

# 普适环境下基于中间件的身份验证模型<sup>\*</sup>

孙立镬, 杨月甫

(哈尔滨理工大学 计算机科学与技术学院, 哈尔滨 150080)

**摘要:** 为了更好地保证普适计算环境中计算资源的安全性, 减少人为的非正常破坏, 提出了普适环境下应用的身份验证需求, 即验证不仅要随时随地, 而且可以随着用户的移动在异构设备和计算环境中移动, 让移动中的用户能够体验到不间断的计算。提出了基于移动代理的普适计算中间件 ValidateAgent, 并结合情境感知技术, 给出了验证模型、算法及原理。此研究对于普适计算在协同设计领域中的应用有重要意义。

**关键词:** 普适计算; 移动代理; 身份验证; 中间件

**中图分类号:** TP391

**文献标志码:** A

**文章编号:** 1001-3695(2009)11-4306-03

doi:10.3969/j.issn.1001-3695.2009.11.088

## Middleware in pervasive computing based on model of validate agent

SUN Li-juan, YANG Yue-fu

(College of Computer Science & Technology, Harbin University of Science & Technology, Harbin 150080, China)

**Abstract:** A new requirement of identity validate was advanced to make better safety of pervasive computing resources, reduce human innormal breakage. Namely, validation should work not just in anytime and anywhere, and also follow mobile users when they change to a different environment, in order to let them enjoy uninterrupted computing experience. This paper proposed a mobile agent based pervasive computing middleware ValidateAgent. By leveraging context awareness techniques, proposed the model of validation, arithmetic, and the principle. This research will play an important role for the application of pervasive computing in cooperative design domain.

**Key words:** pervasive computing; mobile agent; identity validate; middleware

## 0 引言

近年来,随着移动设备、智能设备、无线通信网络技术的发展,物理空间与信息空间的结合日趋紧密,计算资源和计算机网络无处不在,用户将能很方便地获取各种信息服务和计算资源,普适计算的前景日趋明朗<sup>[1]</sup>。作为一种新型计算模式,普适计算将更加关注如何让这些无处不在的计算资源和网络能够更好地为用户提供个性化的服务,使用户从繁琐的人机交互中解放出来,尽可能地减少用户的人为干预,进一步提高工作效率,实现真正的以人为本的计算。基于普适计算的特点,用户可以随时随地登录相应系统,这就涉及到系统资源的安全性等问题,于是负责用户安全任务的身份验证成为了普适计算模式中的一项新的需求<sup>[2]</sup>。身份验证能够保证系统资源的安全性和保密性,与该用户所执行任务相关的应用程序状态、属性、情境信息等都有联系,并且能够适应新场景下可用的计算资源,用户可以在新的位置继续以他所喜爱的方式执行先前的计算任务<sup>[3]</sup>。相比其他技术或系统中应用的身份验证模型,普适计算模式下应用的身份验证方式提出了一些新的需求:a)安全性,即用户无论应用何种移动设备都能进行精确的身份验证;b)连续性,即用户感觉不到角色权限的中断,而且用户的使用偏好仍然能在新的运行环境下得到体现,能够为用户维持一个熟悉的工作空间;c)情境感知的驱动方式,即充分利用智

能环境中部署的传感器感知人的位置、行为等,推导出包括用户情境等的变化,无须用户的干预便可完成验证的动作,实现用户干预的最小化;d)资源的无缝整合,即当用户迁移到新的环境中后,应用能够通过自适应的方式进行重配置,以使用新的可用资源。

本文基于已有对分布式系统中移动代理的研究积累,设计并实现了一个基于移动代理的普适计算中间件平台 ValidateAgent,并提出了此验证平台中身份验证的具体实现模型。

## 1 普适计算

普适计算可以解释为计算的普及性和适应性。前者指网络互连的计算设备以各种形式、形态渗透到人们的生活空间,成为人们获得信息服务的载体,即信息空间普遍存在;后者指信息空间能以适合用户的方式提供能适应变化的计算环境的连贯的信息服务,即信息服务方便适用。普适计算的目标就是在计算和通信无所不在的基础上,建立以人为中心的计算环境<sup>[4]</sup>。普适计算力图将以计算机为中心的计算转变为以人为中心的计算,这种转变将极大地促进信息技术在全社会的普遍应用,具有重要的战略意义。

