

普适环境中的动态更新模型

周文嘉, 黄林鹏, 陈俊清

(上海交通大学 计算机科学与工程系, 上海 200240)

摘 要: 致力于普适计算下的动态更新的研究, 首先分析了普适计算下动态更新的场景, 针对普适环境的动态性, 我们提出了区别于传统更新方式的路径更新; 通过分析集中式更新模型的局限性, 提出了适合普适环境的分布式更新模型; 最后使用类型与效果系统为更新模型做形式化分析。

关键词: 普适计算; 动态更新; 路径更新; 形式化分析

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2011)08-0015-04

Dynamic Updating Model in Ubiquitous Computing

ZHOU Wen-jia, HUANG Lin-peng, CHEN Jun-qing

(Department of Computer Science & Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

Abstract: In this paper, we discuss the dynamic updating in ubiquitous computing, analyze the scenarios of dynamic updating, presents a new way of updating—route updating because of the dynamic of ubiquitous environment, different from the traditional updating way; by analyzing the limitation of the centralized updating model, we design a distributed updating model suitable for ubiquitous computing environment; finally we build a formal model for this updating mechanism using type and effect system.

Key words: ubiquitous computing; dynamic updating; route updating; formal analysis

1 引言

普适计算, 也称为无处不在的计算, 如今日益成为计算机科学的一个研究热点, 它的目标是将信息技术集成到人们的日常生活中, 以一种高度智能化和人性化的模式实现无处不在的计算。

软件系统投入使用后, 就进入了维护阶段, 经常需要进行版本升级或者安装新的修复补丁, 这可能是由于原先设计有缺陷, 用户提出了新的需求, 要提高软件的性能等等。动态更新是指在不中断软件运行的情况下, 对程序进行修改和替换, 从而减少更新对系统可用性的影响。

2 普适计算下动态更新建模

2.1 更新对象分析

由于普适环境的异构性、分布性和动态性等特

点, 我们采用面向服务(SOA)的系统架构, 将普适环境中设备的所有可用资源封装成服务^[1], 向外提供服务接口以供调用。

2.2 更新场景分析

在一个普适环境中, 设备之间多使用无线方式通信, 诸如 WiFi、UWB、蓝牙等, 而且由于普适环境中设备异构性、分布性和动态性等特点, 使得普适环境中的动态更新呈现出不同于传统计算环境的特点。本文在分析普适计算场景的这些特点后, 将普适环境中的动态更新分为两类。

一类是由于设备在普适环境中的移动而产生的更新需求, 我们称这类更新为路径更新, 即找到一条替代路径支持用户对服务的使用。

一类是由于新旧版本服务的替换引起的更新, 这属于传统的动态更新^[2], 但由于普适环境异构性、分布性的特点, 需要找到适合的更新模型, 来支持普

收稿日期: 2011-05-10; 修回日期: 2011-06-23

基金项目: 国家自然科学基金项目(60970010); 高等学校博士学科点专项科研基金课题(20090073110026)

适环境下这类更新的进行。

2.3 更新过程分析

为了实现不中断服务运行的动态更新,整个更新过程必须满足以下两个要求:

要求一:更新正确性,这个要求是指整个更新过程必须是正确的.我们将这个要求细化成三个子要求:一是安全的更新时机;二是更新前后状态一致性;三是更新前后服务调用的正确性。

要求二:用户透明性,这个要求是指更新不应该影响用户对服务的使用,用户不需要了解更新的发生和更新的细节.它包括两个方面的要求:一是更新过程不会影响用户对服务的使用;二是更新之后,用户仍可以以更新之前的服务接口访问服务。

2.4 更新模型

2.4.1 更新机制基础

通过分析普适环境的特点和动态更新的目标效果以及用户的使用界面,我们总结出在普适环境下实现动态更新有以下四个基本操作。

请求接收和缓冲:接收来自其他服务的服务请求,并将请求发给正确的服务.当更新触发时,缓冲更新开始这一时刻到更新结束的服务请求。

请求重定向和释放:更新完成后,所有对目标服务的请求都会被以正确的方式重定向(路径或新版本服务实例),并释放给正确的服务。

路径选择:由于普适环境的动态性,普适环境中的设备组成一个移动的开放的 ad hoc 网络,当触发路径更新或更新的新服务位于另一设备时,我们需要结合使用的通信方式,设计有效的算法,找到合适的服务路径。

