

# 面向移动社交网络的动态信任评估

隋涛<sup>1</sup>, 陈荣赏<sup>2</sup>

(1. 厦门理工学院 商学院, 福建 厦门 361024; 2. 厦门理工学院 计算机与信息工程学院, 福建 厦门 361024;)

**摘要:**数百万用户每天在参与移动社交网络互动及相关资源获取, 在没有直接联系的 2 个用户之间建立信任关系, 对于提高移动社交网络服务质量和增强用户安全感方面具有重要的作用. 在分析移动社交网络体系架构的基础上, 设计了一种综合考虑直接信任、推荐信任、信任风险函数、激励机制等多个影响因子的动态信任评估模型, 并对信任值计算方法、信任决策和信任更新等进行分析. 基于真实社交网络数据集 Epinions.com 的实验表明, 本模型的信任值计算准确可信, 且能够有效抵御恶意节点的攻击.

**关键词:**移动社交网络; 动态信任评估; 模型结构; 信任值

**中图分类号:**TP393 **文献标志码:**A **文章编号:**1672-9102(2014)03-0073-06

## Dynamic trust evaluation method for mobile social network

SUI Tao<sup>1</sup>, CHEN Rongshang<sup>2</sup>

(1. School of Business, Xiamen University of Technology, Xiamen 361024, China;

2. School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China)

**Abstract:** For millions of people are joining mobile social networks every day, it is critical to establish trust among the indirectly connected users for improving the quality of mobile social network services and enforcing the security for them. A dynamic trust evaluation model was proposed to calculate and update trust metrics between one user and another user, which was based on direct trust, recommendation trust, trust risk function, motivate mechanism and the framework of mobile social network. Experiments with a dataset from a real social network Epinions.com show that the predicting trust metrics is accurate and the model effectively resist the attacks of malicious nodes.

**Key words:** mobile social network; dynamic trust evaluation; model structure; trust metrics

WLAN 和 WiFi 的普及与智能移动终端设备的低成本化, 促使 PC 端在线社交网络快速向移动社交网络发展, 移动社交应用层出不穷, 且各种移动 APP 中逐渐加入网络社交功能. 移动社交网络 (Mobile Social Network, MSN) 是由具有相同兴趣的个人通过平板电脑、智能手机等设备, 以无线网络服务为基础的一种虚拟互动社群, 包括熟人社交、陌生人社交、兴趣社交、婚恋社交、图片社交等. 与 PC 端在线社交服务相比, 移动社交应用具有人机交互、实时场景等特点, 能够让用户随时随地创造

并分享位置、照片、心情、活动等多种信息, 其他用户通过关注机制可及时获取移动社交网络上的最新信息, 从而构建一个基于移动互联网的人际关系.

艾瑞咨询集团于 2014 年 3 月 11 日发布的《2014 年中国移动社交应用市场研究报告》显示, 我国移动社交网络应用的用户覆盖率已达 60.2%, 成为移动互联网端巨大的网络流量入口. 移动社交网络在移动营销、个性化推荐、信息分享等方面已被广泛应用. 在面对不确定的服务对象和

目标资源时,用户如何准确评估其可信度,防止网络欺诈、敏感信息泄漏等问题,构建安全可信的移动社交网络已成为目前亟待解决的重要问题.为此,本文以移动社交网络服务框架为基础,研究面向移动社交网络的动态信任评估方法,以预测和量化社交网络中的信任关系.

## 1 相关研究

为准确评估社交网络中节点之间的信任关系,学术界针对不同的应用场景提出了一些信任评估方法.文献[1]将社交网络中不同类型的声誉进行融合后计算节点的信任度,并开发了相应的信任计算系统 REGRET.文献[2]结合人类认知行为的特点,提出了一种具有自适应性的动态信任预测模型,基于 IOWA 算子预测直接信任度,提高了信任预测的动态适应能力和准确性.文献[3]利用自信因子综合直接信任和推荐信任的方法评估网络节点的信任度,并引入奖惩机制实现信任关系的动态更新.文献[4]基于节点的外在相似性、信息的可靠性及其反馈信息判断社交网络节点的可信度,但其中部分影响因子权重的确定缺乏理论依据.文献[5]利用直接信任、间接信任、风险函数等关系属性构建了一种多维决策的信任模型,抑制实体的恶意行为,采用经济激励机制鼓励网络实积极参与诚实合作,以准确预测节点的信任度并控制网络交互风险.