普适计算引发了对一种全新计算模式的探索,具有鲜明的交叉学科的特点。概念设计是产品设计过程中最能体现人的智能并决定产品性能和成本的重要阶段,它影响到后续的产品

收稿日期: 2009-01-10; 修回日期: 2009-03-02 基金项目: 国家自然科学基金资助项目(60173055)

作者简介: 孙立镬(1944-),男,教授,博导,主要研究方向为计算机图形学与 CAD(slq863@yahoo.com.cn); 杨月甫(1983-),男,硕士研究生,主要研究方向为计算机图形学与 CAD。

生产开发、产品市场开发,以及企业经营战略目标的实现。如何利用计算机的高信息存储量及多种通信手段,为设计人员建立一个以人为中心的设计环境,是一个非常具有挑战意义的研究课题。

普适计算环境具备计算密集性、网络密集性、资源密集性以及情境可感知性等一系列特点,这种特点为应用的身份验证提供了良好的基础设施和环境。而如何让应用感知用户行为和环境的變化,主动适应新的环境,却并非显而易见。作为普适计算研究的先行者,CMU 和 UIUC 分别提出了 Aura 计划<sup>[5]</sup>和 Gaia 系统<sup>[6]</sup>。其中,Aura 通过抽象出用户的任务,将组成应用的构件划分为 supplier 和 connector 两类,由运行系统中的任务管理器 Prism 来指导面向任务的应用迁移,利用分布式文件系统实现应用状态的分发和共享,通过 supplier 和 connector 的动态绑定实现应用的重配置。但 Aura 并没有阐述任务如何适应异构的 supplier,关于多任务之间的同步问题亦没有详加探讨。Gaia 要求提供应用的定制描述文件(application customized description),用户切换计算环境后需要通过远程获取该文件,实现应用执行状态的装载和应用程序的连续执行。但这一过程需要用户的干预,而且 Gaia 将移动、协同以及生命周期管理等诸多要素集中于静态协同模块,容易形成计算瓶颈。

2 基于移动代理的普适计算中间件

中间件出现于 20 世纪 90 年代初,是一种独立的系统软件或服务程序,分布式应用软件借助这种软件在不同的软件之间共享资源。它位于客户机与服务器的操作系统之上,管理计算资源和网络通信。它不仅要实现应用系统的互连,还要屏蔽平台差异,实现软件间的互操作。实际应用中,通常要把一组中间件集成在一起,构成一个平台(包括开发和运行功能)来实现中间件的功能。目前,针对普适计算,经常应用 agent 或多 agent 技术来充当中间件。

ValidateAgent 中间件采用了 OSGi 框架,其体系结构如图 1 所示。中间件包含物理层、设备访问层、服务层、代理层和应用层。物理层转换物理信号为计算机可读的形式并发向设备访问层。物理层包括了各种各样的硬件设备,如用于通信的蓝牙、GPRS 和 WLAN 设备,用于感应和控制的传感器和激励器等设备,用于定位和感光的传感器。还有扫描仪、打印机等设备。设备访问层集成了物理层的多种设备,以 OSGi bundle 的形式提供对外可访问的操作接口,成为服务层中的服务。设备访问层的目的是支持新设备的热插拔,在需要时下载和安装设备驱动,以及自动发现和附加已有设备到 ValidateAgent 中间件上。

代理层是 ValidateAgent 中间件的核心层。Agent 容器以 bundle 形式运行在 OSGi 框架中,其中运行着多个 agent。系统将为每一个用户分配一个可以定制的用户 agent,它将负责响应用户的需求和感知用户的情境,捕获用户的任务。ValidateAgent 是其中一种特殊的 user agent,它对用户的特征信息保持敏感,并具有验证能力。Admin agent 提供用户应用的管理服务,包括特征信息的管理、目录服务、情境管理服务。特征管理服务是实现身份验证的关键,它需要通过对来自于物理

环境的情境信息和来自于用户的特征信息进行融合、分类和推理等。System service agent 提供一些可插拔的服务或类库。应用层则可以通过代理层提供的服务和类库,实现应用的验证和重配置。

