基于网络模体的移动社会网络信息可控传播方法

张欣欣 许 力* 徐振宇
(福建师范大学计算机与网络空间安全学院 福州 350007)
(福建省网络安全与密码技术重点实验室 福州 350007)

摘 要：移动社会网络中的信息传播具有突发性、多元性、偏差性等特点，使得相关话题和事件能够在短时间内形成强大的网络和社会舆论场，这有可能被恶意用户利用来散布谣言，给网络环境带来了恶劣的影响。针对这一问题，该文提出一种基于网络模体的信息可控传播方法。首先，提出多实体的竞争性独立级联模型(MCIC)，该模型在信息竞争扩散理论的基础上，首次结合社会网络层用户的社会属性，来感知恶意信息并控制信息传播。其次，该文定义了控制信息流模体(CIFM)，并选择出具有可控传播功能的关键网络模体，设计其在通信层的高效可控传播算法。最后，通过理论推导证明了该文方法具有收敛性。仿真实验表明，与其他方法相比，所提方法不仅在信息传播中最大感染时间和平均感染时间上更有优势，而且在控制信息传播方面的效果也是最好的。

关键词：移动社会网络；信息可控传播；网络模体
中图分类号：TN926; G206 **文献标识码**：A **文章编号**：1009-5896(2023)02-0635-09
DOI: 10.11999/JEIT211429

Information Propagation Control Method in Mobile Social Networks Based on Network Motifs

ZHANG Xinxin XU Li XU Zhenyu
(*College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350007, *China*)
(*Fujian Provincial Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou* 350007, *China*)

Abstract: The abruptness, diversity, and deviation of public opinion information in mobile social networks may encourage malicious users to spread rumors and has a bad impact on the network environment. To solve this problem, a controllable information propagation method based on network motif is proposed. Firstly, a Multi-entity Competitive Independent Cascade (MCIC)model in the social network layer is established. Secondly, this paper defines the Control Information Flow Motif (CIFM), determine the key network motifs and designs its efficient and controllable propagation algorithm in the communication layer. Finally, Theoretical derivation proves that this method has convergence, and the simulation results show that the proposed method not only has more advantages in terms of time efficiency, but also has the best effect in controlling information propagation.

Key words: Mobile social network; Controllable propagation of information; Network motif

1 引言

在线社会网络，也就是通常所说的社交网络，是一类基于Web的社会网络系统，例如脸书、推特和微博等。移动社会网络(Mobile Social Networks, MSNs)则是一个具有相似的某种特性的个人通过移动设备互联而成的网络[1,2]。与社交网络的虚拟性相比，移动社会网络更加强调的是人和移动设备的存在，以及网络行为的无中心和自组织，它是由人类携带移动设备进行数据传输和交互所构成的网络。移动社会网络使人们的观点交流和信息的传播变得极其便捷，病毒营销[3]、舆情控制[4]、推荐系统[5]、公安侦查[6]、社团检测[7]等各种应用和问题也应运而生。移动社会网络包含有通信网络层、社会网络层与数据层，每层都有各自的特点，并且对信息传播都有不同方面的影响。其中，由通信网络和社会接触网络组成的双层耦合网络在结构上存在相互依存关系的同时，还在信息传递过程中起到相互促进的作用。

收稿日期：2021-12-06；改回日期：2022-06-01；网络出版：2022-06-07
*通信作者： 许力 xuli@fjnu.edu.cn
基金项目：国家自然科学基金(U1905211, 61771140, 62171132)，福建省科技项目(2021L3032)，企事业合作项目(DH-1565)
Foundation Items: The National Natural Science Foundation of China (U1905211, 61771140, 62171132), Fujian Science and Technology Project (2021L3032), The Cooperation Projects of Enterprises and Institutions (DH-1565)

社会网络舆情是用户对社会热点问题产生不同看法的网络舆论，它是用户通过互联网对社会和生活中的热点、焦点问题所持有的具有影响力、倾向性的观点和意见的集合[8]。若在短时间内不能对恶意信息的传播进行有效控制，会造成严重的社会危害，威胁社会和谐与国家稳定。例如，2019年出现的新冠肺炎疫情发展至今，已经形成了全球性“大流行”(Pandemic)，与之相伴的则是信息瘟疫(Infodemic)的到来，大量谣言在社交媒体平台上衍生并广泛传播[9]。在移动社会网络中，如何积极传播真实可靠的信息和及时遏制谣言信息，如何根据移动社会网络中社会网络层和物理通信层的关系，结合用户社会属性以及信息传播规律，设计高效可控的信息传播方案是一个值得研究的课题。

