Computer Science and Application 计算机科学与应用, 2021, 11(12), 3028-3037
Published Online December 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.1112306

Hans汉斯

一种相对重要节点挖掘方法及其在犯罪网络中的应用

罗正国[1]，郁　湧[1,2]，于　倩[1]，王莹港[1]，周　彪[1]，高　涛[3*]

[1]云南大学软件学院，云南　昆明
[2]云南省软件工程重点实验室，云南　昆明
[3]云南经济管理学院教育学院，云南　昆明

收稿日期：2021年11月22日；录用日期：2021年12月17日；发布日期：2021年12月28日

摘　要

网络科学中相对重要节点的挖掘具有重要的应用价值，例如，通过已知犯罪分子查找其他犯罪分子。为此，文中提出了一种基于带重启随机游走的相对重要节点挖掘方法，并结合犯罪网络的两个特征来把该方法应用于犯罪网络的挖掘：根据犯罪分子会隐藏自己的特点对随机游走的初值进行设计；根据犯罪分子之间的通信人物很有可能就是罪犯的特点对随机游走的概率转移矩阵进行改进。最后将提出的方法同4个经典的相对重要节点挖掘指标进行对比，同时通过实际的犯罪网络来进行实验和分析，结果表明，文中的算法比经典的方法更能准确预测出犯罪分子。

关键词

复杂网络，相对重要性，节点挖掘，随机游走，犯罪网络

A Relatively Important Node Mining Method and Its Application in Criminal Networks

Zhengguo Luo[1], Yong Yu[1,2], Qian Yu[1], Yinggang Wang[1], Biao Zhou[1], Tao Gao[3*]

[1]School of Software, Yunnan University, Kunming Yunnan
[2]Key Laboratory in Software Engineering of Yunnan Province, Kunming Yunnan
[3]School of Education, Yunnan University of Business Management, Kunming Yunnan

Received: Nov. 22nd, 2021; accepted: Dec. 17th, 2021; published: Dec. 28th, 2021

*通讯作者。

文章引用: 罗正国, 郁湧, 于倩, 王莹港, 周彪, 高涛. 一种相对重要节点挖掘方法及其在犯罪网络中的应用[J]. 计算机科学与应用, 2021, 11(12): 3028-3037. DOI: 10.12677/csa.2021.1112306

Abstract

The mining of relatively important nodes in network science has important application value, for example, searching for other criminals through known criminals. For this reason, this paper proposes a relatively important node mining method based on random walk with restart, and combines the two characteristics of criminal networks to apply this method to criminal network mining: Design the initial value of the random walk according to the characteristic of criminals hiding themselves; Improve the probability transition matrix of random walk based on the characteristic of the communication between criminals who are likely to be criminals. Finally, the proposed method is compared with four classic relatively important node mining indicators. At the same time, experiments and analysis are carried out through the actual criminal network. The results show that the algorithm in this paper can predict criminals more accurately than the classic method.

Keywords

Complex Network, Relative Importance, Node Mining, Random Walk, Criminal Network

1. 引言

节点的重要性研究在复杂网络领域一直备受关注，具有非常重要的意义，其中最主要的作用是找出网络中的核心节点[1]-[6]。但在实际生活中，通常是已知网络中的部分节点为重要节点，利用这些已知的重要节点和网络的拓扑结构，来计算其余节点相对于这些已知重要节点的重要性，从而找出相对重要的节点，这类问题的研究叫做相对重要节点挖掘[7]。相对重要节点挖掘的方法可以成功地应用于犯罪网络的调查，如通过已知罪犯查找剩余罪犯[7] [8] [9]。近几年相对重要节点的挖掘也成为了复杂网络科学中的热门研究方向之一，且有着广泛的应用，不仅可以用于犯罪网络，还可以应用于通过已知致病基因查找未知致病基因[10]，在疾病传播中通过已知感染节点查找或预测风险节点并及时监控隔离等[11]。

犯罪网络可以理解为在法律范围之外运作的网络，其网络成就是以牺牲其他个人、团体或社会为代价的[12] [13]。犯罪网络遍及全球，对国防和安全产生重大影响。犯罪网络试图渗透合法企业和政府，进而获取暴利。因此，面对一些犯罪网络，如儿童色情制品、海上盗版、暗网、恐怖组织、毒品交易、地下洗钱等对社会造成重大损害，需要积极采取措施对其进行打击及破坏[14] [15]。通过犯罪网络分析可以发现一些并不直观的线索，来协助公安机关破案，从而达到打击犯罪行为、维护社会稳定的目的。

