

# 移动电子商务及其关键技术

姜 志<sup>1</sup> 聂志锋<sup>2</sup>

(1. 武汉大学计算机学院, 湖北 武汉 430070; 2. 湖北省移动通信公司, 湖北 武汉 430030)

**摘 要:**介绍了移动电子商务的基本框架,并针对其中的几个关键技术进行了论述,介绍了移动电子商务的底层——无线网络,对移动电子商务中的两个关键标准和规范——WAP 2.0标准和MeT规范进行了说明,分析了移动中间件在移动电子商务中的重要作用,并就其安全性进行了阐明,最后讨论了移动电子商务所面临的问题和其发展前景。

**关键词:**移动电子商务;WAP;MeT;移动中间件;WPKI

**中图分类号:**TN915 **文献标识码:**A **文章编号:**1007-1148(2002)03-0001-04

## 1 引言

随着无线通信技术的发展,移动电子商务已经成为电子商务研究和发展的热点。移动电子商务是将现代信息科学技术和传统商务活动相结合,随时随地为用户提供各种个性化的、定制的在线动态商务服务。现在人们已经意识到它的强大发展潜力,主要的电信设备制造商、电信运营商、软件和服务开发商都在逐步加大对它的投资和研究。各种新的技术和研究成果不断涌现并逐渐在实际中得到应用,这些都极大的促进移动电子商务的发展。

## 2 移动电子商务的基本框架

移动电子商务基本框架分为3个功能层,无线网络层,移动中间件层和商务应用层。

(1) 无线网络层(Wireless Network)是移动电子商务的最底层,它是联系移动用户和应用服务商之间的桥梁。在移动电子商务中,服务质量主要依靠无线网络的资源和容量。

(2) 移动中间件层(Mobile Middleware)能够隐藏底层网络细节,为应用程序的开发提供一个容易的易于使用的接口。中间件的使用对开发新的移动商务应用有着及其重要的作用。

(3) 商务应用层(Commerce Application)用来实现移动电子商务的应用,许多新的应用如移动盘存管理、产品定位、超前服务管理等正在成为现实,部分现有的电子商务应用经过改动也可应用于移动环境。

这种框架的设定极大的简化移动电子商务的设计与开发,不同团体(厂商、提供商和开发者)可以对自己的功能进行定位。移动电子商务的开发不再需要构建移动商务系统的每一个部分,而可将系统建立在他人提供的功能之上。

## 3 移动电子商务的关键技术

### 3.1 无线网络技术

随着计算机技术的发展,各种新的网络通信技术不断涌现。这些新技术的使用使网络的传输速率得到了极大提高。促进了移动电子商务的普及和服务质量的提高,并使新的业务的开展成为可能。

无线广域网中的GPRS是基于GSM制式下的无线广域网技术,其传输速率可达115 Kb/s,它允许用户时时在线,并根据用户流量进行计费,目前通过升级GSM网络实现。它采用TDMA方式传输语音,采用分组的方式传输数据。第3代移动通信系统(3G),国际电联也称IMT-2000,欧洲的电信称为UMTS,包括WCDMA、CDMA 2000、TD-SCDMA 3种标准,其最高传输速率可达2 Mb/s。它能够将语音通信和多媒体通信相结合,其可能的增值服务将包括图像、音乐、网页浏览、视频会议以及其他一些信息服务。

### 3.2 无线应用协议(WAP: Wireless Application Protocol)

它是在数字移动电话、个人数字助理(PDA)、移动计算机等无线设备和因特网之间进行通讯的开放国际标准。它的目标是通过WAP这种技术,就可以将因特网的大量信息及各种的业务引入到移动电话、PAD等无线设备之中。WAP论坛(WAPForum)于

收稿日期:2002-02-12

1998 年发布了它的第一个标准 WAP 1.0,立刻得到大多数数据通信商的支持,随着无线通信技术的发展,WAPForum 提出的新一代国际标准 WAP 2.0。