信息传播控制是设计高效的传播模型，以较小的代价在合适的时机选择最佳的控制点，对大部分甚至整个网络的信息传播进行控制。最初，独立级联模型(Independent Cascade, IC)是由Kempe等人[10]在相互作用粒子系统的模型基础上提出来的，它把节点$v \in V$分为活跃的和不活跃的两个可能的状态，当节点v接收网络传播的新信息、新思想、新产品时，可以看到节点v的活跃状态，而非活动状态表示节点v没有接收新信息、新思想、新产品。Peng等人[11]提出了基于大数据影响建模的社会网络免疫方法，该方法为防止恶意软件或恶意消息在社交网络中的传播提供了一种有效的解决方案。Doostmohammadian等人[12]用图论控制的思想设计了移动社会网络中通过控制措施，合理分配治疗资源给某一个目标群体，实现移动社会网络的资源分配平衡。斯坦福大学Jure Leskovec[13]所在Chan Zuckerberg Biohub团队对移动网络模型进行了深入研究，他们认为在COVID-19爆发之后极大地改变了人类的流动模式，需要建立流行病学模型来捕捉流动性变化对病毒传播的影响，于是该团队建立了疫情状态下的移动模型，能够精准地预测移动网络中的“超级传播者”和在不同移动性条件下感染的风险大小，这一成果为移动社会网络在流行病模型下的信息传播提供了可借鉴的实例。针对移动社会网络信息在不同网络层传播的问题，Wang等人[14]提出了一种新的基于两层多重网络的传染病模型，探讨了正预防信息和负预防信息对传染病传播的影响。

上述研究并未考虑社会网络层用户间的社会属性和物理通信层多条信息之间的竞争性等具体特征对信息传播控制的影响，不能够很好地适应移动社会网络信息传播控制的场景，并且上述研究均从个体角度出发，对于移动社会网络中的群体性特点没有很好的研究。针对以上问题，本文主要的研究工作如下。

(1)本文在移动社会网络双层结构中社会网络层，提出了多实体的竞争性独立级联模型(Multi-entity Competitive Independent Cascade, MCIC)，该模型首次将信息竞争扩散理论与社会网络层用户的社会属性结合，实现信息的可控传播。

(2)本文在移动社会网络双层结构中的物理通信层，从群体角度出发定义了控制信息流模体(Control Information Flow Motif, CIFM)，并选择出具有可控传播功能的关键网络模体，设计其在通信层的高效可控传播算法。

(3)通过理论推导证明了本方法具有收敛性，仿真实验表明本文方法不仅在信息传播中最大感染时间和平均感染时间上更有优势，而且在控制信息传播方面的效果也是最好的。恶意信息感染时间有限和传播恶意信息节点的数量呈下降趋势都意味着恶意信息最终将会从网络中消失，最终能够实现信息可控传播。

2 系统模型

2.1 移动社会网络双层结构

哥伦比亚大学团队于2015年提出并分析了传统和未来移动社会网络系统的总体架构设计，这些体系结构主要采用物理层-用户层-终端层交互方式介绍并分析了一种新的MSNs体系结构[15]。移动社会网络包括通信网络层、社会网络层、数据层，每层都有各自的特点，对信息传播都有不同方面的影响。如图1所示，本文主要研究的是社会网络层与物理通信层之间的关系，社会网络层主要由用户的社会属性、社会关系、社会行为等产生数据形成交互。物理通信层主要功能是为数据端设备提供传送数据的通路，既要保证数据能从其上正确通过，也要提供足够带宽减少信道上拥塞。所以将社会网络层与

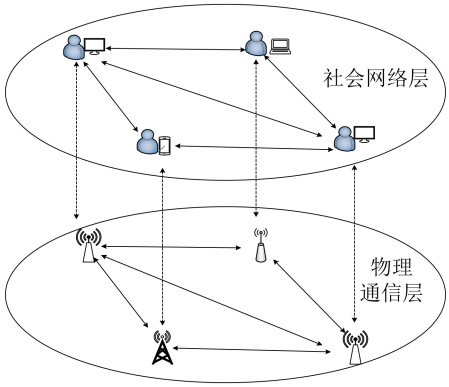

图 1 移动社会网络中的社会网络层与物理通信层关系图

物理通信层结合，考虑层与层之间的互相影响，利用通信模体的动态演化设计高效可靠的信息传播模型对信息可控传播是具有挑战和有实际应用价值的。

2.2 社会网络层中信息传播模型

通常把移动社会网络建模成一个有向图$G=(V,E,W)$，其中，V代表节点集，E代表边集，W表示边权重。一个节点代表移动社会网络中的一个用户，而从u到v的一条边代表用户u和v之间的关系。这种关系是定向的，我们主要关注的是影响关系，也就是说，一个用户u是否容易影响另一个用户v，这种影响关系通常是定向的和非对称的。独立级联模型首先是由Kempe等人[10]在相互作用粒子系统的模型基础上提出来的，该模型的主要特点是沿图中每条边的扩散事件是相互独立的。并可能影响其非活跃邻居变为活跃节点。在此基本模型中，单个影响过程从一组活跃节点开始，在每个时间戳中，只有新的活跃节点才有机会以概率方式影响其非活跃邻居。具体传播方式如图2所示。

第t=0：a节点被激活。

第t=1：a节点以0.5的概率尝试激活b，以0.2的概率尝试激活c。假设b节点在这一时间步内成功被激活。

第t=2：b节点以0.3的概率尝试激活c，并以0.5的概率尝试激活d。假设c节点和d节点在这一时间步内成功被激活。

第t=3：c节点以0.2的概率尝试激活e，d节点以0.2的概率尝试激活e。假设这一时间步内的尝试都失败了，没有新的节点被激活，传播停止。

在信息情报领域，学者在竞争扩散理论框架下，利用贪婪算法等识别限制恶意信息的最优策略，通过刺激“正确”信息的扩散来限制“错误”信息的传播[16]。受到这个思想的启发，本文根据用户的社会属性和信息传播的特点，提出多实体的竞争性独立级联模型(Multi-entity Competitive Independent Cascade, MCIC)，在信息扩散的过程中能够捕获恶意信息的同时传播与恶意信息有竞争关系的正确信息。MCIC模型中节点状态分为以下4类：

