# 普适计算软件体系结构研究*)

姜丽芬[1,2] 卢桂章[1] 辛运帏[1]

(南开大学机器人与信息自动化研究所 天津 300071)[1]

(天津师范大学计算机与信息工程学院 天津 300074)[2]

**摘 要** 普适计算强调人、计算机以及环境的相互融合,这就对传统的软件技术提出了挑战。需要新型的软件架构与之相适应。本文以普适计算环境下的通用软件架构设计为目标,采用面向服务组件和分层次的设计原则,通过中心服务器的管理机制和服务整合的方法,提出了一种基于 Kerberos 认证机制的、面向服务的普适计算软件体系结构。这个软件架构的提出,解决了普适计算环境下设备的本地资源受限性、任务多样性、运行环境的异构性和访问的安全性等一系列问题;并将此软件架构应用于"普适计算智能办公系统"的软件实现中。

**关键词** 普适计算,SOA(Service-Oriented Architecture),Kerberos 认证,粒度,组件复用

## Research on Software Architecture under Pervasive Computing Environment

JIANG Li-Fen[1,2] LU Gui-Zhang[1] XIN Yun-Wei[1]

(Institute of Robotics and Information Automatic System, Nankai University, Tianjin 300071)[1]

(College of Computer and Information Engineering, Tianjin Normal University, Tianjin 300074)[2]

**Abstract** Pervasive computing lays emphasis on the seamless integration of users, devices and environment, which challenges the traditional software technology and requires innovational software architecture. Obviously, software architecture plays a key role in pervasive computing. The service-oriented components and the layered design principle are adopted in order to design general software architecture under the pervasive computing environment. Using the management mechanism of the center server and integration of component services, a general architecture is put forward, which is service-oriented, based on Kerberos authentication mechanism, and open architecture. This service-oriented software architecture resolves many issues in pervasive computing environment, such as local resources limitation, variety of applications, heterogeneous platforms and access security etc. This software architecture is applied to and implemented in the "intelligence office system in pervasive computing environment".

**Keywords** Pervasive computing, SOA (Service-Oriented Architecture), Kerberos authentication, Granularity, Component reuse

普适计算[1,2]是以人为中心的计算,从根本上改变了人去适应计算机的被动式服务方式。普适计算的目的是建立一个充满计算和通信能力的环境。它强调一个无处不在的支持用户完成他们任务的计算环境,而实际参与计算的设备和技术是透明的[3]。只有普适计算模式才能在真正意义上实现以人为本的生活方式。随着网络通信及硬件技术的发展,实现普适计算的设想正在变成现实。由于普适计算设备的多样性、可移动性、资源受限性以及任务的复杂性和特殊性,使其需要一个计算环境和相应的软件系统来支撑其应用。依靠这个系统提供的服务可弥补资源不足和扩展自身功能,从而扩大应用范围。综合各研究机构提出的不同的软件体系结构[4~7],结合普适计算环境的特点,本文提出了一个基于 Kerberos 认证机制的、面向服务的软件体系结构。

## 1 相关工作

自从 Mark Weiser 在 1991 年提出 21 世纪的计算将是一种无处不在的计算(Ubiquitous Computing)模式[1]以来,计算模式正朝普适计算方向发展。目前,美国和欧洲的各知名大学和研究机构都启动了普适计算相关的研究计划。法国计算机科学研究院的 Arles 项目[6]对普适计算的软件体系结构进行了研究。主要从 Web Services、普适计算系统的语义互操作和移动计算环境的感知语义服务方面考虑系统的设计,为普适计算环境的软件架构设计提供了有价值的参考。ISAM 项目提出了 ISAM 软件架构[7],主要从提供可编程模式的环境整合、通过多层合作模型构建 ISAM 核心架构。文[8]提出了支持应用和系统之间的协作关系的感知应用适应系统。然而,它的原型实现只是基于感知网络应用。文[9~11]等提供了对移动应用的适应行为。也有许多特殊领域应用的研究,如多媒体[12]等。国内在普适计算方面也开始了研究工作,如中国科学院软件研究所的"无处不在计算环境下智能人机交互研究"、清华大学人机交互与媒体集成研究所的 Smart Class 项目,北京大学、浙江大学惠普实验室等都有普适计算相关的研究。纵观各研究机构的研究项目和发表的论文,我们可以看到:目前,普适计算的研究热点还主要集中在人机交互和上下文感知计算等方面的研究,普适计算软件体系结构的研究相对还很薄弱,还没有提出一个统一的、完备的体系

