

社交网络中异常用户的检测

数据科学与计算机学院
计算机科学与技术
张佐奇
13349160

目录

- 课题的背景
- 本文的工作
- 实验与分析
- 总结与展望

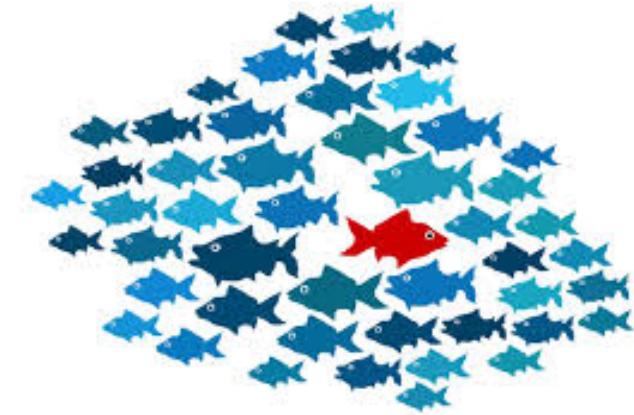
社交网络

- 随着Internet用户的普及以及Web 2.0技术的成熟，社交网络呈现出飞速发展的趋势，越来越多的社交网站出现在我们的生活中。
 - 国外：Facebook、Twitter、LinkedIn等
 - 国内：新浪微博、人人网等
-
- 社交网站聚集了大量的用户。
 - 据统计，截止至2016年12月31日，Facebook已经拥有来自全世界的18.6亿活跃用户，国内的新浪微博的用户注册数也已超过5亿。



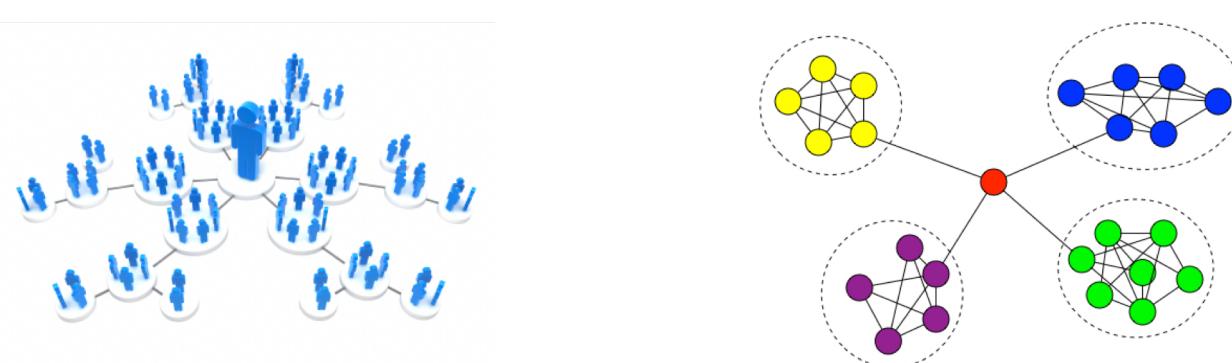
异常用户

- 异常用户：攻击者创建大量的虚假账号和盗用正常用户的账号
- 在社交网络中发布广告、钓鱼等恶意信息
- 严重威胁到正常用户的隐私信息、账号安全以及使用体验
- 严重危害到社交网络的信誉评价体系以及用户之间的信任关系



