

一种基于静态和动态信任的普适环境信任模型

薛 静, 贺 樑, 邱 萌

(华东师范大学 信息科学与技术学院, 上海 200241)

(jxue2007@gmail.com)

摘 要: 针对普适环境中现有信任模型对信任证据的考虑存在片面性的问题, 在分析四种信任证据的基础上, 将信任分为静态和动态两种类型, 并提出了一种基于该分类方法的信任模型, 描述了该模型的工作机制。该模型克服了对信任证据考虑不完整的缺陷, 有利于在普适实体之间建立起可靠的信任关系, 提高系统的安全性。

关键词: 普适计算; 信任管理; 信任模型

中图分类号: TP393.08 **文献标志码:** A

Developing model for pervasive computing environments based on static-dynamic trust

XUE Jing, HE Liang, QIU Meng

(School of Information Science and Technology, East China Normal University, Shanghai 200241, China)

Abstract: To resolve the limitations in the integrality of evidence used for the trust judgment in pervasive environments, a new trust model was proposed based on the analysis of the four trust evidence. In this model, the trust was classified into two groups: namely static trust and dynamic trust. Furthermore, the workflow of the model as well as the method of updating trust was described. By using this model, the reliable trust relationship can be set up between pervasive entities, which can enhance the security performance of the pervasive environments.

Key words: pervasive computing; trust management; trust model

0 引言

普适计算环境是由移动用户、系统的服务、嵌入在物理环境下的传感器和资源组成的联合环境。这种环境具有一些新的特点^[1]: 1) 环境对用户不熟悉, 用户没有与环境拥有者存在信任关系; 2) 数据常常动态产生; 3) 用户访问权限动态变化; 4) 系统典型分散。普适环境的以上特点就对系统的安全性提出了更高的要求, 在系统性能等方面需要有特殊的安全机制来保障。此外, 普适计算系统是在共享通道上进行高度分散的网络通信, 而且他们之间的交易是自发的, 因此普适计算比传统计算更强调信任的作用。为此, 本文提出了一种适用于该环境下的基于静态和动态信任的信任管理模型 (A Static-Dynamic Based Trust Model for Pervasive Computing Environments, SDTMPC)。

所谓信任管理是以评估和决策制定为目的, 对 Internet 应用中与信任关系的完整性、安全性或可靠性相关的证据进行收集、编码、分析和表示的行为。其中证据可能包括凭证、风险评估、使用经验或者推荐信息。分析过程是根据信任需求进行信任评估或计算的过程^[2]。

普适环境下的信任管理由于普适环境本身的特殊性, 需要提供适合于这种环境下的信任管理模型。本文提出的信任管理模型综合考虑了各种信任证据, 首先计算出节点的静态信任值和动态信任值, 并将二者依据具体的信任策略计算得出最终信任值。之后, 实体根据这个结果与信任度高的节点进行交

易, 以此在普适实体之间建立可靠性高的信任关系, 有效防止和不安全节点进行交易, 明显提高系统的效率和安全性。

1 信任证据类型

普适环境下信任证据主要来自四个方面: 属性信任、直接信任、间接信任和上下文信任, 以下分别对各种信任值的概念和度量进行说明。

1.1 属性信任

实体属性信任值 Ta 是实体属性的函数:

$$Ta = F(A_1, A_2, \dots, A_n) \quad (1)$$

其中: A_1, A_2, \dots, A_n 是实体的属性, 属性描述实体的特征, 可以是实体的身份标志, 也可以是实体的物理环境 (如位置, 时间等), 数字签名的文档以及任何建立信任所需要的其他信息。

1.2 直接信任

直接信任也叫经验信任, 是通过实体之间的直接交易信息得到的信任关系, 用 Tb 表示。

由于实体的交易行为一般具有一定程度的一致性, 过去的行为往往预示着未来行为的取向, 所以实体过去的行为是判断其是否值得信任的重要依据。在一次服务完成以后, 根据特定的环境, 可以参考提供服务等待的时间, 完成任务的时间等指标, 给予目标实体一个信任度评估。信任度评估质量代表服务质量和可接受程度。

根据社会学的观点, 信任是对历史经验的总结; 而从统计意义上看, 信任具有随时间衰减的特性, 即相比于久远的信任

收稿日期: 2008-07-07; 修回日期: 2008-09-22。 基金项目: 国家科技部科技支撑计划项目 (2007BAH09B04); 上海市科委重大科技攻关项目 (06DZ15008); 上海市启明星人才计划项目 (07QB14036)。