在简单的犯罪网络中确定犯罪主体，犯罪分子相对较少，人脉关系很少，这通常可以通过肉眼来完成。随着时代的进步，犯罪行为以及犯罪网络变得越来越复杂，调查个人和团体犯罪需要大量资源，并且需要越来越多的领域知识、技能和时间[16]。研究人员发现犯罪网络也可以理解为社交网络，因此可以利用社会网络分析的方法寻找犯罪网络的核心节点。但通常，寻找犯罪网络的核心节点是对犯罪网络掌握了大量信息后才能做的事。在犯罪网络分析的初始阶段，如何利用少量已知的犯罪分子和与其联系的网络知识来挖掘剩下的罪犯也是非常有价值的事。

2. 相对重要节点挖掘以及犯罪网络研究现状

相对重要节点挖掘的工作开始于 Chang 等[17]在 2000 年提出的一种个性化 HITS 算法。接着，Haveliwala 等[18]和 Jeh 等[19]也分别提出了各自的个性化 PageRank 算法。随后 White [7]定义了相对重要节点挖掘问题，总结了一些相对重要节点挖掘算法，并给出一套相对重要节点挖掘的通用框架。Wang 等[20]提出了基于随机游走的方法在相对重要节点挖掘的应用。Jocelyn [21]对传统中心性指标在子网中的应用方法进行了总结归纳。朱军芳等人[22]整理了基于结构特征指标和基于随机游走指标的两套指标和方法，并对其中各种方法指标进行比较，对一些开放性问题和发展趋势进行了讨论。

其中文献[22]将相对重要节点的方法归为两大类，一类是基于结构特征的，一类是基于随机游走的，其实验表明基于随机游走的方法整体优于基于结构特征的方法；但基于随机游走的方法仍存在一些不足，如不能有效的利用已知重要节点在网络中位置的信息；对不同的已知重要节点集，仍用同样的概率转移矩阵进行随机游走。

在犯罪网络研究方面，目前，利用节点重要性方法对犯罪网络进行的研究有很多。如，自 1991 年以来，就开始有人使用社交网络分析法来提取犯罪情报[23]。随后在 2002 年 Kreb 博士在国际社会网分析年会上分享了 911 事件的劫机恐怖分子及其联系人构成的犯罪网络[24]后，这种方法在犯罪网上得到了广泛的应用；Carley [25]等针对恐怖组织结构和成员难以分析的问题，开发了一种工具 NETEST 用以模拟恐怖组织结构；2003 年波士顿大学 Stephen P. Borgatti [26]定义了特殊的社会网络核心人员挖掘问题并提出了挖掘算法。2005 年，Chen 等人[27]基于移除核心成员对网络造成的破坏程度来挖掘犯罪网络的核心成员。2006 年，S.P Borgatti [28]利用社会网络的概念，分析数据来挖掘犯罪网络的核心成员。2014 年，D’Orsogna [29]对基于核心节点移除分析网络的破坏性的方案进行深入地调查和分析。2017 年，Taha [30]等人引出最小生成树的概念，挖掘犯罪网络的核心领导者。Magalingam [31]通过改进介数中心性指标来挖掘犯罪网络中的剩余罪犯。Troncoso 等人[5]为了更加准确的识别犯罪嫌疑人，把个人犯罪倾向纳入节点重要性评估。

虽然犯罪网络方面的研究已取得不少的成果，但大多都是在已知整个犯罪网络信息的情况下来挖掘犯罪集团核心人物的。而在犯罪网络分析的初始阶段，更应该考虑利用少量的犯罪信息，来挖掘更多的信息。如：利用少量的已知罪犯和罪犯所属网络的结构信息，来挖掘剩余罪犯。至今，这类研究较少。

因此，本文提出了一种基于带重启随机游走的相对重要节点挖掘算法。随机游走是研究网络结构和特性的一种重要方法。相对重要节点挖掘中的随机游走是指粒子从已知重要节点出发，以一定的概率游走到它的邻居节点，然后再以一定的概率游走到邻居节点的邻居节点，这样反复达到平衡稳态后结束游走。在本文提出的游走方法中，粒子不仅有概率向邻居节点游走，还有一定概率跳回已知重要节点重新开始游走，而且当粒子游走遍历完整个网络后便结束游走，该方法更能有效的利用已知重要节点在网络中位置的信息。本文将此算法应用于犯罪网络，利用犯罪网络的特点，对随机游走的初值和概率转移矩阵进行设计。