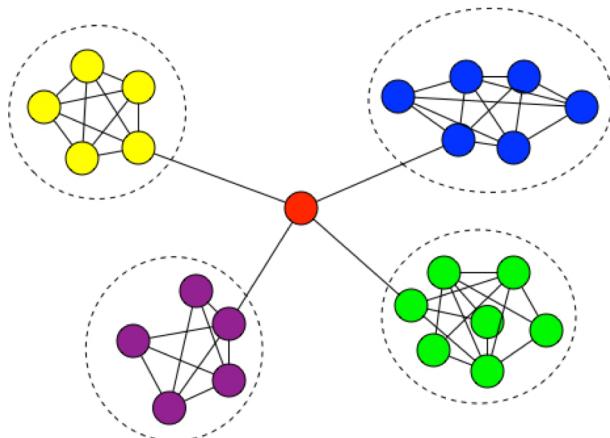
异常用户的定义

- 在现实生活的社交网络中，经常会出现一个用户同时连接了属于多个社区的不同用户的情况。（例如：营销账号）
- 社交网络各个社区之间的界限不明确，进行社区发现时会得到质量不高的结果。如果将这些用户从社交网络中去除，则会使得发现的社区质量明显提高。
- 假设一个用户属于某一个社区，那么他关于这个社区的隶属度应该相对比较大，而关于其他社区的隶属度应该比较小或接近于零。这样对于一个异常用户来说，由于他同时连接了多个不同的社区，所以与多个社区都有一定的相关性，那么他关于所连接的每个社区的隶属度应该倾向于比较接近。



異常用戶的定義

定义：异常用户。在一个社区数量为 k 的社交网络中，对于每一个用户节点 $v_i \in V$ ，令 $\mathbf{y}_i = (y_i^{(1)}, y_i^{(2)}, \dots, y_i^{(k)})$ 为用户节点 v_i 的隶属度向量，其中 $y_i^{(j)}$ 表示用户节点 v_i 关于第 j 个社区的隶属度($0 \leq y_i^{(j)} \leq 1$, $\sum_{j=1}^k y_i^{(j)} = 1$)。求出隶属度向量 \mathbf{y}_i 中所有非零项的平均值 Avg 、最大值 Max 、以及大于等于最大值的项数 Cnt ，计算异常系数 $AScore = \frac{Avg(\mathbf{y}_i)}{Max(\mathbf{y}_i)} \cdot Cnt(y_i^{(j)} \geq Avg(\mathbf{y}_i))$ ，如果 $AScore \geq thre$ ，其中 $thre$ 为人为设定的阈值($threshold$)，那么节点 v_i 所代表的用户为异常用户。



$$\begin{cases} (1,0,0,0) \\ (0,1,0,0) \\ (0,0,1,0) \\ (0,0,0,1) \end{cases} \Rightarrow Ascore = \frac{1}{1} \cdot 1 = 1$$

$$(0.25, 0.25, 0.25, 0.25) \Rightarrow Ascore = \frac{0.25}{0.25} \cdot 4 = 4$$

基于图向量表征的异常用户检测算法

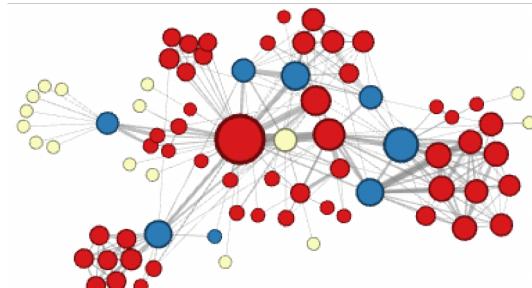
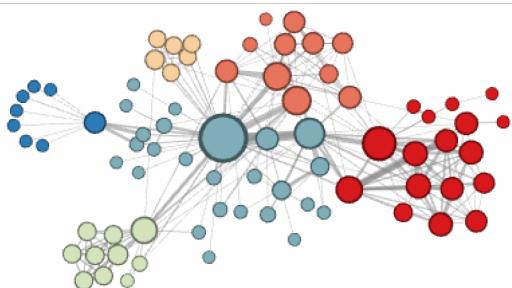
- 图特征的提取
- 目标函数的设计
- 目标函数的求解
- 隶属度向量的学习
- 异常用户的判断

图特征的提取

- 图结构特征：节点的连接关系。
- 为了能够较好的自动提取网络特征，本文使用了近几年新提出的用于处理大规模网络的*Network Embedding* 算法，根据社交网络中用户节点之间的连接关系得到每一个用户节点的图表征向量，作为检测算法的输入。
- 定义：图向量表征。给定网络 $G = (V, E)$ ， V 是网络中的节点的集合， E 是边的集合， 寻找一个映射函数 $f_G: V \rightarrow R^d, d \ll |V|$ ， 将网络中的节点映射到低维向量空间 R^d ， 转换后的低维向量尽可能保留网络的特性。
- 输入：网络的邻接表。
- 输出：所有节点的 d 维图表征向量。

