普适计算的信任计算模型*)

郭亚军[1,2] 洪 帆[1]

(华中科技大学计算机科学与技术学院数据安全与保密实验室 武汉 430074)[1]

(华中师范大学计算机科学系 430079)[2]

摘 要 信任和安全有紧密的联系,当前的安全技术都隐含地与信任相关。普适计算环境是一个开放的环境,相互合作的主体具有自发性和不可预知性。在互相不知道的主体之间进行交互,必须有足够级的信任。普适计算比传统计算更强调信任的作用。本文在分析普适计算的信任特征后给出了适合该环境的信任计算模型。证明了普适计算环境中的信任关系是偏序关系,根据信任 Hasse 图,我们给出了信任评估机制。最后分析表明该模型满足 Lamsal 的普适计算信任建模要求。

关键词 普适计算,信任,安全,信任模型

Trust Computing Model for Pervasive Computing

GUO Ya-Jun[1,2] HONG Fan[1]

(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)[1]

(Department of Computer Science, Central China Normal University, Wuhan 430079)[2]

Abstract There exists a close relationship between trust and security. Current security techniques are involved implicitly in trust. Pervasive computing environment is an open environment in which principals collaborate spontaneously and unforeseeably. High enough trust is essential to ensure security among these principals in which pervasive computing pays more attention to the role of trust than traditional computing. In this paper, after analyzing the characteristics of pervasive computing, we present a formal trust computing model. Meanwhile, we prove that trust relationship in pervasive computing is partial ordering and the approach to evaluate combination trust value is studied based on trust Hasse diagram. In the end, the analysis makes clear that the trust model proposed in this paper can meet Lamsal's trust modeling requirement of pervasive computing.

Keywords Pervasive computing, Trust, Security, Trust model

信任和安全有紧密的联系。当前的安全技术都隐含地与信任相关,如 PKI 技术中,安全来自于对 CA 的信任,交互的双方都相信 CA 提供的证书。普适计算[1,2]环境是由嵌入和遍及在我们环境中的具有通信和计算能力的设备组成。普适计算比传统计算更强调信任的作用,不仅因为普适计算系统在共享通道(如无线连接)上进行高度分散的网络通信,而且它们之间的交互是自发的,不需要干预的情况下操作,如不需要用户输入用户名和密码。并且普适环境是变化的和预先不可知的,在互相不知道的主体之间交互,双方必须有足够级的信任,就如同人类在没有完全的信息情况下用信任促进交互和承担风险一样。本文在分析普适计算的信任特征后给出了适合该环境的信任计算模型。证明了普适计算信任关系是偏序关系,根据信任 Hasse 图,我们给出了信任评估机制。最后分析表明该模型满足 Lamsal 的普适计算信任建模要求。

1 信任及相关工作介绍

信任是人类生活的一个重要方面,我们做的许多事情是与信任相关的。信任是相当复杂的概念。关于信任的研究主要来自社会学、心理学和哲学三个不同的领域。信任的定义也非常多,如基于期望(expectation)的信任,基于机构(institution)的信任,基于认知(cognitive)的信任,基于知识的信任和基于计算的信任等等。文[4~8]等从不同的方面讨论了信任问题。

信任具有下列特性:

· 信任的主观性:不同的主体对同一问题的信任度有所不同。

· 信任的传递性:一般认为信任具有不可传递性,如 A 信任 B,B 信任 C,但 A 不一定信任 C,但为了简化模型,我们认为信任是可以传递的,是条件限制的传递性。如在现实生活中人们通过推荐建立了信任。

· 信任的反对称性:A 信任 B,但 B 不一定信任 A,或者两者互相信任的程度是不同的。

· 信任的上下文相关性:信任是相对于某个上下文而言的。

· 信任的可测量性,信任像信息和知识一样能够被测量。

· 信任的多样性:信任的主体、目的和客体具有多样性。

· 信任的多面性:即使同样的上下文,信任值也会不同,信任来自多方面的。

· 信任的动态性:信任与时间有关,不同的时间信任度会不同,传统的安全技术中,在给定的时间内双方绝对信任,在其他时间内不信任。普适环境的信任应该是随时间渐变的。

研究者常常使用信任进行安全管理。文[9~11]用信任解决证书的委托问题,使用证书委托特权进行安全管理,陌生的用户通过已经授权的用户访问资源,但这里的信任是暗含的,没有解决为什么要信任陌生用户的问题。在文[12~14]中,主要研究普适计算的信任模型,他们从网络安全扩展信任概念,他们把上下文信息引入到系统中,访问控制不仅仅依赖证书,而且还依赖上下文信息,但只是简单地把上下文变量合并到系统中。文[15]使用入侵检测工具的报告动态更新和传播信任,但主体最初的信任是事先分配的,它不适合普适环

