

面向无线自组网的分布式信任管理模型

魏德健, 贾智平, 李 新

(山东大学 计算机科学与技术学院, 济南 250101)

(icefire01@163.com)

摘 要:针对无线自组网的安全问题,提出了一种适用于无线自组网的新的信任管理模型。引入风险值,使模型对恶意行为更加敏感,有利于减少节点行为的突然变化给系统带来的危害。同时,把文件权重因子引入直接信任值计算,有效预防了通过积累信誉实施恶意行为的情况。仿真实验及分析表明,此模型可以有效识别恶意节点,与无信任模型的无线自组网相比,恶意交易的数目明显降低。

关键词:无线自组网;文件共享;信任评估;风险评估

中图分类号: TP393.08 **文献标志码:** A

Distributed trust model in wireless Ad Hoc networks

WEI De-jian, JIA Zhi-ping, LI Xin

(School of Computer Science and Technology, Shandong University, Jinan Shandong 250101, China)

Abstract: For the security of wireless Ad Hoc networks, a new trust model was proposed in this paper. Due to the introduction of risk element, the model becomes more sensitive to malicious behaviors and more immune to the sudden changes of nodes' behaviors. Meanwhile, as a result of direct trust computation with weights assigned to files, it is effective to prevent malicious behaviors implemented through the accumulation of reputation. Subsequent experiments show that, compared with wireless Ad Hoc networks without trust model, the proposed model can identify malicious nodes effectively and reduce the number of bad transactions notably.

Key words: wireless Ad Hoc network; file-sharing; trust evaluation; risk evaluation

0 引言

无线自组网是指一组带有无线收发装置的节点组成的一个多跳的无中心化自治网络^[1]。网络中的节点同时扮演客户端和服务器的角色,也可以实现路由器功能。因此无线自组网是一种典型的对等网络。随着无线网络的日益发展,无线自组网越来越受到人们的青睐,应用也越来越广泛。文件共享机制就是无线自组网上的一个重要应用^[2]。以电表采集器为例,一个小区中每个楼内都安装了一个支持 ZigBee 通信的电表采集器,这些电表采集器就形成了一个无线自组织网络。如果电表采集器需要进行系统升级,它可以先向已升级过的电表采集器发送升级文件下载请求,而无需通过上位机进行系统升级。但是,由于无线自组网开放、无中心化等特性使恶意节点可以任意地加入网络,通过提供恶意服务给其他节点造成损失。在传统网络中,信任关系的建立可以依靠可信第三方,然而无线自组网中节点之间是对等的,不存在可信第三方。针对以上对等网络中存在的安全问题,信任管理模型被提出。研究表明,信任管理模型可以有效地解决这些安全问题。

1 相关工作

信任管理的概念是 1996 年由 Matt Blaze 提出的^[3]。根据信任建立的方式不同,信任管理模型可以分为基于策略和基于声誉的信任管理模型。

基于策略的信任管理模型是通过凭证建立信任关系的。一个节点对其他节点的信任度量值只有信任或不信任两种,非 0 即 1。这种信任模型得出的结论太绝对,不符合现实情况的需要。当今主要的研究方向是基于声誉的信任管理模型。

基于声誉的信任管理模型是通过评估交易历史和推荐信任信息建立信任关系的。一般信任值位于 $[0,1]$ 或 $[-1,1]$ 区间,这样更能准确地反映节点的可信度。文献[4]提出了一个基于矩阵迭代的全局信任模型,每个节点利用自己的交易历史记录计算出对其他节点的本地信任值,然后通过矩阵迭代扩大节点的信任范围,最终形成节点的全局信任值。但是,全局信任模型^[5-7]没有考虑信任的私人化特点,忽略了不同节点对同一个节点信任评价的差异;而且,全局信任模型计算量太大,在大规模对等网络中是否有必要计算全局信任值有待进一步研究。

文献[8]提出的 PeerTrust 模型引入了相似度的概念。节点对于其他不同节点的推荐信息赋予不同的权重,与自己看法一致的节点所提供的推荐信息赋予的权重大,与自己看法不一致的节点所提供的推荐信息赋予的权重就小。文献考查了交易满意总数、总交易次数、交易评价可信度、交易上下文和社区上下文五个因子。该模型首次提出了相似度概念,更加符合现实社会中的信任机制;同时,该模型比较全面地考虑了信任模型中所涉及的因素。实验结果表明 PeerTrust 模型具有良好的表现。