(1)N_0表示节点处于非活跃(inactive)状态，并且当前没有任何信息。

(2)N_{am}表示节点处于活跃(active)状态，并且当前处于恶意信息(misinformation)。

(3)N_{ic}表示节点处于非活跃(inactive)状态，并且当前处于正确信息(correct information)。

(4)N_c表示节点处于活跃(active)状态，并且信息正确(correct information)。

PIC网络模型的初始状态有3种分别为N_0，N_{am}和N_{ic}。N_{am}向网络中邻居节点传递恶意信息，N_0节点收到恶意信息会转变为N_{am}节点并向邻居节点传递信息，此时传递恶意信息的概率是P_m。当N_{ic}节点感知到恶意信息时会被激活变为N_c节点，并开始向邻居节点传播与恶意信息竞争的正确信息，邻居节点收到正确信息从N_0状态转换为N_c状态。当用户获得正确信息就不会再接收恶意信息，正确信息传播概率是P。

节点4种状态的定义展示出节点之间相互转化的关系如图3所示，根据本文设计的MCIC信息扩散模型，处于N_0状态的节点是非活跃状态，它能够被任何一个活跃的邻居所影响。而处于N_{am}状态的节点是活跃的，它可以向非活跃的邻居传递恶意信息。处于N_{ic}状态的节点虽然是非活跃状态，但是它能够明辨是非，从不相信恶意信息，当它感知到恶意信息的时候，能够被激活并开始与恶意信息对抗，向邻居传递正确信息。所以N_{ic}状态下的节点对于整个网络其他状态下的节点有绝对的影响作用，在恶意信息出现的时候承担着与之对抗，并传递信息使得网络节点最终都变成接受正确信息的活跃节点N_c。本文将N_c节点定义为控制信息节点，它的功能是在出现任何恶意信息时被激活并传递正确信息，控制社会网络的信息传播。

2.3 网络模体

在移动社会网络中，人的行为不仅具有个体性，也具有群体性。模体(motif)最早是在生物学的蛋白质网络里表示最基本的功能模块，引入到复杂网络中便可以表示为网络的基本子结构，称为网络模体(Network Motif, NM)。网络模体的结构和类

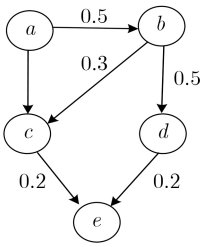

图 2 独立级联模型

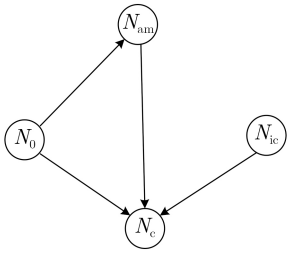

图 3 节点状态转化图

型从微观的角度反映了其所在网络的特点。在社会网络中，对于一个3个用户形成的群体，若3个人相互之间的关系都比较紧密，他们的结构稳定性可能会更高，不易被恶意行为所破坏。本文用网络模体作为社会网络中最基本的构成单元，从微观角度刻画移动社会网络中用户相互作用的特殊模式，有利于描述人行为的群体性，从而来研究群体内的互相作用对于整个社会网络的影响。

在社会网络中，当出现恶意信息时，通过选定的模体来输入正确信息来遏制恶意信息的传播，关键模体的功能是接受并传递正确的信息，并通过自身的影响力可能使恶意信息的节点改变其信念，最终使网络避免接收恶意信息。因此，本文恶意信息遏制问题旨在选择一组正确的信息的模体作为信息控制模体，在社会网络中及早地有效遏制恶意信息传播。在恶意信息遏制问题中，当前相信恶意信息的节点可能会在来自权威来源的正确信息的节点的影响下改变其信念。

根据社会网络模体的定义，本文定义控制信息流模体如下。

定义1 控制信息流模体(Control Information Flow Motif, CIFM)是指包含具备控制信息功能节点N_{ic}的模体。记作

$$\mathrm{CIFM}=\left\{\mathrm{CIFM}_{(v_i,v_j)}|v_i\in N_{\mathrm{ic}},v_j\in V\right\} \tag{1}$$

该模体由N_{ic}产生指令，利用它对于社会网络中其他状态下的节点有绝对的影响作用，将与恶意信息竞争的正确信息发送至邻居节点。这类网络模体承担着遏制恶意信息和传播正确信息的任务。

2.4 物理通信层信息传播

物理通信网络作为真实社会人际关系的映射，具有用户社会行为特征的数据，用户之间通过移动设备建立交互关系。每个移动设备都可以作为一个信号源节点，它们可以向邻接节点发送信息。物理通信层上个体之间可以传递带有恶意的生物元素，对应的是用户接收和传递信息的物理状态，与传染病模型中易感态-感染态(SI)类似，通信层中接收信息的节点称为感染节点，否则称为易感节点。恶意信息和正确信息以竞争的方式传播过程中，社会网络层中的用户能将他们的信念从相信恶意信息转向相信正确信息。两个对通信网络资源竞争激烈的信息流模体，可能地理位置上相近，争夺资源多，扩散信息就多。由于各类信息流模体都是基于底层物理的信息基础设施网进行传输，受物理层信息传输能力的限制，信息流模体相互之间存在通信网络资源竞争，造成彼此相互制约的关系。同时，不同信息流模体之间还存在相互驱动作用。

