效果差异较大,在 clique、2 倍 camo 和 biased camo 伪装攻击下算法检测效果比较好,但是在单倍 camo 伪装攻击和没有伪装攻击下,该方法的检测效果较差,这主要是因为使用 camo 攻击和没有伪装的攻击设置的阈值过低,在这个阈值内没有找到大量的攻击者,少量的攻击者使得欺诈密度大大降低,欺诈检测难度大大增加。

建立决策树模型后需要对该模型进行评估,以判断模型的优劣。学习算法模型使用训练数据集建立模型,使用测试数据集来评估模型。本文使用评估指标来对模型进行有效评估,评估指标有分类准确度、召回率、精确度等。

实验中模仿欺诈者的欺诈攻击行为,并随机

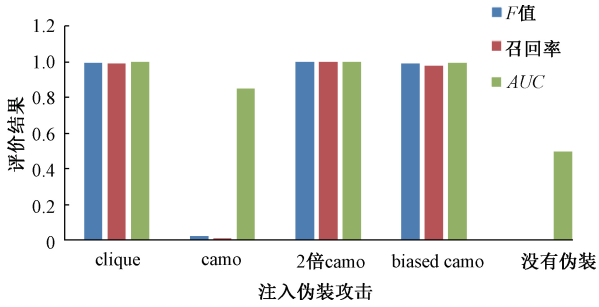

图 4　注入不同伪装攻击下检测结果

Figure 4　Detection results under different injection camouflage attacks

选择一些度数较小的用户作为欺诈对象。因为度数较小也就是不那么受欢迎的用户更加容易受到欺诈攻击者劫持。因此,从整个用户集中统一随机抽取一部分用户作为欺诈者。为了测试不同欺诈密度的欺诈检测结果,抽样欺诈者的数量从 200 到 2 000 不等。这些欺诈者总体上随机地为 200 种产品中的每一种都制造了 200 个假冒边缘。本文测试了欺诈密度为 0.01~0.70 的检测结果。图 5 显示了在 Zip 数据集上的 CPOFD、Fraudar、CrossSpot[16] 算法结果,与 CPOFD 相比,后两者仅考虑拓扑信息,检测低密度的欺诈者比高密度的欺诈者困难得多。而 CPOFD 同时考虑了拓扑以及评分属性,由于 CPOFD 仅在新颖的对比度可疑性中考虑了拓扑信息,因此本文将 CPOFD 与基于图拓扑的基线进行比较。当欺诈密度沿水平轴从右到左减小时,CPOFD 可以在高 F 值下检测到低至 0.05 的欺诈密度,F 值高于 0.8,高于现有的最佳基准。

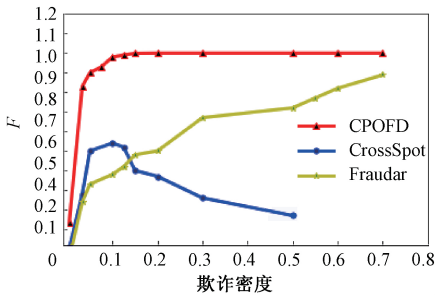

图 5　F 值与欺诈密度的关系

Figure 5　F measure with fraud density

本文对具有不同欺诈密度的 5 个数据集进行比较,表 1 记录了不同算法评价指标 F 值和召回率。该表比较了 CPOFD 和其他算法在不同数据集中的欺诈检测结果。一般来说,一种机器学习方法越好,它检测得到的 F 值越高,可以看到,CPOFD 在给定数据集中具有较高的检测结果,这意味着由于对比可疑框架中信息的整体使用,即

使欺诈者使用几十万个账户为200个对象创建伪造边缘,也可以高精度地检测到欺诈者,还可以准确地检测出欺诈对象。与Fraudar相比,CPOFD的F值普遍提高了40%到60%,CrossSpot偏向于在检测结果中包含大量用户(> 500 000),从中召回了不到150个额外的标记用户,故其F值非常低。HoloScope算法在不同数据集中表现差异过大,性能相对不稳。

表1 CPOFD和其他算法在不同数据集中的欺诈检测结果

Table 1 Fraud detection results of CPOFD and other algorithms in different datasets

数据集	CPOFD		HoloScope		Fraudar		CrossSpot	
	召回率	F	召回率	F	召回率	F	召回率	F
Zip	0.986 5	0.993 2	0.976 5	0.988 1	0.315 8	0.479 9	0.362 8	0.386 2
Yelp_Zip	1.000 0	0.998 8	0.999 9	0.997 3	0.151 5	0.263 1	0.119 2	0.254 3
Yelp_restaurant	0.998 5	0.571 0	1.000 0	0.264 3	0.025 1	0.048 3	0.231 5	0.258 4
Yelp_hotel	0.991 0	0.862 0	0.993 0	0.753 8	0.004 0	0.008 0	0.113 4	0.093 2
Yelp_NYC	0.999 9	0.993 5	0.999 0	0.989 4	0.501 6	0.668 1	0.179 2	0.237 5

