基于增强稳定组模型的移动 P2P 网络信任评估方法

吴 旭

(西安邮电大学计算机科学与技术系 西安 710121)
(西安交通大学计算机科学与技术系 西安 710049)

摘 要 目前,已经有许多文献给出了移动 P2P 网络环境下信任管理技术与具体应用的集成方案.现存的信任模型都存在一个共同的假设,即假设信任信息都来自于稳定的网络拓扑结构环境下,且这些信任信息能够被保证长期有效.然而移动 P2P 网络由于节点频繁的加入和退出造成网络拓扑结构不断变化,不可能保证建立的信任信息长期有效.因此,已有的信任管理系统在这种移动环境下已经不再适用,迫切需要提出新的解决方案.通过研究移动 P2P 节点的信任关系的变化与网络使用者的兴趣、爱好等变化的对应关系,该文提出了一个基于增强的稳定组模型(Enhanced Stable Group Model-based Trust Evaluation Method,SGTM)的信任评估方法,并给出了稳定组构造算法.该机制利用稳定组构造算法对移动 P2P 网络进行有效地分组,相同分组内的节点之间相对保持最大程度的拓扑结构的稳定,从而保证组内节点信任关系的稳定存在.文中在移动环境下对移动模式和信任管理之间的关系问题进行了详细的研究.模拟实验从动态适应力、全局信誉的收敛时间以及全局信任计算所涉及的通讯负载等方面对所提出的信任评估方法的性能进行了评估.

关键词 移动 P2P 网络;信任模型;移动性;稳定组
中图法分类号 TP393 **DOI 号** 10.3724/SP.J.1016.2014.02118

Enhanced Stable Group Model-Based Trust Evaluation Scheme for Mobile P2P Networks

WU Xu

(*Department of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an* 710121)
(*Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an* 710049)

Abstract Although many researchers have studied the establishment and maintenance of trust in mobile P2P networks, the existing approaches to trust establishment usually require a lengthy process and assume long term validation. In contrast, few of these characteristics are prevalent in mobile P2P networks with their unreliable transmission medium, frequent topology changes and variable network lifetimes. Since those solutions developed mainly for the fixed wired networks are not fit in such a scenario, new security solutions are eagerly in demand. In this paper, we propose an Enhanced Stable Group Model-based Trust Evaluation Method (SGTM). Stable group is introduced in collecting trust evidences phase to simplify the process of trust initialization. In the scheme, all group members that move in a similar pattern remain throughout the entire communication session. By doing this, the topology within a group is less dynamic. Since trust evidences of a sensor are main collected in the stable group, the average length of trust chains is much shorter and more robust than other models, and avoids trust dilution. The simulation results prove the effectiveness and the benefits of the proposed model.

Keywords mobile P2P networks; trust model; mobility; stable group

收稿日期:2014-05-10;**最终修改稿收到日期**:2014-07-15.**本课题得到国家自然科学基金**(61373116)、**陕西省自然科学基金**(2011JQ8006)、**陕西省教育厅科研计划项目**(2013JK1132)**资助**.**吴 旭**,**女**,1978 **年生**,**博士**,**副教授**,**主要研究方向为可信计算、普适计算、移动计算和软件工程**. E-mail: xrdz2006@163.com.

1 引　言

信任管理问题是移动 P2P 网络不可忽视的重要问题，信任管理是对传统安全机制的有效补充，是解决移动 P2P 网络中安全问题的有效途径. 传统的网络安全手段专注于信息的保密性和完整性，通过身份鉴别、完整性认证、授权、加密、访问控制和审计等技术的综合应用贯彻安全策略，以网络为对象实施安全防护和入侵检测. 这样的网络安全体系在防护能力、应用范围上存在着局限性. 此外，传统的安全手段也无法解决 P2P 应用中匿名实体之间合作所面临的信任和激励问题. 因此在节点之间建立信任机制，创造一个透明有序的交易环境显得非常有意义. 随着新的网络应用模式的出现，在 P2P、移动自组网、传感器网络和云计算等领域中的信任和信誉机制也成了研究的重点. 目前已经有许多文献给出了 P2P 环境下信任管理技术与具体应用的集成方案，如服务选择、路由等，为节点的协作决策提供信任支持. 这些方案对 P2P 网络的信任管理系统的研究主要集中于对节点进行信任值评估，借助信任值评估增强网络的安全性、健壮性等方面. 比如 Firdhous 等人[1]提出的信任度计算机制以及 Abawajy[2]提出的分布式的构架. 为了过滤恶意推荐，该构架给不同评价者的反馈值分配了一个适当的权重. 虽然该方法通过实验证明了其对节点的反馈行为能够进行有效地监管，但是它需要一个信任中心来收集所有的反馈，存在很大的安全隐患. 类似的方法还包括：方恩光等人[3]为解决信任量化和不确定问题，利用证据理论对信任及信任行为进行建模；谢晓兰等人[4]提出一种基于双层激励和欺骗检测的信任模型；通过引入一组服务属性评价指标，建立对服务提供商服务行为和用户评价的双层激励机制；杜瑞忠等人[5]提出的基于信任和个性偏好的服务选择模型. 在社会网络中，信任关系是人际关系的核心，个体间的信任度往往取决于其他个体的推荐，即基于第三方推荐的间接信任，同时，推荐者的可信度也决定其推荐个体的可信度. 实际上，这种互相依赖的信任关系组成了一个所谓的信任网络(Web of Trust). 在这样的信任网络中，任何个体的可信度都不是绝对可靠的，但可以作为其他个体决定其交互行为的依据. 基于信誉的 P2P 信任模型是现在研究信任模型的焦点所在，也有了较多的科研成果. 比如 Pawar 等人[6]提出的基于信誉的信任模型被用来计算云基础设施提供商的可信性. 目前成功的基于信誉的 P2P 信任模型有 EigenTrust[7]、PeerTrust[8]、SupRep[9]及 PET[10]等. 然而现存的信任模型[11-16]都存在一个共同的假设，即假设信任信息都来自于稳定的网络拓扑结构环境下，且这些信任信息能够被保证长期有效. 然而移动 P2P 网络与传统意义上的 P2P 网络有着本质上的区别，主要体现在节点的移动性. 节点的移动性又区分为身份移动和位置移动. 由于移动 P2P 网络是一个开放的、动态的网络，节点自主决定在网络中的行为，因此节点可以任意以不同的身份或随意变换不同的位置接入网络而不受任何管理和束缚. 节点的这种移动性虽然极大地方便了网络用户，但由于节点频繁的加入和退出造成网络拓扑结构不断变化，不可能保证建立的信任信息长期有效. 因此已有的信任管理系统在这种移动环境下已经不再适用，迫切需要提出新的解决方案.

