

基于隐性社交关系的社交物联网信任评估模型

张红斌^{1,2}, 樊凡¹, 赵冬梅², 刘滨^{3,4}, 尹彦¹, 刘建¹

(1. 河北科技大学信息科学与工程学院, 河北 石家庄 050018; 2. 河北师范大学河北省网络与信息安全重点实验室, 河北 石家庄 050024;
3. 河北科技大学经济管理学院, 河北 石家庄 050018; 4. 河北科技大学大数据与社会计算研究中心, 河北 石家庄 050018)

摘要: 社交物联网是社交网络和物联网融合形成的新范式, 增强了网络的扩展性和可导航性。然而, 由于智能设备的开放性和移动性增强, 智能对象的信息安全、可靠服务提供等方面的安全风险进一步扩大, 安全问题面临严峻挑战。信任被视为提供安全、可靠服务的关键因素, 因此, 从社交关系角度出发, 提出了一种新的信任评估模型。提出一种信任传递算法, 根据节点间的显性社交关系和潜在特征, 挖掘并建立节点间的隐性社交关系, 达到解决社交物联网网络稀疏性、冷启动问题的目的。对社交关系进行细粒度划分, 构建单关系子网, 并将多个单关系子网融合构建多重关系复合网, 从而有效融合节点间多种动态变化的社交关系对信任评估的影响。根据直接信任、间接推荐信任及服务满意度3个信任指标对智能对象进行综合信任评估。通过在真实智慧城市数据集上的实验结果表明, 无论是在不稀疏网络场景还是稀疏网络场景中, 该模型都具有较好的鲁棒性, 能够有效地评估网络中的可信对象和不可信对象, 并提高信任评估的准确性和收敛性。

关键词: 隐性社交关系; 多重社交关系; 社交物联网; 信任评估

中图分类号: TN915

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023021

Trust evaluation model of social internet of things based on implicit social relationship

ZHANG Hongbin^{1,2}, FAN Fan¹, ZHAO Dongmei², LIU Bin^{3,4}, YIN Yan¹, LIU Jian¹

1. School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050018, China

2. Hebei Key Laboratory of Network and Information Security, Hebei Normal University, Shijiazhuang 050024, China

3. School of Economics and Management, Hebei University of Science and Technology, Shijiazhuang 050018, China

4. Research Center of Big Data and Social Computing, Hebei University of Science and Technology, Shijiazhuang 050018, China

Abstract: The social internet of things (SIoT) is a new paradigm that combines social networks and the internet of

收稿日期: 2022-06-21; **修回日期:** 2023-02-22

通信作者: 赵冬梅, zhaodongmei666@126.com

基金项目: 国家自然科学基金(61672206, 61572170); 中央引导地方科技发展资金(216Z0701G), 河北省科技支撑计划(18210109D, 20310701D, 20310802D, 21310101D); 国家文化和旅游科技创新工程(2020年度)

Foundation Items: The National Natural Science Foundation of China (61672206, 61572170), Central Guide Local Science and Technology Development Fund (216Z0701G), S&T Program of Hebei (18210109D, 20310701D, 20310802D, 21310101D), The National Cultural and Tourism Science and Technology Innovation Project(2020)

引用格式: 张红斌, 樊凡, 赵冬梅, 等. 基于隐性社交关系的社交物联网信任评估模型[J]. 网络与信息安全学报, 2023, 9(2): 56-69.

Citation Format: ZHANF H B, FAN F, ZHAO D M, et al. Trust evaluation model of social internet of things based on implicit social relationship[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 56-69.

things to enhance network scalability and navigability. However, with increased openness and mobility of intelligent objects, there are rising security risks related to information security and reliable service delivery, which poses a significant challenge to the SIoT. Trust is a critical factor in providing secure and reliable services. Therefore, a new trust assessment model was proposed from the perspective of social relationships. A trust transfer algorithm was proposed based on the explicit social relationships and potential features between nodes. The algorithm can tap and establish the implicit social relationships among nodes to solve the SIoT sparsity and cold start problem. Additionally, the social relations were fine-grained and divided to build a single-relationship sub-network. Multiple single-relationship sub-networks were fused to build a multiple-relationship composite network. Thus, the impact of multiple dynamically changing social relationships among nodes on trust evaluation can be effectively fused. The comprehensive trust assessment of intelligent objects was conducted based on three indicators: direct trust, indirect recommendation trust, and service satisfaction. The experimental results on real smart city datasets demonstrate the model's robustness in non-sparse and sparse network scenarios. It can effectively evaluate trusted and untrusted objects in the network and improve the accuracy and convergence of trust evaluation.

Keywords: implicit social relationship, multiple social relationships, social internet of things, trust assessment

0 引言

社交物联网 (SIoT, social internet of thing) 是物联网的新兴范例, 是物联网的延伸, 它与社交网络概念相融合, 创建了互联智能对象的社交网络。这种融合使两种范式得以丰富, 从而形成新的生态系统^[1]。社交物联网作为互联网的延伸和扩展, 不仅能实现人与人、人与物之间的互联, 还可实现物与物之间的互联。基于人与人之间的社交行为和社交关系, 智能设备之间也可自发地生成相应的社交关系, 在物与物之间可以建立物品之间的社交网络, 从而实现像人类社会网络那样的可拓展性。在物与人之间, 挖掘人与物联网之间的联系, 用以结合人类社会特征方面的研究; 在人与人之间, 将物联网服务与社交网络服务相结合, 实现更好的服务发现和用户体验; 抽象社交网络模型为物联网的实现与应用提供一种新的研究思路^[2]。在社交物联网世界, 设备与设备、设备与人之间的交互越来越多, 服务的交互也越来越频繁, 因此, 设备与设备之间的信任问题成为社交物联网发展过程中的关键问题。社交物联网结构可以根据需要塑造, 智能对象之间可以根据社交关系及行为建立一定程度的可信度, 以保证网络的可导航性, 从而有效地发现对象和服务, 并像人类社交网络一样保证可扩展性^[3]。因此, 社交关系在社交物联网的信任评估中具有重要作用。在不同领域中, 信任

的概念、度量、评估模型是不统一的^[4]。在社交物联网中, 信任代表智能设备提供服务的可靠程度, 智能对象会与它信任的对象建立关系, 并向那些与其建立了良好关系的人和设备提供所需的服务^[5]。因此, 为了使委托者得到更满意的服务, 提高智能对象间的合作水平, 保证整体网络的安全可导航性, 在社交物联网中进行信任评估是非常必要的。

需要注意的是, 在传统物联网中, 智能对象的位置相对固定, 而在社交物联网中, 智能对象的移动性变强, 使得对象间社交关系复杂多变, 并可能存在数据稀疏的情况, 影响节点的信任评估。针对此问题, 本文利用信任传递算法和节点的潜在特征, 挖掘节点之间的隐性社交关系, 进而扩展社交关系网络, 并将多个单关系子网加载构建多关系复合网, 有效融合了节点间多种动态变化的社交关系对信任评估的影响, 达到提高信任评估准确性、信任收敛速度的目的。

1 相关工作

在社交物联网中, 关于信任评估的研究正处于发展阶段。文献[6]利用乘法属性图在社交物联网背景下量化预定义的社交关系, 进而计算社交物联网节点之间的信任强度, 但只是简单分析了具有预定义社会关系属性间同质和异质亲和力的信任, 并没有充分考虑信任属性及如何将复杂多