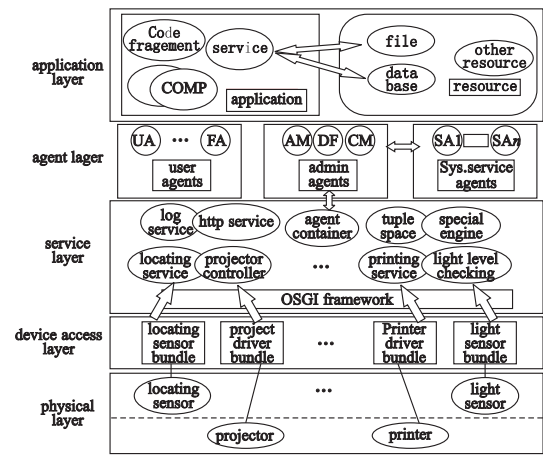


图1 ValidateAgent中间件体系结构

3 身份验证模型

3.1 用户生理特征

在普适计算中,安全问题变得更加敏感与重要,本文提出基于人的生理特征上下文安全服务的解决方法,并根据生理特征上下文,提供灵活的存取控制和策略。

对每个用户来说,其自身都具有一些相对独立的特征,这些相对独立的特征就构成了用户信息的上下文。

通常用户生理特征上下文由指纹、虹膜、面貌、声音、身高、体重构成。

3.2 验证算法

根据用户的生理特征信息,可设计验证算法的描述如下:

可信度 =  $\sum (R \times \text{weight} \times \text{module})$

其中: $R$  表示上下文的特征值取值,仅为 0 或 1。0 代表不具有该上下文项,1 代表具有该上下文项。

Weight 表示该上下文对应的权值。其中  $\sum \text{weight} = 1$ 。对于基本是用户独一无二特征的上下文,其权值应该设定得较大,如上面的六项上下文中,指纹、虹膜、面貌可分别设为 0.4、0.3、0.2;对于用户部分特征的权值应该设定为较小的,声音、身高、体重可分别设为 0.05、0.03、0.02。

Module 代表该上下文与用户信息库中该项数据的吻合程度( $0 \leq \text{module} \leq 1$ )。对某些用户独特特征的数据如指纹、虹膜,其取值仅为 0 或 1。对用户部分特征模糊度的表示需要自己设定。例如一个用户数据库中的身高是 1.75 m,现在,通过传感器测得该用户的身高是 1.78 m,根据常识,一个人可能穿一双较高的鞋,身高变为 1.78 m,但是如果传感器测得该用户的身高是 1.70 m,则可以肯定一定不是该用户。因此,可以构造一个函数来表示关于身高的模糊度:

if (  $\text{height}_1 - \text{height}_0 > 0$  and (  $\text{height}_1 - \text{height}_0 < 8$  ) )  
    module = (  $8 - (\text{height}_1 - \text{height}_0)$  ) / 8  
else if (  $\text{height}_1 - \text{height}_0 > = -3$  and (  $\text{height}_1 - \text{height}_0 < = 0$  ) )  
    module = 1 + (  $\text{height}_1 - \text{height}_0$  ) / 3

其中: $\text{height}_1$  代表用户通过传感器测得的身高, $\text{height}_0$  代表用户

数据库中的身高。基于同样方法,可以讨论体重、面貌等方面的上下文。例如该用户的面貌,可以根据当时传感器传递的图像与库中的图像对比给一个模糊度值。该值当传感器传递新图像信息后,可动态地改变。

3.3 验证原理

为了更精确地验证用户特征信息,对被访问资源,基于可信度划分访问权的子集,如图 2 所示。

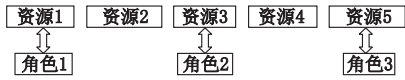


图2 角色资源对应分配图

其中,各角色可访问当前对应资源以及编号小于该资源编号的资源:

- 角色 1 可访问资源:资源 1
- 角色 2 可访问资源:资源 1 资源 2 资源 3
- 角色 3 可访问资源:资源 1 资源 2 资源 3 资源 4 资源 5