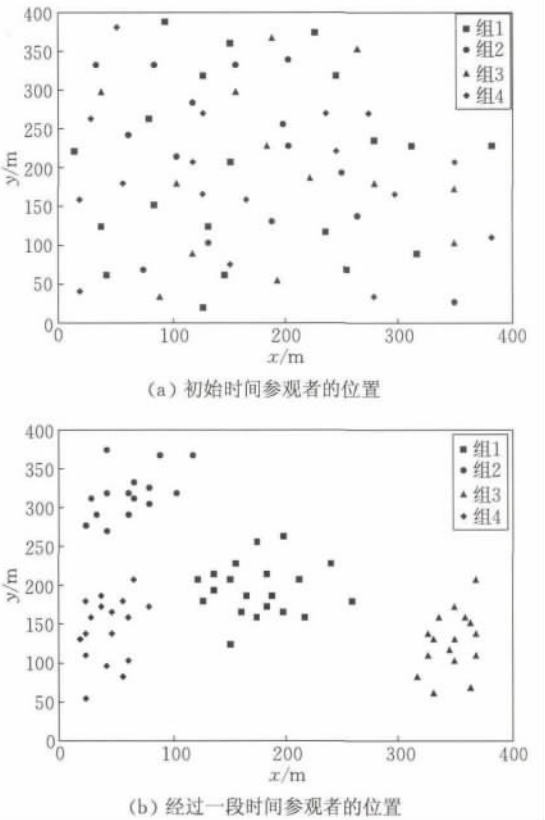
研究发现移动 P2P 网络中节点对等关系和网络拓扑结构的动态变化与现实社会存在着一定的映射关系. 网络世界中，所有的网络设备的使用者都是具有一定的兴趣和爱好，如果两个网络设备的使用者具有相同或相似的兴趣爱好，他们有着很大的可能性进行连接和资源交换. 移动网络的拓扑结构的变化往往是由于网络的使用者自身的兴趣、爱好等发生变化所引起的. 因此能够使用社会模型来解决 P2P 网络中存在的问题，通过社会模型来分析和预测相对应的网络拓扑结构的变化，提高节点之间信任关系的稳定性. 受到这种思想的启发，本文提出了一个基于增强的稳定组模型(Enhanced Stable Group Model-based Trust Evaluation Method，SGTM)的信任评估机制，并给出了稳定组构造算法. 该机制利用稳定组构造算法对移动 P2P 网络进行有效地分组，相同分组内的节点之间相对保持最大程度的拓扑结构的稳定，从而保证组内节点信任关系的稳定存在. 本文首次将稳定组模型应用到移动 P2P 信任评估方法的设计中. 模拟实验从动态适应力、全局信誉的收敛时间、以及全局信任计算所涉及的通讯负载等方面对所提出的信任评估方法的性能进行了评估. 所有模拟实验均运行在 Windows 2000 Server 的平台上. 每个实验均采用多次运行求平均值的办法获得最终数据. 由于 EigenTrust 和 PeerTrust，和我们提出的信任模型在理论层面更为接近，都是采用基于信誉的评估方法，因此在信任计算方面，针对 EigenTrust、GroupRep 和 SGTM 的

基本信任计算形式进行了比较.

2 基于增强的稳定组模型的信任评估方法介绍

2.1 增强的稳定组模型

很多组运动模型被提出来用以描述节点的组运动模式.比如 RVGM 模型[17].他们发现在实际的应用环境中,例如在博物馆里,每个参观者按照自己的兴趣,沿不同的路线,以不同速度运动,但是可以观察到,由于共同的兴趣爱好,参观者的移动过程显示出组群特性,即显示出一定的一致性,如图 1 所示.



(a) 初始时间参观者的位置

(b) 经过一段时间参观者的位置

图 1 参观者的位置

在 RVGM 里,每一个组被称为稳定组.同一稳定组的成员有共同的兴趣和路线,因此成员之间保持相对稳定距离的可能性非常大.既然移动 P2P 本身就是由一些为了协同计算、通信目的构成的网络,因此移动设备的使用者的行为通常不是随机的,而是分组活动.如果能够通过捕捉网络的这些基本特征描述出移动节点的运动模式,就能得到网络拓扑变化的信息,从而对网络在未来,一段时间内的拓扑结构变化趋势做出预测.在稳定组模型里,移动网络根据节点的运动模式被动态的分成若干个稳定组.相同组的成员在整个通讯会话里都以相同的运动模式进行移动.稳定组模型的使用具有以下 3 个主要的优点:第一,稳定组把巨大的网络分成了若干个易于管理的小区域;第二,稳定组使网络的拓扑在同一个组内具有相对很小的变化;第三,由于同一组的移动节点之间发生交互的可能性远远大于不同组的移动节点之间,因此节点在相同的组里很容易建立起信任关系,并且它们之间的信任链也相对稳定可靠.

本文延伸了 RVGM 模型,提出了增强的稳定组模型(Enhanced Stable Group Model,ESGM).增强的稳定组模型中的稳定组的定义基于 RVGM 模型中的稳定组,但 RVGM 没有给出节点之间的距离和其标准方差的计算公式,本文解决了这个问题,并对稳定组定义进行了延伸.延伸的意义在于使移动节点之间建立了稳定的连接,意味着节点之间的距离在一段时间内的稳定.通过增强的稳定组模型能够将移动 P2P 网络分成若干个稳定组,同一组的成员之间的距离保证了相对的稳定.因此不需要依赖第三方,同一个组的成员之间就能够建立起足够可靠的信任关系.

在给出定义之前,首先进行以下假设:在移动网络中,节点之间是对称传输的,即传输范围相同,每个节点能够通过检测信号强弱等方法,获取与周围每一个相邻节点的距离.

当节点第一次加入到网络时,他们是非组状态的.通过使用路由协议周期性的发送 Hello 信息,节点能够获取与周围每一个相邻节点距离.基于 Friss 传输等式,节点接收到的功率为

$$RP = P_t \times G_t \times G_r \times \frac{\lambda^2}{(4 \times \pi \times d)^2} \tag{1}$$

其中,RP 表示接收功率;P_t 表示传输功率;G_t 表示发送方的天线增益;G_r 表示接收方的天线增益;λ 表示波长;d 表示距离.通过式(1),能够计算出节点之间的距离.

$$E[D_{AB}] = \frac{m}{\sqrt{RP}} \tag{2}$$

$E[D_{AB}]$ 表示节点 A 和 B 之间的距离,m 表示一个常量.式(2)并不是旨在得到节点之间的实际物理距离,而是反映了节点之间的运动模式的相似度.