*)基金项目:国家高技术研究发展计划(863)(No. 863-301-1-3);国防预研基金(No. 15-8-4);湖北省自然科学基金(编号:2005ABA243)。郭亚军 在职博士生,副教授,主要研究领域为计算机安全与保密,普适计算;洪 帆 教授,博士生导师,主要研究领域为计算机安全与保密。

境。文[16]则考虑了信任中的隐私问题。

普适计算与传统计算的不同点主要在于普适计算具有移动性、无处不在性和交互的多样性。普适环境中的一些交互要求常常发生在不熟悉的环境和互相不认识的主体之间。当前系统中的暗含的、静止的信任不适合普适环境的信任建模。目前绝大多数的研究者认为信任信息主要来自主体的观察，他们用主体的观察结果和第三方观察的结果(称为直接经验和间接经验)评估信任。但是普适环境中主要涉及陌生主体的交互，最初的信任不可能来自观察的结果。因此我们根据主体具有的属性建立信任。另外我们的信任模型的信任信息还来自于推荐和上下文信息。

2 信任模型

对于任一主体 $p_i \in Principal$，它具有属性 $a_1, a_2, \cdots, a_n$，$a_i \in Attribute$，p_i 的属性集表示为：$A(p_i)=\{a_1, a_2, \cdots, a_n\}$，上下文信息 c。

对于主体 p_i 和 p_j，p_i 对 p_j 的直接信任值表示为：

$T=(T_a, T_c)$

T_a 和 T_c 分别表示由主体的属性和上下文信息而产生的信任值。T_a 是信任值的静态部分，一旦确定后，它的值不会变化，我们把它称为静态信任值。T_c 是信任值的动态部分，它随着上下文信息的变化而变化，我们把它称为动态信任值。T_a 和 T_c 分别离散地表示为{*untrust*, *uncertainty*, *low*, *medium*, *high*}。如主体的信任值(*low*, *medium*)表示由主体属性而产生的信任值为 *low*，由上下文信息而产生的信任值为 *medium*。

2.1 信任关系建立

在普适计算中，建立主体之间的信任主要有两个方面：一是根据主体的属性建立静态信任；二是根据上下文信息建立动态信任。

陌生的双方最初的信任是建立在双方具有的属性基础上。自动信任协商[18~22]是为陌生的交互双方建立信任的技术。双方多次向对方呈现自己的数字信任书(credential)。信任书包含某些属性。自动信任协商是基于对方有什么(即有什么属性)，而不是基于对方是谁(身份)。信任书由信任书发行者签名，证明信任书的拥有者具有哪些属性。数字信任书可以用 X.509 证书实现。访问控制策略(policy)控制访问服务、信任书或者策略本身等资源。协商策略(negotiation strategy)指明要访问一个特殊资源对方应该呈现哪个信任书。由于协商的双方可能有敏感的证书和访问控制策略，因此信任协商可能需要双方进行多次证书交换。所以称之为信任协商。图 1 是信任协商的一个例子。假设在线书店 B 对某高校学生提供七折销售，访问者 A 要求得到学生折扣。在线书店 B 事先没有访问者 A 的信息。在线书店 B 的安全策略是只给该高校学生优惠，因此在线书店 B 请求对方出具有某高校学生的学生号以及银行信用卡号的信任书。A 的安全策略是信用卡号只能给中国银行会员单位，因此在 A 向书店 B 提供自己是该校学生的信任书后，也要求对方显示具有该银行会员的的信任书。在 B 显示自己的信任书后，A 才向 B 出示具有信用卡号的信任书。

TrustBuilder[21]可以用来实现信任协商，它是用 Java 写的一个中间件信任代理，它能够管理密钥、信任书和访问策略，并能决定在协商过程中向对方显示哪个信任书和访问策略。