*)基金项目:天津自然科学基金(06YFJMJC00200),南开大学创新基金,天津市高等学校科技发展基金(20051518)。**姜丽芬** 副教授,博士生;**卢桂章** 教授,博士生导师;**辛运帏** 教授,博士。

结构。

## 2 系统设计思想

普适计算的目标是把人从计算技术本身解放出来，实现信息空间和物理空间的融合，使系统与用户透明地交互。普适计算的应用前景对传统的软件架构提出了挑战。普适计算环境中存在着大量异构的分布式系统，应用软件也具有多样性，这给服务应用带来了很大困难。现有的文献和商业应用认为，SOA[13,14]是未来软件架构的一个发展趋势，基于 SOA 的系统具有减少成本、增加重用等优点。在普适计算环境下，构建一个基于 SOA 的软件架构，对于实现普适计算以人为本的思想有着理论和应用价值。我们结合 Kerberos 认证技术去设计适合普适计算环境的面向服务的软件体系结构。

### 2.1 面向服务的体系结构

面向服务的体系结构(Service-Oriented Architecture, SOA)是一个系统组件以及它们之间交换的架构模式或模型。一个组件提供一个服务，其他组件可以按照服务契约调用这个服务[15]。一个 SOA 由 4 个实体构成：服务提供者、服务注册中心和服务消费者(也称为服务请求者)以及将消费者和提供者联系在一起的契约。服务是以契约定义的功能或行为，它由一些组件实现，并能被别的组件调用以完成特定的任务。服务提供者在一个服务注册中心发布其服务契约，从而使请求者能够了解到其所提供的服务。服务提供者提供的功能和任务以及消费者所需的其他功能和技术信息在 SOA 的最后一个实体“服务定义”或“契约”中进行定义。

整合小的服务到大的服务是面向服务架构的核心。从组件复用的角度考虑，组件的粒度[16]越细，未来组件被直接重用的可能性就越大。然而，从组件的通信量的角度考虑，通信量将随着组件数量的增加而产生组合增长。所以，服务组件粒度的粗细，直接影响服务组件的复用性和系统的整体运行效率。普适计算环境下的灵活多变的业务需求对服务粒度又提出了更高的要求。

本文通过一种可配置的细粒度组件服务的整合方法，寻找上述问题的解决方案。目标是在 SOA 的设计和实现过程中，使用细粒度的组件服务提供基本的功能单元，通过可配置的方法，动态组装这些细粒度服务组件为粗粒度服务组件。由于粗粒度服务组件只是基于细粒度服务组件和流程编排的逻辑服务组件，因此，当业务发生变化时，只需要修改流程编排文件，而无需修改源代码，以此来满足功能变更的需求。

配置组件采用消息机制，通过消息编排把服务联系在一起而非被迫进行大规模新的应用代码的开发，适应普适计算软件环境的需求。

### 2.2 Kerberos 认证机制

普适计算网络一般是以多种无线网和移动网接入互联网实现异构集成的网络。普适计算理念的重点是以人的需求为中心主动提供服务。因此，用户可以随时随地以任意方式联入网络，享受服务。这样，普适计算网络的安全问题显得尤为重要。

在普适计算环境中，可以将每个设备和移动用户都看作是环境中的实体而无须区别对待，它们之间没有本质上的区别。因此，普适网络中的身份认证是广义意义上的，应该扩展到在实体间进行相互认证的双向认证机制。例如，某些网络设备有可能已经被黑客恶意占领，或是某些设备由于资源不足等原因暂时无法为用户提供所需服务，这些情况在双方会话开始之前都应该被感知，以便用户及时地做出相应的对策和选择。因此，不仅设备要认证某用户是否具有使用该设备的权限，用户还要验证该设备是否是“可用的”。因此，在普适计算网络中，进行通信的前提是要保证双方的身份是合法的和真实的，这样才能在彼此信任的基础上开展对话，才能保证相互间信息传输的私密性和安全性。Kerberos[17,18]作为可信任的第三方认证协议，是普适计算环境下安全认证的一个很好的选择。

