# 基于SOA的可信智能空间系统软件研究

明 亮[1] 况晓辉[1] 黄敏桓[1,2] 金 旗[1]
(北京系统工程研究所 北京 100101)[1] (清华大学计算机科学与技术系 北京 100084)[2]

**摘 要** 为了保证智能空间中信息服务的透明性和安全性,提出了一种基于SOA的可信智能空间系统软件模型,以为智能空间的系统软件和普适计算应用提供技术支撑。模型中采用SOA架构,支持智能空间中信息服务的松散耦合;采用混合访问控制策略,支持信息设备与智能空间的可信、透明交互。最后,应用该模型实现了一个可信智能空间原型系统,验证了模型的有效性。

**关键词** 智能空间,系统软件,SOA,可信计算
**中图法分类号** TN915 **文献标识码** A

## Research on System Software of Trusted Smart Space Based on SOA

MING Liang[1] KUANG Xiao-hui[1] HUANG Min-huan[1,2] JIN Qi[1]
(Beijing Institute of System Engineering, Beijing 100101, China)[1]
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[2]

**Abstract** A new architecture of trusted smart space based on SOA (Service Oriented Architecture) was proposed for the security requirement of pervasive computing and implicit interaction. This new architecture can provide scalable information services by using SOA, and support trusted and invisible interaction by adopting a mix-access control based on actor, policy, context, and turst/risk evaluation. Finally, a prototype application was built upon Web service platform, which validated the architecture successfullly.

**Keywords** Smart space, System software, SOA, Trusted computing

智能空间是一个嵌入了计算机、信息设备和多模态传感器的工作空间,其目的是使用户能够方便地访问信息和获得计算机的服务,进而高效地实现个人目标和与他人协同工作[1]。智能空间的标志性特征是信息服务的透明性和随时随地性,使人们可以从烦琐的信息交互中解脱出来,全心关注要完成的任务。智能空间在民用和军事领域都有重要的应用价值,这种价值通常体现在具体用途上,如智能会议室[2]、未来指挥所等。在智能空间中,由于信息服务的随时随地性,因此智能空间的系统软件需要具有较强的伸缩性,能够支持信息服务的按需扩充;由于信息设备(比如智能徽章、电子纽扣、智能手表、传感器、PC、手持电脑、嵌入式计算机、无线通信设备等)的移动性、异构性和交互性,因此,要建立可信的智能空间,除了解决传统的信息系统安全问题之外,还需要考虑智能空间系统软件中新的安全威胁,比如:上述信息设备与智能空间进行透明的接入和交互而带来的新的入侵威胁。目前,主要的智能空间项目的系统软件架构都采用多代理技术来实现[2-4],其优点是:通过代理之间的交互,使服务配置和应用整合更加容易;不足是:不同智能空间之间代理互通性差,不适应智能空间走向融合的趋势。为此,本文提出了一种基于SOA的可信智能空间系统软件架构,并针对智能空间的可信性需要,设计了一种"混合访问控制"和WS-Security[5]等机制相结合的安全保障方法,为建立可信智能空间提供了有效的解决途径。

## 1 基于SOA的可信智能空间系统软件模型

### 1.1 SOA简介

SOA是Service-Oriented Architecture的简称,是一种开放的、可伸缩的、松散的、可组合的软件架构,其核心思想是将所有功能都实现为服务(Service),通过服务注册方式支持服务发布和搜索,实现服务的松散耦合和无缝互用,通过逻辑编排,为用户提供透明的、丰富多样的合成服务,同时,只要在SOA框架中,服务的执行、发现、合成不受其所在地域位置的限制,即可以随时随地满足用户的合法需求。当前,Web服务是SOA的主要实现方式。

### 1.2 概念层次设计

基于SOA的可信智能空间系统软件采用SOA思想,利用SOA环境与智能空间环境在松散耦合、动态交互、开放可扩展等方面的天然共性,较好地满足了智能空间中信息服务的随时随地性、透明性和智能性要求。

基于SOA的可信智能空间系统软件采用层次化结构设计,建立在Web服务平台之上,所有服务都以Web服务方式提供,其架构的概念层次如图1所示。

到稿日期:2009-01-15 返修日期:2009-03-27 本文受国家自然科学基金项目(60372042)资助。
明 亮 博士,助理研究员,研究方向为普适计算和网络安全,E-mail:mingliang78@yahoo.com.cn;况晓辉 博士,副研究员,研究方向为网络技术和网络安全;黄敏桓 博士研究生,副研究员,研究方向为网络技术和网络安全;金 旗 硕士,助理研究员,研究方向为网络安全。