变的社交关系融入信任评估等问题。文献[7]根据服务应用程序要求,从亲密度、服务反馈、社交性和交易重要性4个属性中挑选最合适的描述属性对节点进行信任评估,然而,尽管该模型支持节点移动性,但在模拟过程中,节点被认为是固定的,对于SIoT网络来说,忽略了节点的强移动性带来的社交关系的变化。盖方宇^[8]在车载网中引入社交网络的理论,使其可以更好地服务于信任模型,通过将社交关系量化可以提高信任评估模型的准确性,社交车载网的信任机制就是社交物联网的具体应用,但并未考虑到移动性的增强使得社交关系动态多变,进而影响信任的评估。Wei等^[9]建立了特定的信任模型框架,提出了基于特征-属性匹配模型的情境感知的信任量化模型,采用能力、意愿和社会关系要素来度量信任,但没有充分考虑到节点间不同的社交关系类型对信任评估的影响也不同。文献[10]在信任评估中引入社会关系,以更好地理解一些歧视行为,减少行为偏差在提供服务中的影响,然而作者只是提取节点间的社会相似性来表示节点间的联系强度,并没有考虑到多变社交关系及潜在的隐性社交关系对社交物联网信任管理的重要性。文献[11]考虑了信任的诚实性、协作性、社区兴趣和节点能量等信任属性,并根据直接观察、间接推荐、节点的中心性和可靠性因子来计算信任。文献[12]提出了一个社交物联网下自适应信任管理协议,并通过直接观察和间接推荐来传播和聚合信任。但是,文献[11]和文献[12]的信任评估模型是基于用户的社会网络产生的,这意味着智能设备之间的社交关系受限于它们所有者之间的社会关系,因此不能充分描述智能对象间多样多变的社交关系在信任评估过程中带来的重要影响。文献[13]提出一种基于时间相似性的社交物联网信任模型,该模型融合了社区兴趣属性、朋友属性、协同工作属性3种属性对信任评估的影响。文献[14]提出REK的信任评估模型,通过整合从直接观察、个人经验到全球声誉的异质信息,涵盖信任的多维方面,利用聚合机制,导出信任值。文献[15]提出了一个有效的时间感知机器学习驱动的信任评估模型,该模型利用机器学习驱动的聚合方案来综合基于友谊相似性、社区兴趣属性、协同工

作属性及合作属性4个属性的信任评估。文献[13-15]虽然在评估信任时考虑了多种指标,如合作性、可靠性、协同性等,但都忽略了社交物联网最显著的特征,即智能设备之间动态变化的社交关系对信任评估产生的影响。

以上文献在考虑节点间社交关系对信任评估的影响时,较为单一,忽略了节点的强移动性带来的多变多样的社交关系对信任评估的影响。受文献[16-17]中子网复合模型的启发,本文对社交关系进行细粒度划分,建立单关系子网,并将单关系子网通过子网加载构建多重关系复合网,达到在信任评估中引入节点间多种社交关系的目的;利用信任传递机制建立隐性社交关系,扩充网络,有效解决网络稀疏性问题。

2 系统模型

2.1 社交关系类型

在生活中,人们往往会信任具有亲密社交关系的人,不同的社交关系类型表征出不同的亲密度,因此,社交关系不同导致信任强度不同,如相较同事,人们更信任家人。社交物联网具有很强的可导航性,提高了服务发现、服务选择及服务组合的能力,而每种类型的社会关系对可导航性的影响是不同的^[18-19]。因此,对社交物联网的社交关系进行细粒度划分是非常必要的。根据文献[3]中定义的SIoT的特定对象社会化模型,对象会创建不同类型的社会关系。节点间的每一种社交关系都具有一种信任水平^[20]。

本文将信任值范围设置在(0,1),信任值越高,表示智能对象越可靠,交互成功率越高。当手机、便携式计算机等智能对象属于同一所有者时,会大概率拥有相似的行为,因此,本文给予所有权对象关系最高初始信任值;同一制造商在同一时期生产的智能设备之间存在较高的相似性,因此,本文给予父对象关系较高的初始信任值;在智能家居或智能城市等相同环境中使用的传感器、执行器等智能对象之间发生交互及共同协作完成任务的概率较高,因此,本文给予协同位置对象关系高初始信任值;协同工作对象关系是根据任务类型在相距较远的对象之间建立的,如远程医疗等,距离较远使得智能对象遭受恶意攻击的可能性大,因此,

本文给予协同工作对象关系较低的初始信任值。

本文根据社交关系的定义, 参照文献[18, 21]对社交物联网中社交关系类型导航性和重要性的分析, 在表1中对社交关系初始信任值进行设定, 并在表2中给出本文使用的符号及说明。

表1 社交关系初始信任值
Table 1 Initial trust value of social relationship

社交关系类型	描述	初始值
所有权对象关系 (OOR)	在属于同一用户的异构对象之间建立	0.90
父对象关系 (POR)	在属于同一生产批次的对象之间建立	0.80
协同位置对象关系 (C-LOR)	在同一位置使用的对象 (同质或异质) 之间建立	0.70
协同工作对象关系 (C-WOR)	在提供一个共同的物联网应用程序的对象之间建立	0.60

表2 符号及说明
Table 2 Symbols and their description

符号	说明	符号	说明
ES	显性社交关系矩阵	I_DSR	隐性社交关系信任矩阵
IS	隐性社交关系矩阵	F_DSR_E	显性多关系信任矩阵
RM	正则化矩阵	F_DSR_I	隐性多关系信任矩阵
<i>i</i>	节点 <i>i</i>	RT_{ij}^X	<i>X</i> 属性下 <i>i</i> 对 <i>j</i> 的间接信任
<i>j</i>	节点 <i>j</i>	DT_{ij}^X	<i>X</i> 属性下 <i>i</i> 对 <i>j</i> 的直接信任
DSR	多关系信任矩阵	T_{ij}^X	<i>X</i> 属性下 <i>i</i> 对 <i>j</i> 的综合信任
E_DSR	显性社交关系信任矩阵	F	多关系矩阵

2.2 多重关系复合网

人们往往是信任朋友的, 并会信任朋友的朋友, 这意味没有直接社交关系的人们之间可能存在着潜在的隐性社交关系。针对社交物联网数据

稀疏性问题, 本文根据信任的传递性^[4,22], 提出了一种信任传递算法, 根据节点间的显性社交关系和潜在特征, 挖掘并建立节点间的隐性社交关系, 扩充网络, 并将多个单关系子网加载构建具有多种社交关系的 SIoT 网, 进行信任评估。本文引用文献[12]中的诚实性、合作性和社区兴趣作为表征社交物联网系统的最显著指标, 利用社交关系描述信任属性, 如用节点间的协同位置对象关系和父对象关系来描述社区兴趣属性。接下来, 以社区兴趣属性为例阐述 SIoT 多重关系复合网结构, 如图1所示。

1) 建立 POR 关系矩阵 **ES₁**、C-LOR 关系矩阵 **ES₂**, 得到 POR 关系信任矩阵 **E_DSR₁**、C-LOR 关系信任矩阵 **E_DSR₂**, 计算同时具有两种社交关系的关系程度, 形成显性多关系信任矩阵, 计算如式(3)所示。

$$\mathbf{E_DSR}_1 = 0.80\mathbf{ES}_1 \quad (1)$$

$$\mathbf{E_DSR}_2 = 0.70\mathbf{ES}_2 \quad (2)$$

$$\mathbf{F_DSR}_E(i, j) = \max(\mathbf{E_DSR}_1(i, j), \mathbf{E_DSR}_2(i, j)) + |\mathbf{E_DSR}_1(i, j) - \mathbf{E_DSR}_2(i, j)|^\eta \sigma \quad (3)$$

参数 σ 将信任值控制在 (0,1), 在本文中, $\sigma = 0.01$; 参数 η ($0 < \eta < 1$) 的大小取决于节点社交关系的类型。