社交网络中节点之间存在的利益相关性,可能导致协同作弊和推荐不可信的问题,文献[6]针对分布式网络环境的海量计算节点,提出了一种基于群组信誉的信任评估模型.文献[7]将历史交互窗口和可信推荐数引入信任值计算,构建了一种基于交互感知的动态自适应信任评估模型,并采用实体稳定度实现激励和奖惩,具有较强的抵御伪装实体协同作弊的能力.文献[8]根据每个节点相关的可靠用户群,提出了一种集群信任评估方法,使每个节点可通过设置最大流来识别本地可信用户及其信任级别,利用形成的可信用户群组阻止不可信用户访问个人网络,从而较好地保护个人网络信息.

虽然上述研究的信任关系评估方法考虑了影响信任度的多个因素,并采用奖励和惩罚机制遏制恶意节点的欺诈,但移动社交网络节点的移动性和广泛分布性给信任关系评估提出了新的挑战,影响了现有信任评估模型的准确性.为此,本文从直接信任、推荐信任、信任风险函数、奖惩机制等多个决策因素评估移动社交网络节点的信任度,并根据节点的实时变化动态预测其信任关系,解决信任评估过程中的恶意推荐和协同作弊,提高信任评估的准

确性和时效性.

## 2 移动社交网络的体系结构

在线社交网络中的社会关系很难映射到现实社会中,移动终端设备的泛在性使移动社交网络增加了用户之间随时随地见面沟通的机会,而且可以通过智能手机、平板电脑等方便地参与移动网络社交活动,使得移动社交网络与现实人际关系网络之间的融合更加容易.移动社交网络通常采用客户端/服务器架构(如图1所示),由客户端设备、无线接入网、互联网、服务器端4大模块构成<sup>[9]</sup>.

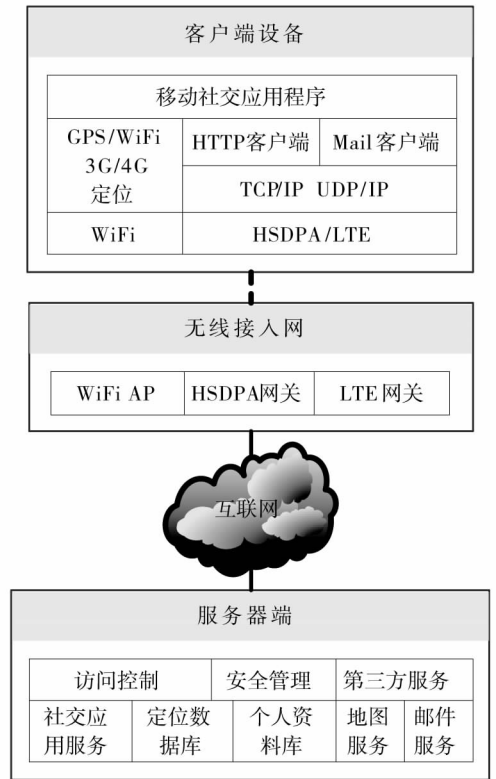


图1 移动社交网络的体系结构

如图1所示,客户端的定位模块用来处理移动终端获取的定位数据和接收服务器端返回的位置服务信息,服务器端包括定位数据库、社交应用服务、访问控制、安全管理、第三方应用服务等.其中,第三方应用服务器主要为移动用户提供E-Mail服务、地图服务等;访问控制与安全管理提供用户身份识别和隐私保护,保证敏感数据信息安全的同时,帮助用户评估其他移动社交网络好友的可信度大小.

## 3 面向移动社会网络的动态信任评估

### 3.1 模型设计

移动社交网络中的信任具有传递性和动态性,

节点间信任关系的评估需要考虑直接信任、推荐信任、信任风险函数、激励机制等多个影响因素. 因此,面向移动社交网络的动态信任评估涉及以下3个基本对象:

1) 目标节点(Service Provider node):移动社交网络中提供资源或服务并被评估的节点,也称为服务提供节点或服务节点,记为 SP.

2) 推荐节点(Service Recommendation node):当 SP 发出信任评估请求时,移动社交网络中为获取相应的利益和信任度而向评估节点推荐服务或资源的节点,记为 SR.

3) 评估节点(Service Requestor node):移动社交网络中对目标节点信任值进行评估的节点,也称为服务请求节点,记为 E.