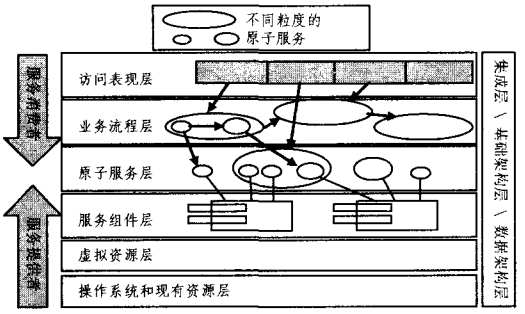


图1 基于SOA的可信智能空间系统软件架构概念图

操作系统和现有资源层。本层提供运行服务组件的操作系统和资源。操作系统包括Windows,Unix,Linux等多种类型;由于该架构允许使用面向服务技术对现有的系统进行打包,并向外界提供可以访问的服务,因此,本层还包括较旧的基于对象的系统实现、业务智能应用程序等现有资源。

虚拟资源层。本层提供对真实物理设备的虚拟化和封装,以及对较旧的系统的打包,可以应用面向服务的打包技术和虚拟机技术,使真实的硬件设备和应用程序成为与架构松散耦合的服务。本层是体现SOA中"服务与资源分离"的关键层,通过本层的屏蔽作用,系统和现有资源层对于服务组件层是透明的。本层可以通过中间件来实现,比如对设备采用ad-hoc组网方式,同时对通信的信道和协议进行抽象,实现对上层通信的持续支持,而不受下层具体物理设备添加、更换和删除的影响。本层采用HTTP,SMTP协议和SOAP消息协议完成语义通信工作。

服务组件层。本层由功能组件和服务质量组件组成。这些特殊的组件,负责对业务单元级支持的智能空间资产进行管理和控制。大多数情况下,本层使用基于容器的技术,比如功能实现组件、负载均衡、高可用性和工作量管理的应用服务器。

原子服务层(简称为服务层)。本层提供被业务选择用来支持和公开的服务。它们可以被发现或者直接静态绑定,然后被调用,或者被编排到合成服务中。这个服务公开层同样提供了获取智能空间范围组件、业务单元特定组件及有些情况下的特定项目组件的机制,并且以服务描述的形式具体化了它们的接口子集。因此,通过使用它们的接口所提供的功能,智能空间组件在运行时可以提供服务实现。本层的接口公开为服务描述,在本层中这些服务描述被公开以提供使用。本层提供的服务可以独立存在或者参与组建合成服务。

业务流程层。本层负责对在服务层中公开的服务进行合成和编排。通过合成、编排,服务被绑定成一个流程,从而作为单独的应用程序被调用。这些应用程序支持特殊的用例和业务过程。可视化的流程合成工具,比如IBM WebSphere Business Modeler, WebSphere Integration Developer, Java Business Integration[6]等都可以用于本层的业务流程设计。

访问表现层。本层SOA将用户接口从组件中分离出来,为用户提供对Web服务的访问。在本层,用户可以不用关心服务实现,专注于任务方案的设计,因此,为设计、建立智能空间应用提供了良好的平台。目前,有关本层的商业标准越来越集中,比如Web服务技术等,这些为在智能空间中开发丰富的应用提供了便利。从逻辑上看,本层是智能空间系统软件架构中直接响应用户需求并为用户提供随时随地、透明服务的层面,是体现基于SOA的智能空间系统软件架构的灵活性、可伸缩性的最终层面。

上述6个层面是智能空间系统软件架构在逻辑上的"正视图",每一个智能空间服务或者应用都具有这样的结构。下面介绍智能空间系统软件架构在逻辑上的"侧视图",其主要描述系统软件架构的服务组织形式,包括集成层、基础架构层、数据架构层3个纵向层面。

集成层。本层使用企业服务总线(Enterprise Service Bus,ESB)[7]提供对Web服务的集成。ESB通常采用一系列可靠的性能机制,比如智能路由、协议中转和其他转换机制,同时借助WSDL的绑定和接口机制,使集成层可以实现位置无关的Web服务集成。

