基于女巫攻击预防技术的电信网络诈骗团伙识别

任泽华
（西安交通大学，自动化系，710049，西安）

摘要：在移动互联网日益普及的今天，电信网络诈骗日益猖獗，而这些诈骗活动往往呈现出冒充多个身份、团伙合作的特点。本文利用面向对等网络中常见的女巫攻击的防御技术，检测识别电信网络中潜在的诈骗团体。我们选取了几个真实的社交网络模型作为实验数据集，对比了几种基于网络拓扑结构的经典检测方法在真实网络环境下的检测精度，找到了最适合于电信网络诈骗检测的算法。最后我们在检测数据中引入用户的特征，使用贝叶斯、K 近邻算法（KNN）等机器学习算法对用户进行分类，并将其与之前的图模型算法相结合，大大提高了诈骗团伙的检测精度，为提前识别发现网络诈骗团体，维护网络空间安全稳定做出了一定的贡献。

关键词：社交网络；网络诈骗检测；女巫攻击；用户行为分析

中图分类号： TP393.0 **文献标识码**： A

Identification of Telecom Network Fraud Group Based on Sybil Attack Prevention Technology

Zehua Ren
(Department of Automation, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: With the increasing popularity of the mobile Internet today, telecommunications network fraud is becoming more and more rampant, and these fraudulent activities often present the characteristics of posing as multiple identities and gang cooperation. This paper uses the defense technology for common sybil attacks in peer-to-peer networks to detect and identify potential fraud groups in telecommunication networks. We selected several real social network models as experimental data sets, compared the detection accuracy of several classic detection methods based on network topology in real network environments, and found the most suitable algorithm for telecommunications network fraud detection. Finally, we introduce the user's characteristics into the detection data, use Bayesian, KNN and other machine learning algorithms to classify users, and combine them with the previous graph model algorithm, which greatly improves the detection accuracy of scam gangs, for early identification The discovery of online fraud groups has made a certain contribution to maintaining the security and stability of cyberspace.

Keywords: social network; network fraud detection; sybil attack; user behavior analysis

随着通信技术的革新与互联网的兴起，网络诈骗愈发猖獗。我们注意到，网络诈骗总是呈现出团伙诈骗的形式，这与人们的信任模式有很大的关系。如果不对这些诈骗团伙进行有效识别与打击，会严重损害网络空间的信任体系，甚至危害到社会的长治久安。而在对等网络（P2P）网络中就存在着一种与

收稿日期：2020-12-12。 作者简介：任泽华（1998-），男，本科生；鄢超波（通讯作者），男，副教授，博士生导师。
基金项目：国家自然科学基金资助项目（编号）。

之相对应的攻击方式：女巫攻击，即单个节点对外表现出多重身份的攻击行为。这种模式和诈骗团伙极为相似，若能迁移到当前情景下进行诈骗团伙的检测，将对于解决这一问题做出极大贡献。

本文主要采用基于网络拓扑结构的女巫节点检测算法，对 Facebook 和微博等社交软件真实的用户网络进行了实验。随机生成了不同类型的女巫攻击用以模拟真实条件下的诈骗团伙，验证了几种不同的检测方法在时间复杂度、空间复杂度、识别准确率等方面的指标，比较分析了这几种算法在不同情景下的优劣。经过实验验证，在分布式网络的条件下，SybilRank 算法在识别精度、时空复杂度方面指标都显示出良好的结果。在此基础上，我们还引入了用户行为的特征，为每一个用户节点建立了独特的身份标识，利用经典的机器学习分类方法对它们进行了聚类分析。我们使用单个样本 F/F 率作为判别标准，在减少计算量的同时满足了条件独立假设。通过与图搜索算法相结合，我们将不良节点检测的精度又提高了一个层次。

本文第一部分主要介绍问题背景，包括女巫攻击的提出，不良团伙的各种组织形式；第二部分介绍了我们使用的几种经典基于随机游走的女巫节点检测算法；第三部分记录了对比实验的过程，比较分析了几种不同的检测方法在各种情境下的表现；第四部分叙述了我们的后续工作，即把用户的行为特征与网络结构结合起来的新方法，并进行了对比测试；第五部分总结了我们工作的成果和贡献，并对未来进一步的工作做出了展望。

