普适计算环境下信任机制的研究进展*)

徐文拴　辛运帏　卢桂章
(南开大学信息技术科学学院　天津 300071)

摘　要　在普适计算环境下,各种资源、设备和用户均是高度动态变化的,服务请求者和服务提供者一般互相不了解,因此普适计算环境下各陌生实体间的相互认证是传统的基于身份的认证机制无法解决的。普适计算信任建模机制可以解决普适计算环境下的不确定性问题,为陌生实体间建立信任关系,因此成为普适计算中的一个研究热点。基于此,本文对于目前国外关于普适计算信任建模机制的研究现状做了一个总结,通过分析和比较,给出了普适计算信任建模的设计原则,探讨了普适计算信任建模问题的未来发展方向。

关键词　普适计算,信任,信任模型

Research and Development of Trust Mechanism for Pervasive Computing

XU Wen-Shuan　XIN Yun-Wei　LU Gui-Zhang
(College of Information Technical Science, Nankai University, Tianjin 300071)

Abstract　In pervasive computing environment, various resources, devices and users are frequently changeable. Service providers and requesters commonly do not know each other. Therefore, it becomes an important foundation to identify unknown entities for pervasive computing security. However, explicit identity is the base for traditional authentication methods. Strange entities can't be authenticated by those conventional solutions. Fortunately, trust model can solve the uncertainty problem in pervasive computing environments and set up trust relationship between strange entities. Consequently, it becomes one of the hot spots in pervasive computing research presently and there is much related work on it. Based on the status quo, an overview is made in this paper, in which different solutions presented are analyzed and discussed. Subsequently, several design guidelines of trust modeling for pervasive computing are summarized, too. Finally, a summary and a prospect for further interesting research directions are proposed.

Keywords　Pervasive computing, Trust, Trust model

自从1994年S. P. Marsh首次将信任机制研究引入计算机领域[1],信任已经被广泛应用于计算机科学的各个领域,如普适计算、对等计算、移动计算等。在普适计算环境下,各种资源、设备和用户均是高度动态变化的,服务请求者和服务提供者一般互相不了解,因此普适计算环境下陌生实体间的相互认证是传统的基于身份的认证机制无法解决的。信任建模机制为普适计算环境下的不确定性问题提出了一个很好的解决方案,通过普适计算信任模型的建立,可以为陌生实体间建立相应的信任关系,从而可以根据不同的信任值确定不同的安全等级,进而已有的一些传统的认证机制就均可应用于普适计算环境之中。可见,如何在普适计算环境中的陌生实体间建立信任关系成为一个难点。目前,存在大量的研究关注于如何在普适计算环境下的实体之间进行信任建模。

1　普适计算环境下信任关系的特点

在普适计算环境下,不同的应用情景、不同的应用目的对于信任关系影响都是较大的。一般来说,信任关系具有如下特点:

- 自反的。也就是实体相信实体本身。
- 条件传递的。如果实体A信任实体B,而实体B又信任实体C,则认为实体A信任实体C,但信任的程度有可能不同。
- 反对称的。也就是,如果实体A信任实体B,但反之,实体B不一定信任实体A。因此,信任关系是反对称的。
- 主观的。实体A对于实体B的信任程度是主观的,按照实体A的意图、状态、行为等因素而不同。
- 上下文敏感的。信任关系是上下文敏感的,不同的时间、环境、位置,信任程度是不相同的。
- 动态的。实体间的信任关系是动态变化的。一般来说,信任关系会随着时间、实体的属性、历史行为、当前行为、未来意图等特性而变化。

已有的一些研究或多或少地考虑到了以上这些因素,利用信任关系的这些特点,按照不同的研究意图,采用不同的理论方法对普适计算环境中的信任关系进行建模。本文第2节将介绍普适计算信任模型面临的挑战;第3节对已有的一些研究工作分类进行分析和总结;在此基础之上,第4节归纳普适计算信任模型的设计原则;最后总结全文并探讨未来的研究方向。

2　普适计算信任模型研究面临的挑战

普适计算环境相对于传统计算环境具有其自身的特点。

*)天津市应用基础研究计划(自然科学基金)项目(06YFJMJC00200);南开大学创新基金项目。**徐文拴**　博士研究生,主要研究方向:普适计算、信息自动化;**辛运帏**　博士,教授,主要研究方向:普适计算、信息加密技术;**卢桂章**　教授,博士生导师,主要研究方向:信息自动化、智能机器人系统。