基础架构层。本层提供了监视、管理和维护QoS的能力,比如安全、性能和可用性等。这是一个通过"感知并响应"(sense-and-respond)机制和检测SOA应用程序运转状况的工具来进行的后台处理过程,包括WS-Management[5]及相关协议的重要标准的实现,以及SOA服务质量标准的实现。

数据架构层。本层提供了统一的数据操作能力。通过对数据进行集中的分析和挖掘,为各种业务决策提供及时、准确的数据支持。

### 1.3 服务模块设计

基于SOA的可信智能空间系统软件架构在逻辑上的"俯视图"——功能服务模块图,如图2所示,主要描述了基于SOA的服务模块设计及其相互关系。为了增强智能空间的可用性和服务集成、编排能力,服务的粒度和抽象度设计应尽量遵循"保持灵活性"原则,使多数的业务需求和变化可以通过实现组装服务和变更服务来完成,而不需要变更服务定义。图2中,智能空间系统软件架构在服务层以上综合采用了服务注册、ESB和服务编排模式3种,在这3种模式的协同下,通过服务的集成与编排,形成了智能空间中丰富多样的应用。下面具体分析图2中服务的功能和作用。

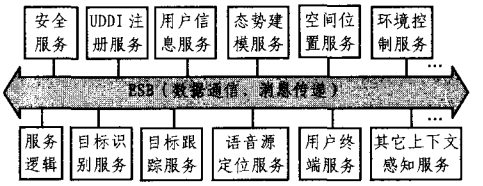


图2 基于SOA的可信智能空间服务模块示意图

基于SOA的可信智能空间系统软件架构中所有服务分为基础服务和高级服务两大类。基础服务包括安全服务、UDDI注册服务、用户终端服务、用户信息服务、态势建模服务、空间位置服务、环境控制服务等。这些服务融合了所有与智能空间基础设施紧密相联的基础服务逻辑,独立于其它服务的装载,提供系统中分布式实体的通信机制,负责控制传感器基础设施,支持高级服务。

UDDI注册管理服务。提供服务提供者与服务请求者之间的中间存储(Intermediate Storage)机制。一方面,服务提供者在注册库中发布服务描述以及相应的策略模式和数据模式;另一方面,服务请求者在注册库中搜索满足其要求的元数据。UDDI还执行整个架构的服务管理功能,其通过重定向服务请求到达合适的匹配服务以满足请求,还允许系统动态地增加新的服务。

服务逻辑。基于外部显式输入和隐含上下文信息的逻辑推理，负责业务流程设计和服务合成等工作。服务逻辑的独立性使多种服务之间的松耦合协作更加灵活，同时也强化了智能空间的逻辑推理和智能决策能力。根据上下文信息触发服务逻辑是智能空间的待候式服务的技术基础。

用户终端服务。负责提出服务请求和接收服务结果，提供所需的图形用户界面(GUI)，实现用户的需求制定与提交、结果过滤与显示等服务。用户终端服务可以帮助用户将需求转换为遵循统一格式和规范的服务请求，能被其它服务正确理解。可以简单地认为，用户终端服务是用户在智能空间中的临时代理人。

用户信息服务。包含智能空间中人员和设备的个性化信息(比如性别、身高、体重、特征、习惯等)服务。用户信息服务维护用户外观，为终端用户定制个性化的服务界面和内容。默认情况下，用户终端服务与服务逻辑的交互过程中都会自动调用个性化服务，根据用户的个性化需求，执行过滤或者修正操作。

空间位置服务。完成智能空间坐标的建立、目标位置的标定等工作。空间位置服务为智能空间提供最基本的空间视图，是态势建模服务的基础。

传感器服务。通过传感器获取智能空间的原始数据(比如：声音、视频流、空间坐标)，然后对这些数据进行处理加工，比如对视频、音频数据进行编码压缩，对空间坐标进行转换等，使其成为有用信息。传感器服务需要具备识别和控制不同厂商、不同类型、不同技术传感器的能力。比如视频传感器服务应该能够接收不同制式(PAL 和 NTSC)、不同编码标准(MPEG-1，MPEG-2 和 MPEG-4 编码格式等)的视频信息，使不同的设备都能在智能空间中提供即插即用的服务。