1 问题背景

微软研究院的 Douceur 教授在 2002 年的一篇论文《The Sybil Attack》[1]中首先提出了 Sybil 攻击的概念。Sybil 攻击，又被译作女巫攻击，它的名称来源是同名小说改编的电影《Sybil》，主要讲述了一个具有 16 重人格的女人的故事，而 Sybil 攻击正是以她的名字来命名的。它被认为是基于对等网络（P2P 网络）进行攻击的一种基本形式。它的主要表现方式为：单一节点具有多重身份标识，通过控制系统中大部分节点来达到削弱网络冗余性、降低网络健壮性、破坏网络正常活动、盗取其他节点个人信息等目的。这种组织方式与诈骗团伙极为相似，通常每个骗子扮演一个特定的角色，对外表现出互不相关的身份。而他们之间密切沟通，分工明确，逻辑清晰，被他们洗脑的被害人往往对他们深信不疑。

1.1 模型概述

在介绍攻击模式之前，我们有必要介绍一下抽象社交网络模型和其中的节点分类。如图 1 所示，我们将社交网络建模为抽象的图模型，在网络中每个节点表示一个账户身份，每条边则表示两个用户之间建立的信任关系。我们根据用户身份将节点分为普通诚实节点、种子节点（被确定为诚实的节点）、攻击节点（具有真实身份的恶意节点）、女巫节点（虚假身份的节点）。节点的诚实程度由他们的邻近节点评分得出。

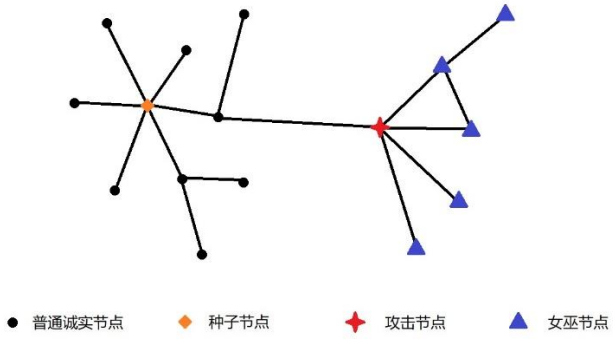

图 1 社交网络图谱的基本模型

由于女巫攻击也常常被用来抵抗僵尸网络病毒[2]，前人的研究中对于不同攻击方式的探讨也比较深入。总体来说，女巫攻击主要有两种形式：孤立攻击和协同攻击[3]。孤立攻击主要表现为单一恶意节点连接其他诚实节点并骗取它们的信任，从而时其相信自己的多重身份。这在网络诈骗中体现为“一人分饰多角”进行的行骗，由于无法在同一时间以多重身份回应受害人，其诈骗难度相对较大。协同攻击主要表现为多个恶意节点与诚实节点建立连接并冒充多个身份，它们之间往往会形成紧密的配合。这种攻击方式对应了电信骗局中的“团伙作案”，诈骗团伙会安排不同的人扮演不同角色，步步诱导，让受害人对他们信以为真。这种诈骗方式往往难于预防，如果不对其进行提前发现与铲除，会造成比较严重的后果。

1.2 孤立攻击

对于孤立攻击，一名攻击者将自己的计算与存储资源分配给自己控制的女巫节点，以通过连接到其他节点来获得他人承认。此时我们假设攻击者只有一个诚实账号，该账号拥有和其他诚实用户的正常数量的连接甚至更多的连接。通过这些连接，攻击者使其控制的女巫节点与受害者建立互联。其主要攻击模式有：

1) 一名攻击者试图连接到一些种子节点并创建一

些 sybil 节点；

2) 一名攻击者试图连接到一些排名最高的诚实用户，并创建一些 sybil 节点；
3) 一名攻击者试图连接到一些诚实用户，并创建一些 sybil 节点；
4) 一名攻击者试图连接到排名最高的诚实者之一，并创建多个 sybil 群组；
5) 种子节点尝试创建一些 sybil 节点；
6) 诚实节点尝试创建一些 sybil 节点。

1.3 协同攻击

对于协同攻击，多名攻击者将自己的计算与存储资源分配给其控制的女巫节点，攻击者能够以任何方式彼此联系。我们假设每个攻击者拥有一个账户，此账户具有与诚实用户的相同或超额数量的直接连接，这些连接可用于与 sybil 账户的互连。攻击可以由一起协作的一个或多个攻击者进行。其主要攻击模式有：