Kerberos 认证协议是利用 DES 加密算法实现加密的。该协议原型是 Needham-Schroder 认证协议，并在原协议基础上加入了时间戳和报文序号机制，以抵抗重发攻击，最终形成现在的 Kerberos 安全认证技术。Kerberos 协议允许用户通过网络向服务器证明其身份，并且也可要求服务器证明身份。

## 3 软件架构设计

### 3.1 软件体系结构

本文提出的普适计算环境的软件体系结构如图 1 所示。双箭头表示服务注册、请求和发布等服务管理过程。单箭头表示客户端连接应用、用户身份验证和服务器身份验证等过程。

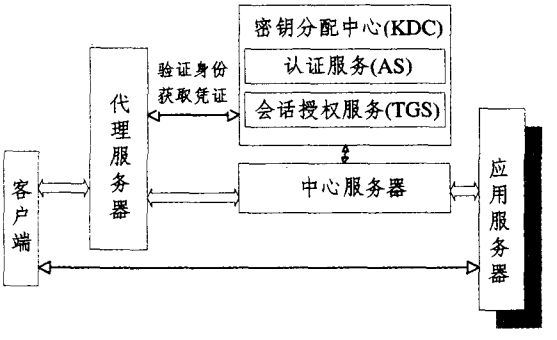


图 1 软件体系结构

该软件体系结构的各组成部分的功能如下：

1)中心服务器

中心服务器包括服务管理系统、服务发布、服务注册、服务查询和服务器身份验证等功能。服务管理系统是以守护进程形式存在的。监听系统中的服务注册请求，完成服务注册；监听来自代理的服务请求，查询注册的服务句柄；服务发布，反馈查询的服务句柄和访问端口描述等。

2)认证服务器

密钥分配中心(Key Distribution Center，KDC)，它是整个认证系统的核心部分，其中维护了所有用户的账户信息。KDC 提供了两种服务，认证服务(AS，Authentication Service)和会话授权服务(Ticket Granting Service，TGS)。认证服务对用户的身份进行初始认证，若认证通过便发放给用户一个称为 TGT(ticket granting ticket)的票据，凭借该票据用户可访问 TGS，从而获得访问应用服务时所需的服务票据。

3)代理服务器

代理服务器在用户登录时将登录密码转换为该用户的长期密钥、发送各种请求信息，并接收从 KDC 返回的信息。它监听客户端发出的连接及服务请求，验证用户，并提供给合法用户所要求的服务信息。向票据服务器发送查询证书和服务证书的申请，并向认证服务器发送查询请求。

为了保证服务质量(QoS)，最大限度地减小向其他服务

器发送数据的延时，代理服务器内部考虑到了缓存功能。考虑到普适计算应用的特点，要求其具有可扩展功能。随着加入网络的客户端数量的增加，允许适当增加代理的数量。

### 3.2 服务认证和服务执行

客户请求服务和服务的执行过程如下：

1)当用户向代理服务器发出服务请求时，代理服务器便向认证服务器发出请求信息(此信息是客户的 ID)，要求得到票证服务器的证书(包括访问发票服务器的门票和一个临时会话密钥)。

2)作为响应，认证服务器通过代理服务器回送给客户一个加密的证书信息，该证书包括会话密钥与 TGS 通信的门票。门票包括客户的 ID 和会话密钥的一个拷贝。用户收到 AS 的响应后获得密钥，从而将该信息解密，得到了与 TGS 通信的会话密钥和访问 TGS 的门票。

3)当客户需要和应用服务器通信时，通过代理向 TGS 发送请求信息，该信息包括门票、应用服务器和一个认证符。作为响应，TGS 通过验证认证符来确认客户请求的合法性，为用户与应用服务器之间的通信生成一个会话密钥。然后 TGS 把会话密钥和服务器的 ID 用客户和 TGS 共享的密钥加密，把客户和应用服务器的共享密钥和客户的 ID 用应用服务器的密钥加密，并把以上两种加密信息回送给客户。这样客户就获得了与应用服务器通信的会话密钥和访问应用服务器的门票。