收稿日期:2010-06-21;修回日期:2010-08-06。

基金项目:国家自然科学基金资助项目(90718032;60903031);中国博士后科学基金资助项目(20090451310)。

作者简介:魏德健(1985-),男(回族),山东德州人,硕士研究生,主要研究方向:嵌入式系统;贾智平(1964-),男,山东即墨人,教授,博士生导师,主要研究方向:嵌入式系统、分布式控制网络、实时系统;李新(1978-),男,山东济南人,讲师,博士,主要研究方向:实时系统、数据流处理、嵌入式系统。

文献[9]首次在信任模型中引入了风险值的概念,考虑了信任值计算中的不确定因素,体现了信任的动态性特征。本文在计算风险值时借鉴了该文献的风险评估方法。

前面所提到的信任管理模型主要是应用于 P2P 网络,目前国内对无线自组网信任管理模型的研究还处于初级阶段。因此本文根据 P2P 网络中信任模型的理论知识和无线自组网本身的特点,提出了一种适用于无线自组网的信任管理模型 SoTrust。该模型利用节点自身的交易记录和其他节点的推荐信息,从直接信任值、间接信任值和风险值三个方面综合考虑,得出节点的最终信任值。在计算直接信任值时,模型考虑了时间因子和文件权重因子,使节点能更准确地计算对方节点的直接信任值。由于无线自组网中资源有限,模型中设置了三个参数以减少节点间的交互次数和模型所占用的存储空间。实验表明,该模型可以有效识别恶意节点,与无信任模型的无线自组网相比,恶意交易的数目明显降低。

2 信任模型

在 SoTrust 中,节点 i 对节点 j 的信任决策依据最终信任值。最终信任值包括综合信任值和风险值,而综合信任值来自于直接信任值和间接信任值。具体结构图如图 1 所示。

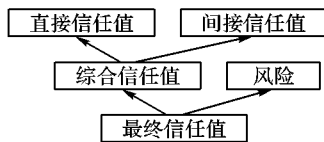


图 1 信任结构图

2.1 综合信任值计算

综合信任值是从信任的正面考虑节点的信任度的,它反映了一个节点通过自己和其他节点的交易历史得出的对某一节点信任值的期望。从图 1 可以看出,综合信任值包括直接信任值和间接信任值两个部分,下面本文将分别介绍这两部分的度量过程。

2.1.1 直接信任值计算

定义 1 交易。网络中两个节点之间发生一次交互为一次交易。本文是以无线自组网文件共享机制为背景的,因此在本文中一次交易代表一次文件下载^[10]。

定义 2 直接信任值 TD_{ij} 。节点 i 通过分析计算节点 j 作为服务提供方时两个节点之间的历史交易信息得出对节点 j 的直接信任值。

那么,为方便获取交易信息,每个节点都要保存一个交易记录表,如表 1 所示。

表 1 交易记录表

节点	评价	时间区间	文件权重	跳数
i	-0.7	5	1	3
j	0.8	6	2	4

从表 1 中可以看出,交易信息包括交易节点、评价、时间区间、文件权重和跳数。其中,跳数用于决策机制,即当多个节点满足信任条件时,选择距离近的节点进行交易。表 1 中列举了两条交易记录,其中第一条记录表示在第 5 个时间区间里,从节点 i 下载了一个文件权重为 1 的文件,根据文件质量给予节点 i 的评价为 -0.7,到达节点 i 的跳数为 3。

在实际环境中,服务节点所提供的下载文件质量是不相同的。因此,两个节点之间每完成一次交易,请求服务节点就会根据文件质量给予提供文件节点一个评价。为了量化该评

价,本文定义了一个评价映射函数,如式(1)所示:

$$r(x) = \begin{cases} 0.8, & x = G \\ 0.5, & x = C \\ -0.3, & x = U \\ -0.7, & x = I \\ -0.9, & x = M \end{cases} \quad (1)$$

根据质量把文件分为五类, G 表示下载的文件完全符合要求, C 表示文件质量一般或者有延迟, U 表示对方无响应, I 表示对方提供的是不真实文件, M 表示对方提供的是恶意文件^[11]。针对这五类文件质量,本文在区间 $[-1, 1]$ 内选取了 5 个相应的值,如式(1)所示。