3 方案设计

3.1 社会网络层关键网络模体的确定

本文研究基于网络模体的信息可控传播方法，其中需要的关键网络模体承载着控制和传播信息的功能。由于结构的稳定性和实验的便捷性，本文的控制信息流模体CIFM选用3元模体$M(v_1,v_2,v_3)$来研究。

定义2 度密度(Degree Density, DD)。对于给定的加权网络$G=(V,E,W)$，$V=(v_1,v_2,\cdots,v_n)$，$i=1,2,\cdots,n$，d_{v_i}表示节点v_i的度数，$d_{\max}$表示图G中最大的节点度，定义为

$$\mathrm{DD}_M=\frac{\sum_{i=1}^{n}d_{v_i}}{n\times d_{\max}} \tag{2}$$

度密度衡量了网络模体对网络中剩余节点的重要性，网络模体中的节点连接到外部越多，对其他节点的影响就越大，该网络模体控制和传播信息的作用就越重要。

定义3 平均加权度 (Average Weighted Degree, AWD)。在给定的加权网络$G=(V,E,W)$中对于$u_i\in V-M,v_j\in M$，其中，$M\subseteq G$,$j=1,2,3$。$W=\{w(e_1),w(e_2),\cdots,w(e_n)\},i=1,2,\cdots,n$。$w(e_i)$表示边$e_i$的权值。$\mathrm{AWD}(u,M)$表示$u$在$M$内的平均加权度，定义为

$$\mathrm{AWD}(u_i,M)=\frac{\sum_{i=1}^{n}\sum_{j=1}^{3}w(u_i,v_j)}{n},(u_i,v_j)\in E \tag{3}$$

平均加权度描述了图G中节点与模体M之间的耦合程度。平均加权度越大，节点与模体内节点联系越紧密，模体对图中其余节点的影响就越大。

本文依据式(2)和式(3)确定社会网络层关键网络模体作为控制信息流模体，对于这一特定的功能，可根据式(4)计算其排名得分并择优选取

$$\mathrm{Score}(M)=0.5\times\mathrm{DD}_M+0.5\times\mathrm{AWD}(u_i,M) \tag{4}$$

3.2 社会网络层具有遏制恶意信息能力的种子节点选取

关键网络模体具有感知恶意信息并传播正确信息的能力，每个关键模体中含有控制信息节点N_{ic}，它利用对于社会网络中其他状态下的节点有绝对的影响作用，产生指令并发送至其他相关的节点。本节主要内容是在关键模体中选取能够遏制恶意信息的控制节点N_{ic}即种子节点。

基于2.2节中信息传播模型，根据3.1节中对网络模体Score(M)进行关键程度排序，然后按照排名的先后顺序选择每个模体中度最大的节点作为种子

节点，如果确定一个种子节点后，将模体序列中含有该种子节点的模体删除，这样可以避免富人俱乐部(Rich Club)现象[17]，循环上述步骤最终根据实际网络大小选取前k个种子节点来作为控制信息传播的初始节点。具体流程如算法1所示。

3.3 物理通信层信息可控传播方案

由于各类信息流模体都是基于底层物理的信息基础设施网进行传输，受物理层信息传输能力的限制，信息流模体之间存在通信网络资源竞争，造成彼此相互制约的关系，同时，不同信息流模体之间还存在相互驱动作用，能够通过协调配合，促进信息传输系统发挥整体能力。于是，本文在SIR传播模型的基础上定义通信层竞争信息传播模型SMCR过程如图4所示。

随着传播过程的进行，由于信息的竞争传播以及周围好友状态的变化恶意信息(M)与正确信息(C)会相互置换。另外，考虑到信息的时效性，传播者会对信息失去传播兴趣或能力，退出传播过程成为免疫者，免疫者将作为信息传播的终极状态。物理通信层的节点处于易感状态，会以不同的概率接受恶意信息和正确信息，由于正确信息与恶意信息存在竞争关系的，具体信息可控传播方案如算法2所示。

支持数据传播的通信网络需要以节点间的传输和接触过程为特征，移动网络中的传输可行性依赖于任意两节点之间的链路，而接触过程会随用户的移动发生变化。在算法2中，社会网络层中已经选取控制信息节点N_{ic}，针对所有信息流$I_i(i=1,2,\cdots,n)$；对于任意信息流I_i；当时N_{ic}感知到该信息为恶意信息，则标记为I_{mi}；通信网络层对来自社会网络层的用户社会关系交互的数据进行分析，在SMCR传播模型上来传播信息，当移动设备接到I_{mi}的命令状态变成Im，并采取免疫机制，否则信息被标记为I_c设备将接收并传递这条正确的消息；直到所有恶意信息达到收敛可控范围。