经过信任协商后双方建立了信任关系，主体的信任值是主体属性的函数。

$T_a = f(A)$

A 是主体的属性，T_a 是由主体属性而产生的信任值。

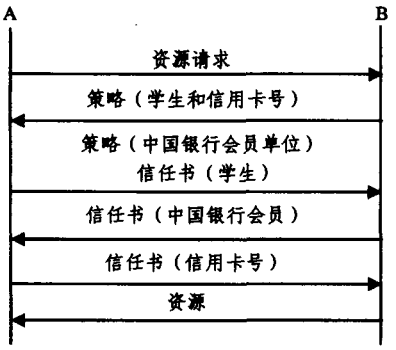

图 1 信任协商过程

在建立了最初的信任之后，主体的信任值将主要由上下文决定。准确安全地采集上下文信息是实现系统安全的基础。传感器可以用来捕获、处理和存储用户活动和交互环境的各种信息。但这要保证上下文信息的安全性，否则系统会作出错误的判断。Srinivasan 等[14]开发的上下文工具包可以用来提取环境状态信息。上下文工具包主要由三个部分组成：上下文窗口小部件(widget)表示通过传感器提取环境信息，它隐藏了对环境的感知和解释。它们是系统其他部件和服务自动传递信息的界面。收集器(aggregator)给应用相关的实体收集信息。解释器负责提取低级上下文信息给更高一级。该上下文工具包是将认证信息(如密钥和证书)分配给所有部件。用令牌来保证信息交换的完整性和隐私问题。所有的工具包部件实现数据加密，保护了上下文信息的机密性。

我们对该上下文工具包作稍微的修改就能适合我们的模型，用它根据资源的信任策略对上下文信息进行信任评估，

$T_c = h(C)$

其中 C 是上下文信息，一旦 C 变化将重新评估 T_c。

2.2 信任计算模型

定理 1 主体之间的信任关系是偏序关系。

证明：主体自己相信自己，信任关系是自反的。A 相信 B，但 B 不一定相信 A 或者两者之间的相互信任值不同，信任关系是反对称的。一般地讲，信任关系不具有传递性，但如果主体之间存在推荐关系，则信任关系是传递的。因此信任关系是偏序关系。

定理 2 如果$\langle T_a; \leqslant_1 \rangle$和$\langle T_c; \leqslant_2 \rangle$是一个偏序集，对于 $\forall (t_{a1}, t_{c1}), (t_{a2}, t_{c2}) \in T_a \times T_c$，定义：$(t_{a1}, t_{c1}) \leqslant_3 (t_{a2}, t_{c2})$ 当且仅当 $t_{a1} \leqslant_1 t_{a2}, t_{c1} \leqslant_2 t_{c2}$，则$\langle T_a \times T_c; \leqslant 3 \rangle$构成一个偏序集。

由 $\leqslant_1$ 和 $\leqslant_2$ 是偏序关系以及定义，很容易证明 $\leqslant_3$ 也是偏序关系。

因此，如果 $(t_{a1}, t_{c1}) \leqslant_3 (t_{a2}, t_{c2})$，则称信任值 (t_{a1}, t_{c1}) 低于信任值 (t_{a2}, t_{c2})。例如，*uncertainty* $\leqslant_1$ *medium*，*untrust* $\leqslant_2$ *uncertaity*，则 (uncertainty, untrust) $\leqslant_3$ (medium, uncertainty)，即信任值(uncertainty, untrust)低于信任值(medium, uncertainty)。

一个主体与其他主体之间存在直接的信任关系或者间接信任关系。显然该主体与其他主体之间的单向信任关系构成一个 Hasse 图。

如图 2 所示，对于 $p_1 \sim p_5$ 五个主体，p_1 与 p_2、p_3、p_4、p_5 存在信任关系。在图中节点表示主体，边表示主体之间的信任关系，主体之间的信任值可能是(*medium*, *low*)，也可能是(*uncertainty*, *medium*)等。

假设主体 A 的信任关系的 Hasse 图中存在 $P_1,\cdots,P_k$ 条路径到主体 B，第 i 条路径上存在推荐者集合为 $C(P_i)=\{R_{i1},R_{i2},\cdots,R_{in}\}$。