3. 问题描述以及方法介绍

对于 N 个节点构成的网络 $G(V,E)$，其中 N_1 个构成重要节点集 V_1，N_2 个节点构成非重要节点集 V_2，重要节点集 V_1 是由已知重要节点集 R 和未知重要节点集 U 组成。未知重要节点集 U 和非重要节点集 V_2 组成目标节点集 T。相对重要节点挖掘是在目标节点集 T 中找到相对于已知重要节点集 R 较为重要的 top_L 个相对重要节点。

由公式表达如下：

$$\begin{aligned} &V = V_1 \cup V_2,\ V_1 \cap V_2 = \varnothing \\ &V_1 = R \cup U,\ R \cap U = \varnothing \\ &T = U \cup V_2 \end{aligned} \tag{1}$$

本文提出的方法是基于带重启随机游走的相对重要节点挖掘方法，并将其根据犯罪网络的特点，对随机游走的初值和概率转移矩阵进行设计。步骤如下：

1) 将带重启的随机游走方法用于相对重要节点挖掘。

2) 利用犯罪网络中犯罪分子会有意识地隐藏自己的特点，即罪犯会更加偏向于和不易于暴露的节点连接，来设计随机游走的初值概率分布 P_0。

3) 利用犯罪网络中罪犯之间的通信人物很有可能就是罪犯的特点，对概率转移矩阵 W 进行改进。

3.1. 带重启随机游走的相对重要节点挖掘方法

带重启的随机游走 RWR (Random Walk with Restart) [32]，从一个节点开始随机游走，在每一步游走时面临两个选择：或者移动到一个随机选择的邻点，或者跳回起点，仅通过一个参数 α 来调节节点跳回起点的概率，在多次模拟第一步随机游走实验过后，会得到这个节点进行第一步随机游走后的稳定概率分布：

$$P^1 = (1-\alpha)P^0 + \alpha W^{\mathrm{T}} P^0 \tag{2}$$

P^1 是网络中起始节点随机游走一步到所有节点的概率分布向量，P^0 是一个初始概率分布向量，P^0 中除了对应的随机游走起始节点(已知重要节点)数值设置为 1，其余所有值都设置为 0，W 是概率转移矩阵。多步随机游走后的概率分布 P^{t+1} 可以描述为：

$$P^{t+1} = (1-\alpha)P^0 + \alpha W^{\mathrm{T}} P^t \tag{3}$$

带重启随机游走的结束游走条件是当节点遍历完整个网络后结束，即 P^{t+1} 向量中的所有值都大于 0 时候，我们认为它已经遍历完整个网络，这是 RWR 方法能设置初始概率分布 P^0 的重要原因。若让随机游走达到稳态才停止，那么无论如何设置初始概率分布 P^0，最终得到的节点的排名是不会发生变化的。最终得到的向量 P^{t+1} 即为相对重要性向量，代表图中所有节点对已知重要节点的相对重要性。如果已知重要节点集中有多个节点，那么我们将根据 3.2 节中的方法确定如何对初值进行设定，同时从多个已知重要节点开始随机游走，最终得到的向量 P^{t+1} 即为相对重要性向量，代表图中所有节点对已知重要节点集的相对重要性。

3.2. 初始概率分布 P^0 的设计

已知重要节点在网络中的位置是设置初始概率分布 P^0 的关键，本文认为在网络中越重要的节点，应赋予对应节点更大的概率分布初值，那么在网络中与初值较大节点直接相连的节点，在随机游走后，越可能获得比与初值较小节点直接相连节点更大的概率分布分数。

为了避免犯罪网络数据的不完整或有多余节点和边所带来的误差，我们希望得到一个节点重要性的大致的排名即可。而 k-shell 方法[16]恰好能对节点进行一个大致的分层，得到我们想要的结果，因此我们采用 k-shell 方法来计算节点重要性。

k-shell 方法是通过递归的移除网络中所有节点度值不大于 k 的节点，并将这些节点归为 k-shell，剩余网络中不含有度值小于或等于 k 的节点时，再递归移除度值不大于 k + 1 的节点，归为 k + 1-shell，直到网络中所有节点被移除。

犯罪分子通常会有意识的隐藏自己，因此，罪犯会倾向于和在显性指标下重要程度较低的节点相连。

而 k-shell 方法是基于节点度的大小进行分层的方法，度指标是一个显性指标，因此本文设定越外层的节点初始概率分布分数越大。

在用 k-shell 方法分层的情况下，本文认为同层的节点拥有相同的重要性，每一层内节点的重要性为该层的基准重要性，属于第 i 层内节点的基准重要性记为 Z_i。