评价对于直接信任值的影响随着时间的推移越来越小,因此本文定义了一个衰减函数,通过此衰减函数可以更加准确地反映历史评价对信任值计算的影响。衰减函数如下:

$$t(i) = \rho^{t_{\text{now}} - t_i} \quad (2)$$

其中 $t(i)$ 表示第 i 次交易的时间权重, ρ ($0 < \rho < 1$) 代表时间因子, t_{now} 表示当前所处的时间区间(本文中时间区间的长度为 1s), t_i 表示第 i 次交易所处的时间区间。在同一个时间区间内的交易,所赋予的时间权重是一样的。

从衰减函数的表示形式可以看出,所发生交易距离当前时刻越远, t_i 越小,则 $t(i)$ 就越小,相应的,该交易所带来的影响就越小;反之,所发生交易距离当前时刻越近, t_i 越大,则 $t(i)$ 就越大,相应的,该交易所带来的影响就越大。

在实际交易过程中,不仅文件质量是不相同的,而且文件的重要性也是有差别的。因此,可以认为针对重要性高的文件所实施的恶意行为带来的危害会更大。为了防止恶意节点通过对重要性低的文件提供良好服务来积累信誉,从而在提供重要性高的文件时实施恶意行为,本文定义了文件权重映射函数,如式(3)所示:

$$c(x) = \begin{cases} 0.5, & x = U \\ 1, & x = C \\ 2, & x = I \end{cases} \quad (3)$$

其中 U 表示不重要文件, C 表示一般文件, I 表示重要文件。SoTrust 中,不重要文件赋予的权重为 0.5,一般文件赋予的权重为 1,重要文件(例如固件升级文件等)赋予的权重为 2。计算直接信任值时,降低了不重要文件的影响,提高了重要文件的影响。

综合考虑时间权重和文件权重,得出节点 i 对节点 j 的直接信任值为:

$$TD_{ij} = \frac{\sum_{k=1}^M r_k(x) c_k(x) t(k)}{\sum_{k=1}^M c_k(x) t(k)} \quad (4)$$

式中 M 表示节点 i 作为服务请求者与节点 j 发生交易的次数。

2.1.2 间接信任值计算

定义 3 间接信任值 R_{ij} 。节点 i 通过整合曾经交易过的节点的推荐信息而计算出的节点 j 的信任值。

假设 诚信服务节点所提供的推荐信息也值得信赖。

在计算间接信任值之前,节点 i 要询问邻居节点对节点 j 的评价。节点 i 对节点 j 的间接信任值为:

$$R_{ij} = \frac{\sum_{k \in \text{Set}(i)} TD_{ik} \times TD_{kj}}{\sum_{k \in \text{Set}(i)} TD_{ik}} \quad (5)$$

式中 $\text{Set}(i)$ 表示与节点 i 交易过且达到信任阈值 φ 的节点集

合。如果节点 k 与节点 j 交互过,则反馈推荐信息;否则,不反馈任何信息。我们规定,当节点 i 向节点 k 询问其对节点 j 的评价时,节点 k 会把对节点 j 的直接信任值反馈给节点 i ,但是节点 i 对这个反馈信息不是完全信任的,节点 i 用对节点 k 的直接信任值作为此反馈信息的可信度。

在得到直接信任值和间接信任值的基础上,计算出节点 i 对节点 j 的综合信任值,如下所示:

$$T_{ij} = \alpha TD_{ij} + (1 - \alpha) R_{ij} \quad (6)$$

其中 $\alpha (0 \leq \alpha \leq 1)$ 表示直接信任权重。当 $\alpha = 0$ 时,表示节点 i 与节点 j 之间没有交易历史,综合信任值完全来自于间接信任值;当 $\alpha = 1$ 时,表示节点 i 只考虑自己的历史交易记录。

2.2 风险值计算

综合信任值是对过去行为的一个累加值,它反映了服务请求者对服务提供者正面的评价。但是,由于计算间接信任值需要一定的时间,综合信任值很难有效地反映节点行为的突然变化。为此,本文引入了风险值来解决这一问题。

