·安全技术· 文章编号：1000-3428(2019)09-0119-05 文献标志码：A 中图分类号：TP399

在线社交网络恶意信息多源定位算法

袁得嵛[1,2]，黄淑华[1,2]，叶萌熙[1]，王小娟[3]

（1. 中国人民公安大学 信息技术与网络安全学院，北京 102623；
2. 安全防范技术与风险评估公安部重点实验室，北京 102623；3. 北京邮电大学 电子工程学院，北京 100876）

摘 要： 针对恶意信息源覆盖范围重叠导致基于全网拓扑的定位算法复杂度高的情况，提出基于社区结构的子图划分算法，将恶意信息多源定位问题分解为多个单源定位问题。在此基础上，利用基于 Jordan 中心的在线社交网络多源定位算法，实现多个子图内的恶意信息单源定位。在随机数网络和 UCIonline 网络上的仿真结果表明，该算法能够有效识别恶意信息源，定位准确率相比基于距离中心、紧密度中心和介数中心的算法提高 11%～30%。

关键词： 在线社交网络；恶意信息；子图划分；Jordan 中心；多源定位

中文引用格式： 袁得嵛，黄淑华，叶萌熙，等. 在线社交网络恶意信息多源定位算法[J]. 计算机工程，2019，45(9)：119-123.

英文引用格式： YUAN Deyu，HUANG Shuhua，YE Mengxi，et al. Multi-source location algorithm for malicious information in online social network[J]. Computer Engineering，2019，45(9)：119-123.

Multi-Source Location Algorithm for Malicious Information in Online Social Network

YUAN Deyu[1,2]，HUANG Shuhua[1,2]，YE Mengxi[1]，WANG Xiaojuan[3]

（1. School of Information Technology and Cyber Security，People's Public Security University of China，Beijing 102623，China；
2. Key Laboratory of Safety Precaution Technology and Risk Assessment，Ministry of Public Security，Beijing 102623，China；
3. School of Electronic Engineering，Beijing University of Posts and Telecommunications，Beijing 100876，China）

【Abstract】 To address the high complexity of the location algorithm based on the topology of the whole network，which is led by a coverage overlap between malicious information sources，a subgraph division algorithm based on community structure is proposed. The algorithm decomposes the location problem of multi-source malicious information into multiple single-source location problems. On this basis，the multi-source location algorithm for Online Social Network（OSN）based on the Jordan center is used for the single-source malicious information location in multiple subgraphs. Simulation results on the random number network and UCIonline network show that the algorithm can effectively identify malicious information sources，and its location accuracy is 11%～30% higher than that of algorithm based on Distance Center（DC），Tightness Center（TC）and Betweenness Center（BC）.

【Key words】 Online Social Network（OSN）；malicious information；subgraph division；Jordan center；multi-source location

DOI： 10.19678/j.issn.1000-3428.0051787

0 概述

近年来，随着 Facebook、Twitter、微博、微信、QQ 等互联网社交媒体的快速发展，在线社交网络（Online Social Network，OSN）成为网络用户参与的重要平台。OSN 在反映现实社会的同时也在影响现实社会。谣言等恶意信息在高度互联的复杂网络上的快速传播通常会带来严重的后果。研究、分析以及控制 OSN 上信息的蔓延扩散过程已成为复杂网络领域的研究热点[1-2]。恶意信息初始发布节点推断对于社会舆论引导、突发事件控制具有重要的现实意义。

对于复杂网络信息源点定位问题，现有很多研究都基于理想假设，即只有一个单一的源节点，如文献[3]利用最大似然检测方式，针对单个信息源进行检测；文献[4]通过多个观测点对谣言传播源进行定位，基于 SI 模型对单个信息源的谣言传播，提出基于联合谣言中心性的统一推断框架，利用多个非独

基金项目： 国家重点研发计划(2017YFC0803700)；国家自然科学基金面上项目“未来超密集异构网络的理论分析与资源协同优化研究”(61771072)；北京市自然科学基金(4184099)；公安部科技强警基础工作专项(2017GABJC38)；中国人民公安大学基本科研业务费专项资金(2016JKF01317)。

