基于拓扑扩展的在线社交网络恶意信息源定位算法

袁得嵛[1,2] 高 见[1,2] 叶萌熙[1] 王小娟[3]

(中国人民公安大学信息技术与网络安全学院 北京 102623)[1]

(安全防范与风险评估公安部重点实验室 北京 102623)[2] (北京邮电大学电子工程学院 北京 100876)[3]

摘 要 随着在线社交网络的飞速发展,社交媒体成为网络用户参与的主要平台。恶意信息常常隐藏于在线社交网络的海量数据中,加之拓扑结构的局部性、恶意信息的伪装性,定位和溯源恶意信息面临着很大困难。一方面,仅仅通过人工标注的方式难以实现全局监控,即使借助语义分析、信息搜索等方式也只能在识别热点后获取当前网络中的信息"碎片";另外,信息在演变过程中的变异,使得一条传播链条会中断分裂为多条,不加以识别和区分会增加信息源头数目,大大增加溯源定位的算法复杂度。另一方面,恶意信息常采用伪装手法,如提供虚假的要素、制造热点吸引用户、水军炒作干扰视线等,使得信息拓扑和网络关系拓扑并不一致。原有的定位算法依赖于当前感染节点的分布和当前拓扑,感染状态从单一化向随机化的变化,使得统计推断框架更复杂,需要改进非观测节点的状态推断方法。在线社交网络的信息传播过程中,信息的传播关系常常附加在信息本身中,可以根据当前网络节点的状态挖掘隐藏信息。结合当前网络节点的状态,提出关系拓扑和信息拓扑的概念,并设计基于信息拓扑的候选源点扩展算法。在此基础上,文中提出基于Jordan中心的恶意信息溯源算法。在模型网络和实际网络上的实验表明,相对于对比算法,所提算法能够有效识别出恶意信息源。

关键词 在线社交网络,拓扑扩展,恶意信息源定位

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.05.020

Malicious Information Source Locating Algorithm Based on Topological Extension in Online Social Network

YUAN De-yu[1,2] GAO Jian[1,2] YE Meng-xi[1] WANG Xiao-juan[3]

(Institute of Information Technology and Cyber Security, People's Public Security University of China, Beijing 102623, China)[1]

(Key Laboratory of Safety Precautions and Risk Assessment, Ministry of Public Security, Beijing 102623, China)[2]

(School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)[3]

Abstract Social media on the Internet has become the main interactive platform for online users with the rapid development of online social network. Malicious information often hides in the massive data of online social networks. In addition, the limitation of topologies and the disguise of malicious information bring a lot of difficulties for locating and tracing malicious information. On the one hand, it is difficult to achieve global monitoring by means of manual labeling. Even by means of semantic analysis and information search, only the information "fragments" in the current network can be obtained after the hotspots are recognized. Coupled with the variation of information in the evolution process, a chain of propagation will be interrupted and split into multiple pieces. Without identifying and distinguishing, the number of information sources will be increased, and the algorithm complexity will be greatly increased. On the other hand, malicious information often uses camouflage techniques, such as providing false elements, manufacturing hotspots to attract users, and manipulating online "water army" to interfere with the public opinions, which makes the information topology and relation topology inconsistent. The original locating algorithm relies on the distribution of the current infected nodes and the current topology. The singularization of the infection state changes to randomization, making the statistical inference framework more complex. It is necessary to improve the state inference method of non-observed nodes. In the process of information dissemination of online social networks, the information propagation relationship is often attached to the information itself. Therefore, hidden information can be mined according to the state of the current network node. Based on the current state of network nodes, this paper proposed the concepts of relation topology and information topology

到稿日期:2018-04-12 返修日期:2018-07-27 本文受国家自然科学基金资助项目(61771072),北京市自然科学基金资助项目(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项目(2016JKF01317)资助。

袁得嵛(1986-),男,博士,讲师,主要研究方向为网络安全、复杂网络,E-mail:yuandeyu@gmail.com(通信作者);**高 见**(1982-),男,博士,讲师,主要研究方向为网络攻防、僵尸网络;**叶萌熙**(1997-),男,主要研究方向为网络安全;**王小娟**(1985-),女,博士,副教授,主要研究方向为复杂网络、智能算法。

and designed a candidate source expansion algorithm based on information topology. Based on this, this paper also presented a malicious information locating algorithm based on Jordan center. Experiments on the generated network and real network show that the algorithm can effectively identify malicious information sources compared with other algorithms.