因此，与传统的基于身份的认证机制相比，普适计算信任机制也具有其独特性。这样，普适计算信任模型的研究就面临很大的挑战：

(1)普适计算环境下的不确定性。不确定性是普适计算环境同传统的计算环境最大的区别之一，也是传统的基于身份的认证方法不可直接应用于普适计算实体认证的重要原因。

(2)信任建模的标准不统一。已有的研究针对不同的目的，采用不同的设计标准和设计理论，导致信任模型没有一个统一的标准。

(3)信任模型正确度的度量标准。目前还没有一种统一的衡量普适计算信任模型的准确度的方法。

(4)信任模型的集成应用问题。信任模型研究的目的就是要将其应用于实际的普适计算环境。因此，如何同已有的一些普适计算软件系统功能模块相互集成、提供服务，是另外一个重要问题。

(5)模型精确性同模型的轻量级之间的矛盾。模型越精确，模型就越复杂。相应地，对于设备的资源开销也就越大，而普适计算环境下存在大量资源受限的设备。因此，如何在二者之间进行一个合理的权衡是必须考虑的又一个重要问题。

由于普适计算环境中存在大量小型嵌入式计算设备，在普适计算环境下进行信任关系建模时，需要考虑以下几个重要因素：①计算能力消耗。信任建模时，对于设备的计算能力不能有过高的要求。②存储能力消耗。信任建模时，对于设备的存储能力不能有过高的要求。③ 电池能量消耗。信任建模时，尽量减少设备的电池能量消耗。

也就是说，信任模型的建立应该是轻量级的，能够适用于普适计算环境下一些计算能力、存储能力、电池能量等资源受限的小型嵌入式设备，而这些设备在未来普适计算环境中规模是相当庞大的。

3 相关研究分析总结

目前关于普适计算信任模型的研究工作有很多。已有的一些研究主要集中在普适计算信任建模理论、普适计算软件体系结构中的信任模块研究以及普适计算信任模型的概念模型、需求分析等方面。

3.1 基于不同理论的普适计算信任模型的研究

基于不同理论的普适计算信任模型的研究有很多，研究的目的不同，采用的建模理论也各不相同。当前的研究主要集中在模糊逻辑、图论、云理论、概率理论等方面。

·基于模糊逻辑的信任模型研究

在信任管理中，间接信息和主观判断是不确定性的主要来源。Z. Wu 等在文[2]中认为这种不确定性不能视为是一种概率，而将模糊逻辑(fuzzy logic)引入到信任的定义和估计之中，提供了模糊规则的表示方法，还提供了一个派生规则集合用于模糊规则的分析和推理，以某种层次的不确定性来执行这些规则。提出的信任模型可以直接用于信任管理中评估、分析、派生规则，为处理不确定性提供了一种新的方法。

· 基于图论的信任模型研究

P. Sant 等在文[3]中提出了一个基于图理论的信任框架，认为应该以全局观点来看待信任，定义了信任图的概念：$G_T=(V, E)$。顶点集合 V 是一个包含人类代理(human agent)以及 m 个软件代理(software agent)的集合；边集合 $E=\{(u, v): u, v\in V\}$ 表示 u 信任 v 的概念；G_T 是一个有向图，它意味着一条边 $e=(u, v)$ 中的一个代理信任另外一个代理；边上的权重 $w(e)$ 代表信任值。然而，该文中没有给出信任值的计算方法，对于信任的传递关系只是给出了两个可能的计算公式，并未验证其准确度。

·基于云理论的信任模型研究

R. He 等在文[4～6]中指出不确定性是信任的一个重要特征，提出了基于云理论对信任建模的方法。首先对云理论按照需求进行了扩展：基于模糊统计方法提出了一种计算云的方法，并且考虑了云的扩散特性(diffusion)；为支持不确定性推理，模型中定义了两种云操作：复合操作(compound operation)和一致操作(consensus operation)。使用复合操作可以处理信任传播(trust propagation)问题，使用一致操作可以处理信任聚合(trust aggregation)问题。然后提出了基于云模型的信任模型 CBTM 和基于扩展的云模型的信任模型 ECMBTM，分别应用于普适计算和对等计算环境。基于云理论的信任模型总结如表 1 所示。

表 1 基于云理论的信任模型总结与比较

应用领域	信任模型
普适计算	CBTM[4,5]
对等计算	ECMBTM[6]

此外，作者还提出了一些信任模型的度量标准：平均信任密度(ATD: Average Trust Density)、成功协作概率(SCP: Successful Cooperation Probability)和正确预测概率(CFP: Correct Forecast Probability)等，用以对信任模型的准确度进行评价。