若一个网络 $G(V,E)$ 用 k-shell 方法被分为了 t 层，第 i 层中的节点个数为 $n_i\ (1\le i\le t)$，令 $N=\sum_{1\le i\le t} n_i$，$n_{t+1}=1$ (使 t 层节点的节点重要性不为 0)，$N_i=\sum_{i\le j\le t+1} n_j\ (1\le i\le t+1)$，则第 i 层中的基准重要性 Z_i 的计算公式如下：

$$Z_i = N_{i+1}/N \tag{4}$$

因此利用 k-shell 方法得到节点 v 的重要性为 $I(v)=Z_i,(v\in i\text{-shell})$。于是初始概率分布值如下：

$$P_v^0=\begin{cases} I(v), v\in R \\ 0, v\notin R \end{cases} \tag{5}$$

3.3. 带游走偏好的概率转移矩阵 W 的设计

White 和 Smyth 指出，节点相对重要性计算指标和方法并非全局重要性指标在子网络中的简单应用，而是对已知重要节点的偏好设计，偏好设计是节点相对重要性方法和指标设计的核心[7]。众多文献表明，介数中心性对于确定犯罪网络的核心节点是非常重要的指标[33] [34]。在犯罪网络中，根据罪犯之间的通信人物很有可能就是罪犯的特点，本文设计了一个在犯罪网络中寻找相对重要节点的偏好策略：在随机游走时，更倾向于向位于已知重要节点对(r_1, r_2)，之间的中间节点 b 进行游走。

传统的概率转移矩阵 T 是根据邻接矩阵 A 得到的，在一个无向无权网络 $G(V,E)$，邻接矩阵 A 中的元素 A_{ij} 的含义如下：

$$A_{ij}=\begin{cases} 1, & \text{如果顶点}i\text{和顶点}j\text{之间存在边} \\ 0, & \text{其他} \end{cases} \tag{6}$$

则概率转移矩阵 W 的生成规则如下：

$$W_{ij}=\frac{A_{ij}}{\sum_{0\le i<n} A_{ij}} \tag{7}$$

概率转移矩阵有以下两个特性：

$$\begin{aligned} &0\le W_{ij}\le 1 \\ &\sum_{0\le i<n} W_{ij}=1 \end{aligned} \tag{8}$$

其中 W_{ij} 表示节点从节点 j 位置游走时向节点 i 位置游走的概率，若想增大游走到节点 b 的概率，增大 $A_{bj}\ (0\le j<n)$ 即可。

若存在这样的中间节点 b，将修改邻接矩阵 A 中的元素：

$$A_{bj}\ (0\le j<n)=\begin{cases} 2, & \text{如果原}\ A_{bj}=1 \\ 0, & \text{如果原}\ A_{bj}=0 \end{cases} \tag{9}$$

利用中间节点集 B 中所有节点修改完邻接矩阵 A 后，再根据修改后的矩阵 A 按照概率转移矩阵生成规则重新计算的得到新的带游走偏好的概率转移矩阵 W，再利用 3.4 中的方法计算目标节点的相对重要性。

判定节点位于已知重要节点对之间的条件如下：

$$sd(t,r_1)+sd(t,r_2)=sd(r_1,r_2) \tag{10}$$

其中，$sd(t,r_1)$ 表示目标节点 t 到已知重要节点 r_1 的最短距离，当且仅当目标节点 t 距离已知重要节点 r_1 的最短距离与已知重要节点 r_2 的最短距离之和等于 r_1 与 r_2 之间的最短距离时，便认为它是一个中间节点。已知重要节点也可能是一个中间节点。

3.4. 带游走偏好的概率转移矩阵 W 的设计

将带重启的随机游走方法(RWR)结合犯罪网络的特点，用 3.2 和 3.3 中的方法改进 RWR 算法中的初始概率分布和概率转移矩阵后应用于犯罪网络中的相对重要节点挖掘，本文简称这种方法为 RWR*算法。

RWR*算法伪代码如下：

RWR*算法
输入：kshell 方法得到的节点重要度 I(v)，带游走偏好的概率转移矩阵 W，已知重要节点集 R，目标节点集 T，重启概率 α

```
def fun_RWR(W, R, T, α):
    for 节点 do:
        I(t | R) ← 0
    end for;
    for 节点 do:
        if  then:
            P_v = I(v)
        else  P_v ← 0 ;
    end for;
    while 任意节点 v 的 P_v^{n+1} = 0 do:
        P^{n+1} ← (1−α)P^0 + αW^T P^n
    end while;
    /*此时得到的 P_t^{n+1} 即为 I(t|R)*/
    return I(T|R)
```