2) 根据信任传递算法来建立节点之间存在的隐性社交关系, 隐性社交关系的关系强度由显性社交关系强度衰减而来, 并根据社会关系类型和间接朋友数量的增加而演变, 因此, 隐性社交关系矩阵计算如式(4)所示。

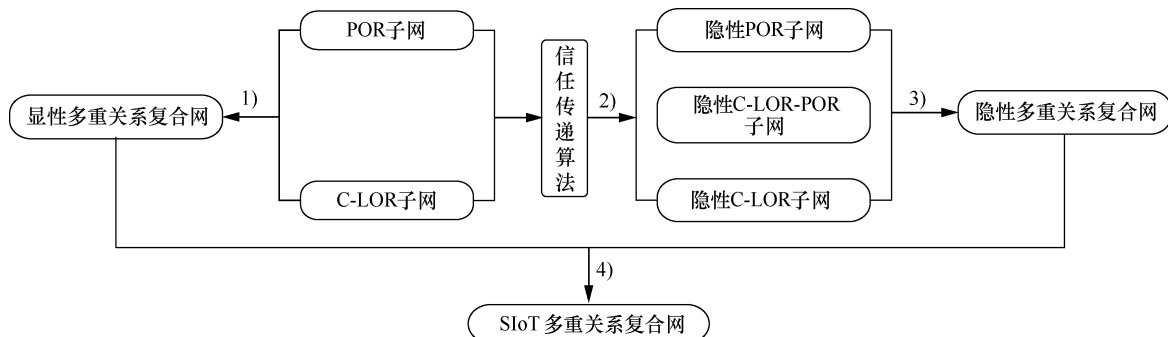


图1 多重关系复合网结构

Figure 1 Multi-relationship composite network structure

$$\mathbf{IS} = \mathbf{ES} \otimes \mathbf{ES} \cdot \mathbf{RM} \quad (4)$$

其中,

$$\mathbf{RM} = \begin{cases} 0, & i = j \\ 1, & i \neq j \end{cases} \quad (5)$$

式(4)中, $\otimes$ 表示外积运算, $\cdot$ 表示内积运算, 正则化矩阵用来排除节点与本身建立隐性信任关系。在隐性社交关系矩阵 $\mathbf{IS}$ 中, 数值 0 表示两个节点之间没有隐性社交关系, 其他数值表示该节点作为间接朋友出现的次数; 因此, 节点间隐性社交关系强度计算如式(6)所示。

$$\mathbf{I_DSR}(i, j) = (1-r)\mathbf{E_DSR}(i, j) - (r \cdot \mathbf{E_DSR}(i, j))^{\mathbf{IS}(i, j)^\eta} \quad (6)$$

$\mathbf{IS}(i, j)$ 表示节点 j 作为节点 i 间接朋友出现的次数, 参数 r 是信任衰减因子, r 的取值为 (0,1)。

下面详细阐述信任传递算法。

算法 1 信任传递算法

输入 $\mathbf{ES}_1, \mathbf{ES}_2, \mathbf{E_DSR}_1, \mathbf{E_DSR}_2, \mathbf{RM}$

输出 $\mathbf{I_DSR}_1, \mathbf{I_DSR}_2, \mathbf{I_DSR}_3$

If $\mathbf{ES}_1(i, j) == 0$ //节点 i 和节点 j 之间无 POR 关系

$\mathbf{IS}_1 = \mathbf{ES}_1 \otimes \mathbf{ES}_1 \cdot \mathbf{RM}$ //得到隐性 POR 矩阵 $\mathbf{I_DSR}_1(i, j) = (1-r)\mathbf{E_DSR}_1(i, j) - (r \cdot \mathbf{E_DSR}_1(i, j))^{\mathbf{IS}_1(i, j)^\eta}$ //得到隐性 POR 信任矩阵

end

if $\mathbf{ES}_2(i, j) == 0$ //节点 i 和节点 j 之间无 C-LOR 关系

$\mathbf{IS}_2 = \mathbf{ES}_2 \otimes \mathbf{ES}_2 \cdot \mathbf{RM}$ //得到隐性 C-LOR 矩阵

$\mathbf{I_DSR}_2(i, j) = (1-r)\mathbf{E_DSR}_2(i, j) - (r \cdot \mathbf{E_DSR}_2(i, j))^{\mathbf{IS}_2(i, j)^\eta}$ //得到隐性 C-LOR 信任矩阵

end

$\mathbf{ES}_3 = \text{xor}(\mathbf{ES}_1, \mathbf{ES}_2)$

if $\mathbf{ES}_3(i, j) == 0$ //节点 i 和节点 j 之间无社交关系

$\mathbf{IS}_3 = \mathbf{ES}_3 \otimes \mathbf{ES}_3 \cdot \mathbf{RM}$ //得到隐性矩阵 $\mathbf{E_DSR}_3(i, j) = \frac{1}{2}(\mathbf{E_DSR}_1(i, j) + \mathbf{E_DSR}_2(i, j))$ //

如果节点 i 和节点 k 之间是 POR, 节点 k 和节点 j 之间是 C-LOR 或节点 i 和节点 k 之间是 C-LOR, 节点 k 和节点 j 之间是 POR 时, 节点间的关系程度

$\mathbf{I_DSR}_3(i, j) = (1-r) \cdot \mathbf{E_DSR}_3(i, j) \mathbf{E_DSR}_3(i, j) - (r \cdot \mathbf{E_DSR}_3(i, j))^{\mathbf{IS}_3(i, j)^\eta}$ //得到基于节点 i 和节点 k 、节点 k 和节点 j 之间两种不同社交关系的隐性关系信任矩阵

end

3) 计算同时具有两种隐性社交关系的关系信任程度, 如式(7)所示。

$$\mathbf{F_DSR}_t(i, j) = \max(\mathbf{I_DSR}_1(i, j), \mathbf{I_DSR}_2(i, j)) + |\mathbf{I_DSR}_1(i, j) - \mathbf{I_DSR}_2(i, j)|^\eta \sigma \quad (7)$$

为防止隐性社交关系的建立导致网络链接过于密集, 本文设置隐性社交关系程度阈值为 0.4, 即当 $\mathbf{F_DSR}_t(i, j) > 0.4$ 时, 节点 i 与节点 j 之间建立隐性社交关系。

4) 节点之间的显性社交关系比隐性社交关系更重要, 所以同时具有显性、隐性社交关系的关系强度用式(8)计算。

$$\mathbf{DSR}(i, j) = \mathbf{F_DSR}_E(i, j) + |\mathbf{F_DSR}_E(i, j) - \mathbf{F_DSR}_t(i, j)|^\eta \sigma \quad (8)$$

3 评估模型

本文模型根据服务应用要求选择最佳信任属性, 以社区兴趣属性为例, 选择 POR 和 C-LOR 描述信任属性, 根据第 2 节所述模型构建具有多种显性、隐性社交关系的多关系复合网。随着时代的发展, 推荐在人们的生活中逐步占据重要地位。因此, 本文根据直接观察和间接推荐两种方式聚合形成直接信任和间接推荐信任, 并考虑服务满意度指标, 在交互结束后对服务进行满意度评分, 进而提高信任动态评估的准确性。信任评估模型如图 2 所示。

本文通过对社交关系的细粒度划分, 利用 POR 和 C-LOR 来描述社区兴趣属性, 根据第 2 节所述, 构成具有显性和隐性社交关系的多关系复合网 F 。一方面, 该模型通过直接观察来传播