1) 一组或多组攻击者试图连接到某些种子节点并创建一些 sybil 节点；
2) 一组或多组攻击者试图连接到一些顶级诚实用户，并创建一些 sybil 节点；
3) 一组或多组攻击者试图连接到某些诚实用户并创建一些 sybil 节点；
4) 一群攻击者试图与一些最诚实的诚实分子建立联系，并创建多个 sybil 群组；
5) 一组或多组种子节点尝试创建一些 sybil 节点；
6) 一组或多组诚实节点尝试创建一些 sybil 节点；
7) 一组种子节点尝试通过为每个 sybil 节点创建一个组来创建一些 sybil 节点，并且所有种子节点都加入该组；
8) 一组种子节点尝试创建多个群集，并将每个群集中的 sybil 节点连接到其他群集中的随机 sybil 节点。

2 基于随机游走的女巫节点检测算法

由于传统的检测方式无不需要大量的计算资源和复杂的密码算法，这无法满足我们对于网络快速性、容错性和减小 Sybil 节点的综合要求。此时，基于随机游走的 Sybil 节点检测方法就应运而生。如图 2 所示，它将网络抽象为社交图谱，将节点分为两部分：诚实节点和 Sybil 节点，同种且相邻近的节点构成了“节点社区”。由于图中只有这两种节点，我们易证，它们之间必然会形成一个二分图，其中连接两部分节点的边叫做攻击边（Attack Edges）。基于这样的假设，近年来出现了许多算法，比如说 SybilGuard、SybilLimit、SybilRank、Sybil Defender、Sybil Shield、Sybil Infer、Symon、Sybil Resist 等[4-6]。我们选取了三个最具代表性的算法进行了分析验证。

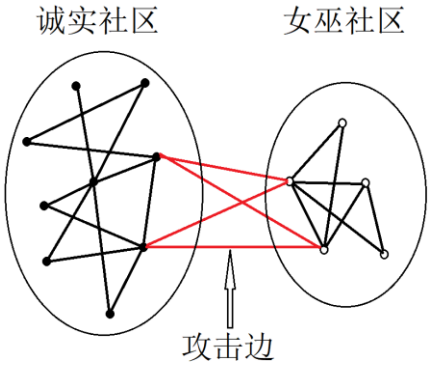

图 2 女巫攻击网络图谱示意

2.1 SybilGuard

Haifeng Yu[7]等人在 2006 年提出了一种基于随机游走检测 Sybil 节点的算法：SybilGuard 法，这也是基于此思想的第一种检测方法。它是一种完全分散的检测算法，所有操作均针对给定节点，它保证了诚实节点以极大的可能接受其他的诚实节点，并且被其他诚实节点接受；还保证了诚实节点只能接受有限数量的 Sybil 节点。该算法基于以下几点基本假设：（1）社交网络正在快速混合，即诚实节点正在快速地于其他诚实节点建立联系（2）初始验证的节点一定是诚实节点，基于这个初始诚实节点来检验其他节点。（3）恶意用户可能会创建多个节点，但是它们能够说服诚实节点接受它们的概率比较小，换句话说就是攻击边相对较少，这就导致了 Sybil 社区相对独立于诚实社区，这就为我们基于网络拓扑检测 Sybil 节点提供了可能。

SybilGuard 法的基本步骤为：

1) 选择一个初始节点 V，保证这个节点为诚实节点，以此为基础进行随机游走；
2) 设该节点的度为 d，从该节点引出 d 条随机路线，每遇到一个节点时都执行随机选择，每条路线的长度为 w；
3) 待测节点 S 也通过随机游走的方式进行路线选择，如果两个节点走出的路线有超过某一阈值 t 的数量相交时，就认为 S 是诚实节点，否则就认为它是 Sybil 节点。一般取 t=d/2。

SybilGuard 法得以实现主要基于以下几点理论：

1) Sybil 社区相对独立于诚实社区，从 Sybil 节点出发的路径到达诚实社区的可能性较小，有时仅为一两条边（如图 3 所示）。
2) 回路只能在路线的起点形成。
3) 随机路线沿相同方向多次穿越某个边缘一次（即循环），或者进入 sybil 区域，则它是有问题的。
4) 若两条路径相交，那么接下来它们将相重合。