如果 $E[D_{AB}] \leq r$(r 是节点间有效传输距离),则将节点 A 和 B 称为相邻结点.同时由于节点 A 和 B 是移动节点,因此它们之间的距离也随结点自身的运动在不断地变化.如果节点 A 和 B 属于相同的组,那么 $E[D_{AB}]$ 变化很小,相对稳定.假设 A 是测量节点,节点 A 在一段时间内测量与 B 之间的距离,

测量的次数为 n. 得到的测量结果表示为 $E[D_{AB}]=\{E[D_{AB}]t,t=0,1,\cdots,n\}$. 令 VD_{AB}，表示与 $E[D_{AB}]$ 的平均值的标准方差，计算公式如下：

$$VD_{AB}=\sigma(|E[D_{AB}]_1-E[D_{AB}]_0|,\ |E[D_{AB}]_2-E[D_{AB}]_0|,\cdots,\ |E[D_{AB}]_n-E[D_{AB}]_0|) \quad (3)$$

定义 1. 对于在移动 P2P 网络的两个移动节点 A 和 B，若它们之间的距离 $E[D_{AB}]$ 的平均值小于 r，并且标准方差 $VD_{AB}<(VD_{AB})_{\max}$，则称节点 A 和 B 构成了邻接组对(Adjacent Group Pair)，表示为 $A \underset{\sim}{0} B$.

定义 2. 如果存在 k 个中间移动节点 $C_1,C_2,\cdots,C_k(k\geq 1)$，它们构成了这样的关系，$A \underset{\sim}{0} C_1, C_1 \underset{\sim}{0} C_2,\cdots, C_i \underset{\sim}{0} C_{i+1},\cdots,C_k \underset{\sim}{0} B$，则称节点 A 和 B 构成了 k 阶邻接组对(k-related Adjacent Group Pair)，表示为 $A \underset{\sim}{k} B$.

定义 2 将这种稳定关系扩展到不直接相邻的结点. 图 2 给出了 0 阶邻接组对与 k 阶邻接组对的例子：

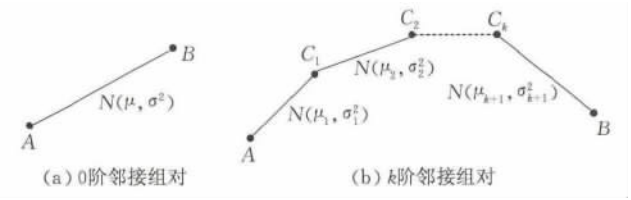


图 2　0 阶邻接组对与 k 阶邻接组对

定义 3. 如果 n 个移动节点 $A_1,A_2,\cdots,A_n$，对于 $\forall i,j,1\leq i,j\leq n$，都有 $A_i\sim A_j$，则称节点 $A_1,A_2,\cdots,A_n$，属于同一个稳定组 G_s 中，表示为 $A_i\in G_s$.

由定义 3，可以得到这样的结论：移动节点处于同一稳定组，表示它们之间的距离在一段时间上保持稳定性，从而揭示了它们一致性的运动特征. 稳定组的定义将那些仅仅是在某一时刻距离近，但是由于彼此具有不同的运动特征而导致未来的某个时刻它们之间的连接发生分裂的节点排除在同一稳定组之外. 因此位于相同稳定组中的移动节点在移动中保持稳定连接的可能性最大.

基于以上定义，可以推导出节点 A,B 及稳定组 G_s,G_{s_1},G_{s_2} 之间的关系规则：

(1) if $A\in G_s$ and $A\sim B$, then $B\in G_s$;

(2) if $A\in G_s$ and $\neg(A\sim B)$, then $B\notin G_s$;

(3) if $A\in G_{s_1}, B\in G_{s_2}$ and $A\sim B$, then $G_{s_1}=G_{s_2}$;

(4) if $A\in G_{s_1}, B\in G_{s_2}$ and $\neg(A\sim B)$, then $G_{s_1}\neq G_{s_2}$;

(5) if $A\in G_{s_1}$ and $A\in G_{s_2}$, then $G_{s_1}=G_{s_2}$.

稳定组的定义基于移动节点之间的稳定连接，稳定连接意味着节点之间的距离在一段时间内的稳定. 基于稳定组模型的移动 P2P 网络被分成若干个稳定组，同一组的成员之间的距离保证了相对的稳定. 因此不需要依赖第三方，同一个组的成员之间就能够建立起足够可靠的信任关系.

ESGM 模型允许移动节点能够发现它们的邻接节点并以完全分布的方式构造它们的稳定组 G_s. 每个移动节点在运行时根据自己本地信息，获得自己所属的稳定组信息. 每个移动节点 P_i 本地都维护着 3 类信息：(1) P_i 与邻居节点的距离；(2) 0 阶邻接组对关系的结点集合 $[AGP(P_i)]$；(3) 成员节点的集合.

在 ESGM 里移动节点能够根据自己本地信息发现 k 阶邻接组对节点，并通过与 0 阶邻接组对节点进行周期性信息交换，从而获得自己所属的稳定组中所有移动节点的集合. 这个过程包括 3 个关键步骤，分别是测量、更新和交换信息，如图 3. 本地稳定组集合构造过程如图 4.

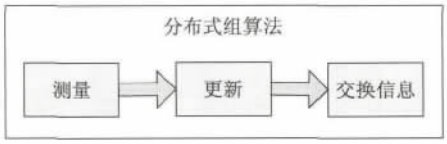


图 3　分布式组算法的关键步骤

$G_S(P_i)$ initialized to $\{P_i, AGP(P_i)\}=\varnothing$;
Let $G_S^P(P_j)$ be the previously received $G_S(P_i)$ from P_j
On receiving $G_S(P_j)$ from P_j
foreach P_k in $G_S(P_j)$
if $P_k\notin G_S(P_i)$ then
　$G_S(P_i)=G_S(P_i)+P_k$;
end
foreach P_k in $G_S^P(P_j)$
s.t. $P_k\in G_S^P(P_j)$, $P_k\in G_S(P_i)$ and $P_k\notin G_S(P_j)$
　$G_S(P_i)=G_S(P_i)-P_k$;
end

图 4　移动节点 P_i 上构造本地稳定组集合 $G_S(P_i)$

2.2　信任评估方法 SGTM 的原理

首先使用 2.1 节中的增强的稳定组模型 ESGM，在网络里动态的形成稳定组. 分组原则为相同分组内的节点之间相对保持最大程度的拓扑结构的稳定，从而保证组内节点信任关系的稳定存在. SGTM 的实现基于信任覆盖层(Trust Overlay Network). 任意节点的全局可信度，由与之发生过交易行为的其他节点对它的局部信任度以及这些节点的全局可信度来计算.