4)客户端将门票和认证符信息传送给应用服务器。因为该会话密钥在客户和服务器之间共享，所以客户就可以用它向应用服器认证自己。如果此通信要求双向认证的话，服务器可以用客户和应用服务器共享密钥加密的时间戳记信息来向客户认证自己。

5)通过以上的认证，客户获得了访问应用服务器的门票和会话密钥，在证书有效的时间内，用户可以随时向应用服务器申请服务，并可用会话密钥加密双方间进一步的通信或者交换另外的子密钥来加密进一步的通信。

6)当客户端经过认证后，通过代理发出服务连接请求。代理向中心服务器的服务管理系统查询服务请求，获得服务列表信息及资源占用情况，通过分析均衡负载以获得服务地址节点，并通过代理通知客户。这样客户端就可以从应用服务器获得服务。

### 3.3 系统层次结构

SOA 要求开发者从服务集成的角度来设计应用软件，并考虑复用现有的服务，或者检查如何让服务被重用。SOA 是一个以服务流程为中心的体系结构，一切从服务的角度出发，首先考虑服务需求。下面仅从组件复用和细粒度组件服务整合的角度论述本文提出的基于 SOA 的系统的层次结构，如图 2 所示。

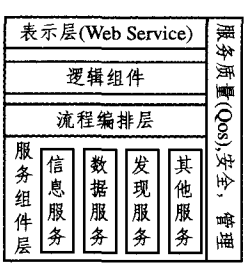


图 2 基于 SOA 的层次结构

其各组成部分的功能如下：

1)底层是细粒度服务组件层。不同的操作系统、信息平台根据最小粒度划分法将逻辑过程或项目划分为若干独立的最小功能和逻辑服务组件模块。

2)第二层是流程编排层。这一层根据业务过程将独立的细粒度服务组件进行流程编排，组合为复合组件。

3)第三层为逻辑组件层。这一层以细粒度组件和流程编排文件为原料，向表示层(如 Web 服务层)提供服务，从 Web 服务层的角度看，逻辑组件层提供的是粗粒度的服务组件。

4)第四层是表示层。它作为一种用户的接口。在“普适计算智能办公系统”的软件实现中，采用了 Web Service 作为表示层。它负责将逻辑组件层生成的粗粒度组件服务发布出去。

5)第五层是服务质量、安全、管理层。这一层通过特定工具、响应机制和标准(如 WS management)来监视 SOA 的运行，以确保服务质量。

通过对细粒度组件进行流程的编排，使其不但能够协作产生粗粒度组件的功能，还能够根据需要，通过改变流程的编排，动态适应业务变化引起的组件功能的改变。在业务变化涉及到组件服务的内部服务时，又能够通过修改配置，重新组装细粒度服务组件，重构粗粒度服务，以适应普适计算的动态任务的需求。

## 4 原型实现和进一步的工作

本文提出的软件体系结构已经在“普适计算智能办公系统”软件的设计与开发中得到应用。我们在机器人所搭建了普适智能办公环境，其环境组成如图 3 所示。

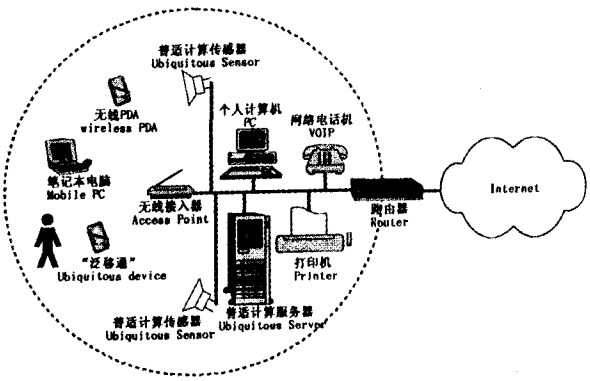


图 3 普适智能办公环境组成

普适智能办公系统主要包括三部分：电话呼叫转移到手持移动设备、应用 RFID 技术的门禁系统、语音交互及定位系统。目前，在语音交换系统的软件实现中完全采用了我们提出的基于 Kerberos 认证的面向服务的软件体系结构。