·基于概率理论的信任模型研究

这方面的研究大部分都集中在对贝叶斯理论的应用方面。如 W. Yuan 等在文[9]中提出的信任模型包含两种措施，以做出信任决策：基于角色的决策和基于朴素贝叶斯分类器(Naive Bayes Classifier)的决策。当服务提供者获取服务请求之后，首先利用基于角色的决策模块做出信任决策；如果服务请求者的角色没有足够的权限以使用某种服务，就要使用朴素贝叶斯分类器动态地做出决策。模型中使用上下文确定服务请求者的角色，角色被定义为层次结构，以便于管理和使用。由于普适计算环境的动态性和不可预知性，信任模型应该动态做出决策。在文[10]中作者又提出了一个基于朴素贝叶斯分类器的信任模型，可以在不同的环境中动态做出决策。该信任模型基于服务提供者的信任级别使用两次朴素贝叶斯分类器动态做出信任决策：首先可以依靠服务提供者自己的预先知识做出决策而没有推荐；如果服务请求者同服务提供者不熟悉或者没有足够的权力访问该服务，那么再利用其他推荐者的推荐并结合服务提供者自己的预先知识来做出最终的决策。PTM[7]则是一个简单信任管理模型，使用模糊逻辑来表达信任关系，还提出了一个数学和一个概率信任变化模型(trust evolution model)，用以减小环境的不确定性。

基于概率理论的普适计算信任模型总结如表 2 所示。

表 2 基于概率理论的信任模型总结与比较

概率理论	信任模型
贝叶斯理论	PTM[7]、D. Quercia 等[8]
朴素贝叶斯分类器	W. Yuan 等[9,10]

·基于信任值矢量的信任模型研究

由于普适计算环境的动态特征，传统的基于数据库认证实体的访问控制机制已经不能满足需要。文[11]基于不同实体的信任值矢量提出了一个信任模型，引入了评估因子来计算信任值以及有效处理错误推荐。信任的评估依赖于实体的推荐，按照以往交互的数量和时间进行衡量。然而，作者并未具体实现这个提出的信任模型并将其应用于普适计算系统之中。文[13]则提出了另外一种基于属性矢量微积分的信任建模方法，可以很方便地获取基于身份和基于上下文的信任关系。该文只是给出了建模的方法，并未具体实现。

·基于 Agent 的信任模型研究

Z. Liu 等在文[14]中引入一个基于 Agent 的信任协调(trust negotiation)框架，通过一种主动的信任协调模式客户端可以同系统建立信任关系。模型使用移动代理对信任协调策略进行编码，并将这些策略动态地分发或上传，代理的移动性、透明性、可配制性使得这个信任框架灵活、自适应。文[15]提出的信任模型利用模糊数字来表示信任，以捕获信任值及其不确定性，将可信 Agent 定义为 type-2 模糊集合，并利用模糊规则计算和模糊控制领域中的方法来制定信任措施。但是，模型中没有考虑 Agent 行为的时间可变性(time variability)，也没有集成声望和风险分析机制。

表 3　基于不同理论的信任模型总结与比较

采用理论、方法	典型信任模型
模糊逻辑	Z. Wu 等[2]、PTM[7]
图论	P. Sant 等[3]
云理论	CBTM[4,5]、ECMBTM[6]
概率理论	PTM[7]、D. Quercia 等[8]、W. Yuan 等[9,10]
信任值矢量	L. X. Hung 等[11,12]、N. Shankar 等[13]
Agent 技术	Z. Liu 等[14]、M. Rehak 等[15]
卡尔曼滤波器(Kalman filter)	L. Capra 等[37]

从表 3 可以看到，基于不同理论对普适计算信任建模的研究是现在研究的一个热点。这其中，大部分研究基于传统理论，如模糊逻辑、概率理论等，来解决普适计算环境下的不确定性问题。同时还应该注意到，其它学科中的一些理论，如控制论中的云理论、图论、Agent 技术等，也被借鉴应用于普适计算信任模型的研究。既充分利用传统的理论方法，同时又不断探索从其它学科引入新的理论，有所创新和突破，这可能是未来普适计算信任模型研究的一个发展方向。