Keywords Online social networks, Topological expansion, Malicious information source locating

近年来,互联网上的社交媒体成为了网络用户参与的重要平台,如天涯社区、新浪微博、人人网、微信、QQ 等,社交媒体上的用户形成了在线社交网络(Online Social Network,OSN)。随着 OSN 的飞速发展,OSN 不仅折射着现实社会,也在深刻影响着现实社会。恶意消息常隐藏于海量数据中,使得网状拓扑对信息高速扩散的作用成为了一把双刃剑。快速定位和溯源恶意信息是控制网络上恶意信息传播的基础。观察蔓延和扩散过程并推断出源节点对舆论引导、恶意事件控制的影响具有重要的现实意义。

从社交媒体上抽取话题信息、话题用户信息,可以得到当前时间段的信息流动快照。然而从 OSN 上产生的海量信息中定位恶意信息面临两方面的困难:1)恶意信息隐藏于海量数据中,仅仅通过人工标注的方式难以实现全局监控,即使借助语义分析、信息搜索等方式也只能在识别热点后获取当前网络中的信息"碎片";2)恶意信息常采用伪装手法(如提供虚假的要素、制造热点吸引用户、水军炒作干扰视线等)使得信息拓扑与网络关系拓扑并不一致,加上用户拓扑和信息具有多源性、异构性等特点,仅根据网络关系拓扑并不能探寻恶意信息的源点。因此,面对 OSN 上恶意信息的局部性、伪装性,需要对当前节点的可信状态进行推断,挖掘隐藏信息。

在线社交网络的信息传播过程中,信息的传播关系常常附加于信息本身,如微博信息中用于表述转发关系的"@"。因此,本文对信息拓扑和关系拓扑进行区分,根据当前网络节点的状态提出基于信息拓扑扩展的信息源点扩展算法。对于拓扑扩展后的恶意信息源点集合,最终提出基于 Jordan 中心的恶意信息溯源算法,为恶意信息的针对性监控提供技术支持。

1 相关工作

当前,对于 OSN 上恶意信息的溯源定位问题,学术界主要从语义分析和拓扑结构两方面展开研究。

1.1 基于语义分析的信息溯源

针对内容的研究主要结合语义分析、用户属性等进行溯源,通过提取信息源的特征来进行定位,沿用的是恶意信息识别的思路。例如,Thomson 等[1]分析了日本地震后的 Twitter 信息,按照信息的用户、位置、语言等特征来追踪消息的来源;Ghosh 等[2]依托群智技术,建立了一个基于主题的专家系统,该系统通过分析用户列表中的元数据等信息推断用户的专业领域,以便识别信息的源头;Yang 等[3]使用官方辟谣服务,运用人工标注的方式实现与主题不相关的微博,还通过选取特征或者提出新特征来训练模型,以对恶意消息进行自动识别,从而得到信息的传播源;Diakopoulos 等[4]从一个新闻工作者的角度提出了一种对 Twitter 事件的所有微博进行过滤和评估的方法,并提出了基于可信度计算的溯源方法,从而找出有用的或者有新闻价值的信息源;还可以借助智能算法标识已知传播源以进行特征学习,Sun 等[5]研究了事件谣言的特点,构建了实践分类器以从海量数据中识别谣言传播者,并且该分类器在新浪微博数据上取得了较好的效果;Canini 等[6]设计并进行了一次实验来计算在线社交网络中的不同因素直接或间接影响信息源可信度评估的不同程度,提出了一个新的方法来自动标识社会网络中的用户,且按照可信度排序定位;Guan 等[7]提出了一种符合新浪微博平台特性的算法,并通过建立数据库与编写程序实现了该新浪微博话题发起者识别应用。

从上述方法可以看出,借助内容对信息源进行识别的特征建模依赖于人工标注,而且恶意信息的识别和信息源的识别并不能进行简单的移植,OSN 上的信息流向在时序关系上给出了源头判定的方法,将内容识别转化为拓扑溯源是近年来的研究热点:Liu 等[8]假设社会网络中的谣言与可靠消息的传播模式不同,通过观察它们传播模式的区别,辨别消息真伪;Gonzalez-bailon 等[9]通过追踪 Twitter 上的数据来追踪抗议活动的进展,联合网络的结构演化和行动过程的信息交互行为,辨识 4 类用户类型来研究信息扩散过程并检测潜在的影响者;Chen 等[10]考虑了时延对信息传播的影响,通过扩展独立级联(Independent Cascade,IC)模型来匹配社交网络中影响传播的时延性质,并提出了两种启发式算法:一种算法基于动态编程过程计算 3 种模型下的实际影响,另一种则是将问题转化为原始的 IC 模型中的问题。然而,这里的拓扑关系的应用仅仅是对信息流动关系的建模,并没有从全局角度以网络的视角进行分析。