作者简介: 薛静 (1984-), 女, 安徽黄山人, 硕士研究生, 主要研究方向: 普适计算、分布式计算; 贺樑 (1973-), 男, 上海人, 副教授, 博士, 主要研究方向: 普适计算、协同技术、移动计算、多媒体技术、分布式计算; 邱萌 (1984-), 女, 浙江绍兴人, 硕士研究生, 主要研究方向: 普适计算、分布式计算。

评估,近期的信任评估与实体的真实信任值关系更加密切。因此在信任评估中引入时间衰减因子 λ , 实体 i 对实体 j 的直接信任值可以表示为

$$Tb_{ij} = \sum_{p=1}^P Tb_{ij}^p \lambda^{M-p}; 0 \leq \lambda \leq 1 \quad (2)$$

其中: P 为实体 i 对实体 j 的评价次序数, λ 为时间衰减因子, M 为实体 i 对实体 j 评估的次数。

1.3 间接信任

间接信任也叫推荐信任,是通过中间实体获得的对目标实体的信任关系,用 Tc 表示。

假设实体 i 需要和实体 j 进行交易,一系列实体 $k(1, 2, \dots, n)$ 是推荐节点,与实体 j 都有直接交易,则实体 i 和实体 j 之间的间接信任值为:

$$Tc_{ij} = \frac{\sum_{k=1}^n C_{ik} Tb_{kj}}{\sum_{k=1}^n C_{ik}} \quad (3)$$

其中: Tb_{kj} 代表实体 k 对实体 j 的直接信任, C_{ik} 代表实体 i 对 k 提供的推荐信任的反馈信任值。根据人类社会的经验:说话人本身信任度高,他的话也相对可信。在本文模型中也采取此方法处理:根据推荐实体本身的信任值来分配相应的推荐权值,而这个权值是实体本身信任度的单调递增函数。特殊地,取 $C_{ik} = Tb_{ik}$, 即实体 k 对实体 j 的推荐权值取实体 i 对 k 的直接信任度。

通过这样的处理,就能使得实体的间接信任综合了各方面的推荐结果,同时本身信任度高的实体的推荐更加可信,从而在一定程度上保证了模型的稳定性。

1.4 上下文信任

移动用户在物理空间内的位置,状态等相关信息的改变称为上下文。上下文包括^[3]: 计算上下文(网络的连接情况,通信成本,通信的带宽和附近的资源),用户上下文(用户的特性,位置,时间,附近的人员,当前的人际关系等),物理上下文(光照,噪声程度,交通条件和温度等)。

上下文信任值 Td 是上下文的函数: $Td = H(D)$ 。其中 D 是实体所处的上下文的信息,主要是由传感器捕获来处理 and 存储的。模型中采用文献[4]开发的上下文工具包来提取环境状态信息。上下文工具包主要由上下文窗口小部件、收集器和解释器这三个部分组成。其中上下文窗口小部件表示通过传感器提取环境信息,是系统其他部件和服务自动传递信息的界面;收集器给应用相关的实体收集信息;解释器负责提取低级上下文信息给更高级。

当收集到上下文信息 D 之后,就可以得出上下文信任值。如果捕获的上下文 D 变化了,将需要重新评估 Td 。这样的评估方法很好地体现了普适系统的动态性。

2 信任综合

2.1 静态信任和动态信任

本模型中将信任分为静态信任和动态信任,其中静态信任代表实体本身的基本信任信息,动态信任反映实体在普适环境的动态变化下的信任信息。

图 1 所示的就是信任的分类和综合情况。

静态信任值 T_{static} 由属性信任,直接信任,间接信任这三种信任证据共同决定:

$$\begin{cases} T_{static} = \sum_{i=a,b,c} W_i T_i \\ \sum_{i=a,b,c} W_i = 1 \end{cases} \quad (4)$$

其中: W_i 是各种信任类型的权值,它依赖于系统和环境的需求,根据普适实体的具体要求被赋予恰当的权值。特殊地,如果一个普适实体对访问它的实体只需要属性这个信任值就能决定实体的静态信任,那么其他的两项的权值赋予 0 即可。根据 Ta, Tb, Tc 可以计算出实体的静态信任值,这个信任值代表实体本身的基本信任情况。