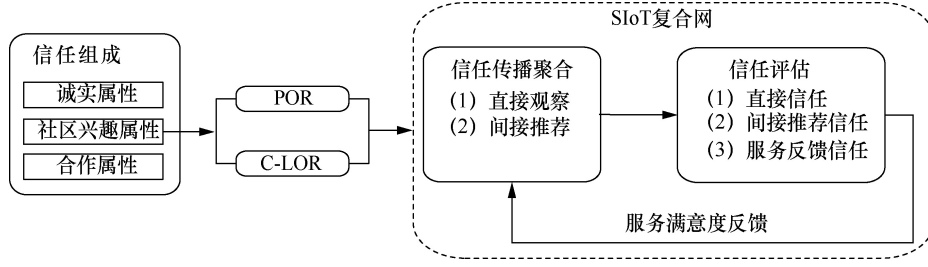


图2 信任评估模型
Figure 2 Trust evaluation model

和聚合节点 i 对节点 j 的直接信任，计算如式(9)所示。

$$DT_{ij}^{CI} = \frac{|F(i) \cap F(j)|}{|F(i) \cup F(j)|} \quad (9)$$

$F(i)$ 表示节点 i 的社交关系集， $F(j)$ 表示节点 j 的社交关系集。

另外，在此过程中，节点 i 会接收来自具有交互关系或社交关系的节点 k 的推荐，形成间接推荐信任值。假设节点 k 有 n 个推荐者，间接推荐信任计算公式如下。

$$RT_{ij}^{CI} = \frac{1}{n} \sum_{k=1}^n \frac{|F(k) \cap F(j)|}{|F(k) \cup F(j)|} \quad (10)$$

在 t 时刻交互结束后，节点 i 会对节点 j 提供的服务进行满意度评分，并作为下一次交互的服务反馈信任，计算公式如下。

$$S_{ij}(t) = \begin{cases} T_{ij}^{CI}(t - \Delta t) \cdot 1, & \text{满意} \\ T_{ij}^{CI}(t - \Delta t) \cdot (-1), & \text{不满意} \end{cases} \quad (11)$$

本文借鉴文献[20]中的信任更新计算，根据服务满意度的反馈对节点之间的关系信任进行更新，如果节点 j 提供的是良好服务，则

$$DSR(k, j) = DSR(k, j) + H(1 - DSR(k, j)) \quad (12)$$

如果节点 j 提供的是恶意服务，则

$$DSR(k, j) = DSR(k, j)(1 - H) \quad (13)$$

参数 $H(0 < H < 1)$ 是激励因子，用来调节关系信任更新大小。

因此，根据直接信任、间接推荐信任和服务反馈信任评估综合信任值，当节点 i 和节点 j 直接交互时，综合信任值为

$$TT_{ij}^{CI} = (1 - \mu)DT_{ij}^{CI}(t) + \frac{\mu}{2} \cdot RT_{ij}^{CI}(t) + \frac{\mu}{2} \cdot S_{ij}(t - \Delta t) \quad (14)$$

当节点 i 和节点 j 间接交互时，综合信任值为

$$TT_{ij}^{CI} = \mu \cdot RT_{ij}^{CI}(t) + (1 - \mu) \cdot S_{ij}(t - \Delta t) \quad (15)$$

$$\mu = DSR(i, k) \cdot DSR(k, j) \quad (16)$$

参数 $\mu(0 < \mu < 1)$ 由节点 i 与节点 k 、节点 k 与节点 j 之间的社交关系程度决定，并用于调整直接信任、间接推荐信任和服务反馈信任 3 个方面对信任评估影响的权衡。

信任管理是一个持续的、动态的过程，它迭代地聚合过去的信息和新的信息^[12]，所以节点交互时，会动态更新信任。信任评估更新公式如下。

$$T_{ij}^{CI}(t) = (1 - \delta) \cdot T_{ij}^{CI}(t - \Delta t) + \delta \cdot TT_{ij}^{CI} \quad (17)$$

Δt 是自上次信任更新以来经过的时间；参数 $\delta(0 < \delta < 1)$ 代表时间衰退对信任的影响，用来权衡旧信任值的衰退和新信任值的贡献。

4 仿真实验与结果分析

本节以社区兴趣信任属性为例，通过实验仿真评估此模型在信任收敛速度、信任评估准确性等方面的性能，将其与多种信任属性的文献^[13]、单信任属性的文献^[11-12]进行对比。实验结果证明了本文所提信任评估模型在社交物联网中的有效性。

本文使用文献[21]中的数据集在 Matlab 中进行仿真。该数据集是基于真实物联网对象，按照 FIWARE 数据模型中引入对象的类型和数据模型进行分类，并基于运动中的小世界模型构建出真实的智慧城市社交物联网。本文随机从该数据集中选出 30 个用户，对其用户拥有的 100 个智能设备构建 SIIoT，并根据第 2 节所述规则创建动态演变的多种社交关系，将节点初始信任值都设为 0.5，进行实验仿真，实验模拟总时长为 100 h。

本文在良好环境下随机选取两组节点进行了

信任评估对比实验,其中一组节点所处网络环境表现为明显的稀疏特征。稀疏网络是社交物联网常见的且不可忽视的应用场景,因此本文对信任评估模型在稀疏网络中的适用性进行评测,对比一般性非稀疏场景和稀疏网络场景中信任评估算法的收敛特征。在实验中,引入均值、标准差、残差及损失函数 4 种参数来更好地对比分析模型。均值和残差用来描述信任评估的准确性,标准差描述信任模型的动态敏感性;损失函数表示拟合的程度,损失函数值越小,表示与真实值拟合程度越高,模型鲁棒性越好。其平均损失计算公式如下。

$$L = \frac{1}{T} \sum_{t=1}^T (\text{Trust}_t - T_{ij}(t))^2 \quad (18)$$

其中, T 表示时间($T=100$), Trust_t 表示在 t 时刻的真实信任值, $T_{ij}(t)$ 表示在 t 时刻的信任评估值。

下面,通过在两种场景下对不同状态节点进行实验评估来验证本文模型的优良性能。

4.1 良好节点信任评估

对随机选取的两组良好节点信任值进行实验评估,一组节点所处网络为一般性非稀疏场景,另一组节点所处网络为稀疏网络场景,理想情况下,良好节点信任评估值趋向于常量 1。将本文模型与文献[11-13]提出的模型进行对比,结果如图 3 所示。

信任评估是一个不断动态变化的过程,因此对图 3 进行数据分析,得出不同时间区间内各个模型的均值、标准差及残差,计算结果如表 3、表 4 所示。

从图 3(a)可以看出,在非稀疏场景下的信任评估过程中,本文模型和文献[11-13]的相关信任评估模型均在 10 h 内呈现了快速收敛特征。从评估过程曲线斜率可以看出,本文模型的收敛速度快于文献[11]、文献[12]提出的模型。从表 3 可以观察到,在 100 h 的仿真实验过程中,本文模型的信任评估值均值相较于文献[11]和文献[12]提出的模型更高,本文模型的信任评估值残差相较于文献[11]和文献[12]提出的模型更小。这反映出所提模型在评估准确性和收敛性方面优于文献[11]、文献[12]提出的模型。虽然在前 10 h 内,本文所提模型的斜率与文献[13]模型相比较小,但从长期情

况分析,本文所提模型的均值只在前 10 h 内的均值低于文献[13]提出的模型,10 h 之后,均值皆高于文献[13]提出的模型,残差皆小于文献[13]提出的模型,说明在整个评估过程中,本文模型在评估准确性方面优于文献[13]提出的模型。相较于文献[11-13]提出的模型,本文模型标准差较大,这反映了所提模型可以防止信任评估过早陷入错误的稳定状态,具有从虚假的评估稳定状态脱离出来的能力。而对比文献的标准差较小,也反映了其过早进入了错误状态。文献[11-13]提出的模型及本文模型的平均损失函数值分别为 0.058、0.042、0.022、0.012,相较于文献[11-13]提出的模型,本文模型的损失函数值更小,与真实曲线拟合程度更高,反映出所提模型的鲁棒性更好。这一方面是由于在信任评估中加入了服务反馈信任,当节点提供良好服务时,会正面影响下一次评估的信任值,并使信任更快向真实值收敛;另一方面是因为节点之间的信任会动态更新,当节点提供良好服务时,节点间关系程度信任增强,提高了信任评估的准确性。