SGTM 中节点信任计算的过程是：每次节点在

完成交易之后，都会彼此之间进行评估，得到的结果称为局部信任度. 局部信任度作为原始数据，输入进SGTM. 在 SGTM 里任意节点的全局可信度，由与之发生过交易行为的其他节点对它的局部信任度，以及这些节点的全局可信度来计算. 由所有节点的全局信任度形成一个信任矢量 $\boldsymbol{V}=(V_1,V_2,\cdots,V_k)$，作为 SGTM 的输出. 并且 $\sum_{\lambda}V_\lambda=1$，其中 $\lambda=1,2,\cdots,k$，k 是信任覆盖层的移动节点个数.

图 5 显示了 SGTM 信任评估方法的总体结构. 圆型的部分代表信任覆盖层(Trust Overlay Network). 信任覆盖层是建立在 P2P 系统上的虚拟网络，其上的用户代表移动 P2P 网络的移动节点. 有向边代表节点之间进行的局部可信度评估. $G_{s_j}(P_i)$ 表示一个移动节点，其中 $j\geq1$，$i\geq1$. j 代表组 ID，i 代表成员 ID. 比如 $G_{s_1}(P_{19})$，表示它所在的稳定组 ID 为 1，成员 ID 为 19. 局部可信度表示为 $f_{(j,i),(j',i')}$. 比如 $f_{(1,19),(1,3)}$，表示移动节点 $G_{s_1}(P_{19})$ 对 $G_{s_1}(P_3)$ 的局部可信度. 有向边的起始点是做出评价的节点，终点是被评价的节点. 每个移动节点都有两个表：与其他节点的交互记录表 1 和局部可信度表 2. 移动节点第 1 次进入网络的时候，会根据 ESGM 模型里的稳定组构造算法加入适合的稳定组. 由于同组的移动节点之间的连接相对稳定，因此在成员节点之间发生交易的概率远远大于非成员节点. 这样的结果导致成员节点之间建立的信任链比非成员节点更稳定和可靠. 所以在 SGTM 里，当节点 P_i 向其他节点询问某个节点的局部可信度时，P_i 会优先询问成员节点. 每次节点完成交易之后，都会对它的局部可信度表进行更新.

表 1 Peer $G_{s_1}(P_2)$ 的交互记录表

节点 ID	全局信任度	交易量/k	交易时间	权重
$G_{s_1}(P_1)$	0.7	300	08/02/2013	0.6
$G_{s_1}(P_5)$	0.9	350	08/06/2013	0.8
$G_{s_2}(P_2)$	0.7	400	08/06/2013	0.5
$G_{s_1}(P_8)$	0.8	764	08/12/2013	0.9
…	…	…	…	…

表 2 Peer $G_{s_1}(P_{19})$ 的局部可信度表

节点 ID	局部信任度
$G_{s_1}(P_5)$	0.7
$G_{s_1}(P_3)$	0.7
…	…

计算局部可信度的方法如下：

SGTM 信任模型在计算局部信任值时引入了以下 5 个参数：

(1) 交易量因子. 交易量因子的大小直接反映了此次交易的重要程度，这个因素可以起到防止一些隐讳的信任攻击. 例如：一些恶意节点可以通过多次小规模成功交易提高它们的信任值，然后在大规模的交易中作假.

(2) 交易满意程度. 这是一个主观的参数，反映了一方对另一方行为的满意程度. 有了这个值，可以使得交易双方在交易中有更加良好的表现. 按照下载的文件质量状况，交易满意程度取值区间为(−1,1).

(3) 交易次数. 这个参数反映的是交易双方相互的重视和熟悉程度. 请求节点从响应节点处下载文件的次数越多，表示交易双方越熟悉，直接信任和间接信任也就越准确.

(4) 时间影响因子. 这个参数反映的是文件下载距离当前时间的远近程度. 因为随着时间的变化，交易的个体也是在不停地变化的. 所以说越是近期的下载行为，它的时间影响因子越大，对于本次下载行为的影响也越大.

(5) 风险因子. 这个参数反映的是节点进行交易所面临的风险，如信息泄露、病毒传播等.

假设在 x 请求从 y 下载文件之前，y 计算对 x 的局部信任度. 本模型中的局部信任度是采用二元组 $D(f_{yx},S)$ 的形式表示的，其中 f_{yx} 是 y 对 x 的局部信任度值，S 是 y 赋予 x 的交易量权限，体现交易规模的大小.

交易量权限 S 满足下面几个规则：

(1) 对于没有任何交易经验的实体，赋予最低的交易量.

(2) 交易量升级是通过判断某个交易量权限内的交易成功次数是否达到规定的次数(这个次数由 peer 自己确定). 交易量权限越低，升级需要的成功交易次数越多.

(3) 出现交易因为欺骗或者恶意攻击而失败的情况，就要增加在此交易量权限范围内升级的交易成功次数.

(4) 只有交易在此交易量权限范围内的交易成功，交易成功次数才增加.

引入交易量权限给了新进入的实体进行交易的机会，解决了很多信任模型没有解决的对新进入实体的信任问题，同时防止它们利用这次机会进行大规模的欺骗行为.