环境控制服务。按照服务逻辑或者用户的要求，对环境设备进行控制。这里环境是指设备和应用的集合，比如站在触摸屏旁的用户用手点击屏幕，环境控制服务就会响应这一行为，将鼠标移动至手点击的位置。与传感器服务类似，环境控制服务需要具有识别和控制不同类型和技术的硬件设备的能力。因此，环境控制服务通常需要调用传感器服务、服务逻辑和空间位置服务等。

态势建模服务(Situation Modelling Service)。负责完整、系统地组织、保存环境中所有上下文信息，为其他服务提供全面的环境态势信息服务。态势建模服务会定期与其它上下文感知服务交互，并及时记录、更新和保存环境的态势信息。态势建模服务与专门的上下文信息服务(比如空间位置服务、语音源定位服务等)不同的是，前者是所有上下文的结构化集成，而后者只提供某一方面的上下文信息。另外，态势建模服务可以根据状态迁移将消息触发至相关的服务[8]。

安全服务。负责对用户身份的认证和授权，对注册设备的识别和确认，对私密信息的控制，以及提供基于信任的访问机制等安全保障工作。

上述基础服务都与环境和硬件紧密相关，由于采用了 SOA 架构，因此，在实现上，可以采用逐步添加的方式提供这些服务。伴随着基础服务，基于 SOA 的智能空间系统软件架构中还有一些应用服务，称为高级服务。它们以基础服务为依托，执行专门的、用户指定的服务逻辑，比如目标识别服务、目标跟踪服务、语音源定位服务等。高级服务可以为用户提供个性化的、丰富多样的、透明的服务，是智能空间“智能化”程度的重要体现。

目标识别服务。对传感器服务提供的数据作进一步的处理，识别感兴趣的目标。其中包括目标建模、特征提取、模式匹配、智能决策等工作，最终得出目标识别的结果。目标识别服务通常需要请求传感器服务、态势建模服务和空间位置服务等。

目标跟踪服务。根据目标特征的识别和匹配，实现对目标的跟踪。目标跟踪服务通常需要请求传感器服务、态势建模服务、空间位置服务和目标识别服务等。

语音源定位服务。根据不同方位传感器获取的语音特征、强度等信息，经过几何计算处理，得出语音源的空间位置等信息。语音源定位服务通常需要请求传感器服务、态势建模服务和空间位置服务等。

其它上下文感知服务。根据不同智能空间中的专门需求，完成其它能够感知环境并获取上下文信息的活动，比如历史记录上下文服务、降雨量变化规律服务、个人情绪波动服务、心率起伏变化服务等。

通过以上这些服务，基于 SOA 的智能空间将软件的复用和自治能力充分发挥出来，提供一整套待候性服务，智能地、尽力地满足智能空间中用户的各种需求。

## 2 智能空间的可信设计

在 Web 服务平台上构建基于 SOA 的智能空间主要存在两类安全威胁：一类来自外部，即智能空间中为支持透明的信息服务而采用的新型的接入和交互方式，比如传感器输入、触摸屏输入、上下文感知交互等；另一类来自智能空间内部，在 Web 服务平台上，主要考虑 Web 服务内部的信息安全：由于 Web 服务可被各种程序数据存储访问，服务之间可能会传递敏感信息，因此 Web 服务需要对整个对话提供端到端的安全模型。于是，提出了“混合访问控制”和 WS-Security[5] 等机制相结合的方法，来着重解决这两类安全问题。

### 2.1 混合访问控制

“混合访问控制”方法是一种综合采用多种访问控制并形成互补关系的混合方法，本质上是一种智能空间中实体认证技术，其包括基于角色、基于策略、基于上下文和基于信任关系度的访问控制，如图 3 所示。基于角色的访问控制主要用于用户和智能设备登录智能空间时，必须进行相应的安全服务认证，根据预设的角色和权限执行相应的操作。基于策略的访问控制主要体现在防火墙、入侵检测系统和核心交换机中，用于根据设定的策略阻止潜在的外来入侵者，防止未授权的访问和滥用权限的访问，这种情况通常发生在随时随地的无线接入中。基于上下文的访问控制主要提供智能的和具有上下文感知能力的访问控制，比如某合法用户在触摸屏旁，就可以自动开启触摸屏许可，反之，如果智能空间系统发现该合法用户已经远离触摸屏，而是某非法用户正在利用合法用户标识使用触摸屏，那么基于上下文的访问控制就会指示触摸屏不作响应。