在移动社交网络中,交互节点之间的信任关系以交互服务为基础. 在信任评估模型中,信任是评估节点 E 对目标节点 SP 可信程度的一种态度和

信念,信任值则是这种信任程度的一种量化. 移动社交网络中推荐的可信程度在很大程度上依赖于推荐节点和评估节点之间的熟悉程度,若推荐节点和评估节点之间存在友好历史交互记录,则评估节点对推荐节点的信任程度高于无好友历史交互记录的推荐节点. 这样,在移动社交网络的评估节点、推荐节点和目标节点之间将形成一种信任推荐关系链,距离评估节点越近的推荐节点,其可信程度越高,反之则越小.

移动社交网络中节点之间的信任关系如图2所示,node1 和 node2 为直接推荐节点,node3 为间接推荐节点,node4, ..., nodei 为陌生推荐节点. 根据人类的认知规律可知,信任程度的评估主要依赖节点间的熟悉程度,如在评估节点 E 对服务节点 SP 的信任程度时,相对 node3 的间接推荐而言,node1 和 node2 的直接推荐信任程度大,node4, ..., nodei 的陌生推荐信任度小.

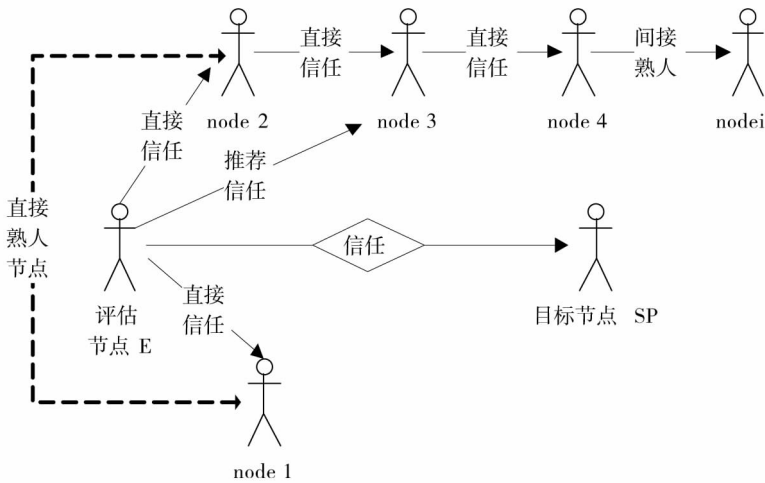


图2 移动社交网络中节点间的信任关系

在移动社交网络中,当评估节点 E 申请目标节点 SP 为其提供服务资源时,节点 E 首先要预测节点 SP 的信任程度,其基本步骤如下:

1) 给每个加入移动社交网络的新节点分配一个初始信任值  $T_0$ , 当新节点经历过一个交互服务之后便开始更新其信任值.

2) 节点 E 根据与节点 SP 历史交互经历的满意度评分、成功和失败的交互次数,计算对节点 SP 的直接信任值;

3) 在节点 E 等待节点 SP 的服务反馈时,接受其直接推荐节点和部分间接推荐节点的推荐服务资源,并根据这些推荐节点推荐信任计算节点 E 对节点 SP 的推荐信任值.

4) 根据节点 E 对信任评估结果的自信程度

(常被称为自信因子  $\lambda(0 \leq \lambda \leq 1)$ ), 对直接信任值和推荐信任值进行综合,得到节点 E 对节点 SP 的综合信任值.

5) 根据综合信任值和信任风险函数判断节点 SP 的服务质量等级,并做出信任决策.

这样,随着移动社交网络节点之间交互活动的发展,不断更新服务请求节点对目标节点信任值的评估,从而形成一种动态更新的信任关系.