算法1　遏制恶意信息的种子节点选取算法

输入：社会网络层中所有网络模体M_s；网络G中不包含在模体中的节点u_i

输出：前k个种子节点集合S

(1) 初始化社会网络G

(2) 初始化所有模体M_s

(3) 根据式(5)计算所有模体的关键程度

(4) for $i=l$ to $i=k$

(5) 生成排序先后为$M_1,M_2,\cdots,M_k$，并选择关键程度最高的模体M_i

(6) 分别比较M_i中d_{v_1},d_{v_2},d_{v_3}大小，取度最大的节点作为第1个种子节点放入S中

(7) 将其余含有该种子节点的模体删除

(8) end for

(9)获取前k个遏制传播恶意信息的种子节点集合S

4　恶意信息传播数量的收敛性

定理1　在MCIC传播模型中，$|V_m(t_i)|$表示$t_i(i=1,2,\cdots,n)$时刻恶意信息的数量，恶意信息的数量在种子节点被激活后随时间的增大而减小，即当$t_2\geq t_1$时，恶意信息数量$|V_m(t_2)|\leq|V_m(t_1)|$。

证明　在一个网络中，对于任意时刻t，$V_m(t)$, $V_c(t)$分别表示该时刻的恶意信息数量和正确信息数量。

当$0\leq t<\gamma$时，γ为延迟时间。由于在极短时间内，恶意节点主动去影响未激活的邻居节点并传递恶意信息，此时正确节点尚未被激活。$V_n(t)$代表未被激活的邻居节点。于是

$$|V_m(t_2)|=|V_m(t_1)|+p_m\cdot|V_n(t_1)| \tag{5}$$

$$|V_m(t_2)|\geq|V_m(t_1)| \tag{6}$$

当$t\geq\gamma$时，在相对较长的时间内处于正确信息状态的节点在感知恶意信息之后将信息传给邻居节点，也就是说当正确信息与恶意信息同时出现时，会优先选择接受正确的信息且$p\geq p_m$，此时，

$$|V_m(t_2)|=|V_m(t_1)|+p_m\cdot|V_n(t_1)|-p\cdot|V_m(t_1)\cap V_c(t_1)| \tag{7}$$

$$p_m\cdot|V_m(t_1)|-p\cdot|V_m(t_1)\cap V_c(t_1)|\leq 0 \tag{8}$$

所以，$|V_m(t_2)|-|V_m(t_1)|\leq 0$，即

$$|V_m(t_2)|\leq|V_m(t_1)| \tag{9}$$

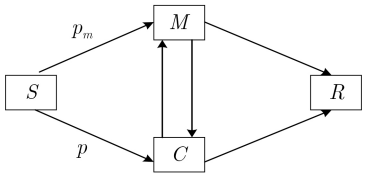

图 4 物理通信层竞争信息传播模型

算法2　信息可控传播算法

输入：I_i，N_{ic}，$V_c(t)$

输出：收敛的传播恶意信息节点集合$|V_m(t_i)|$

(1) 对于t_1时刻的任意一条信息I_i，社会层用户N_{ic}将感知到信息的数据传到通信层

(2)通信层的邻居节点接受正确信息和错误信息的概率分别为p和p_m

(3) 依照SMCR传播模型计算t_2时刻传播恶意信息的节点数：$|V_m(t_2)|=|V_m(t_1)|+p_m\cdot|V_n(t_1)|$

(4) 令$t=1,2,\cdots,i$，按照步骤(3)的方法计算

(5) 直到$|V_m(t_i)|$的大小不再增加

(6) end for

(7) 得到一个收敛的$|V_m(t_i)|$

由于在集合$\{|V_m(t_1)|-|V_m(t_2)|\}$中，部分处于错误信息状态的节点受到控制流的影响改变态度，从集合$\{V_m(t_2)\}$加入到集合$\{V_c(t_2)\}$，所以有

$$|\{V_m(t_2)\}\cap\{V_c(t_2)\}|\geq|\{V_m(t_1)\}\cap\{V_c(t_1)\}| \tag{10}$$

$$|V_m(t_3)|=|V_m(t_2)|+p_m\cdot|V_n(t_2)|-p\cdot|V_m(t_2)\cap V_c(t_2)| \tag{11}$$

由式(9)，式(11)得$p_m\cdot|V_m(t_2)|-p\cdot|V_m(t_2)\cap V_c(t_2)|\leq 0$，于是有$|V_m(t_3)|-|V_m(t_2)|\leq 0$，因此

$$|V_m(t_3)|\leq|V_m(t_2)| \tag{12}$$

由式(9)，式(12)完成证明。 证毕

定理1理论上证明了，本文提出的MCIC传播模型中，随着时间的推移恶意信息的数量有所下降，且最终会达到一个收敛状态，这就控制了移动社会网络中恶意信息的传播。

5 性能分析

5.1 感染时间(Infected time)