定义4 风险值 RI_{ij} 。节点 i 依据与节点 j 的交易历史记录所计算出的节点 j 行为的风险值。

风险值的计算公式如下所示:

$$RI_{ij} = \frac{r(U)N_1 + r(I)N_2 + r(M)N_3}{r(M)N} \quad (7)$$

式中 U 、 I 和 M 分别表示式(1)所列的三种不良交易, $r(U)$ 、 $r(I)$ 和 $r(M)$ 分别表示这三种不良交易所对应的评价, N_1 、 N_2 和 N_3 分别表示三种不良交易发生的次数, N 表示节点 i 和节点 j 发生交易的总次数。

从式(7)中可以看出,我们把风险值标准化到最坏情况,也就是说,把所有不良交易带来的影响占所有交易是最坏交易时所带来影响的比重作为风险值。

通过引入风险评估,信任模型对恶意行为更加敏感,可以更快地发现恶意节点,从而降低恶意交易带来的损失。从另一方面来看,引入风险评估也是对恶意行为的一种惩罚机制。因为在计算直接信任值时已经考虑过恶意行为带来的影响,在评估风险值时再次考虑恶意行为带来的影响,能够放大恶意行为的危害。这样,也符合信任值升慢降快的特点。

2.3 最终信任值计算

定义5 最终信任值 $T_{\text{final}}(i, j)$ 。节点 i 依据最终信任值决定是否与节点 j 进行交易。

前面已经计算出综合信任值和风险值,通过整合这两者,得出最终信任值,如下所示:

$$T_{\text{final}}(i, j) = (1 - \beta) T_{ij} + \beta(1 - RI_{ij}) \quad (8)$$

其中 $\beta (0 \leq \beta \leq 1)$ 表示风险权重。节点 i 会用式(8)所得出的最终信任值与自身的可信阈值(γ)做比较,当 $T_{\text{final}}(i, j) \geq \gamma$ 时,文件请求发生;否则,文件请求不发生。

2.4 参数设置

由于 SoTrust 是应用于无线自组网,为了适应无线自组网资源有限的特点,本文设置了三个参数。

1)有效期 S 。当一个节点计算直接信任值时只考虑有效期内的交易,即距离当前时刻 S 个时间段内的交易。交易记录表中也只保存有效期内的交易信息,超过有效期的交互信息将被删除。由于距离当前时刻太远的交易所对应的时间因子很小,其所起到的影响也随之变小,为了节省存储空间和计算时间,模型只考虑有效期内的交互信息。

2)交易次数阈值 N 。在有效期内,如果两个节点之间的交易次数(对于节点 i 来说,它只记录其作为请求服务节点时的

交易信息,所以交易次数也就是 i 作为请求服务节点时的交易次数)达到 N ,那么节点 i 就不再计算节点 j 的间接信任值了。由于计算信任值时,网络中节点之间的通信大部分来自于间接信任值计算时推荐节点与请求节点之间的信息通信。这样就大大减少了网络中节点之间的通信量。

3)信任阈值 φ 。节点 i 在收集推荐信息时,只询问那些到达信任阈值的邻居节点。因为节点通常不相信信任值低的节点,所以可以认为没有达到信任阈值的节点所给出的推荐信息对间接信任值的影响很小,可以忽略不计。这样可以有效减少网络中无效信任的反馈,降低节点间的通信量,以满足无线自组网中带宽有限的特点。

3 仿真及结果分析

为了验证模型的有效性,本文采用了一款使用非常广泛的多功能仿真软件 NetLogo^[13] 构建模拟无线自组织网络进行仿真实验。NetLogo 仿真软件是一个多主体可编程建模平台,它提供了友好的交互界面,可以通过调节参数来形成不同配置环境^[12]。

3.1 实验环境

实验根据节点的行为把节点分为良好节点和恶意节点两种。良好节点是指始终提供良好服务的节点,而恶意节点是指根据不同的文件提供不同比例恶意服务的节点。对于不重要文件,恶意节点总是提供良好服务,以便积累信誉;对于一般文件,恶意节点会有 80% 的概率提供恶意服务;对于重要文件,恶意节点总是提供恶意服务。实验中节点个数可以由 NetLogo 控件进行改变,其中恶意节点的个数由恶意节点比例决定。

本实验把实验参数分为固定参数和可变参数两种。首先在实验前设置好固定参数,然后通过更改可变参数查看并分析模型的表现。

固定参数设置如下所示: $\alpha = 0.8$, $\beta = 0.3$, $\varphi = 0.6$, $\gamma = 0.5$, $\rho = 0.9$, $S = 5$, $N = 5$ 。