局部信任度值的计算公式如下：

$$f_{yx}=\alpha\sum_{i=0}^{N(x)}\left(\frac{S(y,x)\times M(y,x)\times Z}{N(x)}+pen(i)\frac{1}{1+e^{-n}}\right)+\beta Risk(x) \tag{4}$$

其中，α，β 是权重因子，且 $\alpha+\beta=1$，$N(x)$ 是节点 x 和节点 y 的交易次数，$S(y,x)$ 是 y 对 x 每次交易的主观满意程度. $M(y,x)$ 是每次文件下载的交易量因子(表示这次交易在 x 与 y 所有交易中的重要程度，越重要权值越高). 计算公式为 $M(y,x)=\frac{\text{每一次下载量}}{\text{平均的下载量}}$. Z 是时间影响因子，它表示此次交易是否为最近的交易记录，越靠近当前日期，所占权值越大，这是因为被评估者的交易行为在信任评估中的重要性随时间衰减. 在 SGTM 模型中，时间影响因子值的大小由如下函数定义：

$$Z=u(t_i,t_{\text{now}})=\frac{1}{t_{\text{now}}-t_i},\ Z\in(0,1) \qquad (5)$$

t_{now} 表示当前时间，t_i 表示此次交易时间. $pen(i)$ 表示的是交易欺骗后的惩罚因子，$pen(i)$ 定义如下：$pen(i)=-1$ 表示第 i 次交易因为欺骗或者恶意攻击而失败；$pen(i)=0$ 表示第 i 次交易成功. $\frac{1}{1+e^{-n}}$ 是加速因子，n 是失败的次数. 这个加速因子使信任值在出现失败时迅速下降，同时由于这个因子是随着 n 的增大逐渐增大的，所以可以防止因为一两次无意的欺骗而导致惩罚过重的现象出现. $Risk(x)$ 是节点 y 的风险因子.

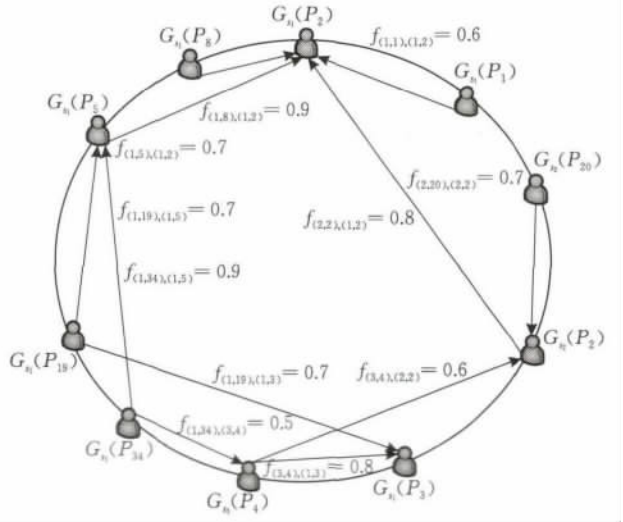


图 5　SGTM 信任评估方法的总体结构

节点的全局可信度计算公式如下：

$$V_x=\sum_{y\in S}\left(\frac{w_y}{\sum_{y\in S}w_y}f_{yx}\right)=\frac{\sum_{y\in S}w_yf_{yx}}{\sum_{y\in S}w_y} \qquad (6)$$

其中 V_x 代表节点 x 的全局可信度，S 是与节点 x 发生过交易的节点的集合. f_{yx} 是节点 y 对节点 x 的局部可信度值. w_y 是局部可信度 f_{yx} 的权重. 整个信任的计算过程采用多次叠代的方法，直到 V_x 收敛到一个稳定的值. 为了减少计算中的通讯负载，在这 SGTM 会根据实际的情况为 w 设置一个阈值，阈值的设定一般与系统的安全策略有关. 只有大于这个阈值的局部可信度才有可能被选择用来计算全局可信度. 图 6 显示了一个全局信任度计算的例子.

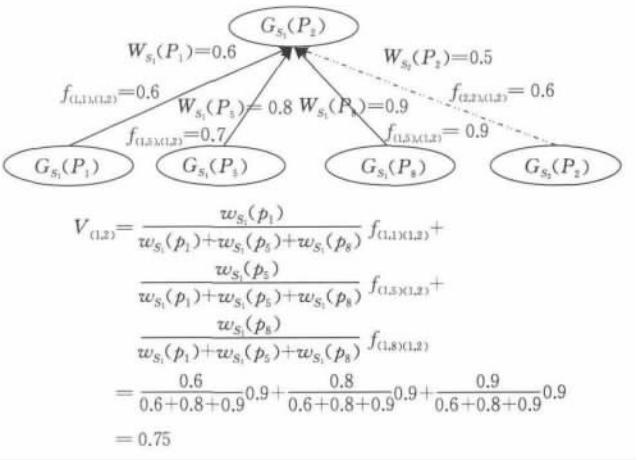


图 6　全局信任度计算的实例

这个例子显示了如何计算节点 $G_{s_1}(P_2)$ 的全局可信度. 其中 w_k 被设置为 0.5. 基于图 5，有 4 个节点与 $G_{s_1}(P_2)$ 发生过交易. 分别为 $G_{s_1}(P_1)$，$G_{s_1}(P_5)$，$G_{s_1}(P_8)$ 和 $G_{s_2}(P_2)$. 但由于 w_k 等于 0.5，因此只有前 3 个节点被选择来计算全局可信度.

SGTM 使用以下 6 个逻辑推理规则推导出局部信任度权重 w. 图 7 显示了一个 w 的大的特征函数实例. 图 8 显示了 w 的 5 个等级.

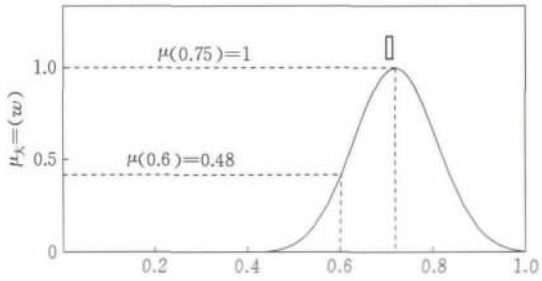


图 7　一个 w 的大的特征函数实例

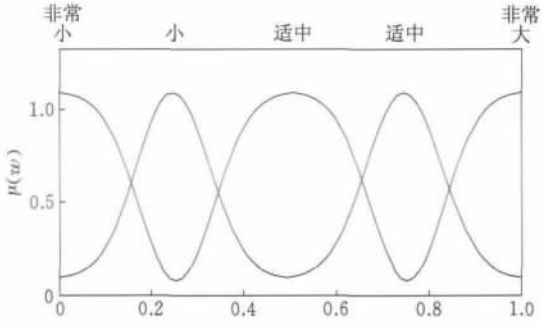


图 8　w 的 5 个等级

(1)当节点之间的交易发生在同组节点之间,如果交易量大,并且交易时间靠近当前时间,那么局部信任度权重 w 被赋予一个大的值.

(2)当节点之间的交易发生在同组节点之间,如果交易量小,或者交易时间远离当前时间,那么局部信任度权重 w 被赋予一个小的值.

(3)当节点之间的交易发生在同组节点之间,如果交易量大,并且节点的信任度高,那么局部信任度权重 w 被赋予一个非常大的值.