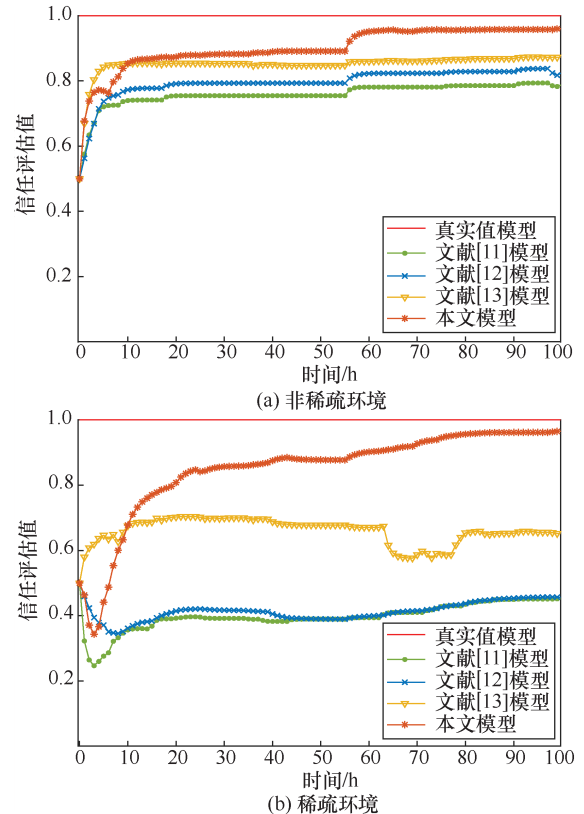


图3 对随机选取一个良好节点的信任评估
Figure 3 Trust evaluation of a randomly selected good node

表3 非稀疏环境下对良好节点信任评估分析
Table 3 Analysis of trust evaluation of good nodes in non-sparse environments

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文
(1,10)	0.696	0.711	0.8	0.779	0.051	0.067	0.057	0.048	0.304	0.289	0.2	0.221
(11,20)	0.745	0.781	0.854	0.869	0.005	0.005	0.001	0.004	0.255	0.219	0.146	0.131
(21,30)	0.755	0.793	0.854	0.881	0	0	0.001	0.002	0.245	0.207	0.146	0.119
(31,40)	0.755	0.793	0.851	0.885	0	0	0.002	0.002	0.245	0.207	0.148	0.115
(41,50)	0.755	0.793	0.848	0.891	0	0	0	0	0.245	0.207	0.152	0.109
(51,60)	0.767	0.805	0.853	0.916	0.012	0.013	0.005	0.026	0.233	0.195	0.146	0.084
(61,70)	0.782	0.823	0.861	0.954	0	0	0.001	0.002	0.218	0.177	0.139	0.046
(71,80)	0.783	0.826	0.864	0.956	0.002	0.002	0.002	0	0.217	0.174	0.137	0.044
(81,90)	0.785	0.829	0.868	0.957	0	0	0	0	0.215	0.171	0.131	0.043
(91,100)	0.791	0.832	0.873	0.958	0.004	0.007	0.001	0.001	0.209	0.168	0.127	0.042

表4 稀疏环境下对良好节点信任评估分析
Table 4 Analysis of trust evaluation of good nodes in sparse environments

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文
(1,10)	0.301	0.378	0.625	0.494	0.037	0.036	0.025	0.112	0.699	0.622	0.375	0.506
(11,20)	0.375	0.391	0.692	0.768	0.014	0.014	0.007	0.029	0.625	0.609	0.308	0.232
(21,30)	0.393	0.419	0.701	0.854	0.001	0.001	0.002	0.009	0.607	0.581	0.299	0.146
(31,40)	0.389	0.414	0.696	0.863	0.004	0.003	0.003	0.005	0.611	0.586	0.303	0.137
(41,50)	0.387	0.393	0.679	0.88	0.003	0.003	0.002	0.002	0.613	0.607	0.321	0.12
(51,60)	0.391	0.393	0.675	0.887	0.002	0.004	0.003	0.009	0.609	0.607	0.325	0.113
(61,70)	0.406	0.408	0.613	0.913	0.006	0.006	0.04	0.007	0.594	0.592	0.387	0.187
(71,80)	0.425	0.426	0.603	0.946	0.008	0.007	0.024	0.008	0.575	0.574	0.396	0.054
(81,90)	0.446	0.448	0.654	0.961	0.004	0.004	0.003	0.001	0.554	0.552	0.346	0.039
(91,100)	0.541	0.456	0.656	0.963	0	0.001	0.002	0.002	0.459	0.544	0.344	0.037

图 3(b)反映了在稀疏网络场景下, 本文模型与文献[11-13]的信任评估模型具有较大差异。文献[11-13]的信任评估模型经历 10 h 信任评估后, 信任值基本稳定。但由于网络稀疏性的影响, 其信任评估值稳定在 0.4 左右和 0.65 左右, 与节点的真实信任值具有较大差异。而本文模型的信任评估值在 10 h 到 20 h 之间仍能向真实值靠拢。这是由于本文通过建立节点间隐性社交关系填充网络, 有效缓解了网络稀疏性导致无法正确对节点信任进行评估的问题。从表 4 可以看到, 在整个实验过程中, 本文模型的信任评估均值基本大于文献[11-13]

的均值, 其残差小于文献[11-13]提出模型的残差; 证明在稀疏场景下, 与单属性信任评估模型和多属性信任评估模型相比, 本文模型都有效提高了评估准确性。在时间区间(1,60)内, 本文模型的标准差基本大于其他 3 种模型, 说明在动态的信任评估过程中, 本文模型具有使评估值不断接近真实值的能力, 而文献[11-13]提出的这 3 种模型的标准差较小, 使得评估值长时间稳定在错误的评估值 0.4 左右和 0.65 左右; 在时间区间(61,100)内, 本文标准差与其他 3 种模型的标准差相差较小, 4 种评估模型都趋于稳定。文献[11-13]提出的模型及本文模

型的平均损失函数值分别为 0.366、0.345、0.116、0.041，相较于文献[11-13]提出的模型，本文模型的平均损失函数值更小，与真实曲线拟合程度更高。

从图 3 可以看出，无论网络环境是否稀疏，本文模型的损失函数值都较小，而其他 3 种模型的损失函数值较大，说明本文模型在稀疏场景下同样具有较好的鲁棒性。

4.2 恶意节点信任评估

对随机选取的两组恶意节点信任值进行实验评估，一组节点所处网络为一般性非稀疏场景，另一组节点所处网络为稀疏网络场景，理想情况下，恶意节点信任评估值趋向于常量 0。将本文模型与文献[11-13]提出的模型进行对比，结果如图 4 所示。