图6为CPOFD方法在Zip数据集上的检测结果。从图6可以发现,异构欺诈者群体检测效果十分明显。图中红色节点为正常用户,蓝色节点为欺诈用户,检测拓扑为用户的时间戳、评论等属性。可以看到在大量正常用户中,欺诈用户不论是大群体协作还是较小的群体协作,均能有效地被检测出来。

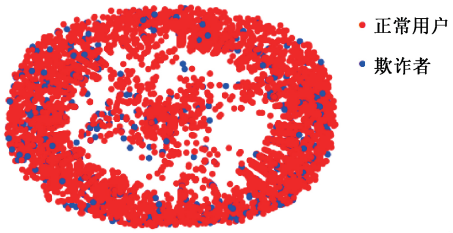

图6 Zip数据集上CPOFD方法得到的检测结果

Figure 6 Detection result obtained by CPOFD method on the Zip data set

为了验证CPOFD复杂性,本文选择的数据集具有较高的体积密度,通过使用不同的攻击注入方法,以使生成的数据量增加,本文的方法是通过Python实现的。图7为边缘数与时间的关系,图7中的点表示边缘数与该方法实际运行时间的关系,通过图中的点,使用线性回归方程得到一条线性直线。CPPFD方法的运行时间随着边的数量而线性增加,说明CPOFD方法的可扩展性良好,由此可见,该方法对于大规模社会舆论检测也适用。

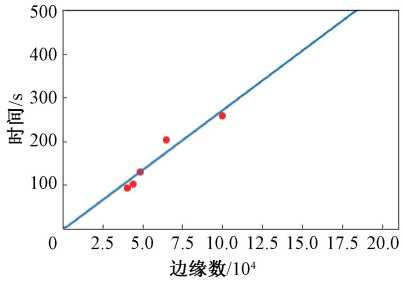

图7 时间复杂度

Figure 7 Time complexity

5 结论

本文提出了CPOFD方法,该方法使用了一种新颖的度量"对比可疑度",该度量主要包括拓扑连接的信息,以更为聚合的方式检测欺诈群体。具体而言,该度量强调了欺诈者和正常用户的动态对比,在拓扑、时间峰值和等级偏差方面强调了欺诈者和诚实用户之间的行为差异。同时,CPOFD方法结合基于密度子图的聚类算法和决策树分类算法将社交网络中用户进行有效分组,且在对聚簇分类时使用模拟退火算法进行剪枝优化,能更加简洁快速地寻找近似最优解。在伪装的情况下,本文方法在实际数据集上均获得了比基线更高的精度。本文方法可以有效地阻止欺诈者并增加欺诈者的时间成本。

参考文献:

[1] PANETTA K. Gartner top strategic predictions for 2018 and beyond[EB/OL].(2019-05-10)[2021-07-20]. https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/.

[2] YE J T, AKOGLU L. Discovering opinion spammer groups by network footprints[C]//Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Cham:Springer,2015:267-282.

[3] HOOI B, SONG H A, BEUTEL A, et al. FRAUDAR: bounding graph fraud in the face of camouflage[C]// Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.

New York:ACM,2016:895-904.

[4] BEUTEL A, XU W H, GURUSWAMI V, et al. CopyCatch: stopping group attacks by spotting lockstep behavior in social networks[C]//Proceedings of the 22nd International Conference on World Wide Web-WWW'13. Rio de Janeiro, Brazil. New York: ACM, 2013:119-130.

[5] SHEHNEPOOR S, SALEHI M, FARAHBAKHSH R, et al. NetSpam: a network-based Spam detection framework for reviews in online social media[J]. IEEE transactions on information forensics and security, 2017,12(7):1585-1595.

[6] LOVISOTTO G, EBERZ S, MARTINOVIC I. Biometric backdoors: a poisoning attack against unsupervised template updating[C]//2020 IEEE European Symposium on Security and Privacy. Piscataway: IEEE, 2020:308-316.

[7] YOU Z, QIAN T, LIU B. An attribute enhanced domain adaptive model for cold-start spam review detection[C]//Proceedings of the 27th International Conference on Computational Linguistics. Santa Fe: COLING,2018:1884-1895.

[8] DA Q B, CHENG J R, LI Q, et al. Socially-attentive representation learning for cold-start fraud review detection[C]//In National Conference of Theoretical Computer Science. Cham:Springer, 2019:76-91.