4. 实验

4.1. 评价指标

本文采用精确率对相对重要节点挖掘的结果进行比较，该指标考虑目标节点集中相对重要性总和排在前 L 位的节点是否预测准确，公式如下：

$$\text{precision} = N_r / L \tag{11}$$

其中，precision 为预测的准确率，N_r 为相对重要性排名前 L 个节点在未知重要节点集中出现的个数。

4.2. 数据集

以 911 恐怖袭击事件真实犯罪关系网络为数据集[24]，该网络有 37 个节点，85 条边。该数据是 Krebs 通过案件公开的 19 个已死亡的劫机者展开调查，分析整理得到的。其中节点编号为 1、4、35、36、37 对应的人物劫持了 11 号航班，节点编号为 1 的是本机上的核心犯罪人员，也是本次恐怖袭击事件的主策划者；节点编号为 2、17、32、28、31 对应的人物劫持了 175 号航班，节点编号为 2 的是本机上的核心犯罪人员；节点编号为 16、18、15、22、21 对应的人物劫持了 77 号航班，节点编号为 16 的是本机上的核心犯罪人员；节点编号为 14、30、29、27 对应的人物劫持了 93 号航班，节点编号为 14 的是本机上的

核心犯罪人员。其他人员没有直接参与本次恐怖袭击事件，节点编号为 10 的是辅助前四个团伙完成任务的核心犯罪分子。本文认为该网络有 19 个重要节点，10 号节点未直接参与本次袭击。该数据的网络结构及分工如图 1 所示。

4.3. 实验比较与分析

实验方法，本文进行三轮实验，每轮分别抽取重要节点集中的三个、四个、五个节点作为已知重要节点集，把剩下的未知重要节点的个数作为我们的预测的个数，进行 20 次独立实验，最后对预测的准确性结果取均值。本文会把 10 号节点考虑为非重要节点和重要节点分别进行实验。

其中通过抽取四个节点作为已知重要节点集来确定 RWR*方法中超参数：随机游走重启概率。

图 2 表明，当 $\alpha = 0.7$ 时，RWR*方法的准确率最佳。

犯罪节点挖掘实验的对比方法为常用效果最好的 PPR [18]、PHIST [7]、KSMar [7]和 Katz [35]，其中

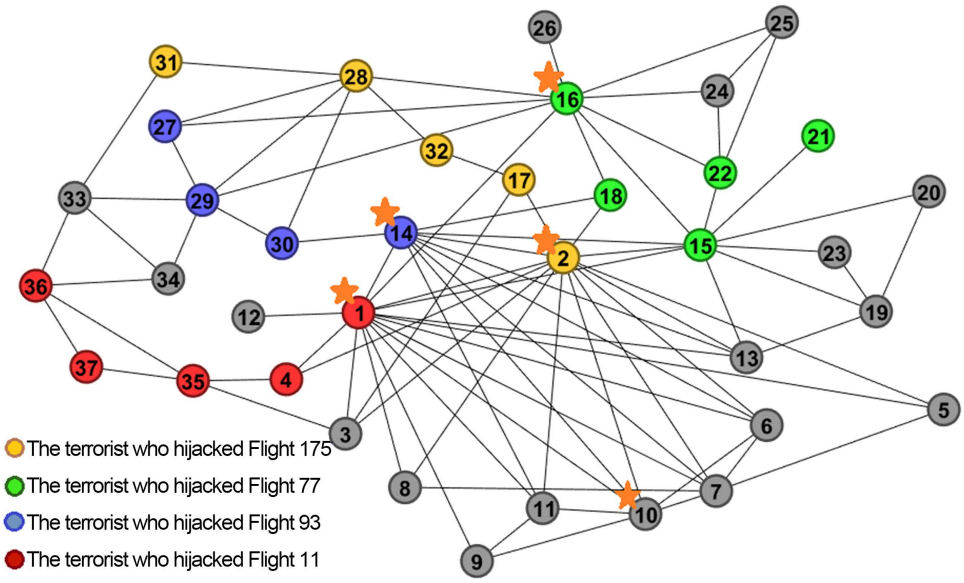

Figure 1. Schematic diagram of the division of labor of the criminals in the 911 terrorist attack
图 1. 911 恐怖袭击事件犯罪分子分工示意图