可变参数为系统中恶意节点的比例,可以通过调节恶意节点比重控件更改此参数。

节点间进行一次交易称为一步,实验中设置系统运行 2200 步。为了便于仿真,假设每步中每个节点有 50% 的概率发送服务请求。

3.2 实验结果分析

在实验中,本文将从服务质量和系统损失两个方面对模型进行分析。在此之前,先说明一下良好服务和恶意服务的含义。良好服务是指文件质量为 G 和 C 的交易。恶意服务是指文件质量为 U 、 I 和 M 的交易。在 SoTrust 信任模型中,节点初始信任值设为 0.5。

3.2.1 服务质量分析

实验将从良好服务和恶意服务所占比例度量服务质量。

在节点个数为 30,恶意节点比例占 30% 的情况下,具有信任模型的系统中良好服务所占比例比没有信任模型的系统中良好服务所占比例明显高。相应地,恶意服务所占比例明显要低。这点可以从图 2 中表现出来。

在其他参数不变的情况下,把恶意节点比例提高到 50%。从图 3 看出,没有信任模型的系统中良好服务所占比例明显降低,而具有 SoTrust 信任模型的系统中随着步数的增多,良好服务的比例会逐步增加,最终会达到和图 2 同样的比例。反观恶意服务,在没有信任模型的系统中所占比例明显提高,而在具有 SoTrust 信任模型的系统中所占比例随着步数

的增加会逐渐降低。原因在于,随着交易的发生,恶意节点已被发现,与恶意节点的交互越来越少,恶意交易也随之减少。

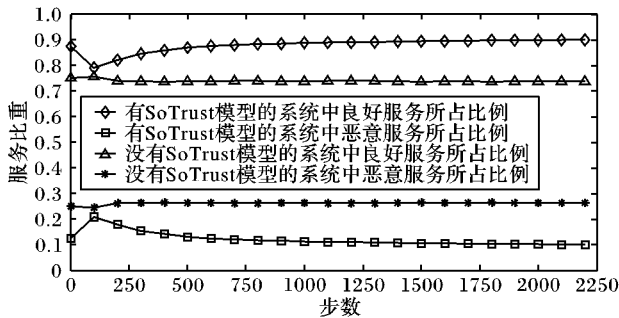


图2 30% 恶意节点存在时服务质量对比

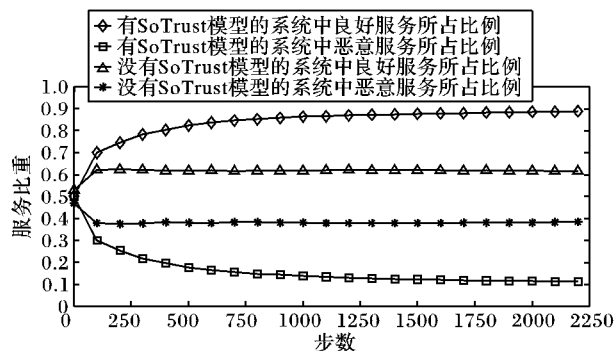


图3 50% 恶意节点存在时服务质量对比

3.2.2 系统损失分析

为了形象地说明系统损失,假定如果下载的文件质量为 U ,系统损失 1 个单位;如果下载的文件质量为 I ,系统损失 2 个单位;如果下载的文件质量为 M ,系统损失 3 个单位。

从图 4 可以看出,在 30% 恶意节点存在时,无信任模型的网络中系统损失最终接近 180,而在具有 SoTrust 信任模型的网络中系统损失只有不到 30,系统损失率降低了 83.3%。