1.2 基于网络拓扑的信息溯源

针对网络拓扑的研究起源于复杂网络的不同传播模型,如 SI 模型[11]、SIS 模型[12]、SIR 模型[13]等。一种方法是根据传染源的数量来划分:如 Bianchi 等[14]利用最大似然检测的方式,针对单个信息源进行检测;Wang 等[15]通过多个观测点来对谣言传播源进行定位,针对单个信息源的谣言传播,从统计学角度基于 SI 模型提出了一个基于联合谣言中心性的统一推断框架,利用多个非独立的观测节点来提高溯源概率;Zang 等[16]利用部分发现的节点感染来估计整个网络中的感染节点情况,提出了一种反向传播算法来检查恢复节点或者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;Antulov-fantulin 等[17]基于动态传播过程,提出了单个传染来源的最大似然估计的统计推断框架,给出了 3 种似然估计函数来确定整个网络中每个潜在源节点的条件概率;Dong 等[18]通过统一的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;对于多个传播源,Zhang 等[19]将溯源问题简化为寻找网络中的关键模块的问题,利用近似划分的方式使得关键模块不断接近多个传播源的全局最优解;Antulov-fantulin 等[20]在任意给定的网络结构中利用蒙特卡洛估计方法来

检测不同的传染病源，针对 SIR 模型推导了检测成功的上限，该结果依赖于传播过程的特征；Luo 等[21]基于感染节点进行关联分析，并提出了整个网络中的感染源以及感染区域的估计方法，通过具有二次复杂性的算法来确定不同网络中真实的感染节点数目以及感染源。另一种方法是根据检测信息的局部特性展开研究，主要是对观测节点推断最大可能的每个节点的信息来源：影响力最大化的研究由 Richardson 等[22]和 Kempe[23]提出；考虑时序特征还原传播路径，Chen 等[24]在期限约束 τ 下探求社交网络时序要求严格的影响最大化，目标是选择出一个能够在 τ 时间内使影响最大化的预算子集进行激活；Goyal 等[25]利用真实的传播痕迹来得到更多的精确的影响模型；Zhuang 等[26]研究了动态社交网络上影响力最大化的最小时间问题，选择影响扩散的阈值 η 和预估阈值 k，使得在可能的最小时间内至少有 η 个节点被激活；Pinto 等[27]提出了一个适用于任意树的搜索策略，达到了正确定位的最大可能性，基于大规模网络上的源定位角度，该策略通过稀疏的观察者所测量的信息可以实现信息传播溯源；Borgeholthoefer 等[28]对动态的活动（如信息交流）和底层结构（如关注、粉丝等关系列表）加以区分，以复杂网络理论为基础，在宏观和微观两个维度上审视了时间演化和动力学过程，定量分析检测哪些节点在信息扩散过程中发挥了特权传播作用，即对信息传播有关键影响的节点，并考虑了 OSN 的局部特性；Luo 等[29]在 SI 模型的基础上，且在考虑感染节点局部观测的情况下，还原了传播路径，并对传播源进行定位；Shah 等[30]提出了将谣言中心作为检测源的估计量，在规则树状的指数传播模型 SI 上，通过观测部分节点的状态来检测谣言源；Zhu 等[31]扩展了 SIR 模型；Shah 等[32]基于 SIR 模型的变体，提出了一个新颖的变量谣言中心性用于估计网络中的源头节点，并通过实验对比表明谣言中心性在通常网络中的性能优于其他中心性；Zhu 等[33]在观测信息较稀疏的情况下，基于样本路径的估计量最小化观察感染节点的最大距离，利用 SIR 模型分析了信息传播源的定位问题。从上述方法可以看出，利用局部观测的方法对多个传播源进行定位的核心思想是对该节点状态的上一步感染过程的推断，由于恶意信息常采用伪装手法，如提供虚假的要素、制造热点吸引用户、水军炒作干扰视线等，仅仅依靠拓扑或者文本的语义进行推断容易产生误判。