本文采用文献[18]中定义的最大感染时间和平均感染时间来衡量本文所提方法的性能。

最大感染时间(The maximum infected time)

$$M(G)=\max\{t(v)|\forall v\in V\} \tag{13}$$

其中，$t(v)$表示$v\in V$保留是恶意信息时所用的时间，如果最大感染时间$M(G)$是有限的，则意味着恶意信息最终将会从网络中消失。

平均感染时间(The average infected time)

$$A(G)=\frac{1}{|V|}\times\sum\nolimits_{\forall v\in V}t(v) \tag{14}$$

类似地，$A(G)$是指节点保留恶意信息的平均时间，如果平均感染时间$A(G)$是有限的，也意味着恶意信息最终将会从网络中消失。本实验的数据集来自Facebook真实数据集(https://toreopsahl.com/datasets)分别是有899个节点和7089条连边的Forum Network与含有1899个节点和13838条连边的Social Network。图5和图6分别在两个数据集上用$M(G)$和$A(G)$对本文方案的仿真实验。如图5和图6所示，横坐标p表示正确信息传播的概率(为了使实验具有一般性，本文设置$p_m=0.5$)，随机选取恶意节点进行实验。实验结果表明，随着恶意信息传播概率增加，最大感染时间和平均感染时间都呈下降趋势。

5.2 正确信息量与恶意信息量的变化

在2.2节定义的节点状态的基础上，本小节采用以下两个传播模型来进行信息可控传播实验。

(1)接触激活模型。为了主动地对抗恶意信息，恶意信息要扩散到正确节点时，该节点被信息激活，就会开始动态地传播正确的信息，此时会产生一个感知信息时间。

(2)延迟激活模型。给定一个社会网络时间，其中在时间t时刻有一些恶意信息的节点，无论是否扩散到正确节点，具有正确信息的节点集都会在时间$(t+\gamma)$变为激活状态，其中γ称为延迟时间。

图7和图8分别是Forum数据集在接触激活模型与延迟激活模型下正确信息与恶意信息数量的变化图。图中曲线显示，两种模型下的传播正确信息节点数量呈大幅度上升后趋于平稳状态，而传播恶意信息节点的数量在正确信息对抗之下呈下降趋势后逐渐平稳。

图9是Social网络数据集在接触激活模型下正确信息与恶意信息数量的变化图。如图所示，恶意信息在接触激活模型传播到$t=3$时刻时扩散到了只传播正确信息的节点，此时传播正确信息的节点被激

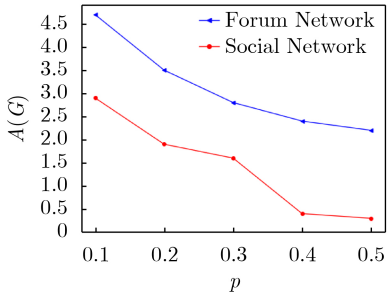

图 5 p对平均感染时间的影响

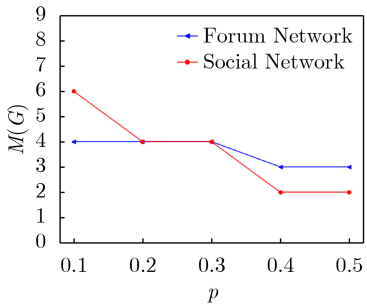

图 6 p对最大感染时间的影响

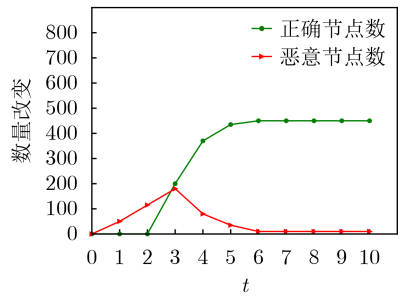

图 7 Forum网络中接触激活模型下正确信息量与恶意信息量变化

活并传播信息，传播正确信息的节点数量开始迅猛增加，传播恶意信息节点由于竞争不过传播正确信息节点，数量呈迅速下降趋势，最终都趋于平稳状态。

图10是Social网络数据集在延迟激活模型下正确信息与恶意信息数量的变化图。如图所示，恶意信息在延迟激活模型传播到延迟时间$\lambda=2$，传播正确信息的节点集合被激活，传播正确信息节点数量开始迅猛增加，使得恶意信息量在$t=3$出现拐点并呈下降趋势。

Forum网络和Social网络两个数据集的实验结果表明，本文方案在网络规模较小的数据集中，采用接触激活模型和延迟激活模型对恶意信息遏制都能发挥重要作用，在网络规模较大的数据集中两种传播模型都能迅速启动对恶意信息遏制，而且延迟激活模型下的恶意信息传播被控制的更为有效。

5.3 与其他方法恶意信息数量变化的对比

在本节两个网络数据集中，本文所提方法对恶意信息遏制的效果与其他两个方案对恶意信息遏制效果对比图，横坐标是时间t的变化，纵坐标是恶意信息数量的变化。如图11—图12所示，可以清楚地看到，在Forum网络中，信息在接触激活模型和延迟激活模型下，本方案对恶意信息遏制的时间比Degree[19]和PageRank快，在$t=3$的时候本方案就将恶意信息控制到最高数量，最终本文方案能将恶意信息数量控制得比其他两个方案的数量都低且达到收敛。图13和图14分别是在Social网络中，信息在接触激活模型和延迟激活模型下，本方案与