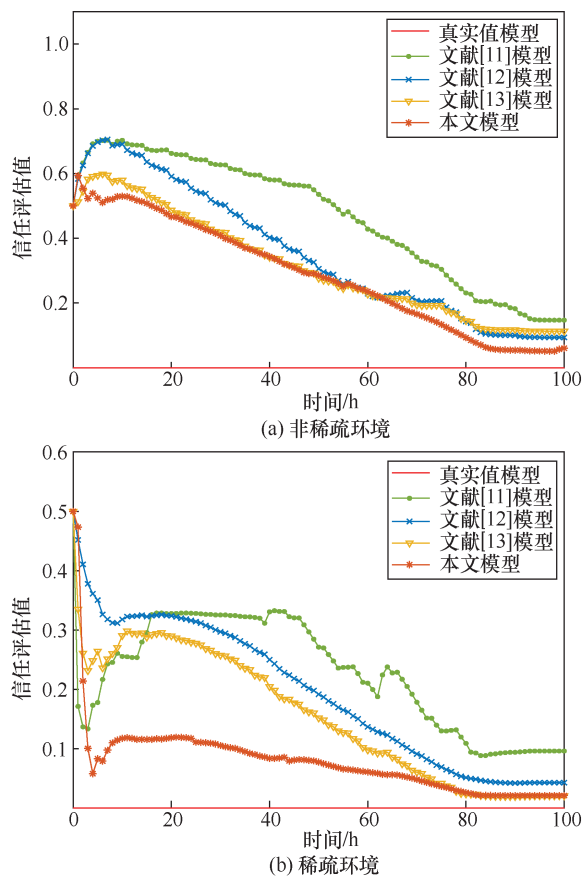


图 4 对随机选取一个恶意节点的信任评估
Figure 4 Trust evaluation of a randomly selected malicious node

通过对图 4 进行数据分析，得出不同时间区间内各个模型的均值、标准差、残差及平均损失

函数值，如表 5、表 6 所示。

从图 4(a)及表 5 可以看出，在一般非稀疏网络场景的信任评估过程中，文献[11-13]提出的这 3 种模型对恶意节点的信任评估曲线在前 10 h 是持续上升的状态，信任评估均值在 0.67 左右和 0.57 左右，这是由于节点在首次交互时，未识别恶意节点；而在前 10 h 内，本文模型的信任评估曲线在瞬时上升后，呈现持续下降状态，其均值为 0.534，且只有第一次交互时，信任评估值高于初始值 0.5，之后就快速向恶意节点的真实值 0 收敛。这是由于本文模型考虑了服务满意度反馈，当节点提供恶意服务时，该模型可快速将服务满意度评价反馈给下一次信任评估并降低节点之间的关系信任。这也正是本文模型的标准差比其他 3 种模型略小的原因，在识别恶意节点后，所提模型快速进入了正确并稳定的评估状态。从整个实验过程可以观察到，相较文献[11-13]提出的模型，本文模型的均值更低，残差更小，提高了对恶意节点信任评估的准确性。这表明本文模型提高了对恶意节点评估的准确率。文献[11-13]提出的模型及本文模型的平均损失函数值分别为 0.254、0.166、0.112、0.109，本文模型的平均损失函数值最小，与真实曲线拟合程度更高。

从图 4(b)及表 6 可以观察到，在稀疏网络场景下，本文模型评估曲线较为平缓，标准差较小，曲线更接近真实曲线；而文献[11-13]提出的模型的评估曲线波动较大，标准差较大，无法正确稳定地向真实曲线靠拢。这说明在稀疏网络场景中所提模型仍具有快速识别恶意节点、快速进入正确并稳定的评估状态的能力。在整个实验评估过程中，相较文献[11-13]提出的模型，本文模型的均值和残差更小，更接近真实值 0，这说明本文模型提高了对恶意节点信任评估的准确性。文献[11-13]提出的模型及本文模型的平均损失函数值分别为 0.058、0.050、0.032、0.009，本文模型的平均损失函数值更小，与真实曲线拟合程度更高。这说明本文模型在稀疏环境中同样具有适用性。

从图 4 可以看出，无论在一般非稀疏网络场景还是稀疏网络场景下，本文模型都提高了识别恶

表5 非稀疏环境下对恶意节点信任评估分析
Table 5 Analysis of trust evaluation of malicious nodes in non-sparse environment

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文
(1,10)	0.677	0.672	0.574	0.534	0.037	0.037	0.025	0.022	0.677	0.672	0.574	0.534
(11,20)	0.678	0.634	0.53	0.501	0.009	0.025	0.023	0.02	0.678	0.634	0.53	0.501
(21,30)	0.644	0.544	0.449	0.437	0.012	0.026	0.021	0.018	0.644	0.544	0.449	0.437
(31,40)	0.601	0.45	0.377	0.37	0.014	0.03	0.023	0.018	0.601	0.45	0.377	0.37
(41,50)	0.563	0.346	0.31	0.307	0.012	0.028	0.018	0.017	0.563	0.346	0.31	0.307
(51,60)	0.478	0.265	0.251	0.257	0.029	0.021	0.012	0.014	0.478	0.265	0.251	0.257
(61,70)	0.385	0.222	0.212	0.196	0.024	0.007	0.008	0.021	0.385	0.222	0.212	0.196
(71,80)	0.288	0.186	0.177	0.128	0.034	0.023	0.017	0.0217	0.288	0.186	0.177	0.128
(81,90)	0.2	0.108	0.122	0.063	0.012	0.012	0.008	0.01	0.2	0.108	0.122	0.063
-91,100	0.151	0.094	0.113	0.054	0.007	0.001	0.001	0.003	0.151	0.094	0.113	0.054

表6 稀疏环境下对恶意节点信任评估分析
Table 6 Analysis of trust evaluation of malicious nodes in sparse environment

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文模型	文献[11]	文献[12]	文献[13]	本文
(1,10)	0.201	0.35	0.261	0.145	0.046	0.045	0.028	0.116	0.201	0.35	0.261	0.145
(11,20)	0.298	0.324	0.293	0.117	0.032	0.001	0.003	0.001	0.298	0.324	0.293	0.117
(21,30)	0.327	0.311	0.273	0.113	0.001	0.008	0.009	0.005	0.327	0.311	0.273	0.113
(31,40)	0.323	0.274	0.233	0.094	0.005	0.014	0.015	0.007	0.323	0.274	0.233	0.094
(41,50)	0.312	0.216	0.174	0.081	0.02	0.016	0.013	0.002	0.312	0.216	0.174	0.081
(51,60)	0.237	0.163	0.123	0.067	0.018	0.016	0.015	0.004	0.237	0.163	0.123	0.067
(61,70)	0.21	0.114	0.081	0.055	0.019	0.014	0.012	0.003	0.21	0.114	0.081	0.055
(71,80)	0.136	0.068	0.039	0.036	0.016	0.012	0.011	0.006	0.136	0.068	0.039	0.036
(81,90)	0.092	0.045	0.022	0.022	0.002	0.003	0.001	0.001	0.092	0.045	0.022	0.022
-91,100	0.096	0.043	0.02	0.021	0	0	0	0	0.096	0.043	0.02	0.021

意节点的速度和信任评估的准确性。

4.3 动态变化节点信任评估

对随机选取的两组状态动态变化的节点信任值进行实验评估，一组节点所处网络为一般性非稀疏场景，另一组节点所处网络为稀疏场景。被评估节点在前50h表现良好，之后由良好节点转变为恶意节点。将本文模型与文献[11-13]提出的模型进行对比，结果如图5所示。

通过对图5进行数据分析，得出不同时间区间内各个模型对信任评估的均值、残差、标准

差和平均损失函数值，如表7、表8所示。

从图5(a)及表7数据对比可以看出，当节点状态为良好时，本文模型的均值高于其他3种模型的均值，残差更小，其整体评估曲线在其他3个评估曲线上方，更接近真实值1；当节点状态转变为恶意时，本文模型的均值低于其他3种模型的均值，其残差更小，其评估曲线在其他3个评估曲线下方，更接近真实值0。文献[11-13]提出的模型及本文模型的平均损失函数值分别为0.127、0.122、0.096、0.076，本文模型的损失函数值最小，