2　传播模型与定位算法

本节将给出本文采用的系统模型、假设以及各种符号，并给出信息拓扑、关系拓扑以及 Jordan 中心的定义。

2.1　信息传播模型

在某一未知时刻，网络中的源点发布恶意消息 m，网络中的其他节点收到消息 m 并向其邻居节点转发该消息。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。本文目标是通过在特定时间点观察到的感染节点集来推断恶意信息源。简便起见，本文将恶意信息传播的载体在线社交网络描述为无向图。

在线社交网络上的信息传播过程中，用户常常将信息的来源附加到信息内部，例如，在微博信息中，“@”符号表示该信息在转发过程中经过的用户，通过观察这些附加信息可以得到信息在传播过程中的拓扑结构，这些路径能够描述信息的真实传播过程的传播路径，本节首先给出关系拓扑和信息拓扑的概念。

定义 1（关系拓扑）　在线社交网络中由关注关系构成的拓扑结构即为关系拓扑，用 $G=(\mathbb{V},\mathbb{E})$ 表示，其中 $\mathbb{V}$ 为节点集，$\mathbb{E}$ 为边集。由边连接的两个节点称为邻居（即存在关注关系）。

定义 2（信息拓扑）　在线社交网络中由可观测到的转发关系构成的拓扑结构，用 $G'=(\mathbb{V}',\mathbb{E}')$ 表示，其中 $\mathbb{V}'$ 为节点集，$\mathbb{E}'$ 为边集。由边连接的两个节点称为邻居（即存在转发关系，例如在微博信息中用“@”符号表示这种关系）。

现有的信息传播模型可以粗略地分为两类：流行病传染模型（如 SI，SIR 和 SIS 模型）和影响力扩散模型（如 IC，LT 模型）。其中 SI 模型是最基本的传播模型，网络中的每个节点处于易感状态（S）或者感染状态（I）。一旦某节点受到了感染，它将永远保持感染状态，每个感染的节点在相同的时隙内会以相同的概率感染处于易感状态的邻居节点。SIR 模型是一个随机过程模型。起初，除初始感染节点外，其他节点均处于易感状态，在每个独立的过程中，感染节点以概率 p 传染它的邻居节点，并且这些感染节点以概率 q 从感染状态恢复，所有恢复的节点无法再被感染。

本文考虑 SIR 模型作为离散时间恶意信息传播模型。每个节点在任何时间可以处于以下几种状态：S,I,R。在每个传播模拟的开始，感染概率 p 指一个感染节点在一个时间段内传染邻居节点的概率。概率 q 指一个感染节点在一个时间段内恢复的概率。

2.2　Jordan 中心

本节给出 Jordan 中心的定义。

定义 3（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（即它们之间的距离）。对于 G 中的任意节点集合 $\mathbb{A}$，定义节点 s 的离心率为 $\bar{d}(s,\mathbb{A})$，即 s 与 $\mathbb{A}$ 中任意节点之间的最大距离，可得：

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

节点集合 $\mathbb{A}$ 的 Jordan 中心被定义为 G 中具有最小离心率的节点。

3　基于拓扑扩展的恶意信息溯源定位算法

在实际网络中，我们通常只能观测到部分传播结果，在符合 SIR 模型的传播模式下，部分节点会从感染节点转变为恢复状态，这无疑增加了信息溯源的难度，从而使得我们难以确定信息的真实来源。本节为了解决观测不完整的问题，提出一种根据被感染节点的信息拓扑来扩展信息源点的方法，最后根据 Jordan 中心来解决恶意信息溯源的问题。

3.1　基于信息拓扑的恶意信息源扩展算法

在实际生活中，只通过观察几个被感染节点来定位恶意信息是非常困难的。一方面，恶意信息传播源发布的消息会采用伪装手段，加上在演变过程中消息的变异，使得一条传播链条会中断分裂为多条，对其识别和区分会增加信息源头数目，大大增加溯源定位算法的复杂度。另一方面，原有的传播

源定位算法依赖于当前感染节点的分布和当前拓扑，且感染状态的单一化向随机化的变化使得统计推断框架变得复杂，需要改进非观测节点的状态推断方法。如图 1 所示，演变过程中的变异可能导致信息拓扑与关系拓扑不一致。