作者简介： 袁得嵛(1986—)，男，讲师、博士，主研方向为网络安全、复杂网络；黄淑华，副教授、硕士；叶萌熙，本科生；王小娟，副教授、博士。

收稿日期： 2018-06-11 **修回日期：** 2018-08-28 **E-mail：** yuandeyu@gmail.com

立的观测节点提高溯源概率;文献[5]基于动态传播过程,提出单个传染来源的最大似然估计统计推断框架,设计 3 种似然估计函数确定整个网络中每个潜在源节点的条件概率;文献[6]通过统一谣言来源的先验分布,将整个传播过程看作一个树状图的形式,从感染节点中确定单一源头;文献[7]对基于观察点的信息源定位方法进行改进,通过筛选候选源点,减小计算量,提高源点定位效率。

对于多个传播源,文献[8]将溯源问题简化为寻找网络中的关键模块的问题,利用近似划分寻找关键模块从而识别多个传播源,最终结果接近于全局最优解;文献[9]利用部分发现的感染节点估计整个网络中的感染节点情况,提出一种反向传播算法来发现已恢复节点和未被发现的感染节点,并通过社区集群算法将多源定位问题转化为单一源定位的问题;文献[10]在任意给定的网络结构中利用蒙特卡洛估计方法检测不同传染病源,针对 SIR 模型推导出检测成功的上限,该结果依赖于传播过程的特征;文献[11]基于感染节点进行关联分析提出整个网络中的感染源以及感染区域的估计方法,确定不同网络中的真实感染节点数目以及感染源。综上所述,现有方法在恶意信息溯源等领域取得了较大进展,但仍存在一些问题:恶意信息源从多传播源进行扩散,导致不同源点的覆盖范围有所重叠,并且基于全网拓扑结构的源点定位算法复杂度过高。为解决上述问题,本文采用分而治之的策略将复杂的多源定位问题分解为多个单源定位问题,提出基于社区结构的子图划分算法及基于 Jordan 中心的恶意信息源定位算法。

1 传播模型

1.1 信息传播模型

考虑在线社交网络 $G=(V,E)$ 上的信息传播过程,其中,V 为节点集,E 为节点连边集合。由边连接的 2 个节点称为邻居,即存在关注关系。为简便起见,本文将 $G=(V,E)$ 描述为无向图。在某一未知时刻,在线社交网络中的源节点发布恶意消息 m,网络中的其他节点收到消息 m 并向其邻居节点转发。本文通过观察特定时刻的感染节点集来推断恶意信息源。

本文采用离散时间扩散模型,其中时间被分成离散的时隙,并且遵循马尔可夫过程。在符合 SI 模型的传播模式下,网络中的每个节点处于易感状态(S)或者感染状态(I)。一旦节点受到感染,将永远保持感染状态。在每个传播模拟的开始阶段,每个感染节点在相同时隙内会以相同概率 p 感染处于易感状态的邻居节点。

1.2 Jordan 中心

定义 1(Jordan 中心) 令 $d(s,u)$ 表示图 G 中节点 s 和 u 之间最短路径的长度,即 2 个节点之间的距离。对于 G 中的任意节点子集 A,定义节点 s 在 A 中的离心率为 $\bar{d}(s,A)$,即 s 与 A 中节点之间的最大距离,得出:

$$\bar{d}(s,A)\triangleq\max_{u\in A} d(s,u) \tag{1}$$

节点集合 A 的 Jordan 中心被定义为 G 中具有最小离心率的节点。

2 恶意信息多源定位算法

本文先提出基于社区结构的子图划分算法,再利用基于 Jordan 中心的恶意信息多源定位算法解决多个子图内的恶意信息单源定位问题。

2.1 基于社区结构的子图划分算法

在社区结构明显的网络中,消息更容易在社区内部的节点间传播,然后蔓延扩散到网络其他区域。因此,社区结构可以区分出多个源点的传播范围。通过划分子图实现恶意信息多源定位的具体过程,如图 1 所示。