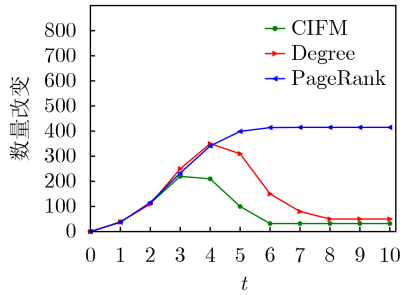

图 11 Forum网络中接触激活模型下恶意信息量变化对比

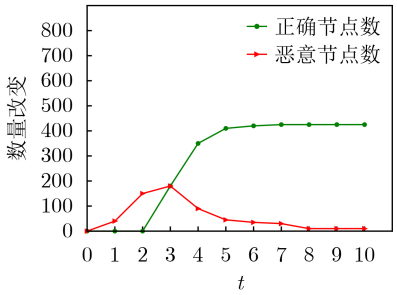

图 8 Forum网络中延迟激活模型下正确信息量与恶意信息量变化

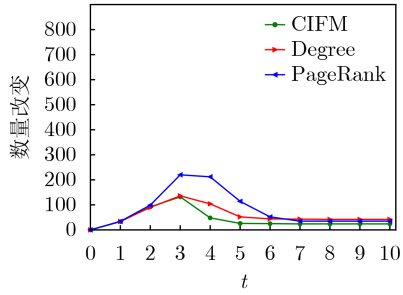

图 12 Forum网络中延迟激活模型下恶意信息量变化对比

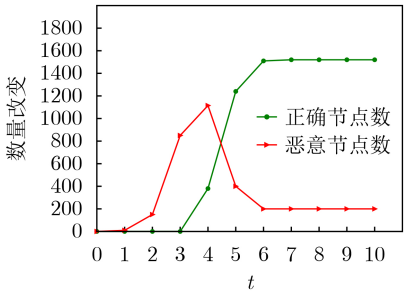

图 9 Social网络中接触激活模型下正确信息量与恶意信息量变化

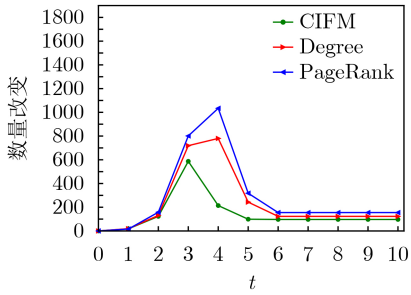

图 13 Social网络中接触激活模型下恶意信息量变化对比

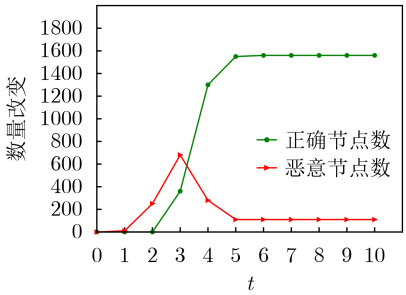

图 10 Social网络中延迟激活模型下正确信息量与恶意信息量变化

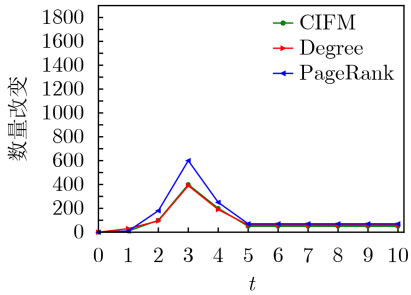

图 14 Social网络中延迟激活模型下恶意信息量变化对比

Degree和PageRank方案的恶意信息量的变化对比图。从两幅图中可以看到，随着时间的推移，恶意信息的数量呈现先增后减的趋势，当$t=3$时，本方案将恶意信息控制到最高数量，比其余两种方案都低，且比PageRank方案中恶意信息数量少了一半。这个实验说明，本文方案能够有效快速控制移动社会网络中的恶意信息数量，且能够使该数量达到收敛，也就意味着最终恶意信息会消失。

6 结束语

本文提出了一种基于网络模体的移动社会网络信息可控传播方法。首先，本文提出多实体的竞争性独立级联模型，该模型首次将信息竞争扩散理论与社会网络层用户的社会属性结合，实现信息的可控传播。其次，本文定义了控制信息流模体，设计关键网络模体在通信层的高效可控传播算法。仿真实验表明本文方法不仅在信息传播中最大感染时间和平均感染时间上更有优势，而且在控制信息传播方面的效果也是最好的，最终能够实现信息可控传播。未来可以进一步探索移动社会网络中信息传播的基本要素与传染病传播特征的关系，通过研究信息传播路径来实现对信息的可控传播。

参 考 文 献

[1] WU Jie and WANG Yunsheng. Hypercube-based multipath social feature routing in human contact networks[J]. *IEEE Transactions on Computers*, 2014, 63(2): 383–396. doi: 10.1109/TC.2012.209.

[2] LIN Limei, XU Li, HUANG Yanze, *et al*. On exploiting priority relation graph for reliable multi-path communication in mobile social networks[J]. *Information Sciences*, 2019, 477: 490–507. doi: 10.1016/j.ins.2018.10.035.

[3] GAO Chuangen, DU Hai, WU Weili, *et al*. Viral marketing of online game by DS decomposition in social networks[J]. *Theoretical Computer Science*, 2020, 803: 10–21. doi: 10.1016/j.tcs.2019.03.006.

[4] ETESAMI S R, BOLOUK S, NEDIĆ A, *et al*. Influence of conformist and manipulative behaviors on public opinion[J]. *IEEE Transactions on Control of Network Systems*, 2019, 6(1): 202–214. doi: 10.1109/TCNS.2018.2806179.