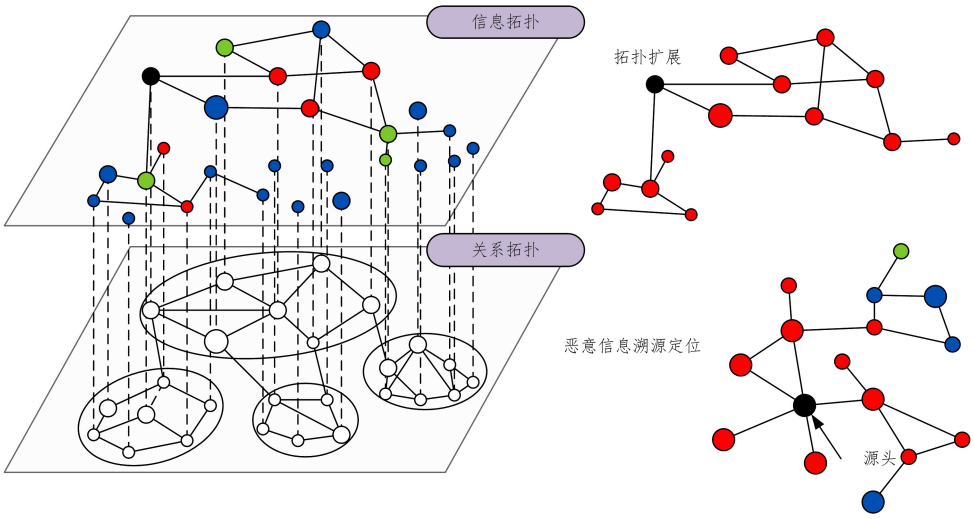


图 1 关系拓扑与信息拓扑的示意图

Fig. 1 Schematics of relation topology and information topology

如 2.1 节所述，本文将网络拓扑分为信息拓扑和关系拓扑，其中信息拓扑即为通过观测恶意信息的转发关系刻画的恶意信息在网络中的传播拓扑，关系拓扑即为网络中节点的关注关系。考虑到节点从感染状态恢复的情况，为了补充这些丢失的信息并简化恶意信息源节点的定位问题，本节提出了一个基于信息拓扑的恶意信息源扩展算法，以找出包括恢复节点与被感染节点的扩展感染网络，算法如算法 1 所示。

算法 1 基于信息拓扑的信息源点扩展算法

输入：在线社交网络关系拓扑图 $G=(\mathbb{V},\mathbb{E})$，其中 $\mathbb{V}$ 为社交网络包含的节点集，$\mathbb{E}$ 为节点连边的集合；在线社交网络信息拓扑图 $G'=(\mathbb{V}',\mathbb{E}')$，其中 $\mathbb{V}'$ 为当前观测到的感染节点集合，$\mathbb{E}'$ 为信息拓扑中有提及关系的节点集合

输出：拓扑扩展的感染节点集合 $\mathbb{I}^*\in\mathbb{V}$，其中 $\mathbb{I}^*$ 包含 $\mathbb{V}'$ 中的感染节点集合、SIR 模型中的恢复节点集、未观测到的感染节点集、在关系拓扑中与感染节点连接紧密从而有可能已被感染的节点集

Initialize：初始化节点集合 $\mathbb{I}^*=\mathbb{V}'$，$\mathbb{I}'=\mathbb{V}'$，算法执行步数 N_{step}。为每一个节点分配唯一的标签 C_n，$\forall n\in\mathbb{V}$，以及唯一的评分函数 S_n，$\forall n\in\mathbb{V}$：

$$C_n,S_n=\begin{cases}1, & n\in\mathbb{I}\\ 0, & else\end{cases} \tag{2}$$

1. for $n\in\mathbb{V}'$ do
2. for $i\in n_{neighors}(\mathbb{V}')$ do
3. $\mathbb{I}^*=\mathbb{I}^*\cup i$
4. end for
5. end for
6. for iter=1 to N_{step} do
7. for $n\in\mathbb{I}'$ do
8. for $i\in n_{neighors}(\mathbb{V})$ do
9. if $C_i=0$
10. $S_i=S_i+S_n$
11. end if
12. $\mathbb{I}'=\mathbb{I}'\cup i$
13. end for
14. end for
15. end for
16. for $n\in\mathbb{V}$ do
17. if $S_n>$BaseScore
18. $\mathbb{I}^*=\mathbb{I}^*\cup n$
19. end if
20. end for
21. Return 扩展感染节点集合 $\mathbb{I}^*$