### 3.2 信任值的计算

移动社交网络中的服务请求者申请评估目标节点的信任值,以得到可信的服务资源;响应服务请求的目标节点计算服务请求者的信任值,以便将服务资源提供给可信的节点. 目标节点的信任度计算分为以下2个方面<sup>[10]</sup>:一是考虑服务请求节点

对目标节点的评价,即直接信任值(Direct Trust);另一个是考虑推荐节点对目标节点的评价,即推荐信任值(Recommendation Trust)。

### 1) 直接信任值的计算

直接信任是评估节点 E 与目标节点 SP 直接交互所获得的信任值,交互是否成功是评估目标节点 SP 可信度的最直接指标。因此,本文采用成功交互次数作为直接信任值的判断标准,既能解决权重系数确定不科学的问题,又可减少因维度多而造成的计算复杂性问题。依据评估节点 E 与目标节点 SP 历史交互记录确定的直接信任值  $DT_{SP}^E$  为

$$DT_{SP}^E = \frac{S_{SP}^E + 1}{S_{SP}^E + F_{SP}^E + 2} \quad (1)$$

式中,  $S_{SP}^E$  表示评估节点 E 和目标节点 SP 的成功交互次数,  $F_{SP}^E$  表示评估节点 E 和目标节点 SP 的失败交互次数。当评估节点 E 和目标节点 SP 无交互记录时,  $S_{SP}^E = 0, F_{SP}^E = 0$ , 此时评估节点 E 对目标节点 SP 的信任度为 0.5, 表示信任与不信任的程度均为 50%, 与现实相符。

### 2) 推荐信任值的计算

移动社交网络中的每个节点都有其直接信任节点,但当直接信任不足以预测目标节点 SP 的信任值时,就可以考虑与它没有直接交互经验的推荐节点 SR 的推荐信任值。推荐信任值是推荐节点 SR 关于目标节点 SP 信任程度的量化,是由与目标节点 SP 相关的若干个推荐节点关于节点 SP 的信任评估。在计算目标节点 SP 的推荐信任值时,只选择  $n$  个信任值较高的推荐节点进行推荐信任值的评估。为防止因节点信任推荐关系链过长而导致信任值过低,依据移动社会网络的小世界性,规定推荐节点和目标节点 SP 之间的间隔节点数至多为 6 个,即推荐信任之间的节点数不超过 6 个<sup>[11]</sup>。

针对目标节点 SP 的推荐信任值  $RT_{SP}$  可采用式(2)计算。

$$RT_{SP} = \sum_{i,j=1,i \neq j}^n Sim(C_{SP}^i, C_{SP}^j) \times (\sqrt[3]{\alpha \times \omega_{SR}^i \times DT_{SP}^i} + \sqrt[3]{\beta \times \omega_{SR}^j \times DT_{SP}^j}) / n \quad (2)$$

式中,  $RT_{SP}$  表示针对目标节点 SP 的推荐信任值;  $i$  表示节点 SP 信任程度较高的第  $i$  ( $0 \leq i \leq n$ ) 个推荐节点  $SR_i$ ;  $j$  表示与目标节点相关的第  $j$  个评估节点  $E_j$ ;  $C_{SP}^i$  表示推荐节点  $SR_i$  和目标节点 SP 的服务资源;  $C_{SP}^j$  表示评估节点  $E_j$  和目标节点 SP 间的服务资源;  $Sim(C_{SP}^i, C_{SP}^j)$  表示  $C_{SP}^i$  和  $C_{SP}^j$  的相似度;  $\omega_{SR}^i$  和  $\omega_{SR}^j$  分别表示熟人推荐权重和陌生人推荐权重。通常,  $\omega_{SR}^i$  取值为节点  $SR_i$  对节点 SR 的直接信任值

$DT_{SR}^i$ , 而  $\omega_{SR}^j$  的初始值设置为 0.5, 即表示可信与不可信程度相等;  $\alpha$  表示熟人推荐节点对服务提供节点 SP 的信任程度,当节点  $SR_i$  是节点 SP 的直接熟人推荐节点时,取值为  $DT_{SR}^i$ ; 否则,当节点  $SR_i$  是节点 SP 的间接熟人推荐节点时,取值为

$$\alpha = \frac{1}{n} \sum_{N=1}^n \prod_{i \neq j \neq k} DT_{SR}^i \times DT_{SR}^j \quad (3)$$

$\beta$  表示陌生人推荐节点对服务提供节点 SP 的信任程度,  $\beta = \frac{1}{n} \sum_{i=1}^n DT_{SR}^i$ , 当  $\beta = 0$  时,是指该陌生人推荐节点  $SR_i$  为新加入节点或为休眠节点。