基于信任关系的访问控制是通过 Trust/Risk 管理支持来自其它区域的未注册的可信用户和设备对智能空间的访问，来支持漫游实体的信任协作和许可。通过在智能空间环境中建模信任关系，来自不同区域的未知实体可以以安全和

私密的方式进行交互，并请求当前区域中的服务和资源。Trust/Risk管理中采用信任度和风险度评价相结合的方法——定义许可度，设置合理的许可度阈值，共同做出访问控制的决策，许可度越高，该访问越安全，反之越危险。

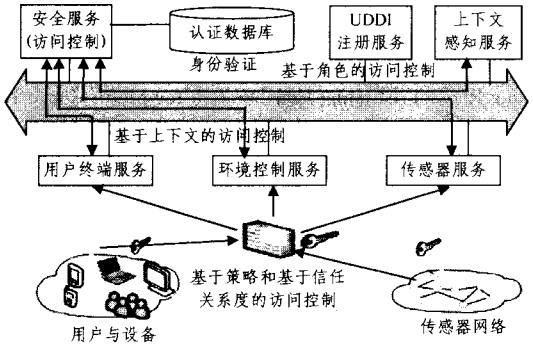


图3 智能空间中“混合访问控制”示意图

许可度可以使用模糊集理论来描述[11]。令$U\times U=\{(u,u)\}$是Trust/Risk关系$R$的对象空间，定义$R$为用户$u$访问智能空间的“许可度”，则$R$可用隶属度函数$\mu_{TF\times RF}$来表示，见式(1)：

$$\mu_{TF\times RF}:U\times U\rightarrow[0,1] \tag{1}$$

其中，$\mu_{TF\times RF}(u,u)$值域的含义如式(2)所示。

$$\mu_{TF\times RF}(u,u)=\begin{cases}1 & \text{表示完全允许用户 } u \text{ 访问智能空间}\\ (0,1) & \text{表示部分允许用户 } u \text{ 访问智能空间}\\ 0 & \text{表示不允许用户 } u \text{ 访问智能空间}\end{cases} \tag{2}$$

其中，模糊集$TF\times RF$可以定义为由“用户及其许可度”构成的有序对集合，如式(3)所示：

$$TF\times RF=\{((u,u),\mu_{TF\times RF}(u,u))\mid u\in U\} \tag{3}$$

其中，$\mu_{TF\times RF}(u,u)$可以由式(4)和式(5)来定义。

$$\mu_{TF\times RF}(u,u)=\mu_{TF}(u,u)\times\mu_{RF}(u,u) \tag{4}$$

$$\mu_{TF}:U\rightarrow[0,1],\mu_{RF}:U\rightarrow[0,1] \tag{5}$$

式(4)和式(5)中，$\mu_{TF}$为智能空间对用户$u$的信任度，$\mu_{TF}$值域区间为[0,1]，值越大，信任度越高，即越安全；$\mu_{RF}$为用户$u$访问智能空间带来的风险度，$\mu_{RF}$值域区间为[0,1]，值越大，风险度越小，即越安全；$\mu_{TF}$和$\mu_{RF}$都是关于用户$u$的单调函数，可以通过自定义算法得到，参见文献[11]。

“混合访问控制”方法通过使用Trust/Risk管理合理地拓展了用户的工作范围和权限，更适合智能空间中的实际需求。图3中用户与设备进入智能空间，需要先经过防火墙进行入侵检测认证，然后，经由用户终端服务和环境控制服务调用安全服务，安全服务根据认证数据库中的信息(比如预先注册的ID、密码等)判定接入的用户和设备是否合法以及是否允许其行使相应的角色和权限。同理，无线传感器网络也要经过类似的身份认证，才能合法地接入到智能空间中。

### 2.2 混合访问控制Web服务内部安全

Web服务平台中安全措施需要对传输级安全、消息级安全、数据级安全、环境级安全逐一考虑。其中传输级安全和环境级安全都是分布式应用共有的安全问题，可以采用传统的解决方法，比如传输级安全采用防火墙、虚拟专用网(VPN)、基本认证、防抵赖及加密性等措施，环境级安全采用管理、登录、审核以及构建信任关系和通信模式的措施。在消息级安全和数据级安全上，我们采用了针对Web服务的WS-Security框架协议[5]。