*node2vec*算法

- *node2vec*是最新的一种常用的*Network Embedding*算法。
 - 随机游走：生成节点序列，相当于构建*word2vec*中的语料库。
 - 优化目标：最大化节点的网络邻居的出现概率。
- *node2vec*算法通过两个参数决定随机游走的采样策略，从而可以生成突出网络的同质性或者结构等价性的两种不同的图向量表征。



目标函数的设计

- 对于一个节点数量为 n 、社区数量为 k 的网络，设计如下的目标函数 O ：

$$\min O = \sum_{i=1}^n \sum_{j=1}^k y_i^{(j)} \cdot \left\| \mathbf{x}_i - \mathbf{m}_j \right\|_2^2 + \alpha \cdot \sum_{i=1}^n \left\| \mathbf{y}_i \right\|_2^2 \quad (0 \leq y_i^{(j)} \leq 1, \sum_{j=1}^k y_i^{(j)} = 1)$$



$$\mathbf{y}_i = (1, 0, 0, \dots, 0) \quad \mathbf{y}_i = \left(\frac{1}{k}, \frac{1}{k}, \frac{1}{k}, \dots, \frac{1}{k} \right)$$

- \mathbf{x}_i 为节点 v_i 的特征向量， \mathbf{y}_i 为节点 v_i 的隶属度向量， \mathbf{m}_j 为第 j 个社区质心的特征向量。
- α 为调节参数(*trade-off*)。

目标函数的求解

$$\min O = \sum_{i=1}^n \sum_{j=1}^k y_i^{(j)} \cdot \left\| \mathbf{x}_i - \mathbf{m}_j \right\|_2^2 + \alpha \cdot \sum_{i=1}^n \left\| \mathbf{y}_i \right\|_2^2$$

- 目标函数 O 是一个包含 \mathbf{y}_i 和 \mathbf{m}_j 两个变量的二元函数。
- 对于这样的二元函数，采用令偏导数等于零的方式求出其极值点，每次固定一个变量优化另一个变量，交替更新直至收敛，从而求出其极小值。

$$\mathbf{m}_j = \frac{\sum_{i=1}^n y_i^{(j)} \cdot \mathbf{x}_i}{\sum_{i=1}^n y_i^{(j)}}$$

$$y_i^{(j)} = \frac{2\alpha + \sum_{j=1}^k \left\| \mathbf{x}_i - \mathbf{m}_j \right\|_2^2 - k \left\| \mathbf{x}_i - \mathbf{m}_j \right\|_2^2}{2k\alpha}$$

隶属度向量的学习

Algorithm Probability Learning³

Input: feature vectors $X = \{x_1, x_2, \dots, x_n\}$ ⁴

number of clusters k ⁴

parameter α ⁴

Output: $y_i^{(j)}, 1 \leq i \leq n, 1 \leq j \leq k$ (possibility of node i belonging to cluster j)⁴

1: **Initialization:** $y_i^{(j)}, m_j$ (by K-Means Algorithm)⁴

2: $t = 0$ ⁴

3: **Repeat**⁴

4: **Update** m_j (by equation (4.12))⁴

5: **Update** $y_i^{(j)}$ (by equation (4.18))⁴

6: $t = t + 1$ ⁴

7: **Until** convergence or $t > t_{max}$ ⁴

- **输入:** 节点特征向量 X 、社区数量 k 、调节参数 α 。
- **输出:** 使目标函数 O 达到最小值时的每个节点 v_i 的隶属度向量 y_i 。
- **初始化:** 使用 $K - Means$ 算法对所有节点进行初始聚类，得到社区质心的初始特征向量，以及每个节点的初始隶属度向量。
- **循环:** 根据变换公式，交替更新 m_j 、 y_i ，直至目标函数 O 的值收敛或超过最大迭代次数 t_{max} 。

異常用戶的判斷

- 根据异常用户的定义，计算异常系数 $AScore = \frac{Avg(y_i)}{Max(y_i)} \cdot Cnt \left(y_i^{(j)} \geq Avg(y_i) \right)$ 。
- 如果 $AScore \geq thre$, $thre$ 为人为设定的阈值，那么该节点所代表的用户被判断为异常用户。