### 3) 综合信任值

目标节点 SP 的综合信任值  $T_{SP}$  采用带权去和的方法将直接信任值  $DT_{SP}^E$  和推荐信任  $RT_{SP}$  进行融合获得。设目标节点 SP 关于自身对于信任值判断结果的自信因子为  $\lambda$  ( $0 \leq \lambda \leq 1$ ), 则综合信任值可表示为

$$T_{SP} = \lambda \times DT_{SP}^E + (1 - \lambda) \times RT_{SP} \quad (4)$$

由式(4)可以看出,综合信任值  $T_{SP}$  既体现了目标节点 SP 自身的交互经验,也考虑了与其相关的其他推荐节点的评价。移动社交网络中的节点在交互过程中,直接交互所获得的信任程度通常高于推荐获得的信任程度。

随着目标节点交互次数的不断增加,评估节点 E 更加信任自身与目标节点 SP 之间的直接交互信任,  $\lambda$  的值也将随着节点交互次数  $k$  ( $0 \leq k \leq n$ ) 的递增而增加,即直接信任所占比重将越来越大,推荐信任所占比重则会减小。同时,对于任何一个待评估的目标节点而言,其初始综合信任值为 0.5。因此,利用如式(5)所示的交易影响力函数来确定自信因子为  $\lambda$ 。

$$\lambda(k) = \begin{cases} 1 - \left(\frac{1}{2}\right)^{\frac{k}{n-k}}, & n - k \neq 0; \\ 1, & n - k = 0. \end{cases} \quad (5)$$

式中,  $\lambda(k)$  表示以交互次数  $k$  为变量的动态函数。当  $k = n$  时,表示评估节点 E 和目标节点 SP 间的所有交互均为直接交互,无其他推荐节点的参与,此时  $\lambda = 1$ ; 当  $k = 0$  时,表示评估节点 E 和目标节点 SP 间无直接信任关系,其综合信任值完全依赖于其他推荐节点对目标节点的推荐信任值。

### 3.3 信任风险函数

目标节点 SP 的直接信任值与恶意节点对移动社交网络实施攻击行为的风险密切相关,设评估节点 E 对目标节点 SP 的信任风险计算函数为<sup>[12-13]</sup>

$$Y(E, SP) = 1 - s \times (1 - T_{SP}) \quad (6)$$

式中,  $s$  为目标节点 SP 的服务质量等级(如表 1 所

示), $s$ 的值越大,目标节点 SP 的信任风险就越大;评估节点 E 对目标节点 SP 的信任程度越高,信任风险就越小,即信任风险与服务质量等级成正比.

表1 服务质量等级

信任程度	信任值范围	服务质量等级
完全不信任服务	[0.0,0.4)	1
基本信任服务	[0.4,0.7)	2
大部分信任服务	[0.7,0.9)	3
完全信任服务	[0.9,1.0)	4

加入信任风险函数这个信任评估维度之后,能够精确预测评估节点的交互行为,提高移动社交网络节点之间交互的成功率.

### 3.4 信任决策

计算得到综合信任值  $T_{SP}$  之后,评估节点 E 便可根据自己的信任要求,决定是否与目标节点 SP 进行交互.假设节点 SP 要求与之交互的节点综合信任值必须大于 0.9,则计算得到的目标节点信任值只有大于 0.9 时才会与其进行交互.当然,信任决策是一个双向交互的过程,节点 E 申请获取节点 SP 服务资源的同时,节点 SP 同样也需要决定是否对节点 E 提供服务,如提供即时通信、返回指定数据等.

### 3.5 信任更新

综合信任值  $T_{SP}$  是评估节点 E 根据其目标节点 SP 的历史交互以及自身每次的交互评价,对目标节点 SP 给出的信任评估结果,每次交互历史和交互评价都会对  $T_{SP}$  产生影响,使直接信任值  $T_{SP}$  随时间的推移而不断更新,且时间越近的交互历史和交互评价对本次信任评估的影响越大.此外,当长时间没有交互记录时,信任值应随时间衰减,为此在每次交互的时间窗(time window)中引入时间敏感函数(time sensitive function),体现时间因素对信任值的影响,更好地体现信任关系的动态属性,提高信任值计算的准确性.