3.2　基于传统认证机制的信任模型研究

将传统安全控制机制改进应用于普适计算信任模型，是目前研究的另外一个发展方向。

关于这个方面的研究工作也有很多，如文[17]提出了一个动态可扩展的开放框架，结合了安全措施、证书和施行协议在普适应用和服务中提供安全和信任；A. A. Pirzada 等在文[18]中提出了一种新的认证和密钥交换方案，设备通过执行认证和密钥交换协议来获取会话密钥，从而获取安全通信，而不利用信任第三方。然而，该方案中的初始化阶段仍然需要密钥分发中心发布设备私钥以及自己的公钥，因此这个密钥分发中心仍然是一个可信第三方；文[19]基于交互历史对实体认证，使用组盲签名(group blind signature)机制来提供一个难以跟踪的签名密钥(密钥证书)，从而使得信任关系成为可能。但是，信任第三方的出现使得该方案在普适计算环境下的应用受到限制；D. Xiu 等在文[38]中提出的动态信任模型包含了信任策略、环境上下文、信任根据(trust evidence)以及来自相应的应用模块的评价结果，其中的信任策略包括访问控制(access control)及 PKI(公钥基础设施)技术、信任商议(trust negotiation)、信任委托(trust delegation)、基于声望的信任(trust based on reputation)、基于上下文和本体的信任(trust based on context and ontology)以及安全的数据流和信息隐私等方面。

表 4 对基于传统认证机制的信任模型进行了总结。传统的认证机制基于身份提供安全或认证控制，对于高度变化的普适计算环境来说是不适用的。此外，传统的加密和认证算法对于设备的计算能力要求过高，不能适用于普适计算环境中的大量资源受限设备。因此，如何针对普适计算环境自身的特点，对传统的加密或认证算法进行改进应用可能是未来研究的一个发展趋势。

表 4　基于传统认证机制的信任模型总结与比较

传统机制	信任模型
公/私钥、签名机制、哈希算法、对称加密、时间戳等	PrudentExposure[16]
安全措施、证书和施行协议	T. Walter 等[17]
公/私钥、密钥分发中心、时间戳等(未引入可信第三方)	A. A. Pirzada 等[18]
组盲签名	L. Bussard 等[19]
假名机制	D. Quercia 等[8]
访问控制及 PKI、基于声望、上下文和本体的信任等	D. Xiu 等[38]

3.3　不同软件体系结构中信任模块的研究

目前在各种普适计算软件体系结构的研究中，大部分都包含了信任管理模块，通过与其它功能模块相集成，可以更加有效地提供服务。典型的有 MARKS 中间件、CAMUS 中间件和 SECURE 项目等的相关研究。

·MARKS 中间件中的信任模块

MARKS 中间件[20]由一系列核心组件和服务组成，其中关于信任组件的研究工作有很多。

信任模型 m-LPN[21]是基于 Hopper-Blum 协议对著名的 LPN(Learning Parity with Noise)的改进形式，未来将会把 m-LPN 作为一个认证服务添加到 MARKS 中间件中。

SSRD[22]是一个安全的资源发现模型，它基于一个轻量级的改进的 PGP(Pretty Good Privacy)信任模型，是 SAFE-RD[23](MARKS 中间件中的资源发现模块)的一部分；SSRD +[24]则是对已有 SSRD 模型的一个扩展，增加了动态的信任关系和一个风险模型，以解决普适计算网络以及 Ad hoc 网络带来的问题。

文[25]为普适计算应用的安全提出了一个灵活的、可管理的、可配置的信任方案，无线设备基于可用资源和要求的安全功能可以分解为不同的策略，未来将把其作为信任服务集成到 MARKS 中间件的核心服务之中。

·CAMUS 中间件中的信任模块

CAMUS 中间件[26]是一个普适计算上下文感知中间件，其中对信任/风险控制的研究工作也有很多。

TBSI[27]信任架构基于组件技术，包含五个主要的模块：认证、访问控制、信任管理、家庭防火墙和入侵检测系统(IDS)。其中信任和风险管理可以支持对于未知用户的认证

和授权。引入家庭防火墙用于保护智能空间中的中心服务器和网络架构，每个模块的设计都是轻量级的。正在研究的安全措施包括访问控制措施、防火墙措施、IDS 措施等，未来将在 CAMUS 中间件中集成应用该架构。

USEC[28]为 CAMUS 中间件而开发，由七个主要组件组成：混合访问控制、实体识别、信任/风险管理、入侵检测、隐私控制和家庭防火墙。混合访问控制是 USEC 架构的核心部件，是 RBAC（Role-Based Access Control）、PBAC（Policy-Based Access Control）、CBAC（Context-Based Access Control）和 TBAC（Trust-Based Access Control）等的集成应用，以避免单一措施的缺点；实体识别模块集成了各种认证方法，如传统的认证方法（账号/口令、PKI、Kerberos 等）和最新的实体识别技术等，可以支持多种设备；信任/风险管理可以为访问控制管理器提供信任值，以支持漫游实体间的信任协作和交互；入侵检测系统用于防止未授权的访问以及合法用户滥用权限；隐私控制提供位置隐私、匿名连接和用户信息的机密性；家庭防火墙用于保护智能空间免受外部攻击。信任/风险管理、入侵检测系统和家庭防火墙等组件可以一起支持实体识别。