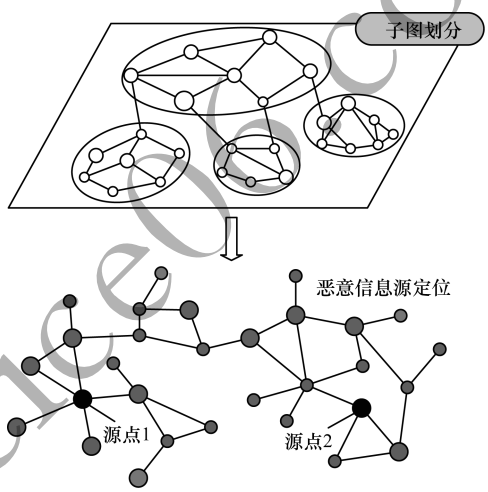

图 1 恶意信息多源定位

为衡量基于社区结构的子图划分算法的优劣,文献[12]提出模块度指标,通过比较现有网络与基准网络在相同社区划分下的连接密度差来衡量网络社区划分的优劣,其中,基准网络是与原网络具有相同序列的随机网络。假设 $\boldsymbol{A}$ 是复杂网络的邻接矩阵,$k_v(k_w)$ 表示节点 $v(w)$ 的度数,m 表示网络图 $\boldsymbol{A}$ 中的连边数目。模块度定义如下:

$$Q=\frac{1}{2m}\sum_{v,w}\left[\boldsymbol{A}_{vw}-\frac{k_v(k_w)}{2m}\right]\delta(c_v,c_w) \tag{2}$$

其中,c_v 表示节点 v 所属社区。如果节点 v 和节点 w 属于同一个社区,即 $c_v=c_w$,那么 $\delta(c_v,c_w)=1$;否则 $\delta(c_v,c_w)=0$。

通过模块度衡量社区划分的优劣,模块度值越高,社区划分效果越好。作为衡量社区划分优劣的重要指标,模块度得到广泛应用,例如 Fast Unfolding 算法[13]便是基于模块度的一种迭代算法。

为评价子图的社区特征,本文根据模块度的定义得到子图适应度函数:

$$Q(C)=\frac{\sum in}{2m}-\left(\frac{\sum tot}{2m}\right)^2 \tag{3}$$

其中,$\sum in$ 表示子图 C 内部边的个数,$\sum tot$ 表示与子图 C 内部点连接的边总数,包括子图内部的边以及子图外部的边。子图适应度函数可以度量子图连边的内聚程度。显然,如果 C 的社区性质越明显,则 Q 值越大,反之越小。

对于一个节点来说,当其连边大多在子图内部时,则更有可能属于该子图。当节点大部分连边都指向子图外部节点时,则不太可能属于该子图。因此,定义节点 n 的评价函数为:

$$f(n)=k_n^C/k_n^G \tag{4}$$

其中,k_n^C 为节点 n 在子图 C 中的度,k_n^G 为节点 n 在整个网络 G 中的度。

本文提出一种基于社区结构的子图划分算法。该算法的基本思路是在网络中随机选择感染节点作为子图的初始节点,以此出发逐步扩充子图结构,直到构造满足条件的局部子图为止,即根据局部子图对网络现有结构进行划分,具体算法如下:

算法 1　基于社区结构的子图划分算法

输入　在线社交网络关系拓扑图 $G=(V,E)$,其中,V 为社交网络中包含的节点集,E 为节点连边集合。初始选择节点数(初始子图数)k,每个子图最大节点数 M

输出　子图划分结构 $C_i,i=1,2,\cdots$

初始化　从感染节点集合中随机选择 k 个节点 V_i,令 $C_i=\{V_i\},i=1,2,\cdots,k$

1. repeat
2. for each C_i do
3. if size(C_i) < M then
4. N_{C_i} = neighbor(C_i), increase. C_i = false
5. repeat
6. $m=\underset{m\in N_{C_i}}{\arg\max}\, f(m)$
7. if $Q(C_i\cup\{m\})>Q(C_i)$ then
8. $C_i=C_i\cup m$, increase. C_i = true
9. end if
10. $N_{C_i}=N_{C_i}-\{m\}$
11. until size(N_{C_i}) = 0
12. end if
13. end for
14. if $C_i\cap C_j\neq\phi$ and $Q(C_i\cup C_j)>\max(Q(C_i),Q(C_j))$
15. then $C_i=C_i\cup C_j$, $C_j=\phi$
16. end if
17. until size(C_i) > M or increase. C_i = false
18. Return 子图划分结构 $C_i,i=1,2,\cdots$

基于社区结构的子图划分算法从随机选择的感染节点集合 $\{V_1,V_2,\cdots,V_k\}$ 出发,沿着边扩展子图。为保证所得子图的社区结构,在扩展过程中需对节点进行筛选。算法选择具有最高评价函数的节点(最有可能属于子图)(步骤 6),判断将该节点加入到当前子图中能否增加子图适应度函数(步骤 7 ~ 步骤 9),若是,则将该节点加入到子图中;否则放弃该节点。重复上述步骤直到子图达到指定规模 M 或子图适应度停止增长为止(步骤 17)。