[9] LI Q, WU Q, ZHU C Z, et al.. Unsupervised user behavior representation for fraud review detection with cold-start problem[C]//In Pacific-Asia Conference on Knowledge Discovery and Data Mining. Cham: Springer, 2019:222-236.

[10] LI Q, WU Q, ZHU C Z, et al. An inferable representation learning for fraud review detection with cold-start problem[C]//2019 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE,2019:1-8.

[11] ZHU C Z,ZHAO W T,LI Q,et al.Network embedding-based anomalous density searching for multi-group collaborative fraudsters detection in social media[J]. Computers, materials & continua, 2019, 60(1):317-333.

[12] MUKHERJEE A,VENKATARAMAN V, LIU B, et al. What yelp fake review filter might be doing? [C]// International AAAI Conference on Web and Social Media.Massachusetts:AAAI,2013:136-144.

[13] OTT M, CHOI Y, CARDIE C,et al.Finding deceptive opinion spam by any stretch of the imagination[C]// Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics. Portland: ACL-HLT, 2011:309-319.

[14] 詹海萍.弱信号模体检测的图搜索算法[D].西安:西安电子科技大学,2010.

[15] 刘波,何希平.高维数据的特征选择:理论与算法[M].北京:科学出版社,2016.

[16] LIU S H, HOOI B, FALOUTSOS C. HoloScope: topology-and-spike aware fraud detection[C]//Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. New York: ACM,2017:1539-1548.

Research on Application of Collaborative Public Opinion Fraud Detection Method in Social Network

WU Xiaoyan[1], LIU Qiang[1], ZHU Chengzhang[2]

(1.College of Computer, National University of Defense Technology, Changsha 410005, China; 2.Institute of War, Academy of Military Sciences, Beijing 100091, China)

Abstract: In order to ensure cyberspace to provide more reliable information, fraud detection became more important. Existing methods only considered the static dense sub-graphs formed between user comments when detecting fraudulent users, while ignored the abnormal behavior of users during the comments, which led to reduced accuracy. Meanwhile, further manual verification was often required to verify the reliability of the results in practice. For this problem, this paper proposed the CPOFD method, which used a new measure "comparative equivocation". This measure mainly included topological connection information to detect fraud groups in a more aggregated manner. Specifically, this metric emphasized the dynamic comparison between fraudsters and normal users, so that the algorithm could effectively detect the fraudster's abnormal behavior in terms of topological connections, timestamps, and scoring information. At the same time, this method combined the

clustering algorithm based on the density sub-graphs and the decision tree classification algorithm to group users in the social network effectively, and used the simulated annealing algorithm to optimize the pruning when classifying the clusters, so as to find the approximate optimum solution more concisely and quickly. The time complexity of the algorithm was linear to the number of fraudsters, and it had high scalability. In experiments based on the Yelp dataset, the accuracy of the CPOFD method for fraudulent public opinion detection reached more than 98%, which verified the effectiveness of the CPOFD method.

Keywords: fraud detection; collaborative fraud detection; unsupervised fraud detection; behavior recognition; social network security

(上接第6页)

Research on Multi-robot Formation Control Based on Speed Compensation Algorithm

ZHANG Fangfang, ZHANG Wenli, WANG Tingting

(School of Electrical Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract: In order to solve the problems of complex algorithm of traditional leader-follower method in formation control of multi-robot system and difficulty in completing circular formation of multi-robot system with common formation control law, the formation problem of multi-robot system was transformed into tracking control problem among robots by improving the traditional leader-follower method, and a velocity compensation algorithm based on position information for multi-robot formation was proposed in this study. The formation control model of robot with velocity compensation algorithm is established, and the formation control law was designed based on the pose error between the following robot and the virtual robot, and it is proved theoretically that the proposed control law could complete the multi-robot formation task. Then, on the basis of studying the multi-robot formation problem, the obstacle avoidance problem in the multi-robot formation process is further studied. The classical artificial potential field method was introduced, and the artificial potential field method was combined with the speed compensation algorithm of this study. The combined algorithm could enable the multi-robot system to maintain formation operation, and not only preventing the robots in the system from colliding with each other, but also adaptively avoiding obstacles in the surrounding environment. The results showed that multi-robots could not only complete the formation task efficiently but also successfully complete the obstacle avoidance task when encountering obstacles. Finally, the proposed algorithm was verified by experiments on multi-robot simulation and physical platform. The algorithm could reduce the number of calling parameters, simplified the formation algorithm, and improve the formation efficiency.

Keywords: leader-follower algorithm; speed compensation algorithm; tracking control; formation obstacle avoidance control