WS-Security定义了一个机制，该机制为SOAP消息增加了消息级和数据级的安全保证，其包含以下安全措施：

认证令牌。WS-Security认证令牌由客户端发出，在SOAP消息头中插入用户名和密码或X.509证书等标准化方式进行认证。

XML封装。WS-Security使用W3C的XML-Encryption规范使得SOAP消息体或消息体的一部分被加密以确保消息的机密性[9]。

XML数字签名。WS-Security使用W3C的XML-Signature规范使得SOAP消息被数字化地签名以确保消息的完整性和不可抵赖性[10]。典型的签名是基于消息自身内容计算的一个值，如果消息在路由过程中被改变了，这个值就会发生相应改变，这个签名就是无效的，表明这个消息的完整性已经遭到了破坏。

## 3 实验分析

根据上述设计方案，我们在NetBeans 5.5中采用JBI(Java Business Integration)[6]模型，开发了一个通过服务组合完成的智能空间应用——“智能请领服务”系统。该系统是在基于SOA的可信智能空间系统软件架构上实现的一个简单的原型系统，其智能化主要通过智能空间中的“用户终端服务”及其与其他服务之间的智能交互来体现。“用户终端服务”可以自动请求智能空间中的其它服务，比如请求“安全服务”获得用户的认证信息，请求“用户信息服务”获得用户的个性化信息，请求“请领单服务”获取请领服务，还可以对请求得到的这些信息进行融合等等。该系统中服务提供者和服务请求者都用Web服务实现，SOA架构为服务提供者和服务请求者分割出业务逻辑，并提供服务的位置透明性。

如图4所示，一个简单的请领业务主要由“用户终端服务”、“安全服务”、“请领单服务”和“库存检查服务”4个服务逻辑组成，其执行过程如下。

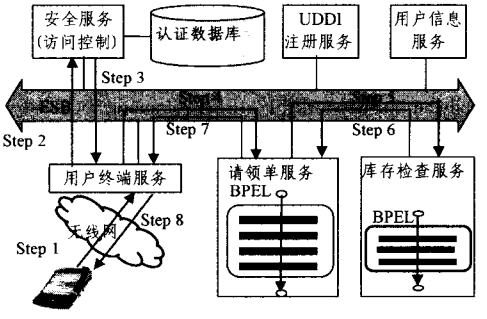


图4 “智能请领服务”系统逻辑示意图

步骤1 智能空间感知到移动用户设备后，由“用户终端服务”负责响应；

步骤2 “用户终端服务”向“安全服务”发起认证请求；

步骤3 认证通过后，“安全服务”通知用户设备可以合法接入智能空间，享受信息服务，比如智能请领服务；

步骤4 用户设备通过“用户终端服务”发出请领单请求，“用户终端服务”按照用户要求形成符合规格的请领单，将其发至“请领单服务”，请求提供相应服务；

步骤5 “请领单服务”逻辑根据请领单内容，向“库存检查服务”发出请求，请求查询当前库存中是否有用户需要的货

物及相关信息；

步骤 6 “库存检查服务”逻辑根据服务请求内容，执行查询，得出“有货物”及“数量”或者“无货物”等结果信息，然后，将查询结果提供给“请领单服务”；

步骤 7 “请领单服务”根据查询结果，形成回执，提供给“用户终端服务”；

步骤 8 “用户终端服务”结合用户的个性化信息，将结果进行过滤和封装，以恰当的方式显示在用户设备上。

对这个请领业务进行测试的输入和输出都是一个包含 SOAP 消息数据的 XML 文件。经测试，采用合法用户 ID，上述智能请领服务可以较好地完成可信接入智能空间，并执行请领功能；采用非法用户 ID，则提示无法进行请领。合法用户的请领过程如图 5 所示。图 5 中，合法用户填写请领信息后，系统就可以通过服务组合与集成的方式完成相应的功能，获得请领结果。实验表明，“用户终端服务”、“安全服务”、“请领单服务”和“库存检查服务”4 个服务功能模块能够较好地进行集成和协作，初步验证了我们提出的基于 SOA 的可信智能空间系统软件模型是有效的。