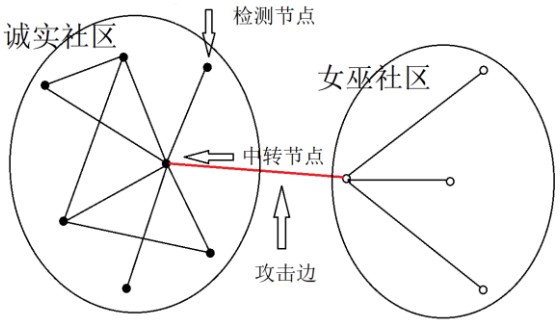

图 3 诚实社区与 Sybil 社区相对独立

关于游走长度的选择也是有讲究的：w 的值必须足够小，以确保（i）验证者的随机路径完全保持在诚实区域内的可能性很高；（ii）sybil 社区的大小不宜过大。另一方面，w 必须足够大，以确保路由以高概率相交。而此处我们选取$w = o(\sqrt{n}\ \log n)$比较合适。对于任何连接且非双向的社交网络，从统一随机诚实节点开始的长度为 w 的随机游走将遍历任何 g 个攻击边缘的概率的上限为gw/n。特别是当$w = o(\sqrt{n}\ \log n)$时，该概率为$o(1)$。

2.2 SybilLimit

同样是 Haifeng Yu[8]等人在 2008 年对自己的算法提出了改进，形成了 SybilLimit 算法。如表所示，它可将 Sybil 攻击值降低为$o(\log n)$，在大型网络中，这种优势尤其明显。它的主要思想为：在初始化阶段，每个节点都构建自己的路由表。在联机阶段，可疑节点会将观众的标识符和地址发送给验证者节点，该节点将比较可疑者列表中的证人以尝试查找匹配项。如果验证者在两个集合中找到匹配项，它将要求两个集合中具有相同身份的观众验证可疑节点的身份，并根据此过程的结果确定是否接受或拒绝该节点。如果两组之间没有交集，则验证程序将中止并拒绝该节点，将其标记为攻击者。

表 1 两种方法的性能比较

攻击边缘数量 g（协议未知）	接受节点数量	
	SybilGuard	SybilLimit
$o(\sqrt{n}\ \log n)$	$o(\sqrt{n}\ \log n)$	$o(\log n)$
$o(\sqrt{n}\ \log n)$到$o(n\ \log n)$	无限制	$o(\log n)$
小于 15,000	2000 左右	10 左右
大于 15,000 且小于 100,000	无限制	10 左右

SybilLimit 区别于 SybilGuard 的主要方面为：

1) 交叉点条件：在 SybilLimit 中，每个节点使用$r = o(\sqrt{n})$个长度为$w = o(\log n)$的随机路径进行游走，而不是像之前一样一次只进行一条线路的游走。从而降低了攻击者利用搜索间隙发动攻击的可能性。在任何给定的情况下，对手都可以伪造 w 条跨越攻击边缘并进入诚实区域的长度为 w 的不同随机路线。此处 SybilLimit 通过使用比 SybilGuard 小得多的 w 来减少此类路由的数量。
2) 平衡条件：SybilLimit 依靠其新的平衡条件来解决原方法中的未命中路线。
3) 参数估计技术：它使用一种新颖的参数估计技术，将 Sybil 节点和诚实节点放在一起估计，这就保证了无论攻击者行为如何，都不会过高地估计参数 r，即同时游走的路线条数。

2.3 SybilRank

在前人算法的基础上，Qiang Cao 等[9]在 2012 年提出了一种更加高效的基于随机游走的女巫节点检测算法。他们在随机游走的基础上添加了排序这一过程，首先将随机游走进行幂次迭代，把正常节点的信任值分配给其他节点，并进行标准化，最后根据标准化结果排序（依靠社交图属性根据用户感知到的伪造可能性对他们进行排名）。SybilRank 的计算成

本不会随其使用的信任种子节点数的增加而增加。这有助于使用多个种子来提高系统对种子选择错误的鲁棒性。

在之前不排序的算法 SybilGuard 和 SybilLimit 中，源自非 Sybil 节点的缩短的随机游走往往会停留在网络的非 Sybil 区域内，这是因为这种游走不太可能会穿越相对较少的攻击边缘。为了避免这点，SybilRank 提出了以下两点创新：（i）根据从非 Sybil 节点着陆到其上的短暂随机游走的程度归一化概率，对社交图中的节点进行排名；（ii）使用了幂迭代这种标准的处理技术，可以有效地计算大型网络图中随机游走的着陆概率。