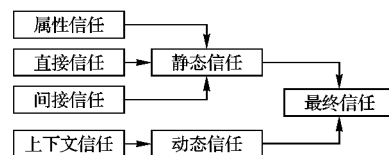


图 1 普适环境下信任值的计算

动态信任值 $T_{dynamic}$ 在本模型中只由上下文信任证据决定: $T_{dynamic} = Td$ 。其中: Td 是动态信任值,反映实体在不同的上下文环境中信任值的变化情况,特殊环境下也可以决定实体的信任程度。这来源于人类社会学中类似的情形:平常很可信的个体,在特定的某种环境下可能会做出不可信的举动。

2.2 最终信任

最终信任值参照文献[5]中信任值的综合方法进行适当的调整以适用于本模型:

$$T = F_{res}(S_{policy}, T_{static}, T_{dynamic}) \quad (5)$$

T : 最终信任值。

F_{res} : 信任值综合函数。

S_{policy} : 信任策略。

T_{static} : 静态信任值。

$T_{dynamic}$: 动态信任值。

根据给定的信任策略决定具体的信任值综合函数,与计算出来的实体静态信任值和动态信任值加以综合,得出最终的信任值,这个信任值是用来判断实体能否访问资源的一个最终评价参数。

3 SDTMPC 模型

3.1 SDTMPC 模型的假设条件:

本文提出的 SDTMPC 模型是基于以下假设的:

1) 同时考虑信息空间和物理空间,其中信息空间中的信任是静态信任,主要由属性凭证信任,直接信任,间接信任共同决定,它反映的是实体本身的基本信任值。物理空间中的信任是动态信任,对信任值进行局部范围内的调整,二者共同决定最终信任值。

2) 模型中每个实体都有唯一的实体标识,每个实体各自维持一张信任值表,存放着本实体对其他实体的信任值,这有别于传统的一个系统级的中央信任信息库,这样可以避免中央数据库单点失效的危险。

3) 当一个实体请求访问资源时,信任模型首先为资源实体加载相应信任策略,根据信任策略对信任证据加以评估,以建立信任。在此过程中,新的信任证据在信任信息存储单元中自动进行核实和更新。

4) 不同信任证据都有相应的信任评估模块来对其进行评估,如果系统中有多个信任证据同时到达,信任模型就会调用多个模块来评估各种信任证据。

3.2 SDTMPC 模型的工作机制

SDTMPC 的工作机制如图 2 所示。

1) 实体 j 进入环境请求访问实体 i 中的资源或服务,信任模型首先为实体 i 的资源加载相应信任策略,同时开始搜集

实体 j 的所有的信任证据。

2) 将收集到的信任证据按照来源不同进行分类。

3) 将各种信任证据用适当的策略进行信任评估得到相应的信任值, 如果收集不到那一项信任证据, 则该项信任证据的权值取 0, 否则, 同时计算各种信任证据的信任值。

4) 计算静态信任值 T_{static} 和动态信任值 $T_{dynamic}$ 。

5) 根据具体的信任策略来决定在该环境中的静态信任和动态信任综合所要采用的函数, 计算出最终的信任值 T 。

6) 实体 i 中事先存储了要访问该实体所要达到的信任阈值, 根据信任值 T 与阈值的关系来决定实体 j 的不同的信任等级, 做出相应的信任决策: 是提供服务还是拒绝服务或者是提供受限制的服务。

