一个基于普适计算的动态协同的信任模型①

惠晓威 邹 璐 (辽宁工程技术大学 电子与信息工程学院 葫芦岛 125105)

摘 要: 普适计算环境是一个具有高度动态性的分布式环境，进行信息交互的实体之间存在着自发性和不可预知性。因此，普适计算比传统计算更强调信任的作用，对系统安全也提出了更高的要求。综合了影响信任决策的多个凭证因素，并结合信息安全风险评估，提出一个由信任-信誉模块和风险模块组成的动态协同模型。该模型克服了对影响信任决策的凭证考虑不完整的问题，有利于在实体间建立可靠的信任关系，提高普适环境和信息的安全性。

关键词: 普适计算; 动态; 协同; 信任模型

Dynamic Collaborative Trust Model Based on Pervasive Computing

HUI Xiao-Wei, ZOU Lu(Liaoning Technical University, School of Electronic and Information Engineering, Huludao 125105, China)

Abstract: Pervasive computing environment is a highly dynamic distributed environment in which principals collaborate spontaneously and unpredictably. Therefore, the pervasive computing puts more emphasis on the role of trust and puts forward higher request to system security than traditional calculation. A new dynamic collaborative trust model composed trust-reputation module and risk module was proposed based on combining credence elements and information safety risk assessment. This model resolve the limitations in the integrality of evidence used for the trust judgment, and in favor of setting up the reliable trust relationship in the entities, and improving environment and information security of universal.

Keywords: pervasive computing; dynamic; collaborative; trust model

1 引言

普适计算(Pervasive Computing,简称 PVC，普遍渗透的计算)的思想最早是由已故的前 Xerox PARC 首席科学家 Mark Weiser 博士于 1991 年在《Scientific American》“The Computing for the 21st Century”中提出的[1]，他主张计算机的使用应迎合人的习性，融入人的日常环境及工具中，并自主地与使用者产生互动。他认为普适计算的发展将带领人们进入“平静技术”时代--让技术无缝地融入日常生活，使人们摆脱技术带来的压迫感，使技术处于非妨碍状态，无需用户分散精力进行干预，为人们描绘了一个美好的未来信息世界。

本文对普适计算定义为：在信息空间与物理空间相融合的智能空间中，信息设备与环境进行流畅自主的信息交互而完成用户信息任务的服务。

普适计算以人的需求为中心，从根本上改变了人去适应机器被动式服务思想，打破了计算只局限于桌面进行的传统，它使用户在不被打扰的前提下主动、动态的接受网络服务，用户可以以各种灵活的方式享受计算能力和系统资源。因此，普适环境具有一些新的特点[2]:

(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) 数据动态产生;

(3) 用户访问权限动态变化;

(4) 系统典型分散。由于其高度动态性，普适计

① 基金项目:辽宁省教育厅基金项目(基于 SDR 的智能天线基站信道分配优化算法研究)(2004D028)
收稿时间:2010-03-30;收到修改稿时间:2010-04-26

算比传统计算更强调信任的作用，对系统的安全性提出了更高的要求。为此，本文提出了一种适用于普适环境下的动态协同信任模型。

2　信任-信誉模块

目前绝大多数的研究者认为信任信息是主要来自主体的观察，他们用主体的观察结果和第三方观察结果(称为经验)评估信任[3]。但是普适环境中主要涉及陌生主体的交互，最初的信任不可能仅仅只来自观察的结果。因此，我们综合实体的属性，经验，第三方推荐和上下文信息来建立信任-信誉评估模型。

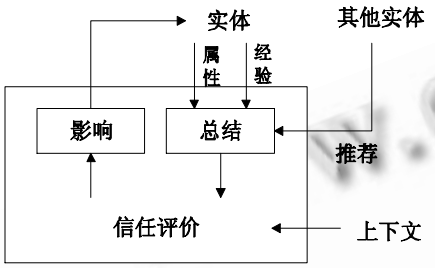

图 1　信任-信誉模块

在普适计算中，建立主体之间的信任主要有两个方面：一个是根据主体的属性等建立的静态信任；二是根据上下文信息建立动态信任[3]。

对于主体 p_i 和 p_j，p_i 对 p_j 的信任值表示为：$T=(T_a,T_e,T_r,T_c)$。

其中，T_a 是由主体的属性产生的信任值，T_e 是主体历史经验决定的信任值，T_r 是第三方对实体的推荐信任值。

这三个部分是信任值的静态部分，一旦确定后，它的值不会变化，文中称其为静态信任值。

T_c 是信任值的动态部分，它随着上下文信息的变化而变化，文中称其为动态信任值。

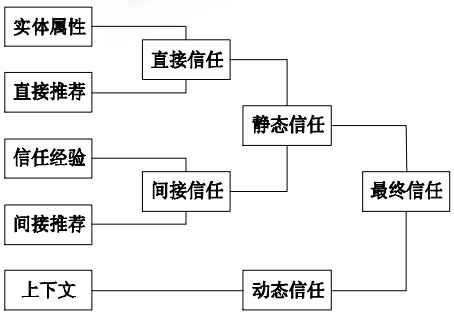

图 2　信任分类

信任值 T 离散地表示为(-1，0，1，2，3，4)，分别表示 distrust, ignorance, minimal, average, good, complete 这六个等级。