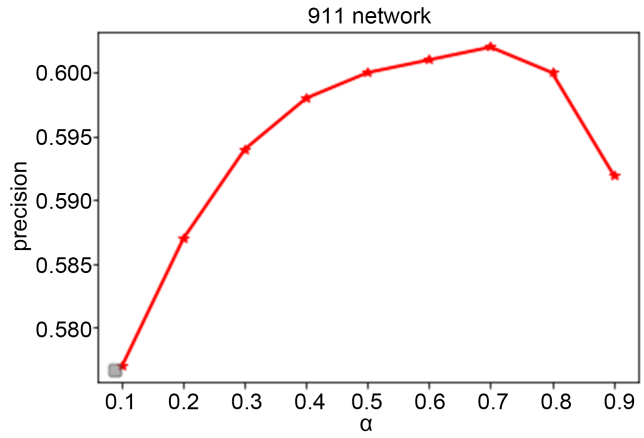

Figure 2. RWR* algorithm hyperparameter experiment
图 2. RWR*算法超参数的实验

PPR 方法中的 $s=0.75$，PHIST 中的 $s=0.1$，KSMar 中 $K=3$，Katz 中 $\varphi=0.0001$，前三种方法是文献[22]实验中基于随机游走效果最好的方法，Katz 是文献[22]实验中基于结构特征效果最好的方法。

从图 3 的实验结果可以看出，本文提出的 RWR*方法在 911 犯罪网络数据上更能准确的利用已知罪犯挖掘剩余罪犯。无论在已知三名、四名、五名罪犯的情况下都是表现最好的算法。且在三次实验的平均值准确率上，RWR*算法比平均准确率排第二的算法高出 4 个百分点左右。

PPR 算法与本文的 RWR*算法最大的区别是，PPR 算法当概率分布达到稳态时才终止随机游走，无论如何改变初始概率分布，最终节点概率分布的排名都不会发生变化，因此 RWR*算法较 PPR 更能有效利用已知重要节点提供的信息。

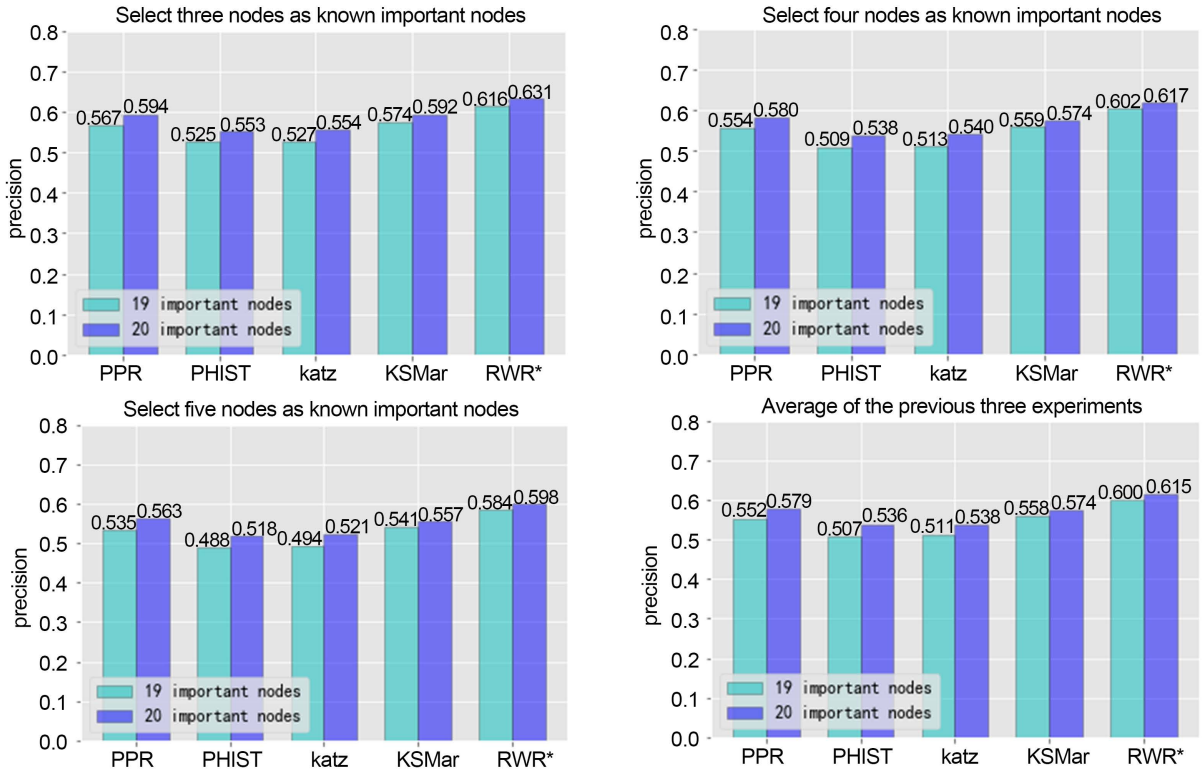

Figure 3. Comparison of relatively important node mining experiments
图 3. 相对重要节点挖掘实验对比