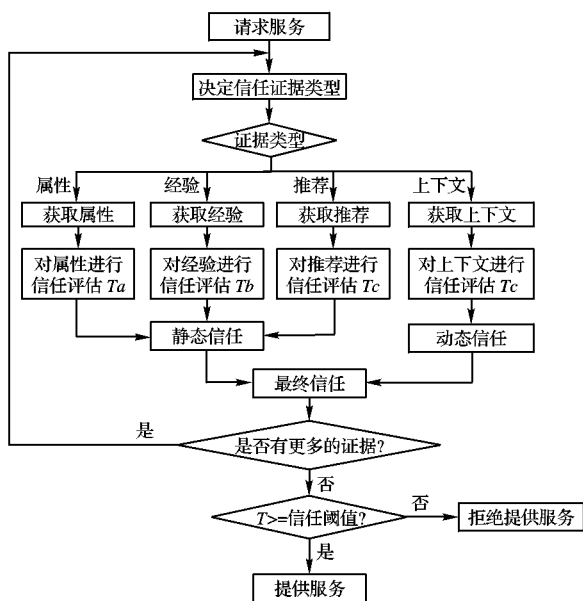


图2 信任管理逻辑流程

这个信任模型是分布式的信任模型, 它首先将信任评估分配给各信任模块, 然后将各自应用模块的评估结果加以综合。

3.3 信任更新

信任具有时间滞后性, 需要经过不断的学习和经验累积形成, 更新的信任只能在下一次的选择中使用。对于信任值的更新, 我们采用的是一种自学习的反馈策略。

更新时间是信任更新的一个重要方面, 只有在适当的时机更新信任值系统才能获得较高的效率。本模型中采用准确度很高的事件驱动更新机制对信任值进行更新, 即在一次交易完成之后, 根据服务的满意程度对直接交易实体和推荐者的信任值进行更新。

对直接交易实体信任值的更新比较简单。交易完成之后, 实体对目标实体给出一个信任评估值 $T_{ij}(\text{new})$, 这个评估值将用于计算下一次直接信任值。采用一个 FIFO 队列来模拟直接信任值随时间衰减的特性: 将 $T_{ij}(\text{new})$ 插入到定长的直接信任值队列尾, 同时所有的信任值向前移动一个位置, 而队首的交易信息被丢弃。队列的长度取决于对历史信息的重视程度, 对历史信息越重视, 队列长度 M 就越大。

在对推荐者信任值更新的过程中首先需要考虑更新推荐实体的反馈信任值。在本文模型中将静态信任值 T_{static} 作为信任更新时相对准确的信任值, 因为动态信任值主要是反映实体的上下文变化情况的, 不是实体本身信任值的表现。将 T_{static} 与推荐者的推荐信任值进行比较, 取绝对差值, 即 $\Delta =$

$|Tb_{kj} - T_{static}|$, 又设节点 i 对节点 k 容忍的最大评价偏差为 Θ , 如果 $\Delta > \Theta$ 则认为是恶意推荐^[6]。那么反馈信任值可以通过下面的公式进行更新:

$$C_{ik}(\text{new}) = \begin{cases} C_{ik}(\text{old}) + \frac{1 - C_{ik}(\text{old})}{2} \times (1 - \frac{\Delta}{\Theta}), & \Delta < \Theta \\ C_{ik}(\text{old}) - \frac{C_{ik}(\text{old})}{2} \times (1 - \frac{\Theta}{\Delta}), & \Delta \geq \Theta \end{cases} \quad (6)$$

由于在本文模型中的 i 对 k 的反馈信任值取的是 i 对 k 的直接信任值, 即 $C_{ik} = Tb_{ik}$, 因此可以对推荐实体的直接信任值进行适当的更新, 以使得提供诚实推荐的实体的信任值得到提高, 而提供恶意推荐的实体的信任值下降。因此根据上述公式就能得出对推荐实体的信任值的更新公式:

$$Tb_{ik}(\text{new}) = \begin{cases} Tb_{ik}(\text{old}) + \frac{1 - Tb_{ik}(\text{old})}{2} \times (1 - \frac{\Delta}{\Theta}), & \Delta < \Theta \\ Tb_{ik}(\text{old}) - \frac{Tb_{ik}(\text{old})}{2} \times (1 - \frac{\Theta}{\Delta}), & \Delta \geq \Theta \end{cases} \quad (7)$$

从以上公式还可以看出: 当推荐实体的推荐信任值在阈值 Θ 范围内时, 即提供诚实推荐时, 信任增长的比较慢, 但是, 如果提供恶意推荐, 那么推荐实体的信任度就会下降得很快, 这也符合人类社会的特征: 建立信誉的过程很缓慢, 但是破坏信誉却很快。这样就可以降低实体通过积累信任值来进行恶意推荐的危险性。

4 应用实例

下面通过一个具体的实例来对 SDTMPC 模型的应用加以说明。

某教授进入某普适环境, 通过自己的 PDA 请求打印服务, 请求发出后, 打印机实体首先加载相应的信任策略, 并开始搜集所有的信任证据, 这当中包括代表属性信任的身份信息、打印机实体可能存有的直接交易信息、其他实体的推荐信息以及目前打印机本身的上下文信息(比如打印机现在是否能够正常工作)等, 根据模型中的评价方法最终得出教授在此刻能否获得打印这项服务。假如此时计算出上下文信任值过低(比如缺纸等), 即动态信任值过低, 尽管静态信任值可能高, 但是根据信任策略计算出的最终的信任值很低, 因此教授无法获得打印服务。