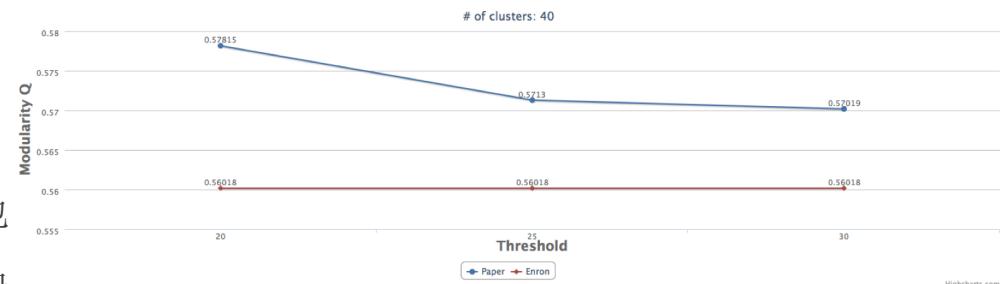
实验过程与结果分析

- 数据集
 - 安然公司(*Enron*)邮件数据集
 - 无向图，节点数：36692，边数：183831
- 算法评价标准
 - 模块度(*Modularity*)：
$$Q = \sum_{c \in C} \left(\frac{I_c}{E} - \left(\frac{2I_c + O_c}{2E} \right)^2 \right)$$

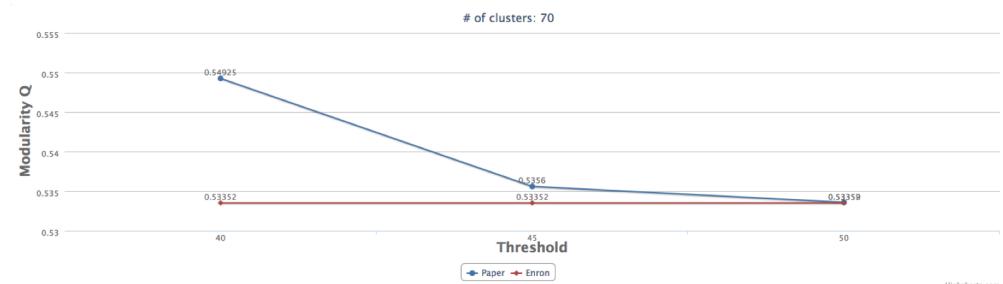
实验过程与结果分析

◦ 实验结果与分析

- 社区数量分别取40、50、70时，模块度分别提高了3.2%、2.0%、2.9%。
- 删除了同时连接多个社区的异常用户后，跨社区连接的边也被删除，从而使得每个社区内部的连接更加紧密，所以模块度变大。



Highcharts.com



Highcharts.com

总结与展望

- 总结

- 为了检测社交网络中存在的异常用户，本文首先提出了一个对于异常用户的合理的定义，在此基础上提出了基于图向量表征的异常用户的检测算法。利用学习出的节点的隶属度向量计算其异常系数从而判断该节点所代表的用户是否为异常用户。然后使用公开的社交网络数据集进行实验，成功检测出了符合定义的异常用户，提高了网络的模块度。

总结与展望

◦ 未来的工作

- 由于社交网络为无标度网络，在现实生活中确实会存在少量用户拥有较大的度，例如在推特中有像美国总统特朗普这样非常受欢迎受关注的用户，他们的确同时连接了多个社区的正常用户，然而在实际生活中我们并不会将他们归类于异常用户，所以在未来的工作中还需要进一步挖掘其他特征并改进算法，将这一小部分用户从异常用户中排除。
- 本文的检测算法比较依赖于开始时通过*Network Embedding*算法获得的用户节点特征向量，由于*node2vec*算法的开源程序的参数较多，在输入命令时对参数的配置不够精确可能使得*node2vec*算法的准确率有所降低。未来还需要在调参过程中慢慢尝试，找到最适合于相应的社交网络数据集和图向量表征目标的参数配置。



THANKS