K 步马尔可夫方法(KSMar)，利用前 K 步随机游走后的概率分布的累积总和来衡量节点的相对重要性。K 步马尔可夫方法公式如下：

$$I(t \mid R)=\left[TP+T^2P+\cdots+T^KP\right] \tag{12}$$

其中 TP 为第一步随机游走后得到的概率分布，T^2P 代表第二步随机游走后得到的概率分布，离初始随机游走越近的节点会获取越高的相对重要性，即与犯罪分子越亲密的人嫌疑越大。

而本文提出的改进后的带重启的随机游走方法，更能考虑已知重要节点的重要性，根据犯罪网络的特点对不同的已知重要节点集设计不同的概率转移矩阵，用于挖掘罪犯时效果会更佳。

5. 结束语

本文提出了一种新的带重启随机游走的相对重要节点挖掘方法，并在应用于犯罪网络中时，根据犯

罪网络的特点对随机游走方法的初值概率分布和概率转移矩阵进行改进：根据犯罪分子会隐藏自己的特点对随机游走的初值进行改进，根据罪犯之间的通信人物很有可能就是罪犯的特点对随机游走的概率转移矩阵进行改进。最后通过 911 恐怖袭击事件犯罪网络实验证明，在符合一定条件的犯罪网络中，本文提出的方法比经典的相对重要节点挖掘方法更能准确地挖掘出罪犯。在未来的工作中，仍有许多值得深入研究的地方：1) 如何利用已知重要节点挖掘得到的相对重要节点作为已知重要节点进一步挖掘。2) 本文是在等概率随机游走转移矩阵的基础上进行修改的，还可以尝试用不等概率随机游走概率转移矩阵进行研究，并对不等概率随机游走概率转移矩阵进行修改。3) 在使用相对重要节点挖掘方法实际落地应用时，对于不同类型的网络应该设计不同的偏好设计。

参考文献

[1] 赫南, 李德毅, 淦文燕, 等. 复杂网络中重要性节点发掘综述[J]. 计算机科学, 2007, 34(12): 1-5.

[2] Zhou, F., Lv, L.Y. and Mariani, M.S. (2019) Fast Influencers in Complex Networks. *Communications in Nonlinear Science and Numerical Simulation*, **74**, 69-83. https://doi.org/10.1016/j.cnsns.2019.01.032

[3] Liu, Y.S., Wang, J.J., He, H.T., *et al*. (2021) Identifying Important Nodes Affecting Network Security in Complex Networks. *International Journal of Distributed Sensor Networks*, **17**, 1-10. https://doi.org/10.1177/1550147721999285

[4] Bright, D.A., Greenhill, C., Reynolds, M., *et al*. (2015) The Use of Actor-Level Attributes and Centrality Measures to Identify Key Actors. *Journal of Contemporary Criminal Justice*, **31**, 262-278. https://doi.org/10.1177/1043986214553378

[5] Troncoso, F. and Weber, R. (2020) Integrating Relations and Criminal Background to Identifying Key Individuals in Crime Networks. *Decision Support Systems*, **139**, Article ID: 113405. https://doi.org/10.1016/j.dss.2020.113405

[6] Kitsak, M., Gallos, L.K., Havlin, S., *et al*. (2010) Identification of Influential Spreaders in Complex Networks. *Nature Physics*, **6**, 888-893. https://doi.org/10.1038/nphys1746

[7] White, S. and Smyth, P. (2003) Algorithms for Estimating Relative Importance in Networks. *The* 3*th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington DC, 24-27 August 2003, 266-275. https://doi.org/10.1145/956750.956782

[8] Alzaabi, M., Taha, K. and Martin, T. (2015) CISRI: A Crime Investigation System Using the Relative Importance of Information Spreaders in Networks Depicting Criminals Communications. *IEEE Transactions on Information Forensics & Security*, **10**, 2196-2211. https://doi.org/10.1109/TIFS.2015.2451073

[9] Magalingam, P. (2016) Complex Network Tools to Enable Identification of a Criminal Community. *Bulletin of the Australian Mathematical Society*, **94**, 350-352. https://doi.org/10.1017/S000497271600040X

[10] 赵静, 林丽梅. 基于分子网络的疾病基因预测方法综述[J]. 电子科技大学学报, 2017, 46(5): 755-765.

[11] 周涛, 汪秉宏, 韩晓璞, 等. 社会网络分析及其在舆情和疫情防控中的应用[J]. 系统工程学报, 2010, 25(6): 742-754.

[12] Milward, H.B. and Raab, J. (2006) Dark Networks as Organizational Problems.