由于子图初始节点选择的随机性,从不同感染节点出发构造的子图结构可能重叠,因此对于重叠的子图,算法通过判断合并后的适应度函数 Q 是否增加来选择是否需合并重叠子图(步骤 14 ~ 步骤 16)。因此,在选择初始节点数 k 时,考虑子图划分过程中可能出现的子图合并情况。为定位所有的恶意信息传播源点,k 应尽可能大于网络中的源点数。

本文为降低算法复杂度,通过设置合理的子图大小 M 的取值,当子图扩展到预先制定的期望大小 M 时算法停止,从而达到定位恶意信息源点的目的。

2.2　基于 Jordan 中心的恶意信息多源定位算法

本节提出基于 Jordan 中心的恶意信息源定位算法,利用该算法在每个局部子图中独立进行源点定位,p 为感染节点传染它的邻居节点概率。对于任意易感节点 $v\in V$,$p(v)$ 为其在下一时刻被感染的概率。令 $\alpha=\min\limits_{v\in V}p(v)$,$\beta=\max\limits_{v\in V}p(v)$。

假设 1　在 SI 模型中,对于每个节点 $v\in V$:

$$\beta\leqslant\frac{\alpha}{(1-\alpha)^4} \tag{5}$$

在式(5)中,假设 SI 模型中各个节点被感染的概率 $p(v)$ 不会剧烈变化。这是因为在真实网络中,不知道每个节点的实际感染概率。如果网络中存在部分比其他节点更容易感染的节点,则定位结果会产生偏差。

定理 1　对于感染节点集合 I,如果其关系拓扑为无限树且假设 1 成立,那么在 SI 传播模型下,感染节点集合 I 的 Jordan 中心即为恶意信息源点。

定理 1 的具体证明参考文献[14]。定理 1 表明,对于关系拓扑为无限树的网络,并且恶意信息的传播过程符合 SI 模型时,Jordan 中心将是一个定位恶意信息传播源的最优标度。因此,本文提出基于 Jordan 中心的恶意信息多源算法,具体如下:

算法 2　基于 Jordan 中心的恶意信息多源定位算法

输入　子图划分结构 $C_i,i=1,2,\cdots$,子图 C_i 中感染节点的集合 I_i

输出　恶意信息源点 $\{u_i^*\}$

1. for each I_i do
2. for $n\in I_i$ do
3. 计算节点 n 的离心率 $\bar{d}(s,I_i)$
4. end for

5. $u_i^* = \min_{u \in I'} \bar{d}(u, I_i)$

6. end for

7. Return 恶意信息传播源点$\{u_i^*\}$

3 仿真结果与分析

为评估本文算法的定位效率,本节通过仿真实验分别在生成的随机树网络和实际的 UCIonline 网络[15]上进行验证。通过 NetworkX 生成具有 2 000 个节点的随机树网络,每个节点的度在[3,6]内随机选择。实际网络选择具有明显社区结构的 UCIonline 网络数据集,该网络包含 1 893 个节点[16]。算法实现均由 Python 语言编写。

在仿真初始化时,从在线社交网络 $G=(V,E)$ 中随机选择 k 个节点作为恶意信息传播源点,根据信息传播模型和算法进行模拟及实现,对于每种网络和恶意信息传播过程分别进行 1 000 次仿真并对最终结果取平均值。本文通过命中次数来衡量定位准确率,如果某次仿真通过算法定位的源点集合与实际源点集合相同,则此次仿真称为命中。命中的仿真次数除以总仿真数即为算法的定位准确率。

对于多源定位算法,首先要解决的问题是识别出在线社交网络中恶意信息源点的实际个数。因此,需验证基于社区结构的子图划分算法的有效性,即该算法能否准确识别网络中的源点个数。本文分别选择 k 个源点($k=2,3,\cdots,17$)随机部署到在线社交网络中,并且对 1 000 次模拟中算法识别的源点个数取平均值,结果如图 2 所示。可以看出,该算法基本能够识别出源点个数,即以实际源点个数、算法识别出的源点个数分别为 X 轴、Y 轴所画的曲线形状与斜率为 1 的直线形状基本符合。同时可以看出,当实际源点较多时,算法识别出的源点个数要低于实际源点个数,这是因为源点部署的随机性,源点个数越多,多个源点越有可能落在一个社区的覆盖范围。当实际源点较少时,算法识别出的源点个数要大于实际的源点个数,这是因为源点个数越少,源点越有可能落入社区的边界区域。