SybilRank 法的基本步骤为：

1) 通过$w = O(\log n)$幂次迭代，信任概率从已知的非 Sybil 节点（信任种子）流出，在整个网络中扩展并偏向非 Sybil 区域；
2) 根据节点的程度归一化信任度对其进行排名；
3) 在排名列表中选取前几名的用户，并向全体用户公告它们被怀疑为 Sybils 账户。

在每次迭代期间，节点首先将其信任度平均分配给其邻居。然后，它收集邻居分配的信任，并相应地更新其自身的信任。该过程如下图所示：节点 A 原始信任度为 100，它有 4 个邻居，所以下一轮中这 4 个邻居中的每个都会收到 25 点信任度。同理，它也会收到这些邻居传递来的信任值。请注意，信任总量保持不变。

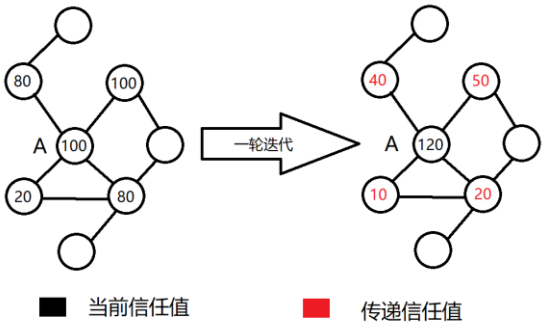

图 4 信任传递模型

SybilRank 的优势：

SybilRank 的计算成本为$O(\mathrm{n}\log n)$。这是因为每回幂次迭代的成本为$O(n)$，我们迭代$O(\log n)$次。根据节点的归一化信任度对节点进行排序的成本也为$O(\mathrm{n}\log n)$。估计社区的成本为$O(m)$（m 为社区个数）因为该方法中的每个迭代都具有与边数成线性关系的计算成本，并且该图仅需进行几次迭代即可迅速缩小。由于社交网络中的节点度始终受到限制，因此社区估计成本为$O(n)$（与信任种子的数量无关），总体计算成本为$O(\mathrm{n}\log n)$。在引入信任模型的基础上没有提高过多的时间复杂度。

3　实验验证

3.1　使用的网络模型

我们使用 *Network Repository* 网站上面的开源网络数据集进行测试，使用 Facebook 上面的三个真实网络图谱数据 *Caltech36*、*Reed98* 和 *American75* 进行了测试。我们随机生成了一些女巫节点并模拟女巫攻击的各种方式对不同的检测算法的运行时间、检测成功率等指标进行了测试。

其中 *Caltech36* 数据集包含了 769 个节点，16.7k 条边；*Reed98* 数据集包含 962 个节点，18.8k 条边；*American75* 数据集包含 6.4k 个节点，217.7k 条边。包含了小型和大型网络，下图是它们的拓扑结构：

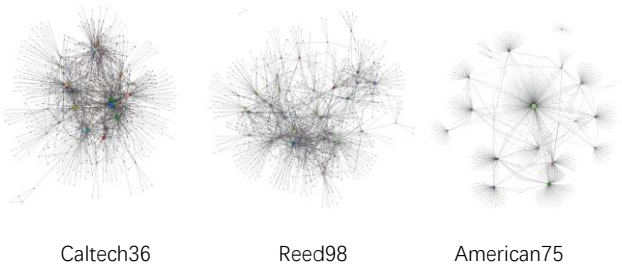

图 5 数据集网络拓扑

从网络拓扑图中可以看出，*Caltech36* 呈现中心化的结构，整体比较紧凑且节点之间联系紧密；相比之下，*Reed98* 呈现了较明显的两簇，这对应了多中心的网络结构；而 *American75* 则比较复杂，其中包含许多个中心节点，整体呈现分布式的结构，这也是普通检测算法最难处理的分布式社交网络的典型结构。由于分布式网络整体呈现出的分散性和稀疏性，传统的检测算法往往会将正常的节点社区误判为 sybil 社区，这也为我们的算法增加了难度。

3.2　对比分析

我们利用 python 编程语言分别编写了 SybilGuard、SybilLimit 和 SybilGuard 三种算法的检测程序。同时为了验证它们的准确度，我们使用随机生成的方法模拟各种不同的攻击方式。经过分析代码运行时间和检测精度，评估了三种算法在不同应用场景下的检测效果，为简化评估流程，我们仅选取最有代表性的攻击种子节点和攻击信用度高的诚实