目前，机器人所的“基于 RFID 的普适计算环境下的广义物流系统”项目的软件开发工作正在进行中。进一步的工作将把此软件架构应用于广义物流系统的上下文感知的软件实现中。

**结论** 与传统软件开发方法相比，基于 SOA 的软件架构增加了系统的灵活性、易用性，软件系统能迅速适应变化的业务流程等。

本文针对普适计算环境的需求，将 SOA 思想和分层次设计的原则引入到普适计算软件体系结构中，实现了动态组织细粒度组件到粗粒度组件，解决了普适计算环境中设备的移

动性，资源的受限性和高度的动态性等问题。结合基于 Kerberos 认证机制保证了普适计算的安全性。该软件架构在普适计算智能办公系统的原型实现说明了本文提出的普适计算软件体系结构适应普适计算环境的应用需求，也展示了该软件体系结构的可行性，为普适计算软件架构的设计提供了一个参考模型。

## 参 考 文 献


1 Weiser M. The Computer for the Twenty-First Century. Scientific American, 1991, 265(3): 43～50

2 Agoston T C, Ueda T, Nishimura Y. Pervasive Computing in a Networked World. In: Global Distributed Intelligence for Everyone, INET2000: 10th Annual Internet Society Conference in Yokohama, Japan, 2000. 213～215

3 Banavar G, Beck J, Gluzberg E, et al. Challenges: An Application Model for Pervasive Computing. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, 2000. 266～274

4 Grimm R, Anderson T, Bershad B, et al. A System Architecture for Pervasive Computing. In: Proceedings of the 9th ACM SIGOPS European Workshop, Kolding, Denmark, 2000. 177～182

5 Kindberg T, Fox A. System Software for Ubiquitous Computing Magazine. IEEE Pervasive Computing, 2002, 1(1): 70～81

6 Mokhtar S B, Georgantas N, Issarny V, et al. Software Architectures for Pervasive Computing Systems. http://www.inria.fr/rapportsactivite/RA2005/arles/uid41.html, updated : 11/24/2005

7 Augustin I, Yamin A C, Barbosa J L V, et al. ISAM, A Software Architecture for Adaptive and Distributed Mobile Applications. In: Proceedings of the Seventh International Symposium on Computers and Communications, 2002. 333～338

8 Noble B. System Support for Mobile, Adaptive Applications. IEEE Personal Communications(IEEE pers. Commun.), 2000, 7(1): 44～49

9 Bolliger J, Gross T. A Framework-based Approach to the Development of Network-Aware Applications. IEEE Transactions on Software Engineering, 1998, 24(5): 376～390

10 Chen G, Kotz D. A Survey of Context-Aware Mobile Computing Research: [Technical Report: TR 2000-381]. 2000

11 Gray R, Caripe W, Cybenko G. Network-Awareness and Mobile Agent Systems. IEEE Communications Magazine, 1998, 36(7): 44～49

12 Kunz T, Black J P. An Architecture for Adaptive Mobile Applications. In: Proceedings of Wireless99, the 11th International Conference on Wireless Communications, Canada, 1999. 27～38

13 Wong-Bushby, Egan R I, Isaacson C. A Case Study in SOA and Re-Architecture at Company ABC. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006, 8: 4～7

14 van Thanh D, Jorstad I. A Service-Oriented Architecture Framework for Mobile Services. In: Proceedings of the Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop, Lisbon, Portugal, 2005. 65～70

15 Nickull D. Service Oriented Architecture Whitepaper. http://www.adobe.com/enterprise/pdfs/Services_Oriented_Architecture_from_Adobe.pdf

16 杜攀，徐进. SOA 体系下细粒度组件服务整合的探讨. 计算机应用，2006(3): 99～702

17 Cervesato, Jaggard A D, Scedrov A, Walstad C. Specifying Kerberos 5 cross-realm authentication. In: Proceedings of the 2005 workshop on Issues in the theory of security (WITS'05), Long Beach, California, 2005. 12～26