状态转移:当触发新旧服务更新时,如果更新的服务是有状态的,那么需要将旧版本服务的运行状态初始化给新版本服务。

2.4.2 适合普适环境的服务通信方式

在分析运行时服务的通信方式时,我们将服务的提供者和服务的消费者之间的通信抽象为一般的客户端/服务器模型(C/S 模型)。

文献[3]中提出了一个基于组件的动态更新更新模型,在他们的模型中,使用一个集中式的中介控制器来协调组件提供的服务与服务消费者之间的通信.这种集中式的更新模型逻辑比较简单,但所有的服务请求和服务应答都必须通过中介,而且作为模型的核心,中介控制器必须连续运行,这就导致这种模型不适合使用在移动的开放的普适环境中。

基于以上的分析,我们提出一种分布式的更新

模型(图 1),为每个服务添加一个代理,通过服务代理之间的通信来完成服务的调用、更新等操作。

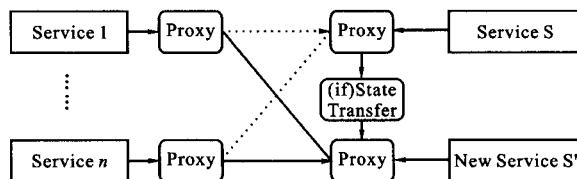


图 1 分布式更新模型

2.4.3 路径选择算法

在普适环境中,设备之间维护一个弱连接 ad hoc 网络,设备每隔一段时间以洪泛方式向周围设备广播自己的心跳,环境中的其他设备若能接收到这个心跳信息,则认为该设备是可连接的,并将其加入到自己的可连接设备列表中.当一段时间没有收到该设备的心跳时,则将其从列表中删除。

当一个设备 A 需要在环境中寻找一条到另一设备 B 的路由时,首先查看自己的可连接设备列表,若设备 B 在列表中,则路径已找到;若设备 B 不在列表中,则向可连接设备列表中的所有设备发送查找设备 B 的请求并设置 timeout,收到该请求的设备如果已经处理过该请求,则忽略该请求,如果没有处理过该请求,则查找自己的可连接设备列表,如果设备 B 在列表中,则按路径返回查找成功和路径信息,否则向其可连接设备转发.如果设备 A 等待时间超过设置的 timeout,仍未收到查找成功和路径信息,则认为设备 B 不可达。

2.4.4 路径更新

如图 2 所示,假设普适环境中,服务 A 通过服务 C 所在设备调用服务 B,某一时刻,服务 C 所在设备移动到一个新的位置,此时服务 A 所在设备与服务 C 所在设备不可连接,服务 B 与服务 C 所在设备也不可连接,而且此时服务 B 有向服务 A 发送的服务响应,服务 C 所在设备也有服务 B 向服务 C 发送的服务响应,服务 A 有向服务 B 发送的服务请求.因为服务 A 到服务 C 和服务 C 到服务 B 都不可达,此时各服务中介缓冲向其已不可连接的服务发送的服务请求或响应,直到下一个心跳重新组成一个新的 ad hoc 网络,然后使用路径选择算法获取新的路径,释放缓冲的请求或响应,并重定向服务 A 对服务 B 的服务请求。

2.4.5 服务更新

在我们的模型中,我们将服务的动态更新分为四步骤的操作流程(等待安全更新时机、加载新服务和状态转移、服务重定向、释放旧服务资源)和三个

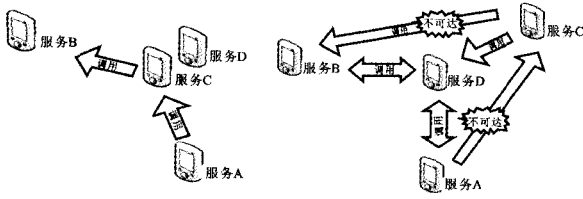


图2 路径更新通信模型

辅助流程(版本兼容性校验、依赖处理、容错)。当涉及设备之间的路由时,运用上面的路由算法。

版本兼容性校验:即新版本服务向外提供的服务必须是旧版本服务向外提供的服务的超集,新版本本依赖的外部服务必须是旧版本依赖的外部服务的子集。

等待安全的更新时机:当更新请求到达后,服务中介将缓冲这一刻之后到达的服务请求,等待服务完成当前正在处理的服务请求。当服务空闲下来时,进入下一步。

加载新服务和状态转移:新版本服务加载成功后,系统进入一个新旧版本服务并存的状态,这时如果更新的目标服务是有状态服务,需要将旧版本服务的状态信息提取出来,初始化给新版本服务实例。