将时间轴划分为若干个长度为  $t_0$  的时间窗,假设每经过时间间隔  $|t_0|$  时,综合信任值  $T_{SP}$  就衰减一次.若评估节点 E 加入移动社交网络的时间为  $t_i$ ,对目标节点 SP 进行信任评估的时间为  $t$ ,且  $t > t_i$ ,则此时间间隔内经历了  $k = \left\lfloor \frac{t - t_i}{t_0} \right\rfloor$  个时间窗.设第  $i(i = 1, 2, \dots, k)$  个时间窗的开始时间为  $t_s^i$ ,结束时间为  $t_e^i$ ,节点 E 在  $t_s^i$  时刻对节点 SP 的信任评估值为  $T_s^i$ ,节点 E 在  $t_e^i$  时刻对节点 SP 的信任评估值为  $T_e^i$ ,则时间敏感函数为

$$\text{sen}(T^i) = T_e^i \left[ 1 + \left( \sum_{i=1}^k \frac{T_e^i - T_s^i}{T_s^i} \right) / k \right]. \quad (7)$$

经过式(7)修正之后的信任值,既能作为某一个时间窗内的奖惩机制,也能反应长时间没有新历史交互时信任值随时间衰减的情况.这是因为移动社交网络节点间的交互往往是不对称的,从而使稀缺资源的分配变得不公平,产生以稀缺服务资源为目标的竞争行为,导致一些影响目标节点信任值计算的恶意攻击行为,如对目标节点提交虚假评价信息.在信任评估模型中加入激励机制可增强移动社交网络信任评估的安全性.

## 4 实验过程与分析

### 4.1 数据集预处理

为验证本文所研究的动态信任评估模型的有效性和准确性,我们利用从线社交网络 Epinions.com 上获取的数据集进行实验验证<sup>[14]</sup>.Epinions.com 网站允许用户针对产品进行评分和发布评论,以表达其对相关产品评分和评论的信任程度.Epinions.com 数据集包含 49 290 名用户针对 139 738 个项目发布的 664 824 条评论(其中 487 181 条被标注为可信评论),这些数据分别存储在 ratings\_data.txt 和 trust\_data.txt 2 个文档中.项目评分文档 ratings\_data.txt 包含用户编号(user\_id)、项目编号(item\_id)和对该项目的评分(rating\_value)共 3 个字段,将评分分别为 {1,2,3,4,5} 共 5 种得分,如记录“23 387 4”表示 23 号用户对 387 号项目的评分为 4 分.信任评分文档 trust\_data.txt 包含资源发布者编号(source\_user\_id)、资源申请者编号(target\_user\_id)、信任等级(trust\_statement\_value)共 3 个字段,trust\_statement\_value 的取值范围为 {0,1},如“22 605 18 420 1”表示用户 22 605 信任用户 18 420 的评论.

首先,对 ratings\_data.txt 中的数据按照 item\_id 列进行排序,删除 item\_id 对应评价总数小于 5 的记录,剩余 328 696 条记录;其次,删除 trust\_data.txt 中的用户自评价记录,即 source\_user\_id 值和 target\_user\_id 值相同的记录,剩余 397 862 条记录,防止用户进行信任作弊.

### 4.2 实验分析

为证明本文设计的动态信任评估模型预测结果的准确性,经过多次实验比较分析,当自信因子  $\lambda$  设为 0.8 时,综合信任值的计算结果最优.同时,选取 Epinions.com 数据集中交互次数最多的 4 条边 {A, B, C, D},设恶意节点比例相同,针对本文的信任评估模型 ST、文献[3]中的信任评估模型 JT 和文献[6]中的信任评估模型 HT 分别计算综合信任值  $T$ ,其结果如图 3 所示.