文[29,30]提出了另外一种基于上下文的方法为普适计算环境中的信任模型发现可靠的推荐以及过滤不平等的推荐，上下文用于分析用户的行为、状态和意图，使用基于增量学习的神经网络处理上下文来检测可疑推荐。然而，这个基于上下文的信任模型中并未考虑风险分析机制。

· SECURE 项目的信任模块

文[31]提出了一个动态的信任模型，模型包括信任形成（trust formation）、信任演化（trust evolution）和信任应用（trust exploitation）等几个方面，可以提供更加细粒度的信任关系，它是 SECURE 项目的一部分。

表 5　几种典型普适计算软件体系结构中的信任模块总结

研究项目	信任模块	采用方法
MARKS 中间件[20]	m-LPN[21]	基于 Hopper-Blum 协议对 LPN 的改进
	SSRD[22]	信任模型同安全模型相结合，信任模型基于改进的 PGP
	SSRD+[24]	是对 SSRD 的扩展，增加了动态的信任关系和风险模型
CAMUS 中间件[26]	TBSI[27]	认证、访问控制、信任管理、家庭防火墙和入侵检测系统
	USEC[28]	混合访问控制、实体识别、信任/风险管理、入侵检测、隐私控制和家庭防火墙
	W. Yuan 等[29,30]	基于增量学习的神经网络
SECURE 项目	C. English 等[31]	包含信任形成、信任演化、信任应用等，信任关系粒度更细

对 MARKS 中间件、CAMUS 中间件和 SECURE 项目中的信任模块的总结如表 5 所示。目前关于普适计算软件体系结构的研究开展得非常广泛，而信任模块是软件体系结构中不可缺少的一个组成部分。未来的研究可能更加关注于如何开发信任模块，使得其可以与其它功能模块（如服务发现模块、上下文服务模块等）更好地集成在一起，为用户提供综合性应用服务，从而提高系统的集成性和可用性。其中，中间件组件的实现形式可能是一个比较好的选择。可以采用不同方法开发不同类型的信任组件，进而再把这些组件集成到一个完整的软件系统中，提供更为有效的应用。

3.4　对于信任模型的概念模型的研究

从软件工程的角度，对普适计算信任模型的需求进行总结和分析，进而提出普适计算信任模型的概念模型或建立方法，是目前研究的又一个重点。

如 Z. Yan 在文[32]中为建立一个可信的移动环境提出了一个概念架构，从信任的相关概念（concept）、建模的理论和方法（theory）、建模标准（practice）和实际应用（application）四个方面对这个概念架构进行了阐述；文[34]则主要研究在普适计算及 ad hoc 网络环境下信任建模的需求，提出的信任建模方法包含五个步骤：情景分析和概念需求、概念模型开发、数学模型开发、软件开发和构建信心（confidence building）。基于此，提出信任建模的需求应该包括以下几个方面：可配置性、访问控制、应用、设备和连接、商议协议、信任的量化、安全的声明周期和上下文等。

表 6 总结了相关的研究情况，这些工作对于未来信任模型的研究可以起到很好的借鉴和指导作用。

表 6　信任模型的概念模型的研究总结与比较

主要研究内容	相关研究
信任的概念模型	Z. Yan[32]
信任建模的需求、信任建模的方法	P. Lmsal[34]

国外关于普适计算环境下的信任机制的研究工作还有很多[39~46]。限于篇幅，这里不再一一介绍。下面将从几个方面总结和探讨普适计算信任模型的设计原则以及未来的发展方向。

4　普适计算信任模型的设计原则

基于以上对于相关研究情况的分析和比较，以及第 2 节对普适计算信任模型面临的主要问题的总结，再结合普适计算环境的主要特征，可以归纳普适计算信任模型的设计原则如下：

（1）根据不同的研究目的选择合适的理论进行建模。研究目的不同，可能对于信任值的计算方法不同，因此选择恰当的理论和方法进行信任建模非常重要。

（2）能够合理解决不确定性问题。普适计算信任模型的主要目标就是为了解决环境中的不确定性，进而采取措施进行相应的安全控制，这是设计的首要目标。

（3）集成风险分析、声望等机制。信任同风险分析、声望等紧密相关。良好的风险分析以及声望等机制的运用，可以使信任模型发挥更好的效果。

（4）动态地计算信任关系。信任模型应该能够根据普适计算环境的变化及时做出合理的信任决策，这就要求信任模型必须是动态的，必须能够根据上下文计算信任值，做出正确的信任决策。