在另外一种情况下, 某学生也进入了该普适环境, 请求打印服务, 请求发出后, 假设打印机实体依照相同的信任策略计算出的静态信任值过低, 这时候即使打印机能够正常服务, 即动态信任值很高, 但是由于计算出的实体最终信任值小于某一信任阈值, 同样学生也不能够获得打印服务。

5 结语

本文提出的信任管理模型综合考虑了各种信任证据, 解决了根据单一的信任证据计算普适环境下信任值的不完整性。将信任分成静态信任和动态信任, 其中静态信任决定实体的基本信任状况, 由属性信任, 直接信任和间接信任这三种信任证据组成; 动态信任由上下文信任证据决定, 它体现了普适环境的动态性。最终信任值是由静态信任值和动态信任值计算得来的, 它决定是否为请求者提供服务。此外, 采用了事件驱动的更新机制, 对直接交易的实体和推荐实体的信任值进行了更新。

(下转第 272 页)

集的建立不带有主观因素,因而能比较客观地反映生物序列间的关系。与 FDOD 方法相比,它简化了信息集的建立,并且对于相似度较高的序列,信息集的变化对结果的影响很小,具有实现简单、空间复杂度和时间复杂度小的优点。本文方法可以对 DNA 序列的相似性进行有效分析,其计算复杂度随序列长度的增加呈线性增长,因此可用于处理大规模数据。这种方法可以用于序列比较、物种分类、生物进化关系研究等领域,以及多序列的比较问题。

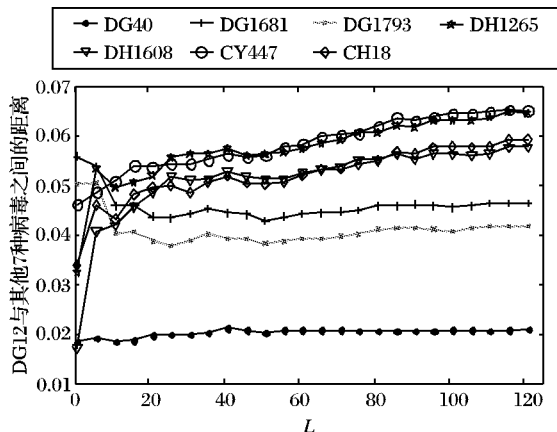


图3 DG12与其他7种病毒的距离随L的变化曲线

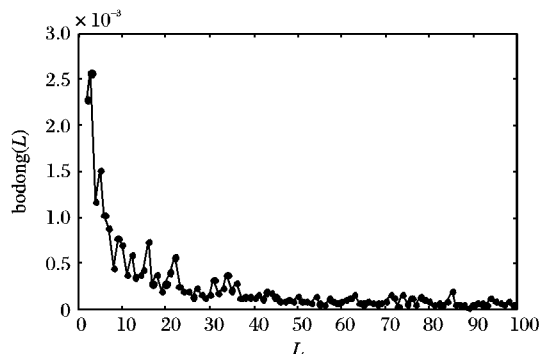


图4 $bodong(L)$ 随L的变化曲线

参考文献:

- [1] 郝柏林, 张淑誉. 生物信息学手册[M]. 上海: 上海科学技术出版社, 2000: 184 - 199.
- [2] 张永, 王瑞. 生物信息学中的序列比对算法[J]. 电脑知识与技术, 2008(1): 181 - 184.
- [3] ZHANG R, ZHANG C T. Z curves: An intuitive tool for visualizing and analyzing the DNA sequences[J]. Journal of Biomolecular Structure and Dynamics, 1994, 11(4): 767 - 782.
- [4] RANDIC M, VRACKO M, NANDY A, et al. On 3-D graphical representation of DNA primary sequence and their numerical characterization[J]. Chemical Information and Computer Sciences, 2000, 40(1): 1235 - 1244.
- [5] LIAO B, WANG T M. Analysis of similarity/ dissimilarity of DNA sequences based on 3-D graphical representation[J]. Journal of Molecular Structure: THEOCHEM, 2004, 388: 195 - 200.
- [6] ZHAO H Q, TONG R F. PN-curve: A 3D graphical representation of DNA sequences and their numerical characterization[J]. Chemical Physics Letters, 2007, 442: 434 - 440.
- [7] FARACH M, NOORDEWIER M, SAVARI S, et al. On the entropy of DNA: Algorithm and measurements based on memory and rapid convergence[C]// Proceedings of the 6th Annual ACM-SIAM Symposium on Discrete Algorithms. San Francisco, 1995: 48 - 57.
- [8] HARID A, WEBER B, OLMSTED J. On the validity of Shannon-information calculations for Molecular biological sequences[J]. Journal of Theoretical Biology, 1990, 147: 235 - 254.
- [9] FANG W W, ROBERTS F S, MA Z R. A measure of discrepancy of multiple sequences[J]. Information Science, 2001, 137: 75 - 102.
- [10] 张文, 唐焕文, 方伟武, 等. 基于全蛋白质组的微生物系统发育树构建[J]. 大连理工大学学报, 2005, 45(6): 925 - 930.
- [11] WANG J H, FANG W W, LING L X, et al. Gene's functional arrangement as a measure of the phylogenetic relationships of microorganisms[J]. Journal of Biological Physics, 2002, 28: 55 - 62.
- [12] JIN L X, FANG W W, TANG H W. Prediction of protein structural classes by a new measure of information discrepancy[J]. Computational Biology and Chemistry, 2003, 27: 373 - 380.
- [13] 齐震, 狐昱, 李蔚等. 基于全基因组比较的 SARS 冠状病毒种系进化分析[J]. 科学通报, 2003, 48(12): 1242 - 1245.
- [14] SONG J, TANG H W. Accurate classification of homodimeric vs other homooligomeric proteins using a new measure of information discrepancy[J]. Journal of Chemical Information and Computer Sciences, 2004, 44: 1324 - 1327.
- [15] 宋杰, 唐焕文. 基于一种新的信息离散性度量方法的同源寡聚蛋白质分类[J]. 数学的实践与认识, 2007, 37(8): 36 - 42.
- [16] 宋杰. 基于离散度函数的 DNA 序列的相似性分析[J]. 计算机与应用化学, 2007, 6(24): 729 - 733.
- [17] LI W, FANG W W, LING L J, et al. Phylogeny based on whole genome as inferred from complete information set analysis[J]. Journal of Biological Physics, 2002, 28(3): 439 - 447.
- [18] LUO J W, ZHANG X Z. New method for constructing phylogenetic tree based on 3D graphical representation [C]// The 1st International Conference on Bioinformatics and Biomedical Engineering, Wuhan: IEEE Press, 2007: 324 - 327.
- [19] RUAN Y J, WEI C L, EE L A, et al. Comparative full-length genome sequence analysis of 14 SARS coronavirus isolates and common mutations associated with putative origins of infection[J]. The Lancet, 2003, 361(9371): 1779 - 1785.

(上接第 151 页)

通过本模型中所提出的信任建立和更新策略,使得实体在交易之前充分考虑普适环境下实体的信任证据,同时对即将交易的实体进行全面的信任评估,从而能够做出正确的交易决策,提高了系统的安全性。下一步的研究工作方向是在本模型基础上给出更加优化的函数来保持模型中信任值计算的准确度。此外还需要在模型中增加相应的机制来识别协同作弊恶意节点并对其进行惩罚,以保障整个普适系统的安全性和稳定性。

参考文献:

- [1] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management [C]// Proceedings of the 17th symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996: 164 - 173.
- [2] JOSANG A. Trust management for E-Commerce[C]// Proceedings of the Virtual Banking. Heidelberg: Springer Berlin Press, 2000.
- [3] 郭亚军, 王亮, 洪帆, 等. 基于信任的普适计算的动态授权模型[J]. 华中科技大学学报: 自然科学版, 2007(8): 70 - 73.
- [4] SHAND B, DIMMOEK N, BACON J. Trust for ubiquitous, transparent collaboration [C]// Proceedings of the 1st Annual IEEE Conference on Pervasive Computing and Communications. Texas: Springer Netherlands Press, 2003: 153 - 160.
- [5] XIU D X, LIU Z Y. A dynamic trust model for pervasive computing environments [C]// Proceedings of the 4th Annual Security Conference. Las Vegas: IEEE Computer Society Press, 2005.
- [6] 常俊胜, 王怀民, 尹刚. DyTrust: 一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报, 2006, 29(8): 1301 - 1307.