[13] Morsello, C. (2009) Inside Criminal Networks. Springer, New York. https://doi.org/10.1007/978-0-387-09526-4

[14] Office EP (2011) EU Organized Crime Threat Assessment 2011.

[15] Aitken, P. (2010) The Globalization of Crime: A Transnational Organized Crime Threat Assessment. UN Office on Drugs and Crime (UNODC).

[16] Jennifer, J.X. and Hsinchun, C. (2005) CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery. *ACM Transactions on Information Systems*, **23**, 201-226. https://doi.org/10.1145/1059981.1059984

[17] Chang, H. and Mccallum, A. (2000) Learning to Create Customized Authority Lists. *Proceedings of the* 17*th International Conference on Machine Learning*, Stanford, CA, 2000, 127-134.

[18] Haveliwala, T.H. (2003) Topic-Sensitive PageRank: A Context-Sensitive Ranking Algorithm for Web Search. *IEEE Transactions on Knowledge and Data Engineering*, **15**, 784-796. https://doi.org/10.1109/TKDE.2003.1208999

[19] Jeh, G. and Widom, J. (2003) Scaling Personalized Web Search. *Proceedings of the* 12*th International Conference on World Wide Web*, Budapest, 20-24 May 2003, 271-279. https://doi.org/10.1145/775152.775191

[20] Wang, H., Chang, C.K., Yang, H.I., *et al*. (2013) Estimating the Relative Importance of Nodes in Social Networks. *Journal of Information Processing*, **21**, 414-422. https://doi.org/10.2197/ipsjjip.21.414

[21] Jocelyn, R.B. (2014) Subgroup Centrality Measures. *Network Science*, **2**, 277-297. https://doi.org/10.1017/nws.2014.15

[22] 朱军芳，陈端兵，周涛，等. 网络科学中相对重要节点挖掘方法综述[J]. 电子科技大学学报，2019，48(4): 595-603.

[23] Sparrow, M.K. (1991) The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects. *Social Networks*, **13**, 251-274. https://doi.org/10.1016/0378-8733(91)90008-H

[24] Krebs, V.E. (2002) Mapping Networks of Terrorist Cells. *Connections*, **24**, 43-52.

[25] Dombroski, M.J. and Carley, K.M. (2002) NETEST: Estimating a Terrorist Network's Structure. *Computational & Mathematical Organization Theory*, **8**, 235-241. https://doi.org/10.1023/A:1020723730930

[26] Borgatti, S.P. (2003) Identifying Sets of Key Players in a Network. *International Conference on Integration of Knowledge Intensive Multi-Agent Systems*, Cambridge, MA, 30 September-4 October 2003, 127-131.

[27] Xu, J.J. and Chen, H. (2005) CrimeNet Explorer.

[28] Borgatti, S.P. (2006) Identifying Sets of Key Players in a Social Network. *Computational & Mathematical Organization Theory*, **12**, 21-34. https://doi.org/10.1007/s10588-006-7084-x

[29] D'orsogna, M.R. and Perc, M. (2015) Statistical Physics of Crime: A Review. *Physics of Life Reviews*, **12**, 1-21. https://doi.org/10.1016/j.plrev.2014.11.001

[30] Taha, K. and Yoo, P.D. (2017) Using the Spanning Tree of a Criminal Network for Identifying Its Leaders. *IEEE Transactions on Information Forensics & Security*, **12**, 445-453. https://doi.org/10.1109/TIFS.2016.2622226

[31] Magalingam, P., David, S. and Rao, A. (2015) Ranking the Importance Level of Intermediaries to a Criminal Using a Reliance Measure.

[32] Page, L., Brin, S., Motwani, R., *et al*. (1998) The PageRank Citation Ranking: Bringing Order to the Web. Stanford Info Lab.

[33] Farasat, A., Gross, G., Nagi, R., *et al*. (2015) Social Network Extraction and High Value Individual (HVI) Identification within Fused Intelligence Data. In: *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction*, Springer, Cham, 44-54. https://doi.org/10.1007/978-3-319-16268-3_5

[34] Lindelauf, R.H.A., Hamers, H.J.M. and Husslage, B.G.M. (2013) Cooperative Game Theoretic Centrality Analysis of Terrorist Networks: The Cases of Jemaah Islamiyah and Al Qaeda. *European Journal of Operational Research*, **229**, 230-238. https://doi.org/10.1016/j.ejor.2013.02.032

[35] Katz, L. (1953) A New Status Index Derived from Sociometric Analysis. *Psychometrika*, **18**, 39-43. https://doi.org/10.1007/BF02289026