(4)当节点之间的交易发生在不同组节点之间,如果交易量大,并且节点的信任度高,那么局部信任度权重 w 被赋予一个适中的值.

(5)当节点之间的交易发生在不同组节点之间,如果交易量小,或者交易时间远离当前时间,那么局部信任度权重 w 被赋予一个小的值.

(6)如果节点的信任度低,那么局部信任度权重 w 被赋予一个非常小的值.

3 仿真实验及结果分析

3.1 仿真环境

本文使用 PlanetSim 3.0 作为移动 P2P 系统的模拟软件的模型仿真[18]. 为了与 EigenTrust 和 GroupRep 进行比较,实验网络采用分布式的结构. 在 SGTM 中,节点本地可保存 25 个节点的信任信息. 每一个节点都连接了一定数量的邻居节点,由节点发出的查询消息通过邻居节点向网络中扩散,消息的跳数由其 TTL 指定. 节点或群组发送的信任请求消息的 TTL 为 4.

在实验中,所有的节点都共享了一定数量的文件,并周期地选择本地不存在的文件向网络中发出查询消息. 在收到文件查询消息时,如果本地发现了所查询的文件则返回一个响应消息,请求节点根据响应节点的全局信任度从中选择一个作为下载源. 实验中,诚实节点分为强、中、弱三类,体现了节点提供服务的能力. 实际可以包含有多个性能参数,如上载速度,响应时间和带宽等. 另外,恶意节点通常上载 3 类不真实的文件:功能与描述不符的文件,哈希值不正确的文件,含有病毒或木马的文件. 显然,后两种情形比较严重,尤其是文件含有病毒或木马时,可能会严重的影响终端系统的安全.

为了使模拟更接近于真实的移动 P2P 系统,在模拟的过程中为每一个移动节点任意设置了一个休眠周期,范围在[100 s,500 s]. 在休眠期间不再响应其他节点的任何请求. 比如设置节点每隔一个小时进入休眠 100 s. 设置休眠周期的目的是为了模拟真实的移动 P2P 网络中节点任意加入和离开的特性.

在信任计算方面,针对 EigenTrust、GroupRep 和 SGTM 的基本信任计算形式进行比较. EigenTrust 和 GroupRep 的基本信任计算形式表达为参考文献[12-13]. 对 SGTM 来说,稳定组的构造基于算法见图 4,信任度的计算见 2.2 节信任度评估方法. SGTM 基本的参数设置为 $\alpha=0.7$,$\beta=0.3$,$w_k=0.5$. 对于所有节点来说可信度判断的阈值 $\psi=0.65$. 下载源选择的信任度阈值 $\gamma=0.75$,即信任度大于 0.75 的响应节点都可被选择作为下载源. 更多的基本参数设置如表 3.

表 3 SGTM 模拟参数表

参数	值
查询消息的 TTL	4
每一个结点的邻居数量	4
不同文件的版本数目	1500
休眠周期/s	[100, 500]
每个节点初始具有的文件数	15
三种服务节点的比率/%	40,35,25
恶意节点提供三种不真实文件的比率/%	55,35,10
节点移动的最大速度/(m/s)	20
节点的通讯范围/m	70
α, β	0.7, 0.3
w_k, ψ, γ	0.5, 0.65, 0.75

3.2 动态适应力评估

在这组实验里,通过模拟节点任意加入和离开的过程考察信任评估方法对网络动态性的适应能力. 由于本组实验集中模拟网络的动态变化,因此,在节点构成中没有考虑恶意节点. 网络中的所有节点都是诚实节点. 实验评估了网络的动态变化对其性能的影响. 共设计了 4 组实验,第 1 组模拟节点的离开过程,其中节点的总数为 10 000,随机分布在 5000 m×5000 m 区域. 离开节点的数量占节点总数的最大比率为 25%. 第 2 组模拟节点的加入过程,其中节点的总数为 10 000,随机分布在 5000 m×5000 m 区域. 加入节点的数量占节点总数的最大比率为 25%. 第 3 组模拟节点的离开/加入过程,其中节点的总数为 10000,并随机分布在 5000 m×5000 m 区域. 第 4 组模拟节点的离开/加入过程,节点的总数分别为 6000,并随机分布在 1000 m×1000 m 区域.

4 组实验中,节点每进入休眠状态一次被视为离开网络一次,反之为加入网络一次. 一个节点加入和离开网络的可能性等于 0.5,这意味着节点加入网络和离开网络的机会是相等的. 在第 1 组实验里,节点离开的数量分别设置为 500、1000、1500、2000、

2500. 在第 2 组实验里，节点加入的数量分别设置为 500、1000、1500、2000、2500. 在第 3 组和第 4 组实验里节点加入和离开网络的次数总共模拟 3000 次. 在实验过程中每隔 250 个间隔收集 1 次实验结果. 实验结果对应网络性能 NP，$NP=\frac{n_p}{n_t}$. 网络性能的值是网络中节点的总数 n_p 与信任链数量 n_t 的比率. 信任链数量 n_t 是信任覆盖层中有向边的数量. 网络性能 NP 体现了信任评估方法的信任度计算能力. NP 越小说明信任度的计算能力越强. 第 1 组、第 2 组实验的结果分别如表 4 和表 5. 第 3 组和第 4 组实验结果如图 9 所示.

表 4　节点离开时的网络性能

节点数	节点离开前	节点离开后*
500	2.26	2.29
1000	2.14	2.17
1500	2.05	2.08
2000	1.90	1.94
2500	2.41	2.44

表 5　节点加入时的网络性能

节点数	节点加入前	节点加入后*
500	1.04	1.01
1000	1.62	1.64
1500	2.37	2.42
2000	3.74	3.77
2500	2.32	2.32

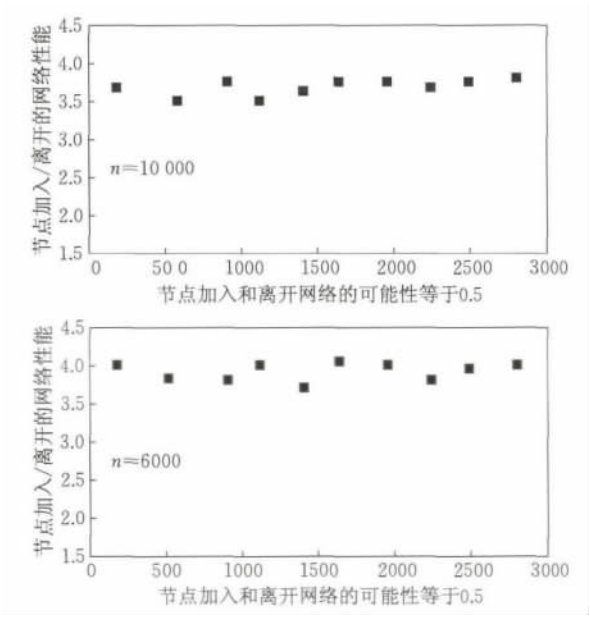


图 9　节点离开/加入时的网络性能

根据实验结果可以得出以下结论：

(1) $N=10000$，节点任意离开的数量分别为 500、1000、1500、2000、2500. 在离开节点占到总节点数量的 25% 以后，网络仍然保持一个良好的性能，由此可以推断出节点的任意离开对网络性能的影响很小.