定义 1 $P_1,\cdots,P_k$ 条路径是不相关的，如果存在：

$\forall P_i,P_j,\forall C(P_i)\bigcap C(P_j)\equiv\Phi$，其中 $1\leqslant i,j\leqslant k$

定义 2 $P_1,\cdots,P_k$ 条路径是相关的，如果存在：

$\exists P_i,P_j\ \exists C(P_i)\bigcap C(P_j)\neq\Phi$，其中 $1\leqslant i,j\leqslant k$

在 Hasse 图中，每条推荐路径的信任值为：

$T_r=\min\{T_{A1},T_{12},T_{23},\cdots,T_{nB}\}$

其中 T_{A1} 表示 A 对第一个推荐者的信任值，T_{12} 表示第一个推荐者对下一个推荐者的信任值。

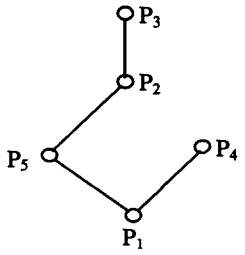

图 2　信任关系的 Hasse 图

其中 T_{A1} 表示 A 对第一个推荐者的信任值，T_{12} 表示第一个推荐者对下一个推荐者的信任值。

(1) 当 k 条路径是不相关时，综合信任值为：

$$T_f=\frac{1}{k}\sum_{i=1}^{k}T_i$$

如果考虑不同的推荐路径有不同的推荐效果，则可以引入权值 ω_i（其中 $\omega_i\geqslant 0$，且 $\sum_i^k\omega_i=1$），综合信任值为：

$$T_f=\sum_{i=1}^{k}\omega_i\times T_i$$

(2) 当 k 条路径是相关的，存在 m 条路径是不相关的，$m<k$，综合信任值为：

$$T_f=\frac{1}{m}\sum_{i=1}^{m}T_i$$

如果考虑不同的推荐路径有不同的推荐效果，引入权值 ω_i（其中 $\omega_i\geqslant 0$，且 $\sum_i^m\omega_i=1$），综合信任值为：

$$T_f=\sum_{i=1}^{m}\omega_i\times T_i$$

3　模型应用

我们利用 Lamsal[3] 的三个应用情节说明该信任模型是否能够满足他们的要求。三个情节分别是：

· 普适服务：教授回到自己的办公室，办公室的门检测到教授的移动设备和设备的使用者后自动打开。同样，办公室里的设备通过认证会主动提供一些服务，如打开桌上台灯，给教授订购咖啡等等。

· Ad Hoc 网络的建立：教授和一些行业代表用移动设备构建 Ad Hoc 网，传输一些机密文件。

· 受限的普适服务：学生使用教授的移动设备不能得到一些服务，如办公室的门不会为他打开。但他可以获得基本的服务，如使用移动设备订购免费咖啡。

上面三个情节是普适环境的主要应用场景，它体现了普适计算对信任建模的要求。我们的信任模型主要基于属性、上下文和推荐。教授能够使用移动设备获得普适服务，学生用同样的设备只能得到部分的普适服务，教授和学生具有不同的属性，因此具有不同的信任值，设备和系统根据信任值提供不同的服务。

教授和其他代表组织一个会议，交流一些敏感数据，这应该建立三级信任：网络级信任、设备级信任和应用级信任。属性和上下文可以分为相对应的三类属性，即与网络级相关的属性和上下文、与设备级相关的属性和上下文以及与应用级相关的属性和上下文。在建立连接前，他们进行信任协商，多次互相向对方呈现自己的信任书，根据各自的信任策略计算对方的信任值，逐步建立三级信任。信任值不是一成不变的，它随着上下文和时间而变化，如果信任值低于安全策略规定的信任值，那么该设备将不值得信任，它就不能连入网中。显然，基于属性、上下文和时间的信任模型达到了普适环境信任要求。

结束语　安全通信是建立在信任的基础上，目前的安全技术暗含了信任，实际上信任是基于身份的，这种基于身份的信任不适合普适环境变化的要求。在普适环境中，不同的应用，不同的上下文，信任的要求不同。在互相不认识的主体之间信任应该来自属性（如位置、设备类型等）和上下文（如计算机上下文，用户上下文和物理上下文等）信息，与身份联系很少。在这篇文章中我们提出了灵活的信任计算模型。通过分析可以看到该模型满足了普适计算信任建模要求。模型有较高的通用性，基于它能够给普适计算应用建立了一个信任安全授权框架。