3　风险模块

在普适计算环境中，为了向用户提供透明和自发的信息服务，系统需要通过环境中的无处不在的计算设备获得用户的上下文信息。鉴于上下文信息的高度动态性以及不确定性，为进一步保证普适计算中信息的完整性、准确性和安全性，需要引入风险[4]模块来协同做出信任决策。

风险模块的任务就是对信息安全进行风险评估，是对信息在产生、存储、处理、传输等过程中的保密性、完整性、可用性、可控性、不可否认性等信息安全属性遭到破坏的可能性以及由此产生的后果所作的评价或估计。

在本文认为风险由“相对的动态变化”引起。在普适系统中，超过正常范围内的动态变化才是能够引起信息风险的真正变化[5]。因此，通过监视普适计算上下文信息的动态变化来感知风险。

文中这样定义风险界限：

风险 $risk=(I,Q,j)$。

其中，$I=\{S,E,R\}$。I 表示监视的上下文信息的集合，S 表示空间信息，E 表示环境信息，R 表示可访问的资源信息。

$Q=\{q_1,q_2,q_3|0<q_i<1,\sum_i^3 q_i=1\}$。$Q$ 表示引起风险的各个变化因素在整个普适系统的“风险”判定中所占的权重。充分考虑不同后果属性的权重，才能真正得到切合被评估对象的实际情况的安全风险评估结果[6]。

用 j 来表示风险的判定阈值，倘若有：$S\times q_1+E\times q_2+R\times q_3>j$，认为有风险，反之，认为无风险。

4　动态协同模型

在普适计算中，主体的信任度是由多方面的因素决定的，因而在确定各主体的信任向量时必须考虑多方面的影响因素。本模型对受到多个因素制约的主体做出信任评估，由于信任的模糊性导致很难做出准确的信任决策，因此采用模糊综合评估法作为本模型的

多因素决策方法。

信任因素集为$T=\{T_a,T_e,T_r,T_c\}$，各因素权重分配为$P=\{p_1,p_2,p_3,p_4\}$，$\sum_i p_i=1$，$0<p_i<1$。

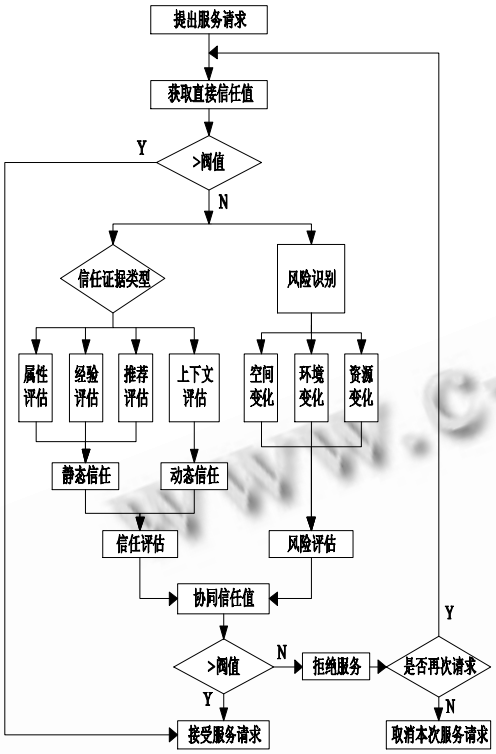

图 3　动态协同模型

评估等级为$\{4,3,2,1,0,-1\}=\{$完全信任，非常信任，一般信任，有点信任，不确定，不信任$\}$，将等级量化为$L=\{1,0.8,0.6,0.4,0.2,0\}$。

得到信任因素的评估矩阵$M=(m_{ij})_{T\times L}=(m_{ij})_{4\times 6}$，综合评估为$V=P\circ M$。

(T,L,M)构成模糊信任评估。在评估过程中，只需要根据主体的具体情况就可推算出主体的信任向量。结合另一方面的风险评估，若此次信息任务不存在风险，则仅用信任评估值对应到信任等级来判别此次信息任务是否值得信任；若存在风险，则用信任评估值与风险值进行运算后再转到相应的信任等级来判别此次信息任务是否值得信任。

由于信任具有时间滞后性，信任值随着时间的增长而衰减，并且在很大程度上受推荐信任的影响而变化，在模型中引入信任更新盒(如图 4)，其目的有二，一方面对过于繁杂的历史信任信息进行整理清除，达到普适系统的轻量级计算的要求，另一方面根据本次普适服务的满意程度对直接交互实体和其推荐实体的信息值进行更新，达到降低恶意推荐的危险性，若推荐者提供诚实推荐，基信任值就增长；若推荐者提供恶意推荐，其信任值就下降，这也很符合人类社会的信誉特性。