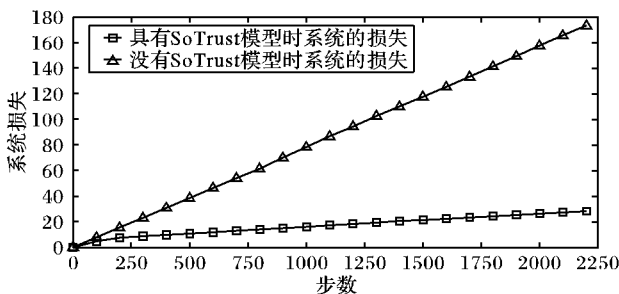


图4 30% 恶意节点存在时系统损失对比

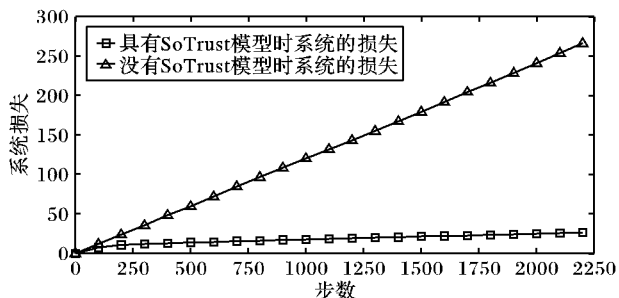


图5 50% 恶意节点存在时系统损失对比

然后,把网络中恶意节点的比例提高到 50%,如图 5 所示,可以看出具有 SoTrust 信任模型的网络中,系统损失一直维持在 30 左右,而无信任模型的网络中,系统损失上升到了 270。与存在 30% 恶意节点的网络相比,系统损失率增加了 58.8%。这是因为,通过前期的信任建立过程,节点间已经建

立了信任关系,恶意节点也已经被发现,之后的交易基本都是发生在可信节点之间,而可信节点之间的交易都是良好交易,所以系统损失不会再升高了。

从实验中可以看出,应用 SoTrust 信任模型可以提高网络中良好服务的比例,降低恶意服务的比例;同时可以把系统损失维持在一个较低的水平,而且随着恶意节点的增加,系统损失不会出现大幅度的增加。

4 结语

针对无线自组网的安全问题,本文提出一种适用于无线自组网的信任管理模型 SoTrust,该模型考虑了文件的重要性,引入了风险值,并且加入了适应无线自组网的参数阈值。实验表明,SoTrust 模型提高了网络的服务质量,降低了系统损失。但是,由于引入了信任管理模型,系统的时间和空间开销都大幅度增加了。在今后的研究中,我们将努力降低模型运行的时间和空间开销,使该模型能表现出更好的效果。

参考文献:

- [1] 叶阿勇,马建峰.一种移动自组网中信任评估模型的设计[J].计算机研究与发展,2008,45(5):765-771.
- [2] DING GANG, BHARGAVA B. Peer-to-peer file-sharing over mobile Ad Hoc networks [C]// Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. Washington, DC: IEEE Computer Society, 2004: 104.
- [3] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management [C]// Proceedings of the 1996 IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 1996: 164-173.
- [4] KAMVAR S D, SCHOLSSER M T, GARCIA-MOLINA H. The eigentrust algorithm for reputation management in P2P networks [C]// Proceedings of the 12th International Conference on World Wide Web. New York: ACM, 2003: 640-651.
- [5] 张骞,张霞,文学志,等. Peer-to-Peer 环境下多粒度 Trust 模型构造[J].软件学报,2006,17(1):96-107.
- [6] SONG S, HWANG K, ZHOU R. Trusted P2P transactions with fuzzy reputation aggregation [J]. IEEE Internet Computing, 2005, 9(6): 24-34.
- [7] REPANTIS T, KALOGERAKI V. Decentralized trust management for Ad-Hoc peer-to-peer networks [C]// MPAC 2006: Proceedings of the 4th International Workshop on Middleware for Pervasive and Ad-Hoc Computing. New York: ACM, 2006: 6.
- [8] LI XIONG, LING LIU. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [9] LIANG ZHENGQIANG, SHI WEISONG. PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing [C]// Proceedings of the 38th Hawaii International Conference on System Sciences. Washington, DC: IEEE Computer Society, 2005: 201-202.
- [10] 彭冬升,林闯,刘卫东.一种直接评价节点诚信度的分布式信任机制[J].软件学报,2008,19(4):946-955.
- [11] 田春岐,邹仕洪,王文东,等.面向 P2P 网络应用的基于声誉的 Trust 管理模型[J].通信学报,2008,29(4):63-70.
- [12] LIANG ZHENGQIANG, SHI WEISONG. Analysis of ratings on trust inference in open environments [J]. Performance Evaluation, 2008, 65(2): 99-128.
- [13] Netlogo [DB/OL]. [2010-06-08]. <http://ccl.northwestern.edu/netlogo/>.