其中，步骤 1－步骤 5 基于信息拓扑的连边关系，将与感染节点有连边关系的未观测到的感染节点或已恢复节点（例如，感染节点提及到转发自某个节点）加入到候选源点集合中。步骤 6－步骤 20 根据关系拓扑关系，通过对 BaseScore 的计算将关系拓扑中与感染节点连接紧密（可能已被感染）的节点增加到候选源点集合中。通过执行以上算法，建立新的网络来进行定位分析，我们将这个网络作为拓扑扩展之后的扩展感染网络。

3.2 基于 Jordan 中心的恶意信息源定位算法

如 2.1 节所述，p 为感染节点传染其邻居节点的概率。对于任意易感节点 $v\in\mathbb{V}$，$p(v)$ 为其在下一时刻被感染的概率。令 $\alpha=\min\limits_{v\in\mathbb{V}}p(v)$，$\beta=\max\limits_{v\in\mathbb{V}}p(v)$。

假设 1 在 SIR 模型中，对于每个 $v\in\mathbb{V}$，有：

$$0\leqslant p_i(v)\leqslant\sqrt{\frac{\alpha}{\beta}} \tag{3}$$

受文献[34]的启发，本文提出以下定理：

定理 1 对于扩展感染节点集合 $\mathbb{I}^*$，如果其关系拓扑为无限树且假设 1 成立，则在 SIR 传播模型下，节点集合 $\mathbb{I}^*$ 的 Jordan 中心即为恶意信息源。

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 SIR 模型的情况下，Jordan 中心将是一个定位恶意信息传播源的最优方式。

算法 2 基于 Jordan 中心的恶意信息源定位算法

输入：扩展感染节点集合 $\mathbb{I}^*$

输出：恶意信息源点 u^*

1. for $n\in\mathbb{I}^*$ do

2. 根据式(1)计算节点 n 的离心率 $\bar{d}(s,\mathbb{I}^*)$

3. end for

4. $u^*=\min_{u\in\mathbf{I}}\bar{d}(u,\mathbb{I}^*)$

5. Return 恶意信息传播源点 u^*

4　仿真分析

本节通过仿真实验来验证算法的有效性。为了评估本文所提算法的定位效率，在生成网络和实际网络上进行实验，以验证算法的性能。其中随机树网络(Random trees)为生成网络，其节点度随机选择于区间[3,5]。Political-blogs 网络[35]为包含 1 222 个节点的实际网络。

本文使用大范围的随机生成参数来评估所提算法的鲁棒性。对于任意节点 $v\in\mathcal{V}$，在[0,1]范围内随机选择感染概率 $p(v)$、恢复概率 $q(v)$以及信息拓扑标记概率 r(即每个被感染节点以概率 r 记住信息传播来自的节点)。对于每一种网络和恶意信息传播过程，进行 1000 次模拟实验。在每次实验的开始，随机挑选一个节点作为恶意信息的传播源点并使用上述选定的传播模型和参数。当被感染节点数大于 80 时，结束传播过程，并分析本文所提算法与对比算法的性能。

本文首先对比未经过拓扑扩展的恶意信息传播源点估计算法和本文所提基于拓扑扩展的源点估计算法，选择平均错误距离(即在结构拓扑上，算法识别出的恶意信息传播源点和实际源点之间相隔的跳数)作为评价标准，结果如图 2 所示。可以看出，与未经拓扑扩展的候选源定位算法相比，利用基于信息拓扑的源点扩展算法对恶意信息源点的识别率有显著提高。

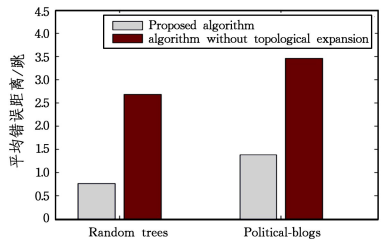


图 2　是否采用拓扑扩展的算法平均错误距离的对比

Fig. 2　Comparison of average error distance of algorithms using topology extension or not

接着，本文选择距离中心(Distance Center，DC)，紧密度中心(Closeness Center，CC)和介数中心(Betweenness Center，BC)作为对比算法与本文所提基于 Jordan 中心的算法进行比较，并选择平均错误距离作为评价标准，结果如图 3 所示。