信任的时间衰减函数$f(t)$[7]：

指数衰减函数：$f(t)=e^{-at},t\geq 0$

倒数衰减函数：$f(t)=\frac{1}{a\times t+1},t\geq 0$

式中a为衰减系数，控制着信任值的时间衰减速率。

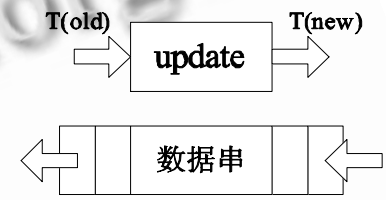

图 4　信任值更新

每一次完成信息交互任务之后，实体得到的信任值将用于计算下一次的直接信任值。采用一个数据队列来模拟该实体的历史信任，新的最终信任值插入到队尾，同时对所有的历史信任值向前移动一个位置，队首的信任值直接被删除。若在此次信息任务中有第三方实体对该实体给予推荐信任，则对此推荐者也进行信任值更新，根据此次服务的满意度　来增减推荐者的属性信任。

5　应用实例

本模型通过计算主体的综合信任度来确定主体是否值得信任。信任评估阶段的影响因素有属性信任，经验信任，推荐信任和上下文影响的信任，因此以这四个要素作为参数进行信任评估分析。而由空间变化、环境变化和资源变化引发的风险作为影响风险评估的三因素来进行分析。动态的风险评估更具有现实意义[8]。

设：信任因素集$T=\{T_a,T_e,T_r,T_c\}$的各因素权重分配为$P=\{0.3,0.2,0.2,0.3\}$，建立信任评估矩阵：

$$M=\begin{bmatrix}0.6 & 0.1 & 0.2 & 0.1 & 0 & 0\\ 0.3 & 0.3 & 0.1 & 0.1 & 0.2 & 0\\ 0.4 & 0.2 & 0.1 & 0.2 & 0 & 0.1\\ 05 & 0.1 & 0.2 & 0 & 0.1 & 0.1\end{bmatrix}$$

计算得综合评估：$V = P \circ M = (0.47 \quad 0.16 \quad 0.16 \quad 0.09 \quad 0.07 \quad 0.05)$ 根据信任等级量化值 $L = \{1,0.8,0.6,0.4,0.2,0\}$ 可知，该实体的最终信任评估结果为：$W = V \circ L = 0.744$。

又设：风险因素集 $I = \{S, E, R\}$ 的各因素权重分配为 $P = \{0.4,0.2,0.4\}$，建立风险评估矩阵：

$$N = \begin{bmatrix} 0.5 & 0.2 & 0.1 & 0 & 0 & 0.2 \\ 0.3 & 0.2 & 0.2 & 0.1 & 0.1 & 0.1 \\ 0.4 & 0.1 & 0 & 0.3 & 0.2 & 0 \end{bmatrix}$$

计算得最终风险评估 $U = 0.654$ (大于风险门限值 $j = 0.5$)，那么认为此次信息任务存在交易风险。

协同信任值为 0.486576，对应到信任等级 $1.6 > 0$。则判定此次信息任务值得信任。

6 结语

本文提出的动态协同信任模型综合考虑了影响最终信任决策的多种凭证因素，并结合普适服务中必然存在的安全风险，使得系统能够做出较为正确的交互决策，有利于实体的全面信任评估和系统的安全稳定性。下一步的研究工作方向是在本模型的基础上设计出更优化的函数及算法来保持其信任度的准确度量，此外还需要全面考虑如何更有效的进行隐私保护和防止恶意攻击对实体和系统带来的扰乱影响，确保整个普适系统的安全性和稳定性，以及在普适环境下信息交互的准确性和高效性。

参考文献

1 Li Shiqun, Shane Balfe, Zhou Jianying, Chen Kefei. Trust Based Pervasive Computin. Wuhan University Journal of Natural Sciences, 2006,11(6):1477—1480.

2 BLAZEM, FEIGENBAUM, LACY J. Decentralized trust management. Proceedings of the 17th symposium on Security and Privacy. Oakland IEEE Computer Society Press. 1996:164—173.

3 郭亚军,洪帆.普适计算的信任计算模型.计算机科学, 2005,32(10):59—62.

4 牛旭明,李智勇,桂坚勇,耿振国.信息安全风险评估中的关键技术.信息安全与通信保密, 2007,4:17—20.

5 马彬.基于云理论的普适计算协同信任模型.计算机工程, 2008,34(9):162—166.

6 杨洋,姚淑珍.一种基于威胁分析的信息安全风险评估方法.计算机工程与应用, 2009,45(3):94—100.

7 孙道清.基于信任和服务模型的普适计算安全问题研究[博士学位论文].东华大学, 2008.10.

8 史简,郭山清,谢立.一种实时的信息安全风险评估方法.计算机工程与应用, 2006,42(42):109—111.