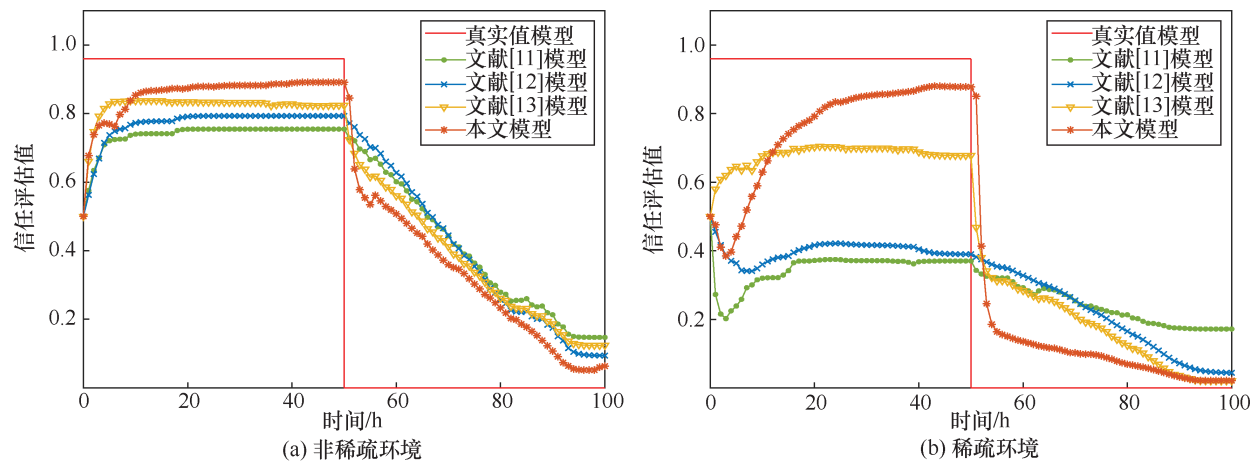


图5 对随机选取一个动态节点的信任评估
Figure 5 Trust evaluation of a randomly selected dynamic node

表7 非稀疏环境下对动态变化节点信任评估分析

Table 7 Analysis of trust evaluation of dynamically changing nodes in non-sparse environments

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文模型	文献[11]	文献[12]	文献[13]	本文模型
(1,10)	0.696	0.711	0.787	0.779	0.05	0.067	0.054	0.048	0.304	0.289	0.212	0.211
(11,20)	0.745	0.781	0.835	0.869	0.005	0.006	0.002	0.004	0.255	0.219	0.164	0.131
(21,30)	0.755	0.793	0.833	0.88	0	0	0.001	0.001	0.245	0.207	0.166	0.12
(31,40)	0.755	0.793	0.83	0.885	0	0	0.003	0.002	0.245	0.207	0.171	0.115
(41,50)	0.755	0.793	0.823	0.891	0	0	0.001	0	0.245	0.207	0.176	0.109
(51,60)	0.667	0.702	0.625	0.581	0.14	0.046	0.047	0.095	0.667	0.702	0.625	0.581
(61,70)	0.515	0.527	0.478	0.427	0.048	0.055	0.044	0.044	0.515	0.527	0.478	0.427
(71,80)	0.353	0.342	0.328	0.295	0.046	0.053	0.042	0.039	0.353	0.342	0.328	0.295
(81,90)	0.244	0.211	0.22	0.167	0.018	0.02	0.021	0.035	0.244	0.211	0.22	0.167
-91,100	0.155	0.108	0.132	0.061	0.014	0.019	0.013	0.012	0.155	0.108	0.133	0.061

表8 稀疏环境下对动态变化节点信任评估分析

Table 8 Analysis of trust evaluation of dynamically changing nodes in sparse environments

指标	模型均值				模型标准差				模型残差			
	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文	文献[11]	文献[12]	文献[13]	本文
(1,10)	0.264	0.372	0.625	0.488	0.04	0.036	0.025	0.08	0.736	0.628	0.375	0.512
(11,20)	0.348	0.392	0.692	0.739	0.022	0.015	0.007	0.04	0.652	0.608	0.307	0.261
(21,30)	0.373	0.419	0.701	0.835	0.001	0.002	0.003	0.013	0.627	0.581	0.299	0.165
(31,40)	0.369	0.413	0.697	0.86	0.003	0.003	0.003	0.005	0.631	0.587	0.303	0.14
(41,50)	0.37	0.392	0.679	0.879	0	0.003	0.002	0.001	0.63	0.608	0.32	0.121
(51,60)	0.318	0.354	0.331	0.258	0.015	0.016	0.053	0.213	0.318	0.354	0.331	0.258
(61,70)	0.277	0.29	0.249	0.116	0.011	0.02	0.019	0.009	0.277	0.29	0.248	0.116
(71,80)	0.227	0.206	0.165	0.088	0.011	0.026	0.025	0.011	0.227	0.206	0.164	0.088
(81,90)	0.187	0.114	0.075	0.05	0.01	0.028	0.028	0.011	0.187	0.114	0.074	0.05
-91,100	0.172	0.05	0.023	0.023	0.001	0.001	0.003	0.002	0.172	0.05	0.023	0.023

这表明与真实曲线拟合程度更高。当节点状态在时刻 50 h 由良性转变为恶意时, 本文模型评估曲线相较于其他 3 种模型, 更快更准确地向新的真实值 0 收敛; 其变化相邻区间的均值由 0.891 下降为 0.581, 均值变化大小为 0.31, 而文献[11-13]提出的模型的均值变化都小于 0.2; 在时间区间(51,60)内, 相较于其他 3 种模型, 本文模型标准差最大 (为 0.213), 反映了本文模型对节点状态变化更敏感。这是因为本文模型在评估信任时考虑到服务满意度反馈影响, 使得该模型可以快速识别恶意节点, 向新的真实值快速收敛。综上分析, 在对动态变化节点进行信任评估时, 本文模型在准确性、敏感性及收敛性方面优于其他 3 种模型。

图 5(b)反映了在稀疏网络场景的信任评估过程中, 本文模型与文献[11-13]的信任评估模型具有较大差异。这是由于网络数据稀疏影响了文献[11-13]模型对节点的信任评估。当节点状态为良好时, 本文模型的均值高于其他 3 种模型的均值, 其残差更小, 更接近真实值 1; 当节点状态转变为恶意时, 本文模型的均值低于其他 3 种模型的均值, 其残差更小, 更接近真实值 0。文献[11-13]提出的模型及本文模型的平均损失函数值分别为 0.245、0.209、0.072、0.053, 本文模型的损失函数值最小, 表明所提模型的评估曲线与真实曲线拟合程度更高, 鲁棒性更好。这说明在稀疏网络场景下对动态变化节点进行信任评估时, 本文模型有效缓解了网络数据稀疏性问题, 提高了信任评估准确性。当节点状态在时刻 50 h 转变为恶意时, 本文模型评估曲线相较于其他 3 种模型, 更快更准确地向新的真实值 0 收敛; 其相邻变化区间的均值由 0.879 下降为 0.258, 均值变化为 0.621, 而文献[11]、文献[12]的均值变化都在 0.05 左右, 文献[13]的均值变化在 0.3 左右, 且在时间区间(51,60)内, 本文模型标准差较大, 这反映了在稀疏场景下, 本文模型对节点状态变化仍然具有较好的灵敏度。