参 考 文 献

1　Weiser M. The computer for the twenty-first century. Scientific American, 1991, 265(3): 94～104

2　徐光祐，史元春，谢伟凯. 普适计算. 计算机学报，2003，26(9)：1042～1050

3　Lmsal P. Requirements for modeling trust in ubiquitous computing and Ad Hoc networks. In HUT TML - Course T－110. 557 - Publication ISBN 951-22-6309-2 ISSN 1456-7628 TML-C8, Ad Hoc Mobile Wireless Networks - Research Seminar on Telecommunications Software, Autumn 2002. http://www.tml.hut.fi/Studies/T－110.557/2002/papers/

4　McKnight D H, Chervany N L. The meanings of trust. In Working Paper 96-04, Management Information Systems Research Center. Carlson School of Management, University of Minnesota, 1996. Last revised: April 1, 2000

5　Gray E, Seigneur J M, Chen Y, Jensen C. Trust propagation in small worlds. In: Nixon P, Terzis S, eds. Proc. of the First Intl. Conf. on Trust Management (iTrust2003), volume 2692 of Lecture Notes in Computer Science, Heraklion, Crete, Greece, May 2003. 239～254

6　Gray E, et al. Towards a framework for assessing trust-based admission control in collaborative ad hoc applications: [Technical Report 66]. Department of Computer Science, Trinity College Dublin, 2002

7　Grandison T, Sloman M. A survey of trust in Internet applications. IEEE Communications Surveys and Tutorials, 2000, 4(4): 2～16

8　Carbone M, Nielsen M. A formal model for trust in dynamic networks. In: Proc. of IEEE International Conference on Software Engineering and Formal Methods (SEFM '03), Brisbane, Australia, Sept. 2003

9　Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Proc. of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 1996. 164～173

10　Blaze M, Feigenbaum J, Ioannidis J, Keromytis A. The KeyNote trust-management system, version 2. IETF, RFC 2704, Sept. 1999

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

12 Shankar N, Arbaugh W A. On trust for ubiquitous computing. In Workshop on Security in Ubiquitous Computing. UBICOMP 2002, Goteborg, Sweden, Sept. 2002
13 English C, Nixon P, Terzis S, McGettrick A, Lowe H. Dynamic trust models for ubiquitous computing environments. In: Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Goteborg, Sweden, Sept. 2002
14 Shand B, Dimmock N, Bacon J. Trust for ubiquitous, transparent collaboration. In: Proc. of the First Annual IEEE Conf. on Pervasive Computing and Communications, Dallas-Ft. Worth, TX, USA, March 2003. 153～160
15 Liu Z Y, Joy A W, Thompson R A. Thompson R A. A dynamic trust model for mobile Ad Hoc networks. In: The 10th IEEE Intl. Workshop on Future Trends of Distributed Computing Systems (FTDCS'04), Suzhou, China, May 2004. 80～85
16 Bussard L, Roudier Y, Molva R. Untraceable Secret Credentials: Trust Establishment with Privacy. In: The Second IEEE Annual Conf. on Pervasive Computing and Communications Workshops, Orlando, Florida, March 2004. 122～126
17 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究. 软件学报,2003,14(8):1401～1408
18 Winsborough W, Li N. Towards practical automated trust negotiation. In: Proc. of the Third Intl. Workshop on Policies for Distributed Systems and Networks (POLICY 2002), Monterey, CA, IEEE Computer Society Press, June 2002. 92～103
19 Yu T, Winslett M, Seamons K. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. ACM Transactions on Information and System Security, 2003, 6(1): 1～42
20 Winsborough W, Seamons K, Jones V. Automated trust negotiation. In: DARPA Information Survivability Conf. and Exposition Hilton Head, SC, IEEE Press, 2000, 1: 88～102
21 Winslett M, Yu T, Seamons K, Hess A, Jacobson J, Jarvis R, Smith B, Yu L. Trust negotiation on the Web. IEEE Internet Computing, 2002, 6(6): 30～37
22 Winsborough W H, Li N. Safety in Automated Trust Negotiation. In: the Proc. of IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Berkeley, California, May 2004. 147～160

(上接第 19 页)