18 Steiner J G, Neuman B C, Schiller J I. Kerberos: An Authentication Service for Open Network Systems. In: Proceedings of the Winter 1988 Usenix Conference, 1988. 191～201


(上接第 199 页)

表 1 两种自适应 PSO 算法的比较

| 函数 | 最优点 | 最优解 | 经典自适应 PSO 最优点 | 经典自适应 PSO 最优解 | 改进的自适应 PSO 最优点 | 改进的自适应 PSO 最优解 |
|---|---|---|---|---|---|---|
| $f_0(x)$ | (0.0,0.0) | 0 | (0.000071,0.000012) | 0.000001 | (0.000001,0.000000) | 0.000000 |
| $f_1(x)$ | (0.0,0.0) | 1 | (0.0097,0.0048) | 0.9998 | (0.77e−6,−0.12e−6) | 1 |
| $f_2(x)$ | (0.0,0.0) | 1 | (−0.0095,0.0286) | 0.9991 | (−0.12e−6,0.17e−6) | 1 |
| $f_3(x)$ | (−0.0898, 0.7126)(0.0898, −0.7126) | −1.031628 | (0.1120,−0.7150) | −1.029734 | (0.0893,−0.7121) | −1.031615 |
| $f_4(x)$ | (0.0,0.0) | 0 | (0.1207e−6, 0.0712e−6) | 0.000644 | (0.903e−7,0.324e−8) | 0 |

**结论** 本文提出的自适应 PSO 算法在传统的自适应 PSO 上更进了一步，在寻优过程中不仅对惯性权重 $w$ 加以调整，同时又通过调整 $k$ 值改变种群拓扑结构来评价每个粒子。这样使算法在优化过程中不断缩小优化变量的搜索空间，不断加深优化变量的搜索精度，搜索的效率很高，并且能有效地避免陷入局部最优解。

## 参 考 文 献


1 Kennedy J, Eberhart R. Particle swarm optimization[A]. In: IEEE Int Conf. on Neutral Networks[C]. Perth, 1995. 1942～1948

2 Eberhart R, Kennedy J. A new optimizer using particle swarm theory[A]. In: Proc. 6th Int Symposium on Micro Machine and Human Science[C]. Nagoya, 1995. 39～43

3 Millonas M M. Swams Phase Transition and Collective Intelligence[M]. MA: Addison Wesley, 1994

4 Shi Yuhui, Eberhart R. A modified particle swarm optimizer [A]. In: Proc. IEEE Int Conf. on Evolutionary Computation[C]. Anchorage, 1998. 69～73

5 Kennedy J. The particle swarm: Social adaptation of knowledge [A]. In: Proc. IEEE Int Conf. on Evolutionary Computation[C]. Indiamapolis, 1997. 303～308

6 Kennedy J, Mendes R. Population structure and particle swarm performance[A]. In: 2002 World Congress on Computational Intelligence. Honolulu, HI, May 2002

7 Kennedy J, Mendes R. Neighborhood topologies in fully informed and best-of-neighborhood particle swarms[A]. IEEE Transactions on Systems, Man and Cybernetics, Part c Applications and reviews, 2006, 36(4)

8 Kennedy J, Eberhart R. Swarm Intelligence. Morgan Kaufmamn Academic Press, 2001

9 Kennedy J. Small words and mega-minds: Effects of neighborhood topology on particle swarm performance. In: Proceedings of the 1999 Conference on Evolutionary Computation, 1999. 1931～1938

10 Watts D J. Small Worlds: The Dynamics of Networks between Order and Randomness. Princeton University Press, 1999

11 Watts D J. Strogatz. Collective dynamics of 'small-world' networks. Nature, 1998, 393: 440～442

12 Shi Y, Eberhart R. A modified particle swam optimizer. In: Proc. IEEE World Congress on Computation Intelligence, 1998. 66～73

13 Li Junjun, Wang Xihuai. A modified particle swarm optimization algorithm. In: Proceeding of the 5th World Congress on Intelligent Control and Automation, Hangzhou, P R China, June 2004

14 谢晓峰，张文俊，杨之廉. 微粒群算法综述. 控制与决策，2003(2): 129～134