（5）能够集成应用于普适计算软件体系结构。在普适计算环境下，信任模型研究的最终目的是应用于普适计算软件体系结构中，同软件系统的其它模块相整合，从而发挥普适计算软件的整体功能。

（6）遵循已有的设计标准及模型度量标准。信任模型的设计必须考虑到已有的设计标准，在模型的正确性评估时也应该以已有的度量标准为依据，这样才能有利于普适计算应用的推广和普及。

（7）轻量级的。信任模型的设计对计算能力、存储能力、

电池能量消耗等不能有过高的要求，因为在普适计算环境下，存在大量的嵌入式资源受限的设备，必须考虑到信任模型的应用对象。

总结及讨论 普适计算信任建模机制的研究是目前普适计算领域中的一个研究热点。本文分类总结了国外已有的相关工作，在此基础之上归纳总结了普适计算信任建模时需要考虑的若干问题。通过对现有研究成果的分析和比较，结合国外的一些研究[32~36]，可以得出未来普适计算信任模型研究的发展方向：

(1)普适计算信任模型建立标准的研究。从目前已有的一些研究情况来看，大部分都是针对某一具体的目的，选择相应的理论或方法对普适计算环境下的信任关系进行建模，而没有一个统一的信任模型建立标准。随着普适计算应用的推广和普及，未来关于这方面的研究很有必要。

(2)普适计算信任模型度量标准的研究。也就是对信任模型的准确度、有效性进行合理的评价和分析。目前关于这个方面的研究还不多见，大多是在提出信任模型之后对于信任模型有一个评测，但还没有一个标准的通用的度量标准。随着普适计算信任模型研究的进一步深入，关于模型度量标准的研究已经显得尤为重要。

(3)应用于某种具体场景的普适计算信任模型的研究。目前普适计算的应用正日益深入，不同场景的应用亟需对应的普适计算信任模型对环境的安全提供保障。随着普适计算应用的进一步推广，这个方面的研究会越来越多。

(4)集成其它安全机制的普适计算信任模型的研究。目前普适计算信任模型中对于实体间信任关系的建立主要依赖于历史交互经验，以及其他实体的推荐。然而，其它一些比较重要的因素，如声望、风险、安全等级等，却较少考虑。一个全面的行之有效的信任模型应该考虑到各个方面的要素。未来集成其它各种安全机制的普适计算信任模型的研究应该是发展的一个方向。

(5)基于其它理论的普适计算信任模型的研究。从第3节的总结可以看出，目前已经有一些研究借鉴其它学科的理论，如云理论、图论等，对信任关系进行建模。未来的研究应该是更加开放的，相关研究也会越来越广泛。

(6)普适计算信任模型实现机制的研究。目前的一些研究已经开始关注于信任建模的实现机制，如基于 Agent 技术的实现、基于中间件技术的实现等，但还不成熟。未来这个方面的研究也是一个很有潜力的发展方向。借鉴不同实现技术具有的优点，为信任模型的建立提供更加便利的条件，这可能是未来普适计算信任模型实现机制研究的一个发展趋势。

(7)轻量级普适计算信任模型的研究。第3节中已经介绍了一些关于轻量级普适计算信任模型的研究。随着普适计算应用的推广和普及，会有越来越多的小型嵌入式资源受限设备出现，因此，轻量级普适计算信任模型的研究和开发必将成为一个十分重要的问题。

参 考 文 献

1 Marsh S P. Formalizing trust as a computational concept: [Ph D Thesis]. University of Stirling, 1994

2 Wu Z, Weaver A C. Application of fuzzy logic in federated trust management for pervasive computing. In: Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06), Chicago, Illinois, USA, September 2006. 215～222

3 Sant P, Maple C. A graph theoretic framework for trust - from local to global. In: Proceedings of 10th International Conference on Information Visualization (IV 2006), London, UK, July 2006. 497～503

4 He R, Niu J, Zhang G. CBTM: A trust model with uncertainty quantification and reasoning for pervasive computing. In: Pan Y, Chen D, Guo M, et al. eds. Proceedings of the Third International Symposium on Parallel and Distributed Processing and Applications (ISPA 2005), Nanjing, China, November 2005. 541～552

5 He R, Niu J, Yuan M, et al. A novel cloud-based trust model for pervasive computing. In: Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'04), Wuhan, China, September 2004. 693～700

6 He R, Niu J, Hu K. A novel approach to evaluate trustworthiness and uncertainty of trust relationships in peer-to-peer computing. In: Proceedings of the Fifth International Conference on Computer and Information Technology (CIT'05), Shanghai, China, September 2005. 382～388