从图 5 可以看出, 无论网络环境是否稀疏, 本文模型提高了对动态变化节点信任评估的收敛速度和准确性, 并且对节点状态变化更敏感。

良好环境下对节点信任评估分析总结如表 9 所示。

表 9 良好环境下对节点信任评估分析
Table 9 Analysis of node trust assessment in a good environment

模型	场景	节点状态	准确性	收敛速度
文献[11]	非稀疏	良好	低	慢
		恶意	低	慢
		动态变化	低	慢
	稀疏	良好	低	慢
		恶意	低	较慢
		动态变化	低	慢
文献[12]	非稀疏	良好	较低	较慢
		恶意	较高	较慢
		动态变化	较低	较慢
	稀疏	良好	较低	较慢
		恶意	较高	慢
		动态变化	较低	较慢
文献[13]	非稀疏	良好	较高	快
		恶意	较低	较快
		动态变化	较高	较快
	稀疏	良好	较高	快
		恶意	高	较快
		动态变化	较高	较快
本文模型	非稀疏	良好	高	较快
		恶意	高	快
		动态变化	高	快
	稀疏	良好	高	较快
		恶意	高	快
		动态变化	高	快

5 结束语

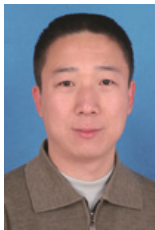
本文提出了一种基于隐性社交关系的社交物联网信任评估模型, 与其他模型不同, 本文通过信任传递算法在建立显性社交关系的同时挖掘并建立节点间隐性社交关系, 使模型在稀疏网络环境中同样适用。本文所提模型将不同种类的社交关系进行融合, 达到将复杂多变的社交关系对信任的影响融入信任评估的目的。实验仿真结果表明, 本文模型无论是在稀疏网络环境还是非稀疏网络环境下, 都具有较好的鲁棒性, 提高了信任评估准确性及收敛性。目前, 本文考虑的信任属性较少, 并且仅考虑了良好环境下复

杂多变的社交关系对信任评估的影响, 如何综合多信任属性对信任评估的影响, 并使信任评估模型在恶意环境下仍能保持较好性能是未来进一步的研究内容。

参考文献:

- [1] KHAN W Z, ARSHAD Q U A, HAKAK S, et al. Trust management in social internet of things: architectures, recent advancements, and future challenges[J]. IEEE Internet of Things, 2021, 8(10): 7768-7788.
- [2] 弭宝瞳, 梁循, 张树森. 社交物联网研究综述[J]. 计算机学报, 2018, 41(7): 1448-1475.
MI B T, LIANG X, ZHANG S S. Review of social internet of things[J]. Chinese Journal of Computers, 2018, 41(7): 1448-1475.
- [3] LUIGI A, ANTONIO I, GIACOMO M, et al. The social internet of things (SIoT)—when social networks meet the internet of things: concept, architecture and network characterization[J]. Computer Networks, 2012, 56(16): 3594-3608.
- [4] ARTZ D, GIL Y. A survey of trust in computer science and the semantic web[J]. Journal of Web Semantics, 2007, 5(2): 58-71.
- [5] ATZORI L, IERA A, MORABITO G. From "smart objects" to "social objects": the next evolutionary step of the internet of things[J]. IEEE Communications Magazine, 2014, 52(1): 97-105.
- [6] PREMARATHNE U S. MAG-SIoT: a multiplicative attributes graph model based trust computation method for social Internet of Things[C]//Proceedings of IEEE International Conference on Industrial and Information Systems (ICIIS). 2017: 1-6.
- [7] EKBATANIFARD G, YOUSEFI O. A novel trust management model in the social internet of things[J]. Journal of Advances in Computer Engineering and Technology, 2019, 5(2): 57-70.
- [8] 盖方宇. 物联网中基于信任管理的安全机制研究[D]. 长沙: 国防科技大学, 2017.
GAI F Y. Research on security mechanism based on trust management in internet of things[D]. Changsha: National University of Defense Technology, 2017.
- [9] WEI L, WU J, LONG C, et al. On designing context-aware trust model and service delegation for social internet of things[J]. IEEE Internet of Things Journal, 2021, 8(6): 4775-4787.
- [10] JAFARIAN B, YAZDANI N, HAGHIGHI M S. Discrimination-aware trust management for social internet of things[J]. Computer Networks, 2020, 178: 107254.
- [11] MEENA KOWSHALYA A, VALARMATHI M L. Dynamic trust management for secure communications in social internet of things (SIoT)[J]. Sādhanā, 2018, 43(9): 1-8.
- [12] CHEN I, BAO F, GUO J. Trust-based service management for social internet of things systems[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(6): 684-696.
- [13] SAGAR S, MAHMOOD A, KUMAR J, et al. A time-aware similarity-based trust computational model for social internet of things[C]//Proceedings of GLOBECOM 2020 Global Communications Conference, 2020: 1-6.
- [14] TRUONG N B, LEE H, ASKWITH B, et al. Toward a trust evaluation mechanism in the social internet of things[J]. Sensors, 2017, 17(6): 1346.
- [15] SAGAR S, MAHMOOD A, SHENG M, et al. Towards a machine learning-driven trust evaluation model for social internet of things: a time-aware approach[C]//Proceedings of MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 2020: 283-290.
- [16] 周双, 宾晟, 邵峰晶, 等. 基于多子网复合复杂网络模型的物质扩散推荐算法[J]. 复杂系统与复杂性科学, 2018, 15(4): 77-84.
ZHOU S, BIN S, SHAO F J, et al. Material diffusion recommendation algorithm based on multi subnet composite complex network model[J]. Complex Systems and Complexity Science, 2018, 15 (4): 77-84.
- [17] 隋毅. 多子网复合复杂网络模型及其相关性质的研究[D]. 青岛: 青岛大学, 2012.
SUI Y. Research on multi subnet composite complex network model and its related properties[D]. Qingdao: Qingdao University, 2012.
- [18] MARCHE C, ATZORI L, IERA A, et al. Navigability in social networks of objects: the importance of friendship type and nodes' distance[C]//Proceedings of IEEE Globecom Workshops (GC Wkshps). 2017: 1-6.
- [19] NITTI M, ATZORI L, CVIJKJ I P. Network navigability in the social internet of things[C]//Proceedings of 2014 IEEE World Forum on Internet of Things (WF-IoT). 2014: 405-410.
- [20] OUECHTATI H, NADIA B A, LAMJED B S. A fuzzy logic-based model for filtering dishonest recommendations in the social internet of things[J]. Journal of Ambient Intelligence and Humanized Computing, 2021: 1-20.
- [21] MARCHE C, ATZORI L, NITTI M. A dataset for performance analysis of the social internet of things[C]//2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). 2018: 1-5.
- [22] 秦琴, 张恒汝. 基于信任传递机制的三支推荐[J]. 模式识别与人工智能, 2020, 33(7): 600-609.
QIN Q, ZHANG H R. Three recommendations based on trust transfer mechanism[J]. Pattern Recognition and Artificial Energy, 2020, 33 (7): 600-609.

[作者简介]



张红斌（1976- ），男，河北赵县人，博士，河北科技大学教授，主要研究方向为网络安全与管理、社交物联网。



刘滨（1975- ），男，河北唐山人，博士，河北科技大学教授，主研方向为大数据、社会计算、人工智能。



樊凡（1998- ），女，河北邢台人，河北科技大学硕士生，主要研究方向为社交物联网与信任。



尹彦（1997- ），女，山东德州人，河北科技大学硕士生，主要研究方向为网络安全与管理。



赵冬梅（1966- ），女，河北深州人，博士，河北师范大学教授，主要研究方向为网络空间安全、人工智能及应用。



刘建（1992- ），男，河北邢台人，河北科技大学硕士生，主要研究方向为社交物联网与访问控制。