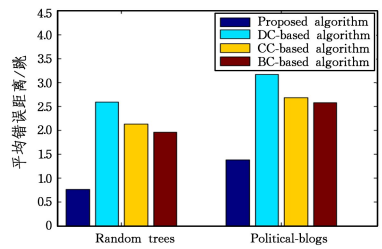
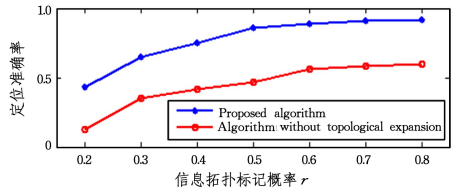


图 3　基于不同测量标度的算法的平均错误距离的对比

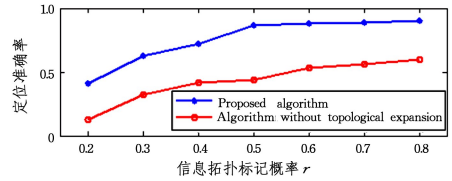
Fig. 3　Comparison of average error distances of algorithms based on different measurement scales

可以看出，与距离中心、紧密度中心和介数中心相比，本文所提算法的识别率始终优于其他测量标度；此外，本文所提算法定位出的传播源点即使不是真实的传播源点，其与真实传播源点的距离也很近(平均在 1.5 跳以内)，这说明了算法的有效性。

图 4 说明了信息拓扑标记概率 r 与定位准确率的关系，将识别准确率作为评价标准，可以看出，随着 r 的增加，定位准确率也随之增加，说明信息拓扑越详细，基于拓扑扩展的恶意信息溯源算法的定位准确率越高。



(a) Random trees



(b) Polltical-blogs

图 4　信息拓扑标记概率与定位准确率的关系

Fig. 4　Relationship between information topology marker probability and location accuracy

结束语　为了应对 OSN 上恶意信息的局部性、伪装性，本文对当前节点的可信状态进行推断，挖掘隐藏信息，提出了基于信息拓扑的恶意信息源点扩展算法。在此基础上，提出了基于 Jordan 中心的恶意信息源定位算法。在模型网络和实际网络上进行的实验表明，相比于对比算法，本文所提算法能够有效定位出恶意信息源点。

参 考 文 献

[1] THOMSON R, ITO N, SUDA H, et al. Trusting tweets: The Fukushima disaster and information source credibility on Twitter[C]// Proceedings of the 9th International ISCRAM Conference. 2012: 1-10.

[2] GHOSH S, SHARMA N, BENEVENUTO F, et al. Cognos: crowdsourcing search for topic experts in microblogs[C]// Proceedings of the 35th International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM, 2012: 575-590.

[3] YANG F, LIU Y, YU X, et al. Automatic detection of rumor on sinaweibo[C]// Proceedings of the ACM SIGKDD Workshop on Mining Data Semantics. ACM, 2012.

[4] DIAKOPOULOS N, DE CHOUDHURY M, NAAMAN M. Finding and assessing social media information sources in the context of journalism[C]// Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012: 2451-2460.

[5] SUN S, LIU H, HE J, et al. Detecting Event Rumors on Sina Weibo Automatically [M]// Web Technologies and Applica-

tions. Berlin:Springer,2013:120-131.

[6] CANINI K R,SUH B,PIROLLI P L. Finding Credible Information Sources In Social Networks Based On Content And Social Structure[C]// 2011 IEEE Third International Conference on and 2011 Privacy,Security,Risk and Trust (PASSAT). 2011:1-8.

[7] GUAN W,GAO H,YANG M,et al. Analyzing user behavior of the micro-blogging website Sina Weibo during hot social events [J]. Physica A Statistical Mechanics & Its Applications,2014,395(4):340-351.

[8] LIU Y,XU S,TOURASSI G. Detecting Rumors Through Modeling Information Propagation Networks in a Social Media Environment[M]// Social Computing, Behavioral-Cultural Modeling, and Prediction. Springer International Publishing, 2015: 121-130.

[9] GONZALEZ-BAILON S,BORGE-HOLTHOEFER J,MORENO Y. Broadcasters and Hidden Influentials in Online Protest Diffusion[J]. American Behavioral Scientist,2012,57(7):943-965.

[10] CHEN W,LU W,ZHANG N. Time-Critical Influence Maximization in Social Networks with Time-Delayed Diffusion Process [C]// Twenty-Sixth AAAI Conference on Artificial Intelligence. 2012.

[11] ZHOU T,LIU J G,BAI W J,et al. Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity [J]. Physical Review E,2006,74(5):056109.