节点这两种攻击方式进行测试，结果为 10 次测试取均值。

3.2.1 孤立攻击检测

1) 攻击种子节点

表 2 孤立攻击种子节点性能比较

数据集	检测方法	时间/秒	准确率/%
Caltech36	SybilGuard	0.019	98.85
	SybilLimit	0.015	98.69
	SybilRank	0.026	98.64
Reed98	SybilGuard	0.029	97.95
	SybilLimit	0.022	97.50
	SybilRank	0.039	98.18
American75	SybilGuard	0.125	95.69
	SybilLimit	0.106	95.78
	SybilRank	0.195	97.50

从上表可以看出，SybilGuard 和 SybilLimit 算法在检测精度上差别不大，而 SybilLImit 检测时间短于前者。在集中式网络中三种算法的检测精度差不多，但对于分布式网络 *American75* 来说，SybilRank 算法的检测精度更高。

2) 攻击高排名诚实节点

表 3 孤立攻击诚实节点性能比较

数据集	检测方法	时间/秒	准确率/%
Caltech36	SybilGuard	0.016	98.15
	SybilLimit	0.017	97.98
	SybilRank	0.027	98.65
Reed98	SybilGuard	0.026	97.58
	SybilLimit	0.023	96.10
	SybilRank	0.035	98.65
American75	SybilGuard	0.139	94.26
	SybilLimit	0.124	94.64
	SybilRank	0.203	98.71

由于高排名诚实节点分布不均，在检测方面也会耗费较多的资源，所以检测时间比之于种子节点攻击更长，而 SybilRank 算法检测精度仍然最高。

3.2.2 协同攻击检测

1) 攻击种子节点

表 5 协同攻击种子节点性能比较

数据集	检测方法	时间/秒	准确率/%
Caltech36	SybilGuard	0.168	95.26
	SybilLimit	0.146	94.10
	SybilRank	0.195	96.15
Reed98	SybilGuard	0.192	95.65
	SybilLimit	0.167	94.26
	SybilRank	0.268	96.10
American75	SybilGuard	0.217	94.26
	SybilLimit	0.253	95.16
	SybilRank	0.391	96.73

2) 攻击高排名诚实节点

表 6 协同攻击诚实节点性能比较

数据集	检测方法	时间/秒	准确率/%
Caltech36	SybilGuard	0.279	93.16
	SybilLimit	0.261	92.56
	SybilRank	0.367	95.43
Reed98	SybilGuard	0.294	92.46
	SybilLimit	0.306	91.56
	SybilRank	0.435	94.10
American75	SybilGuard	0.305	91.20
	SybilLimit	0.319	91.68
	SybilRank	0.453	93.15

与孤立攻击相比，在忽略微小误差的情况下三种算法的检测效果相差不多。由于协同攻击时各攻击节点可以互相通信“合谋”，这就为女巫节点的检测增加了难度。它在本小节实验数据上体现为检测时间整体偏长、检测精度整体偏低。

4 基于节点行为的检测

谈磊等[10]于 2012 年提出了使用复合分类模型识别网络中女巫节点的方法，我们参考他们的工作进行了基于节点属性和行为的检测，相比于随机游走算法，基于行为的方法表现出了更高的检测精度。

由于此模型需要用户的其他数据，之前的数据集无法使用，所以我们使用斯坦福大学的 SNAP 数据库中的 *Higgs Twitter Dataset* 数据集，它是 2012 年推特中用户行为的真实数据。其中用户的行为包括粉丝数、关注数、点赞数和当前状态（注销、封禁等等），基于此数据集进行了进一步分析。

4.1 模型

为了对不同属性进行降维处理，以简化分析的复杂度，我们对每一对行为属性进行相关性分析，得到了如表 7 所示的分析结果。从表中我们可以看出最具相关性的一对属性为粉丝数和关注数。

其中相关系数的计算公式为：

$$R_{X,Y}=\frac{\sum(X-\bar{X})(Y-\bar{Y})}{\sum(X-\bar{X})^2\sum(Y-\bar{Y})^2}$$

表 7 相关系数比较表

属性	粉丝数	关注数	点赞数	状态
粉丝数	1			
关注数	0.8982	1		
点赞数	-0.2081	0.1296	1	
状态	0.5826	0.4963	0.0281	1

由于目前流行的分类算法多种多样，不可能全部实现，我们选取最常用的 KNN 和朴素贝叶斯分类算法的搭配。原因是 KNN 算法计算量较大，而朴素贝叶斯算法要求类条件独立性假设。所以我们使用单个样本的 F/F 率来进行判断，交替使用两种分类算法，在减少计算量的同时满足了条件独立假设。