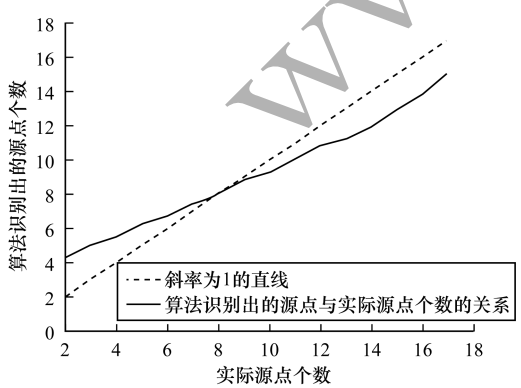

图 2 子图划分算法识别出的源点与实际源点个数的关系

为分析本文提出的多源定位算法的定位准确率,参考文献[14]中的思路,选择基于距离中心(Distance Center,DC)、紧密度中心(Tightness Center,TC)和介数中心(Betweenness Center,BC)的算法作为对比。具体而言,通过在每个社区中找到具有最大距离中心性、紧密度中心性和介数中心性的节点,启发式地找到多个 DC、TC 和 BC 作为定位的恶意信息源点集合。在仿真开始时,将源点个数分别设置为 2 和 3 并选择定位准确率作为评价标准,仿真结果如图 3、图 4 所示。可以看出,相较于其他对比算法,本文算法的定位准确率更高,较对比算法准确率能够提高 11%~28%,并且在 UCIonline 网络中,算法定位准确率更优,准确率能够提高 18%~30%,这是因为 UCIonline 网络的社区结构更明显。

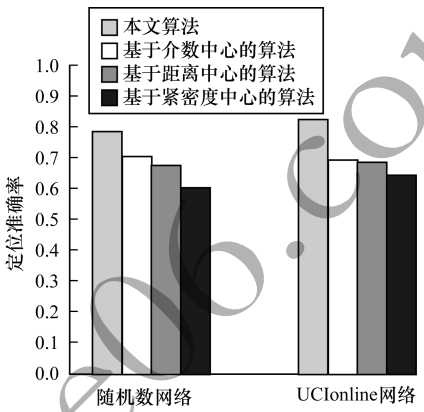

图 3 源点数为 2 时算法定位准确率对比

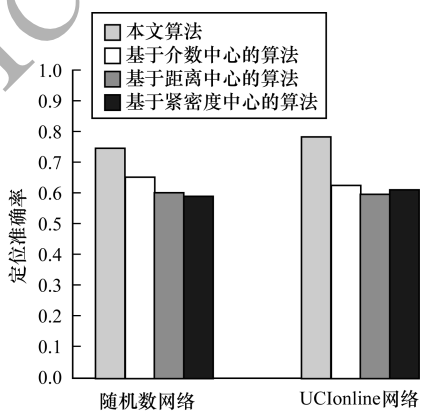

图 4 源点数为 3 时算法定位准确率对比

本文分析定位源点集合不准确时的情形,定义错误距离为算法识别出的恶意信息传播源点与实际源点之间相隔的最短距离,选择各错误距离值占所有错误距离的百分比作为分析对象,结果如图 5、图 6所示,其中恶意信息源点个数设置为 3。可以看出,由本文算法定位出的传播源点集合即使不是真实的传播源点,真实传播源点也总在由算法定位的恶意信息源点附近(大多数在 2 跳、3 跳内),从而验证本文算法的有效性。