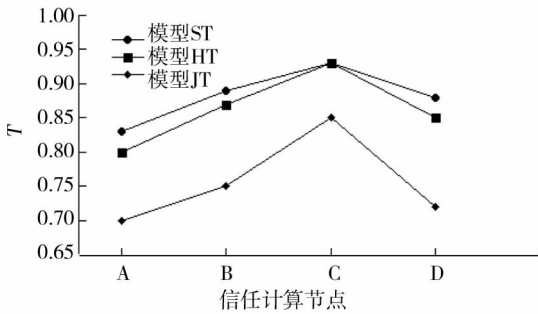


图3 信任计算结果比较

为验证本文信任评估模型的稳定性和健壮性,当恶意节点的比例不同时,针对某一个用户在某个时刻的综合信任值  $T$  进行计算和比较,其结果如图4所示。

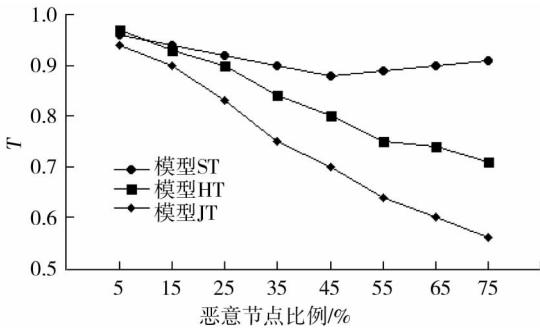


图4 抗恶意节点攻击的比例

由图3所示,在参数取值相同的情况下,本文所研究的动态信任评估模型的信任值计算结果更符合表1所示的服务质量等级,表明本文设计的信任评估模型更可信。图4的实验结果表明随着恶意节点比例的不断增加,综合信任值将会降低,但当恶意节点比例超过45%时,本文信任评估模型计算得到的综合信任值将则会因恶意节点的辨别而缓慢回升,说明本文信任评估模型能够有效识别恶意节点、弱化恶意节点的影响,具有防御大量恶意节点攻击的能力。

## 5 结论

针对现有信任评估模型在客观性和准确性方面的不足,设计了一种面向移动社交网络的动态信任评估模型,并对其设计思想和工作原理进行分析论述,最后采用社交网络信任数据集 Epinions.com 进行实验分析和比较。实验结果表明,本模型可以根据交互历史记录和间接推荐信任准确计算用户之间的可信度,降低恶意攻击节点对信任值计算的影响,具有较高的可靠性和稳定性。本信任评估模型通过用户之间的相互协作实现目标用户信任值的计算,预测和鉴别恶意用户的攻击行为,提高了移动社交网络的安全防御能力,促使用户主动遵守相关网络行为规范,有助于构建安全可信的移动社

交网络服务。如何结合移动社交网络中的动态信任评估模型提供个性化推荐服务,提高移动社交网络中资源和服务推荐的准确性和有效性是下一步需研究的重要问题。

## 参考文献:

- [1] Sabater J, Sierra C. REGRET: Reputation in gregarious societies [C]//Proceedings of the 15th International Conference on Autonomous Agents. Montreal: ACM Press, 2001.
- [2] 李小勇,桂小林. 动态信任预测的认知模型[J]. 软件学报,2010, 21(1):163-176.
- [3] 甘早斌,丁倩,李开. 基于声誉的多维度信任计算算法[J]. 软件学报,2011,22(10):2401-2411.
- [4] Zhan J, Fang X. A novel trust computing system for social networks [C]//Proceedings of the 2011 IEEE International Conference on Privacy, Security, Risk and Trust. Boston: IEEE Computer Society, 2011.
- [5] 罗柏发,蔡国永. 一种基于社会网络的激励兼容的信任模型[J]. 计算机应用研究,2011(5):1932-1936.
- [6] Robson O A, Luis J V, Tai H K. Gtrust: group extension for trust models in distributed systems[J]. International Journal of Distributed Sensor Networks,2014(2):1-9.
- [7] 李峰,申利民,司亚利,等. 基于交互感知的动态自适应的信任评估模型[J]. 通信学报,2012(10):60-70.
- [8] Samah A O, Heung N K, Abdulmoteleb E S. A group trust metric for identifying people of trust in online social networks[J]. Expert Systems with Applications, 2012,39(18):13173-13181.
- [9] Wu Z, Zhang C H, Ji Y. Towards cloud and terminal collaborative mobile social network service [C]// IEEE International Conference on Social Computing. Minneapolis: IEEE Computer Society, 2011.
- [10] Young A K, Hee S S. Strategies for predicting local trust based on trust propagation in social networks [J]. Knowledge-Based Systems, 2011(24):1360-1371.
- [11] Giangiacomo B, Flaminio S, Riccardo B. Trust and partner selection in social networks: an experimentally grounded model [J]. Social Networks, 2012(34):481-492.
- [12] Sanjog R, Ambuj M. Improving prediction accuracy in trust-aware recommender systems [C]//43rd Hawaii International Conference on System Sciences. Honolulu: IEEE Computer Society, 2010.
- [13] 刘彦宾,李丽琼. 基于模糊理论的P2P电子商务信任评估模型[J]. 湖南师范大学自然科学学报, 2013,36(1):34-38.
- [14] Massa P, Avesani P. Trust-aware bootstrapping of recommender systems [C]//Proceedings of ECAI Workshop on Recommender Systems. Minneapolis: ACM New York,2006.