[12] LEE H K,SHIM P S,NOH J D. Epidemic threshold of the susceptible-infected-susceptible model on complex networks. [J]. Physical Review E,2013,87(6):88-90.

[13] YUAN-YUAN M A,ZHUANG X T. Susceptible-infected-removed (SIR) model of crisis spreading in the correlated network of listed companies and their main stock-holders[J]. Journal of Management Sciences in China,2013,7(16):80-94.

[14] BIANCHI P,DEBBAH M,MAIDA M,et al. 1Performance of Statistical Tests for Single Source Detection using Random Matrix Theory[J]. IEEE Transactions on Information Theory, 2010,57(4):2400-2419.

[15] WANG Z,DONG W,ZHANG W,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.

[16] ZANG W,ZHANG P,ZHOU C,et al. Discovering Multiple Diffusion Source Nodes in Social Networks[J]. Procedia Computer Science,2014,29:443-452.

[17] 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 2014 IEEE Eighth International Conference on Self-Adaptive and Self-Organizing Systems Workshops. 2013:78-83.

[18] DONG W X,ZHANG W,TAN C W. Rooting out the Rumor Culprit from Suspects[C]// 2013 IEEE International Symposium on Information Theory Proceedings (ISIT). IEEE,2015, 18(3):731-747.

[19] ZHANG E,WANG G,GAO K,et al. Finding critical blocks of information diffusion in social networks[J]. World Wide Web-internet & Web Information Systems,2013:521-532.

[20] ANTULOV-FANTULIN N,LANCIC A,SMUC T,et al. Detectability limits of epidemic sources in networks[J]. Physical Review Letter,2014,114(10):589-596.

[21] LUO W,TAY W P,LENG M. Identifying Infection Sources and Regions in Large Networks[J]. IEEE Transactions on Signal Processing ,2013,61(11):2850-2865.

[22] RICHARDSON M,DOMINGOS P. Mining Knowledge-Sharing Sites for Viral Marketing[C]// Eighth Intl. Conf. on Knowledge Discovery and Data Mining. 2002:61-70.

[23] KEMPE D. Maximizing the Spread of Influence Through a Social Network[J]. Kdd Proceedings of the Ninth AcmSigkdd International Conference on Knowledge Discovery & Data,2003: 137-146.

[24] CHEN W,WANG Y,YANG S. Efficient influence maximization in social networks[C]// Proc. of Acm Kdd. 2009:199-208.

[25] GOYAL A,BONCHI F,LAKSHMANAN L V S. A Data-Based Approach to Social Influence Maximization[J]. Proceedings of the VLDB Endowment,2011,1(5):73-84.

[26] ZHUANG H,SUN Y,TANG J,et al. Influence Maximization in Dynamic Social Networks[C]// 2013 IEEE 13th International Conference on Data Mining (ICDM). IEEE,2013:1313-1318.

[27] PINTO P C,THIRAN P,VETTERLI M. Locating the Source of Diffusion in Large-Scale Networks[J]. Physical Review Letters,2012,109(6):1-5.

[28] BORGE-HOLTHOEFER J,RIVERO A,MORENO Y. Locating privileged information spreaders during political protests on an Online Social Network[J]. Holthoefer,2011,85(6):4454-4463.

[29] LUO W,MEMBER S,TAY W P,et al. How to Identify an Infection Source with Limited Observations[J]. IEEE Journal of Selected Topics in Signal Processing,2013,8(4):586-597.

[30] SHAH D,ZAMAN T. Rumor centrality:a universal source detector[C]// ACM SIGMETRICS Performance Evaluation Review. ACM,2012,40(1):199-210.

[31] ZHU K,YING L. Information source detection in the SIR model:A sample path based approach[C]// Information Theory and Applications Workshop (ITA). 2013:1-9.

[32] SHAH D,ZAMAN T. Detecting sources of computer viruses in networks:theory and experiment[J]. Acm Sigmetrics performance Evaluation Review,2010,38(1):203-214.

[33] ZHU K,YING L. A robust information source estimator with sparse observations[C]// INFOCOM. IEEE,2014:2211-2219.

[34] LUO W,TAY W P,LENG M. On the Universality of Jordan Centers for Estimating Infection Sources in Tree Networks[J]. IEEE Transactions on Information Theory,2014,PP(99):1-1.

[35] ADAMIC L,GLANCE N. The political blogosphere and the 2004 US election[C]// International Workshop on Link Discovery. ACM Press,2005:36-43.