其中 F/F 率计算公式为：

$$F(s)=\frac{1}{n}\sum_{i=1}^{n}F(X_i)$$

算法流程如下：

1) 计算平均 F/F 率
2) 如果 0.5F(S)＜F(X)＜1.5F(S) ，使用 KNN 算法
3) 否则使用朴素贝叶斯算法
4) 返回分类结果

4.2 分析验证

经过几轮运算分析，我们将其与随机游走算法进行比较，得出了如下表所示的运算结果：

表 8 几种方法对比

检测方法	攻击类型	时间/秒	准确率/%
SybilGuard	孤立种子	1.315	97.25
	协同种子	1.519	97.98
	协同诚实	1.936	96.15
SybilLimit	孤立种子	1.264	97.16
	协同种子	1.397	96.10
	协同诚实	2.156	95.18
SybilRank	孤立种子	1.356	98.15
	协同种子	1.496	96.49
	协同诚实	2.218	95.17
行为检测	孤立种子	0.358	98.42
	协同种子	0.454	96.18
	协同诚实	0.526	96.58

经过对比，基于节点行为的检测算法在精度差别不大的情况下很明显地缩短了运行时间。

5 结论与展望

经过对比不同的基于随机游走的女巫攻击检测算法在测试网络上的检测结果，我们发现 SybilRank 算法在检测精度上效果最好。对于中心化的网络，几种算法精度差别不大，而此时 SybilRank 要花费更多的时间；而对于分布式网络，SybilRank 在牺牲一些检测时间的基础上拥有较好的检测结果。所以我们在选用算法时需要根据网络结构灵活决定。在此基础上，我们引入用户行为，对用户进行了画像，使用 KNN 和朴素贝叶斯等机器学习分类手段对用户进行了判别。与之前的网络图检测算法相结合，算法效率与准确度取得了较大的提高。

在接下来的工作中，我们打算进一步深化用户行为检测的算法。在进一步调研中我们发现 Zhou Q 等[11]使用受害者预测模型来提高检测精度，这是一个全新的角度，站在被攻击对象的角度建模，估计哪些用户是潜在的被攻击对象，及时向他们发出危险警报，这在未来的女巫攻击团伙检测中将是一个全新的发展方向。相信在女巫攻击的攻防博弈中，我们能够不断进步，将网络诈骗扼杀在摇篮中。

致谢

感谢鄢超波老师在我写论文时给予的点评与帮助，感谢刘烃老师在上学期网络安全课中对我的女巫攻击研究予以肯定，激励我继续完成后续的研究。

参考文献：

[1] Douceur J R. The Sybil Attack[C]. international workshop on peer to peer systems, 2002: 251-260.
[2] Davis C R , Fernandez J M , Neville S , et al. Sybil attacks as a mitigation strategy against the Storm botnet[C]// International Conference on Malicious & Unwanted Software. IEEE Computer Society, 2008.
[3] Mohsen K. BrightID Anti-Sybil[EB/OL]. [2020.11.06].https://github.com/BrightID/BrightID-AntiSybil
[4] Valarmathi M L, Meenakowshalya A, Bharathi A, et al. Robust Sybil attack detection mechanism for Social Networks - a survey[C]. international conference on advanced computing, 2016: 1-5.
[5] Gunturu R. Survey of Sybil Attacks in Social Networks.[J]. arXiv: Cryptography and Security, 2015.
[6] Garg R, Sharma H. Prevention Techniques for Sybil Attack[C]. international conference on bioinformatics, 2012, 11(10): 3060-3064.
[7] Yu H, Kaminsky M, Gibbons P B, et al. SybilGuard:

defending against sybil attacks via social networks[C]. acm special interest group on data communication, 2006, 36(4): 267-278.
[8] 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, 2008: 3-17.
[9] Cao Q , Sirivianos M , Yang X , et al. Aiding the Detection of Fake Accounts in Large Scale Social Online Services[C]// Usenix Conference on Networked Systems Design & Implementation. USENIX Association, 2012.
[10] 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.
[11] Zhou Q, Chen G. An Efficient Victim Prediction for Sybil Detection in Online Social Network. [J]. IEEE Access. 2020: PP. 1-1. 10.1109/ACCESS.2020.3007458.