(2) $N=10\,000$，节点任意加入的数量分别为 500、1000、1500、2000、2500. 在加入节点占到总节点数量的 25% 以后，网络仍然保持一个良好的性能，由此可以推断出节点的任意加入对网络性能的影响很小.

(3) 节点的任意离开/加入对其网络性能影响很小，并且 $N=10\,000$ 与 $N=6000$ 相比基本没有变化，NP 在 3.5～4.0 范围内上下波动.

因此通过以上 4 组实验，可以证明 SGTM 具有很强的动态适应能力，能够很好的适应移动 P2P 网络的动态变化.

3.3　全局信誉的收敛时间评估

在这组实验里，对信任模型 EigenTrust、GroupRep 和 SGTM 建立全局信任所需的收敛时间进行了对比. 实验结果如图 10 所示. 节点总数从 100 增加到 10 000，在实验过程中共取 7 次结果作比较.

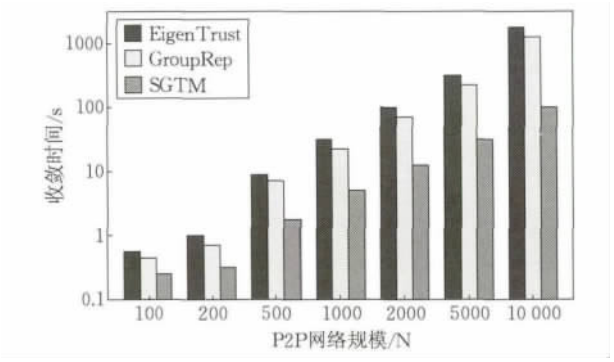


图 10　收敛时间比较

根据实验结果可以得出以下结论：

(1) EigenTrust 同 GroupRep 的收敛时间非常接近，GroupRep 比 EigenTrust 收敛更快一点.

(2) 与 SGTM 相比，EigenTrust 和 GroupRep 的收敛时间远远高于 SGTM.

(3) 三者的收敛时间均同网络的规模成正比，并呈现出线性增加的特点.

在计算全局信任时，收敛性是最大的挑战，通过以上实验，可以证明 SGTM 很好的解决了信任计算中的收敛性问题.

3.4　全局信任计算所涉及的通讯负载评估

这组实验对信任模型 EigenTrust、GroupRep 和 SGTM 的全局信任计算所涉及的通讯负载进行了评估和比较. 在实验过程中，分别应用这 3 种信任评估方法来计算 5 个不同的移动节点的全局信任度. 共进行了两组实验：第 1 组实验节点数量 $N=1000$，第 2 组实验结点数量 $N=10\,000$. 实验结果如

图 11 和图 12 所示. 第 1 组实验,EigenTrust 为了计算节点的全局信任度所产生的平均消息数为 59.06,GroupRep 为 32.04,SGTM 为 30.02. 第 2 组实验,EigenTrust 的平均消息数为 628 000.06,GroupRep 为 165 500.03,SGTM 为 94 700.08. 根据实验结果可以得出以下结论:

(1) 当 $N=1000$ 时,GroupRep 和 SGTM 的全局信任计算所涉及的通讯负载比较接近,均小于 EigenTrust.

(2) 当 $N=10000$ 时,SGTM 的全局信任计算所涉及的通讯负载远远小于 EigenTrust 和 GroupRep.

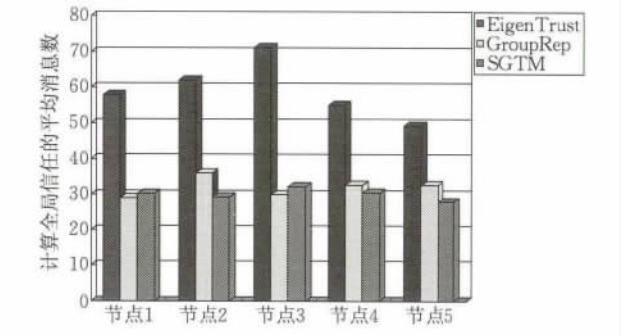


图 11 $N=1000$ 时计算全局信任的平均消息数

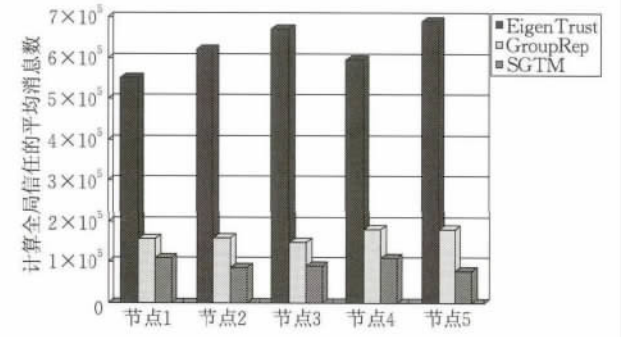


图 12 $N=10000$ 时计算全局信任的平均消息数

通过以上实验,可以证明出 SGTM 很好的解决了全局信任计算所涉及的通讯负载问题. SGTM 随着系统规模的增加,通讯负载远远低于 EigenTrust 和 GroupRep,说明 SGTM 非常适合处理大规模的移动 P2P 服务.

4 结 论

本文提出了一个基于增强的稳定组模型(Enhanced Stable Group Model-based Trust Evaluation Method, SGTM)的信任评估方法. 并使用分布式的稳定组划分算法,在网络里动态的形成稳定组. SGTM 的实现基于信任覆盖层(Trust Overlay Network). 与 P2P 系统的其他信任模型相比,SGTM 使用一种基于稳定组运动模型划分移动网络的机制,这种机制能够自发重新组合网络,形成新的具有共同兴趣、利益的组群. 同时,对网络在未来一段时间内的拓扑结构变化趋势做出预测. 在 SGTM 里任意节点的全局可信度,由与之发生过交易行为的其他节点对它的局部信任度以及这些节点的全局可信度来计算. 本文首次将稳定组模型应用到移动 P2P 信任评估方法的设计中. 模拟实验表明,SGTM 有效地解决了节点之间的动态信任关系建模问题. 在保证信任评估效果的前提下能够极大的降低通信负载.