[5] 张宪立, 唐建新, 曹来成. 基于反向PageRank的影响力最大化算法[J]. 计算机应用, 2020, 40(1): 96–102. doi: 10.11772/j.issn.1001-9081.2019061066.

ZHANG Xianli, TANG Jianxin, and CAO Laicheng. Influence maximization algorithm based on reverse PageRank[J]. *Journal of Computer Applications*, 2020, 40(1): 96–102. doi: 10.11772/j.issn.1001-9081.2019061066.

[6] 顾益军, 解易, 张培晶. 面向有组织犯罪分析的人际关系网络节点重要性评价研究[J]. 中国人民公安大学学报:自然科学版, 2013, 19(4): 66–68.

GU Yijun, XIE Yi, and ZHANG Peijing. Research on the importance evaluation of interpersonal network nodes for organized crime analysis[J]. *Journal of People's Public Security University of China:Science and Technology*, 2013, 19(4): 66–68.

[7] BÓTA A and KRÉSZ M. A high resolution clique-based overlapping community detection algorithm for small-world networks[J]. *Informatica*, 2015, 39(2): 177–187.

[8] 黄宏程, 赖礼城, 胡敏, 等. 基于严格可控理论的社交网络信息传播控制方法[J]. 电子与信息学报, 2018, 40(7): 1707–1714. doi: 10.11999/JEIT170966.

HUANG Hongcheng, LAI Licheng, HU Min, *et al*. Information propagation control method in social networks based on exact controllability theory[J]. *Journal of Electronics & Information Technology*, 2018, 40(7): 1707–1714. doi: 10.11999/JEIT170966.

[9] 陈慧敏, 金思辰, 林微, 等. 新冠疫情相关社交媒体谣言传播量化分析[J]. 计算机研究与发展, 2021, 58(7): 1366–1384. doi: 10.7544/issn1000-1239.2021.20200818.

CHEN Huimin, JIN Sichen, LIN Wei, *et al*. Quantitative analysis on the communication of COVID-19 related social media rumors[J]. *Journal of Computer Research and Development*, 2021, 58(7): 1366–1384. doi: 10.7544/issn1000-1239.2021.20200818.

[10] KEMPE D, KLEINBERG J, and TARDOS É. Maximizing the spread of influence through a social network[C]. The Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Washington, USA, 2003: 137–146. doi: 10.1145/956750.956769.

[11] PENG Sancheng, WANG Guojun, ZHOU Yongmei, *et al*. An immunization framework for social networks through big data based influence modeling[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(6): 984–995. doi: 10.1109/TDSC.2017.2731844.

[12] DOOSTMOHAMMADIAN M, RABIEE H R, and KHAN U A. Centrality-based epidemic control in complex social networks[J]. *Social Network Analysis and Mining*, 2020, 10(1): 32. doi: 10.1007/s13278-020-00638-7.

[13] CHANG S, PIERSON E, KOH P W, *et al*. Mobility network models of COVID-19 explain inequities and inform reopening[J]. *Nature*, 2021, 589(7840): 82–87. doi: 10.1038/

s41586-020-2923-3.

[14] WANG Zhishuang, XIA Chengyi, CHEN Zengqiang, *et al*. Epidemic propagation with positive and negative preventive information in multiplex networks[J]. *IEEE Transactions on Cybernetics*, 2021, 51(3): 1454–1462. doi: 10.1109/TCYB.2019.2960605.

[15] HU Xiping, CHU T H S, LEUNG V C M, *et al*. A survey on mobile social networks: Applications, platforms, system architectures, and future research directions[J]. *IEEE Communications Surveys & Tutorials*, 2015, 17(3): 1557–1581. doi: 10.1109/COMST.2014.2371813.

[16] 顾洁, 王筱纶, 胡安安. 社交网络信息竞争扩散的关键节点策略研究[J]. 情报科学, 2020, 38(3): 78–86. doi: 10.13833/j.issn.1007-7634.2020.03.013.

GU Jie, WANG Xiaolun, and HU An'an. Seeding strategy of competitive diffusion in social network[J]. *Information Science*, 2020, 38(3): 78–86. doi: 10.13833/j.issn.1007-7634.2020.03.013.

[17] COLIZZA V, FLAMMINI A, SERRANO M A, *et al*. Detecting rich-club ordering in complex networks[J]. *Nature Physics*, 2006, 2(2): 110–115. doi: 10.1038/nphys209.

[18] GHOSHAL A K, DAS N, and DAS S. Influence of community structure on misinformation containment in online social networks[J]. *Knowledge-Based Systems*, 2021, 213: 106693. doi: 10.1016/j.knosys.2020.106693.

[19] SAXENA A, MALIK V, and IYENGAR S R S. Estimating the degree centrality ranking of a node[J]. *Social Analysis and Mining*, 2018, 8(1): 1–20.

张欣欣：女，博士生，研究方向为移动社会网络、网络与信息安全.
许　力：男，教授，博士生导师，研究方向为移动社会网络、大数据与信息化无线通信与物联网、智能信息处理等.
徐振宇：男，硕士生，研究方向为网络与通信安全.

责任编辑：马秀强