7 Almenarez F, Marin A, Dyaz D, et al. Developing a model for trust management in pervasive devices. In: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), Pisa, Italy, March 2006. 267～271

8 Quercia D, Hailes S, Capra L. B-trust: Bayesian trust framework for pervasive computing. In: Proceedings of the 4th International Conference on Trust Management (iTrust), Pisa, Italy, May 2006

9 Yuan W, Guan D, Hung L X, et al. A trust model with dynamic decision making for ubiquitous environments. In: The 14th IEEE International Conference on Networks (ICON2006), Singapore, September 2006. 236～239

10 Yuan W, Guan D, Lee S, et al. A dynamic trust model based on naive bayes classifier for ubiquitous environments. In: Gerndt M, Kranzlmüller D. eds. Proceedings of the 2006 International Conference on High Performance Computing and Communications (HPCC-06), Munich, Germany, September 2006. 562～571

11 Jameel H, Hung L X, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values. In: Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM'05), Irvine, California, USA, December 2005. 674～679

12 Hung L X, Jameel H, Cho S J, et al. A trust model for uncertain interactions in ubiquitous environments. In: Mehrotra S, et al. eds. Proceedings of IEEE Intelligence and Security Informatics Conference (ISI 2006), San Diego, California, LNCS 3975, May 2006. 755～757

13 Shankar N, Arbaugh W A. On trust for ubiquitous computing. In: First Workshop on Security in Ubiquitous Computing at the Fourth Annual Conference on Ubiquitous Computing (Ubicomp2002), Gothenburg, Sweden, September 2002

14 Liu Z, Xiu D. Agent-based automated trust negotiation for pervasive computing. In: Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), Northwestern Polytechnical University, Xi'an, P. R. China, December 2005. 300～309

15 Rehak M, Foltyn L, Pěchoucek M, et al. Trust model for open ubiquitous agent systems. In: Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT), IEEE Computer Society, Washington, DC, September 2005. 536～542

16 Zhu F, Mutka M W, Ni L M. A private, secure, and user-centric information exposure model for service discovery protocols. IEEE Transactions on Mobile Computing, 2006, 5(4): 418～429

17 Walter T, Bussard L, Robinson P, et al. Security and trust issues in ubiquitous environments — The Business-to-Employee dimension. In: Proceedings of the 2004 Symposium on Applications and

the Internet-Workshops (SAINT 2004 Workshops), Tokyo, Japan, January 2004. 696～701

18 Pirzada A A, McDonald C. Secure pervasive computing without a trusted third party. In: Proceedings of the IEEE/ACS International Conference on Pervasive Services (ICPS'04), IEEE Computer Society, Washington, DC, July 2004. 240～240

19 Bussard L, Roudier Y, Molva R. Untraceable secret credentials: Trust establishment with privacy. In: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), Orlando, Florida, March 2004. 122～126

20 Sharmin M, Ahmed S, Ahamed S I. MARKS (Middleware Adaptability for Resource Discovery, Knowledge Usability and Self-healing) for mobile devices of pervasive computing environments. In: Proceedings of the Third International Conference on Information Technology: New Generations (ITNG 2006), Las Vegas, Nevada, USA, April 2006. 306～313

21 Haque M, Ahamed S I. M-LPN: An approach towards a dependable trust model for pervasive computing applications. In: Proceedings of the International Conference on Parallel Processing Workshops (ICPPW'06), Columbus, Ohio, USA, August 2006. 189～195

22 Sharmin M, Ahmed S, Ahamed S I. An adaptive lightweight trust reliant secure resource discovery for pervasive computing environments. In: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), Pisa, Italy, March 2006. 258～263

23 Sharmin M, Ahmed S, Ahamed S I. SAFE-RD (Secure, Adaptive, Fault Tolerant, and Efficient Resource Discovery) in pervasive computing environments. In: Proceedings of the IEEE International Conference on Information Technology (ITCC 2005), Las Vegas, NV, USA, April 2005. 271～276

24 Sharmin M, Ahamed S I, Ahmed S, et al. SSRD+: A privacy-aware trust and security model for resource discovery in pervasive computing environment. In: Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC 2006), Chicago, USA, September 2006. 67～70

25 Wolfe S T, Ahamed S I, Zulkernine M. A trust framework for pervasive computing environments. In: Proceedings of the 4th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Dubai, UAE, March 2006. 312～319

26 Ngo H Q, Shehzad A, Liaquat S, et al. Developing context-aware ubiquitous computing systems with a unified middleware framework. In: Yang L T, et al. eds. The 2004 International Conference on Embedded & Ubiquitous Computing (EUC2004), LNCS 3207, Aizu, Japan, August 2004. 672～681