式的结构图,限于篇幅,此处只显示类的数据域。

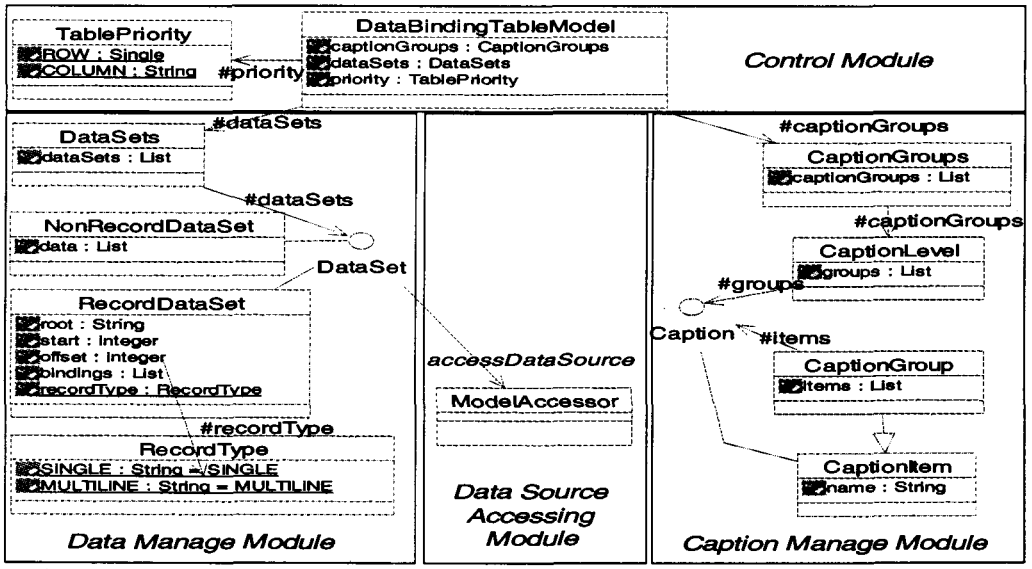

图 6 面向数据绑定的表格模型

实现模型分为以下功能模块:控制模块(Control Module)、标题管理模块(Caption Manage Module)、数据管理模块(Data Manage Module)和数据源访问模块(Data Source Accessing Module),每个模块都提供了相应的访问接口,分别实现了对标题和数据的管理以及和异构数据源的集成。

结论和今后工作 针对当今各行业信息系统在处理异构的海量信息时对表格的多样化需求,本文详细分析了实际应用中对表格的需求,研究了包括 Swing 和 SWT 等支持表格构件的软件开发工具包中表格模型的定义,提出了面向数据绑定的表格模型,并给出了模型的形式化定义和实现结构。本文提出的表格模型不仅满足实际应用中对表格的多样化需求,还通过引入 Xpath 标准支持和异构数据源的集成。这一表格模型已经被成功应用于清华大学-日本 IT Frontier 株式会社知识工程联合实验室研究并开发的基于 XML 的图形化用户界面描述语言 GUI XML 及其实现系统中,并取得了满意的效果。在今后的研究工作中,我们将进一步完善表格模型的定义,以求能方便地支持更多的实际应用中的表格类型,同时进一步改进表格模型的实现,提高其性能。

参 考 文 献

1 清华大学—IT Frontier 株式会社知识工程联合实验室. GUI XML for JFC Swing 规范, 2004. 8
2 Clark J, DeRose S. XML Path Language (XPath) Version 1. 0. http://www. w3. org/TR/xpath/, 16 November 1999
3 Dubinko M, Klotz L L, et al. XForms Specification 1. 0, http://www. w3. org/TR/xforms/, Oct. 2003
4 Beatty J, Brodsky S, Ellersick R, Nally M, Patel R. Service Data Objects, Version 1. 0. Nov. 2003
5 徐鹏. 元数据驱动的半结构化信息智能处理模型的研究:[清华大学工学博士学位论文]. 2003
6 Lim S-J, Ng Y-K. An automated approach for retrieving hierarchical data from HTML tables. In: Proc. of the eighth intl. conf. on Information and knowledge management, 1999. 466～474
7 李建中,高宏. 一种数据仓库的多维数据模型. 软件学报, 2000, 11(7): 908～917
8 李涛涛,刘连忠,陈梦东. 基于 XML 技术实现表格的灵活构建. 计算机应用研究, 2004