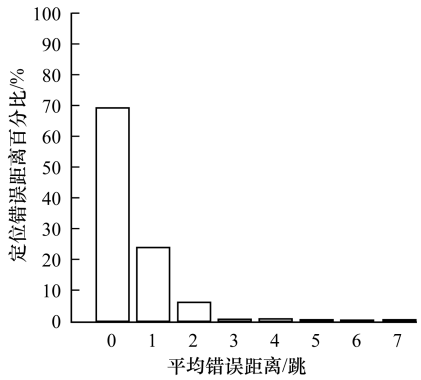

图 5　本文算法在随机数网络上的定位错误距离分布

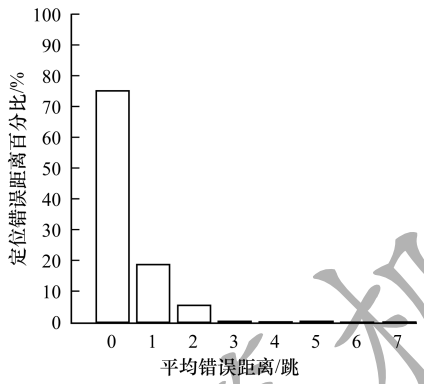

图 6　本文算法在 UCIonline 网络上的定位错误距离分布

4　结束语

通过社区结构可以区分多个源点的传播范围,因此可以利用网络社区结构区分信息源的传播范围,采用分而治之的策略将复杂的多源定位问题分解为多个单源定位问题。本文针对恶意信息源的覆盖范围重叠导致基于全网拓扑的算法复杂度高的问题,提出基于社区结构的子图划分算法,在此基础上利用基于 Jordan 中心的恶意信息源定位算法,在多个子图内分别解决恶意信息单源定位问题,并在生成网络和实际网络上进行大规模实验,验证了本文算法的有效性。下一步将基于多传播源点定位算法研究恶意信息传播的逆向干预技术,提高定位准确率。

参考文献

[1] 李栋,徐志明,李生,等. 在线社会网络中信息扩散[J]. 计算机学报,2014,37(1):189-206.

[2] 刁劼庭,傅秀芬. 微博谣言免疫策略的研究[J]. 计算机工程,2017,43(5):294-298.

[3] BIANCHI P,DEBBAH M,MAIDA M,et al. Performance of statistical tests for single source detection using random matrix theory[J]. IEEE Transactions on Information Theory,2010,57(4):2400-2419.

[4] WANG Zhaoxu, DONG Wenxiang, ZHANG Wenyi, et al. Rooting out rumor sources in online social networks:the value of diversity from multiple observations[J]. IEEE Journal of Selected Topics in Signal Processing,2015,9(4):663-677.

[5] ANTULOV-FANTULIN N,LANCIC A,STEFANCIC H,et al. Statistical inference framework for source detection of contagion processes on arbitrary network structures[C]// Proceedings of the 8th International Conference on self-adaptive and self-organizing systems. Washington D. C.,USA:IEEE Press,2013:78-83.

[6] DONG Wenxiang,ZHANG Wenyi,TAN C W. Rooting out the rumor culprit from suspects[C]//Proceedings of IEEE International Symposium on Information Theory. Washington D. C.,USA:IEEE Press,2013:2671-2675.

[7] 张聿博,张锡哲,徐超,等. 社交网络信息源快速定位方法[J]. 东北大学学报(自然科学版),2016,37(4):467-471.

[8] ZHANG Ende, WANG Guoren, GAO Kening, et al. Finding critical blocks of information diffusion in social networks[C]//Proceedings of the 14th International Conference on Web-Age Information Management. New York,USA:ACM Press,2013:521-532.

[9] ZANG Wenyu, ZHANG Peng, ZHOU Chuan, et al. Discovering multiple diffusion source nodes in social networks[J]. Procedia Computer Science, 2014, 29: 443-452.

[10] ANTULOV-FANTULIN N, LANCIC A, SMUC T, et al. Detectability limits of epidemic sources in networks[EB/OL]. [2018-05-13]. https://arxiv.org/abs/1406.2909v1.

[11] LUO Wuqiong, TAY W P, LENG Mei. Identifying infection sources and regions in large networks[J]. IEEE Transactions on Signal Processing, 2013, 61(11): 2850-2865.

[12] NEWMAN M E. Fast algorithm for detecting community structure in networkss[EB/OL]. [2018-05-13]. https://arxiv.org/abs/cond-mat/0309508.

[13] BLONDEL V D,GUILLAUME J L,LAMBIOTTE R,et al. Fast unfolding of communities in large networks[J]. Journal of Statistical Mechanics,2008(10):155-168.

[14] LUO Wuqiong, TAY W P, LENG Mei. On the universality of Jordan centers for estimating infection sources in tree networks[J]. IEEE Transactions on Information Theory,2017,63(7):4634-4657.

[15] OPSAHL T, PANZARASA P. Clustering in weighted networks[J]. Social Networks,2009,31(2):155-163.

[16] 张聿博,张锡哲,张斌. 面向社交网络信息源定位的观察点部署方法[J]. 软件学报, 2014, 25(12): 2837-2851.

编辑　陆燕菲