服务重定向:恢复对服务的访问,修改服务发布地址并通知目标服务的连接者连接到新的地址,并且将之前缓冲的服务请求释放给新版本服务实例。

释放旧服务资源:这一阶段主要是做一些后续清理工作,将旧版本服务移除,并释放占有的资源。

依赖处理:假设服务A对服务B有依赖,而且对A更新时也需要更新B,我们将对A发出更新请求,并将B的更新请求包含其中,然后由A触发对B的更新。

容错:当更新过程出现影响更新效果的错误时,将进入错误恢复阶段,回滚到更新前的状态。

3 形式化分析

本文将使用类型与效果系统形式化分析更新模型。文献[4]对类型和效果系统作了较为全面的介绍。

首先,先对更新模型中的服务进行建模^[5],在我们的形式化模型中,引入了扩展的 λ 演算。

$$s, s' ::= \alpha \mid \mu \mid \text{if } b \text{ then } s \text{ else } s' \mid \lambda_z x. s \mid s s' \mid \Theta(s') \mid s \rightarrow s'.$$

$$b ::= \text{true} \mid \text{false}.$$

$$\rho. s \rightarrow \rho'. s'.$$

$$\Theta(s') \sim s.$$

其中, s, s' 表示服务; α 表示单个的行为; μ 表示

行为变量; $\text{if } b \text{ then } s \text{ else } s'$ 是条件语句,其中 b 为布尔值; $\lambda_z x. s$ 表示函数的抽象, z 为自变量; $\Theta(s')$ 表示对服务 s' 做兼容性验证; $s \rightarrow s'$ 表示将服务 s 更新为 s' 。

$\rho. s \rightarrow \rho'. s'$ 为服务基本的操作语义,表示服务 s 演化到 s' 时, ρ 扩展到 ρ' ,其中 ρ 表示服务运行时的行为序列。 $\Theta(s') \sim s$ 表示服务 s' 与 s 是兼容的。

然后,我们对服务的行为建模,建立服务的行为表达式。

$$A, A' ::= \epsilon \mid \alpha \mid \mu \mid A; A' \mid A + A' \mid A \mid A' \mid \text{REC}_\mu A.$$

$$\alpha, \alpha' ::= \dot{O} \mid f(\alpha) \mid f(\alpha \alpha').$$

其中, ϵ 表示空的行为; α 表示单个行为; μ 表示行为变量; $A; A'$ 表示行为表达式的顺序关系; $A + A'$ 表示行为表达式的选择关系; $A \mid A'$ 表示行为表达式的并发关系; $\text{REC}_\mu A$ 表示行为表达式 A 在上递归。 $\dot{O}$ 表示服务中的原子属性或对象; f 表示函数或方法,其作用对象为一个 α 或两个 α 。

引入类型与效果系统, Γ 表示类型环境, τ 表示服务接口类型, A_u 表示用户感知的服务行为。

$$\tau, \tau' ::= \text{void} \mid \text{int}^\circ \mid \text{string}^\circ \mid \text{boolean}^\circ \mid \dots \mid \tau \rightarrow \tau'$$

$$\Gamma ::= \Phi \mid \Gamma U \{s : \tau \mid s : \tau \notin \Gamma\}$$

$\Gamma, A, A_u \vdash_{\text{PATH}} s : \tau$ 表示服务 s 的类型为 τ ,运行时会产生以 A 表示的服务行为,用户通过PATH路径获取服务,且用户可感知的服务行为为 A_u 。

定义1 对于两个服务 $\Gamma, A, A_u \vdash_{\text{PATH}} s : \tau$ 和 $\Gamma, A', A'_u \vdash_{\text{PATH}} s' : \tau'$,如果满足 $\Theta(s') \sim s$,则认为服务 s 可以由服务 s' 更新,记为 $\hat{U}_t(s \rightarrow s')$;否则认为是不可更新的, $\hat{U}_f(s \rightarrow s')$ 。