27 Hung L X, Phuong T V, Giang P D, et al. Security for ubiquitous computing: Problems and proposed solution. In: Proceedings of the 12th IEEE International Conference on Embedded and Real-time Computing Systems and Application (RTCSA'06), Sydney, August 2006. 110～113

28 Hung L X, Giang P D, Zhung Y, et al. A trust-based security architecture for ubiquitous computing systems. In: Mehrotra S, et al. eds. Proceedings of IEEE Intelligence and Security Informatics Conference (ISI 2006), LNCS 3975, San Diego, California, May 2006. 753～754

29 Yuan W, Guan D, Lee S, et al. Finding reliable recommendations for trust model. In: Aberer K, et al. eds. The 7th International Conference on Web Information Systems Engineering (WISE 2006), Wuhan, China, October 2006. 375～386

30 Yuan W, Guan D, Lee S, et al. Filtering out unfair recommendations for trust model in ubiquitous environments. In: Bagchi A, Atluri V. eds. Proceedings of the Second International Conference on Information Systems Security (ICISS 2006), LNCS 4332, Kolkata, India, December 2006. 357～360

31 English C, Nixon P, Terzis S, et al. Dynamic trust models for ubiquitous computing environments. In: First Workshop on Security in Ubiquitous Computing at the Fourth Annual Conference on Ubiquitous Computing (Ubicomp2002), Gothenburg, Sweden, September 2002

32 Yan Z. A conceptual architecture of a trusted mobile environment. In: Proceedings of IEEE 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU06), Lyon, France, June 2006. 75～81

33 Ries S. Engineering trust in ubiquitous computing. In: Kortuem G. Ed. Proceedings of Workshop on Software Engineering Challenges for Ubiquitous Computing, Lancaster University, UK, 2006. 91～92

34 Lmsal P. Requirements for modeling trust in ubiquitous computing and Ad Hoc networks. In HUT TML- Ad Hoc Mobile Wireless Networks - Research Seminar on Telecommunications Software, Autumn 2002. Available at: http://www. tml. tkk. fi/Studies/T-110. 557/2002/papers/pradip_lamsal. pdf

35 Haque M, Ahamed S I. Security in pervasive computing: Current status and open issues. International Journal of Network Security, 2006, 3(3): 203～214

36 Ries S, Kangasharju J, Mühlhäuser M. A classification of trust systems. In: Meersman R, Tari Z, Herrero P. eds. On the Move to Meaningful Internet Systems 2006: OTM Workshops, Springer Verlag, Heidelberg, Germany, 2006. 894～903

37 Capra L, Musolesi M. Autonomic trust prediction for pervasive systems. In: Proceedings of IEEE International Workshop on Trusted and Autonomic Computing Systems (TACS'06), in conjunction with 20th IEEE International Conference on Advanced Information Networking and Applications (AINA 2006), Vienna, Austria, April 2006. 481～488

38 Xiu D, Liu Z. A dynamic trust model for pervasive computing environments. In: Proceedings of the Fourth Annual Security Conference, Las Vegas, NV, March 2005

39 Almenárez F, Marín A, Campo C, et al. PTM: A pervasive trust management model for dynamic open environments. In: Proceedings of the First Workshop on Pervasive Security, Privacy and Trust, PSPT'04 in conjunction with Mobiquitous 2004, Boston, MA, USA, August 2004

40 Balfe S, Li S, Zhou J. Pervasive trusted computing. In: Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06), Lyon, France, June 2006. 88～94

41 Cahill V, Gray E, Seigneur J M, et al. Using trust for secure collaboration in uncertain environments. IEEE Pervasive Computing, 2003, 2(3): 52～61

42 Kagal L, Finin T, Joshi A. Trust-based security in pervasive computing environments. IEEE Computer, 2001, 34(12): 154～157

43 Lahlou S, Langheinrich M, Röcker C. Privacy and trust issues with invisible computers. Communications of the ACM, 2005, 48(3): 59～60

44 Shand B, Dimmock N, Bacon J. Trust for ubiquitous, transparent collaboration. In: Proceedings of the First IEEE international Conference on Pervasive Computing and Communications (PERCOM'03), Worth, TX, USA, March 2003. 153～160

45 Mcnamara L, Mascolo C, Capra L. Trust and mobility aware service provision for pervasive computing. In: International Workshop on Requirements and Solutions for Pervasive Software Infrastructures (co-located with Pervasive 2006), Dublin, Ireland, May 2006

46 Liu Z, Joy A W, Thompson R A. A dynamic trust model for mobile Ad Hoc networks. In: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04), Suzhou, China, May 2004. 80～85