再基于该可信度授权该用户:

```
if 可信度 > = 0.89
    role = 3/* 代表是该用户,获得该用户的所有权限 */
else if 可信度 > = 0.70
    role = 2/* 代表可能是该用户,可分配给该用户部分日常权限 */
else if 可信度 > = 0.50
    role = 1/* 代表稍有可能是该用户,可分配给该用户小部分日常权限 */
else
    role = 0/* 代表不可能是该用户,不分配给该用户任何权限 */
如果 role = 3 在确定是该用户后,将反映该用户部分特征的上下文(模糊度值不为 1)记录到用户信息数据库,经过一段时间后,可以根据新的知识(按照用户部分特征的上下文同一取值概率的大小)调整用户信息数据库,这样,验证将更加准确。
```

例如,某用户到达一个需要身份验证的地方,传感器测得该用户的(指纹、虹膜、面貌、声音、身高、体重)上下文后,通过移动 agent 将这些信息发送往用户所在的 agent 系统。

```
context( 指纹,location,client)
context( 虹膜,location,client)
context( 面貌,location,client)
context( 声音,location,client)
context( 身高,location,client)
context( 体重,location,client)
假设
Weight:
指纹 0.4
虹膜 0.3
面貌 0.15
声音 0.08
身高 0.05
体重 0.02
```

若对比指纹、虹膜都相同,其模糊度为 1,面貌由于传感器测得的数据不清晰,对比图像后设定模糊度为 0.6,声音对比模糊度为 0.5,身高测得的数据 173 cm,用户数据库中的信息

记录为 170 cm,则该用户身高的模糊度为

(8 - ( 173 - 170 ))/8 = 0.625

同样的方法处理体重,假设模糊度为 0.5,则该用户的可信度为

0.4 × 1 + 0.3 × 1 + 0.15 × 0.8 + 0.08 × 0.5 + 0.05 × 0.625 + 0.02 × 0.5 = 0.90

可信度对应该用户的权限 role = 3,可以确定此用户是验证的用户。

虽然一个用户仅使用一个特有的生理特征上下文也可以作为验证标志(如指纹),但是所做的验证并不可靠(非法用户能够窃取合法用户指纹,进行伪造,则非法用户可以通过验证,同时将获得合法用户的所有权限)。验证设计如图 3 所示。

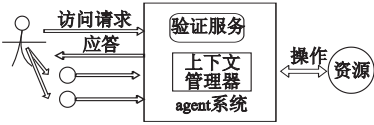


图3 验证过程图

4 结束语

本文详细地分析了普适计算模式下应用的身份验证的特点和需求,设计并实现了一个基于移动代理的普适计算中间件平台 ValidateAgent,且在此中间件平台上实现了身份验证的模型、算法和其实现原理。与之前的工作以及其他一些支持普适计算的身份验证工作相比较,本文具有以下特点:

- a)给出基于移动代理的普适计算中间件平台的体系结构。ValidateAgent 是一种用于普适计算的轻量级中间件平台,其显著特点是采用 OSGi 框架,使得系统内核占用资源非常少,可以方便地部署在移动设备和嵌入式设备中。而其面向服务的体系架构也为应用迁移到新环境后可能进行的自适应重配置提供了基础支持,包括服务查找和重绑定。
- b)本文针对身份验证及其所运行的环境特点,详细地描述了身份验证的策略和实现。对普适计算在协同设计领域中的应用提出了新的挑战,具有重要意义。

参考文献:

[1] 徐光祐,陶霖密,张大鹏,等. 物理空间与信息空间的对偶关系[J]. 科学通报,2006,51(5):610-616.

[2] SATYANARAYANAN M, KOZUCH M A, HELFRICH C J, et al. Towards seamless mobility on pervasive hardware[J]. Pervasive and Mobile Computing,2005,1(2):157-189.

[3] YU P, CAO J N, WENW D, et al. Mobile agent enabled application mobility for pervasive computing[C]//Proc of Ubiquitous and Intelligent Computing. Wuhan:Springer,2006:648-657.

[4] POPESCU-ZELETIN R, STEGLICH S, ARBANOWSKI S. Pervasive communication: a human-centered service architecture[C]//Proc of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems. 2004:141-146.

[5] GARLAN D, SIEW IOREK D, SMAILAGIC A, et al. Project Aura: toward distraction-free pervasive computing[J]. IEEE Pervasive Computing,2002,1(2):22-31.

[6] ROMAN M, HESS C K, CERQUEIRA R, et al. Gaia: a middleware infrastructure to enable active spaces[J]. IEEE Pervasive Computing,2002,1(4):74-83.