参 考 文 献

[1] Firdhous M, Ghazali O, Vijaykumar P, Hassan S. A trust computing mechanism for cloud computing//Proceedings of the ITU Fully Networked Human-Innovations for Future Networks and Services. Cape Town, South Africa, 2011: 1-7

[2] Abawajy J. Establishing trust in hybrid cloud computing environments//Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications. Changsha, China, 2011: 118-125

[3] Fang En-Guang, Wu Qing. Evidence theory based cloud computing trust model research. Computer Application and Software Technology, 2012, 29(4): 68-70(in Chinese)
(方恩光, 吴卿. 基于证据理论的云计算信任模型研究. 计算机应用与软件, 2012, 29(4): 68-70)

[4] Xie Xiao-Lan, Liu Liang, Zhao Peng. Trust model based on double incentive and deception detection for cloud computing. Journal of Electronics & Information Technology, 2012, 34(4): 812-817(in Chinese)
(谢晓兰, 刘亮, 赵鹏. 面向云计算基于双层激励和欺骗检测的信任模型. 电子与信息学报, 2012, 34(4): 812-817)

[5] Du Rui-Zhong, Tian Jun-Feng, Zhang Huan-Guo. Cloud service selection model based on trust and personality preferences. Journal of Zhejiang University (Engineering Science), 2013, 47(1): 53-61(in Chinese)
(杜瑞忠, 田俊峰, 张焕国. 基于信任和个性偏好的云服务选择模型. 浙江大学学报, 2013, 47(1): 53-61)

[6] Pawar P S, Rajarajan M, Nair S K, Zisman A. Trust model for optimized cloud services//Proceedings of the 6th IFTP International Conference on Trust Management. Surat, India, 2012: 97-112

[7] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks //Proceedings of the 12th International World Wide Web Conference. Budapest, Hungary, 2003: 640-651

[8] Tian Hui-Rong, Zou Shi-Hong, Wang Wen-Dong, Cheng Shi-Duan. A hierarchical reputation model for P2P networks. Journal of Electronics and Information Technology, 2007, 29(11): 2560-2563(in Chinese)

(田慧蓉，邹仕洪，王文东，程时端. P2P 网络层次化信任模型. 电子与信息学报，2007，29(11)：2560-2563)

[9] Chhabra S, Damiani E, De Capitani di Vimercati S, et al. A protocol for reputation management in super-peer networks// Proceedings of the 15th International Workshop on Database and Expert Systems Applications. Zaragoza, Spain, 2004: 973-983

[10] Liang Z, Shi W. PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing//Proceedings of the Hawaii International Conference on System Sciences. Hawaii, USA, 2005: 201-201

[11] Tian Chun-Qi, Zou Shi-Hong, Wang Wen-Dong, Cheng Shi-Duan. A new trust model based on recommendation evidence for P2P networks. Chinese Journal of Computers, 2008, 31(2): 271-281(in Chinese)
(田春岐，邹仕洪，王文东，程时端. 一种基于推荐证据的有效抗攻击 P2P 网络信任模型. 计算机学报，2008，31(2)：271-281)

[12] Yan Bin-Yu, Liu Fang-Yuan, Deng Min-Jian, et al. Trust model based on risk evaluation in wireless sensor networks. Journal of Central South University(Science and Technology), 2011, 42(6): 1657-1662(in Chinese)
(严斌宇，刘方圆，董敏坚等. 一种基于风险评价的无线传感器网络信任模型. 中南大学学报(自然科学版)，2011，42(6)：1657-1662)

[13] Zhang J, Shankaran R, Orgun M A, et al. A trust management architecture for hierarchical wireless sensor networks// Proceedings of the 35th Annual IEEE Conference on Local Computer Networks. Denver, USA, 2010: 264-267

[14] Felix G M, Gregorio M P. Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication Systems, 2010, 46(2): 163-180

[15] Lopez J, Roman R, Agudo I, Carmen F G. Trust management systems for wireless sensor networks: Best practices. Computer Communications, 2010, 33(9): 1086-1093

[16] Guan Shang-Yuan, Wu Wei-Guo, Dong Xiao-She, Mei Yi-Duo. Survey of trust management in open distributed environments. Computer Science, 2010, 37(3): 22-35 (in Chinese)
(官尚云，伍卫国，董小社，梅一多. 开放分布式环境中的信任管理综述. 计算机科学，2010，37(3)：22-35)

[17] Zonoozi M M, Dassanayake P. User mobility modeling and characterization of mobility patterns. IEEE Journal on Selected Areas in Communications, 1997, 15(7): 1239-1252

[18] Wu Xu, He Jing-Sha, Xu Fei. A distributed decision-making mechanism for wireless P2P networks. Journal of Communication and Networks, 2009, 11(4): 359-367

WU Xu, born in 1978, Ph. D., associate professor. Her research interests include trusted computing, pervasive computing, mobile computing, and software engineering.

Background

Trust management is essential to the security framework of any network. In this paper, the proposed trust management model mainly focuses on constructing much shorter and more robust trust chains with high probability in mobile P2P networks. In traditional fixed networks, most trust evidences come from an assured processes, and assumed to be valid on a long term. In contrary, trust evidences generated aren't ensured to be valid on a long term in a mobile P2P network due to the dynamic nature. Since those solutions developed mainly for the fixed wired networks are not fit in such a scenario, new security solutions are eagerly in demand. In this paper, we propose an Enhanced Stable Group Model-based Trust Evaluation Method. Stable group is introduced in collecting trust evidences phase to simplify the process of trust initialization. In the scheme, all group members that move in a similar pattern remain throughout the entire communication session. By doing this, the topology within a group is less dynamic. Since trust evidences of a sensor are main collected in the stable group, the average length of trust chains is much shorter and more robust than other models, and avoids trust dilution. The simulation results prove the effectiveness and the benefits of the proposed model. The work in this paper is supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China (Program No. 2011JQ8006) and Shaanxi Provincial Education Department (Program Nos. 11JK1060 and 2013JK1132) and National Natural Science Foundation of China (Program No. 61373116) and special funding for key discipline construction of general institutions of higher learning from Shaanxi province and special funding for course development from Xi'an University of Posts and Telecommunications.