定义2 服务 $s, \Gamma, A, A_u \vdash_{\text{PATH}} s : \tau$,其中 $A = \alpha_1 \alpha_2 \alpha_3 \dots \alpha_{i-1} \alpha_i \dots \alpha_n$,当正要进入 α_i 时,更新 $\hat{U}$ 发生,服务 s 被更新为 s' , $\Gamma, A', A'_u \vdash_{\text{PATH}} s' : \tau'$,其中 $A' = \tilde{A} \alpha_k \dots \alpha_{j-1} \alpha_j \dots \alpha_n$,则 $\tilde{A} \approx \alpha_1 \alpha_2 \alpha_3 \dots \alpha_{i-1}$,即在对各自原子属性或对象的作用上 $\tilde{A}$ 和 $\alpha_1 \alpha_2 \alpha_3 \dots \alpha_{i-1}$ 等价。

定义3 对于两个服务 $\Gamma, A, A_u \vdash_{\text{PATH}} s : \tau$ 和 $\Gamma, A', A'_u \vdash_{\text{PATH}} s' : \tau'$,且 $\hat{U}_t(s \rightarrow s')$,当更新 $\hat{U}$ 发生前后, $A_u = A'_u$,即更新前后用户感知的服务行为相同。

定义1和定义2分别从服务的兼容性和状态一致方面保证了更新的正确性;定义3保证了更新的发生满足用户透明性。综合起来完成了对模型正确性的验证。

4 结束语

我们现在的日常生活越来越依赖各种各样的移动数字设备和传感设备,普适计算逐渐成为我们生活中一个不可或缺的角色,为了提高部署在普适环境中系统的可用性,需要相应的动态更新技术来支持系统的持续运行.本文在国内外相关领域研究成果的基础上,通过分析普适环境的特点和现有更新模型的局限性,提出了路径更新方式和分布式更新模型;最后对提出的更新模型做形式化分析,从理论上验证了模型的正确性.在以后的工作中,我们将在真实的普适环境中逐步实现我们的更新模型.

参考文献:

- [1] Gu X, Messer A, Greenberg I, et al. Adaptive offloading for pervasive computing[J]. IEEE Pervasive Computing, 2004,3(3):66-73.
- [2] Fei Shen, Siqi Du, Linpeng Huang. A dynamic update framework for OSGi applications[C]// Proceedings of 2nd International Conference on High Performance Computing and Applications (HPCA2009). China: Shanghai, 2009.

- [3] Junrong Shen, Xi Sun, Gang Huang, et al. Towards a unified formal model for supporting mechanisms of dynamic component update[C]// Proceedings of the 10th European software engineering conference help jointly with 13th ACM SIGSOFT international symposium on Foundations of software engineering. Lisbon, Portugal, 2005.
- [4] Bartoletti M, Degano P, Ferrari G L. Types and effects for secure service orchestration[C]// Proc. the 19th Computer Security Foundations Workshop. Italy, Venice, 2006:57-69.
- [5] 曾慧清, 黄林鹏, 陈俊清. 基于 ASM 的普适环境下的服务动态组合[J]. 微电子学与计算机, 2010,27(8):86-90.

作者简介:

周文嘉 男,(1988-),硕士研究生.研究方向为普适计算、动态更新.

黄林鹏 男,(1963-),教授,博士生导师.研究方向为程序设计语言、并行分布式计算、人工智能等.

陈俊清 男,(1982-),博士研究生.研究方向分布式计算、普适计算、形式化分析.

(上接第 14 页)

- [3] Joon-Sang Park, Gerla M. Codecast: a network coding based ad hoc multicast protocol [J]. Wireless Communication, IEEE, 2006,13(5):76-81.
- [4] 焦进,杨铭熙. 基于网络编码的 Ad Hoc 网 PUMA 协议研究 [D]. 武汉:武汉理工大学,2009.
- [5] Ravindra Vaishampayan, Garcia Luna Aceves J J. Efficient and robust multicast routing in mobile Ad Hoc networks[C]// IEEE International Conference on Mobile Ad-hoc and Sensor Systems. Italy: Rome, 2004:304-313.
- [6] 黄化吉,冯德力. NS 网络模拟和协议仿真[M]. 北京:人民邮电出版社,2010.
- [7] Royer E, Perkins C. Multicast operation of the ad hoc

on-demand distance vector routing protocol[C]// Proceedings of Mobicom. USA: Washington, 1999.

作者简介:

谭国平 男,(1975-),博士,副教授.研究方向为移动自组网、无线多媒体通信、随机网络优化与控制及网络信息论等.

倪新洋 男,(1988-),硕士研究生.研究方向为移动自组网、网络编码.

季敏 女,(1988-),硕士研究生.研究方向为移动自组网、网络编码.

马赛赛 男,(1988-),硕士研究生.研究方向为无线多媒体通信.