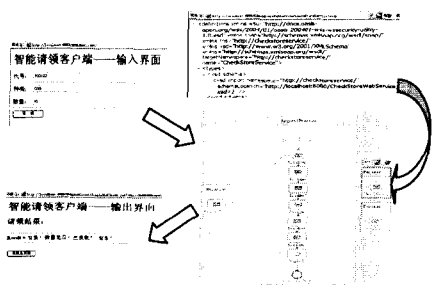


图 5 智能请领服务”系统实现示意图

**结束语** 基于 SOA 的可信智能空间系统模型为构建智能空间提供了一般性的设计方案，其具有良好的伸缩性和系统的安全性，有利于智能空间的不断丰富和扩展。下一步将深入验证该模型在大型复杂智能空间中的适应性。

## 参 考 文 献


[1] Rosenthal L, Stanford V. NIST Information Technology Laboratory Pervasive Computing Initiative[C]// Proceedings of IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. NIST, USA, 2000: 30-36

[2] Chen Enyi, Shi Yuanchun, Zhang Degan, et al. Intelligent Meeting Room: Facilitating Collaboration for Multi Mobile Devices on Contextual Information[C]// Proceedings of the 8th International Conference on Computer Supported Cooperative Work in Design. 2003: 82-87

[3] Saif U, Pham H, Paluska J M, et al. A Case for Goal-oriented Programming Semantics[C]// Proceedings of System Support for Ubiquitous Computing Workshop at the 5th Annual Conference on Ubiquitous Computing. 2003: 74-83

[4] Tesauro G, Chess D M, Walsh W E, et al. A Multi-Agent Systems Approach to Autonomic Computing[C]// Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'04). Vol. 1, New York, USA, 2004: 464-471

[5] Web Services Security Specifications Index Page. (URL: http://msdn2. microsoft. com/en-us/library/ms951273. aspx)

[6] JBI(Java Business Integration)模型(URL: http://java. sun. com/integration/)(2008-12 Updated)

[7] 徐涵. Understanding SOA with Web Services(中文版)[M]. 2006

[8] Crowley J L. Context Driven Observation of Human Activity[C]// Proceedings of the European Symposium on Ambient Intelligence. 2003, 11: 101-118

[9] XML-Encryption(URL: http://www. w3. org/Encryption/)

[10] XML-Signature (URL: http://www. w3. org/Signature/)

[11] Yang Qiuwei, Wu Sunyong, Hong Fan, et al. Authorization Management Framework Based on Joint Trust-Risk Evaluation [J]. Wuhan University Journal of Natural Sciences, 2007, 12 (1): 9-12


(上接第 22 页)


[55] Hanzo L Ⅱ, Tafazolli R. A survey of QoS routing solutions for mobile ad hoc networks[J]. IEEE communications survey & tutorials, 2007, 9(2): 50-70

[56] Chiu Chun-Yuan, Kuo Yu-Liang, Hsiao-Kuang W E, et al. Bandwidth-constrained routing problem in wireless ad hoc networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(1): 4-14

[57] Chou C-F, Suen H-P. Topology - control - based QoS Routing (TLQR) in wireless ad hoc networks[C]// IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications. 2006: 1-4

[58] Wang M, Kuo G S. An application-aware QoS routing scheme with improved stability for multimedia applications in mobile ad hoc networks[C]// Proceedings of IEEE vehicle Technology Conference. 2005: 1901-1905

[59] Kim P J, Tsudik P G. SRDP: securing route discovery in DSR [C]// Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services 2005. 2005: 247-260

[60] Zapata M G. Secure ad hoc on-demand distance vector routing [J]. IEEE Mobile Computing and Communications Review, 2006, 6(3): 106-107

[61] Eichler S, Roman C. Challenges of secure Routing in MANETs: A Simulative Approach using AODV-SEC[C]// IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS2006). 2006: 481-484

[62] Li Zhi, Kwok Yu-Kwong. A new multipath routing approach to enhancing TCP security in ad hoc wireless Networks[C]// Proceedings of the 2005 International Conference on Parallel Processing Workshops(ICPPW'05). 2005: 372-379

[63] Jin Lu, Zhang Zhongwei, Lai D, et al. Implementing and evaluating an adaptive secure routing protocol for mobile ad hoc network[C]// IEEE Wireless Telecommunications Symposium, 2006(WTS '06). 2006: 1-10

[64] Hu Yih-Chun, Perrig A, Johnson D B. Ariadne: a secure on-demand routing protocol for ad hoc networks[J]. IEEE Wireless Networks, 2005, 11(1/2): 21-38

[65] 周满元，周力为. 基于不同源节点数目的 AODV 路由协议的性能比较研究[J]. 计算机工程与应用，2007，43(18)：94-96