### 3.2.1 WAP 2.0 的特点

(1)提供了对标准因特网通信协议(如:IP、TCP、HTTP)的支持,增加了因特网与无线通信环境的互操作性。

(2)保持与 WAP 1.x 的兼容性,加强了对 GPRS、3G 技术的支持。

(3)为数字移动电话、PDA 和其他无线设备提供了一个丰富的开发环境。

(4)充分考虑到无线设备的独有特点(如:小屏幕,小电池),加强了对这些特点的用户体验。

(5)最小化对设备电力的使用,使其以最小的资源获得最大的性能。

### 3.2.2 WAP 2.0 网络模型

WAP 2.0 网络模型与 WAP 1.x 类似主要由 3 部分组成,即 WAP 微浏览器、代理网关和应用服务器。其中在 WAP 1.x 中代理网关起着协议的翻译作用,是联系无线网与因特网的桥梁,但在 WAP 2.0 中用户和服务器之间可直接通过 HTTP/1.1 进行通信,代理网关的作用主要是对移动服务进行增强,如:定位、内容适配、PUSH 功能的实现等;应用服务器存储着大量的信息,以提供移动用户来访问、查询、浏览等。当用户从 WAP 设备中键入他要访问的应用服务器的 URL 后,信号经过无线网络,以 WAP 协议方式发送请求至代理网关,再以 HTTP 协议方式与应用服务器交互,最后代理网关将返回的内容处理后返回 WAP 用户。

### 3.2.3 WAP 2.0 的体系结构

WAP 2.0 为增强对 2.5 G 和 3 G 的支持,提出了一种新的协议层次结构。

无线应用环境(WAE: Wireless Application Environment)是基于移动技术和 Web 结合基础之上的应用环境,目的是在 WAP/Web 应用程序和包含一个微浏览器的无线设备之间提供交互。WAP 2.0 提供一种应用于微浏览器的标记语言 XHTMLMP(XHTML Mobile Profile Markup Language),它是对 W3C 定义的 XHTML 的扩展,使其能更好的满足 WAP 的要求,同时它还通过对 CSS(Cascade Style Sheet)的支持,来增强对内容的表达。为了保持与 WAP 1.x 中的 WML1(Wireless Markup Language 1)的兼容性,WAP 2.0 提出了 WML 2,它是为了保持对 WML 1 的向下兼容而对 XHTMLMP 的扩展,可以使用 XSLT(eXtensible Stylesheet Language Transformation)将 WML 1 代码转换为 WML 2 代码。

无线 HTTP(WP - HTTP: Wireless profiled HTTP)它是为了增强在无线环境中的应用并保持于 HTTP/1.1 互操作性而定义的 HTTP 的一个子集。

无线传输层安全(WP - TLS: Wireless Profiled Transport Layer Security)它是 TLS 的一个子集,允许对安全事务的互操作性。它包括密码组、认证格式、签名算法和会话恢复的使用等。它还为 TLS 定义了对传输层端对端(End - To - End)安全性支持的方法。

无线 TCP(WP - TCP: Wireless Profiled TCP)提供面向连接的服务,它为在无线环境应用并保持于 TCP 的互操作性而进行了优化。

从 WAP Device 到 Web Server 使用这些协议的一种方法中,TLS 为移动终端和服务端之间的 HTTP 事务提供了端对端的安全,TCP \* 则使用了 WP - TCP 协议进行传输。

### 3.3 移动电子交易(MET: Moblie Electronic Transactions)

MET 是由 Ericsson, Motorola、Nokia 发起制定的一个安全移动交易框架,其目的是使消费者无论在什么地方都能无缝的对商品和服务进行访问,保证移动电子交易的安全性。

随着移动通信业的发展,移动电话不再仅仅是一个无线电话,而是一种个人可信任设备(PTD: Personal Trusted Device),它能够处理广泛的新的服务和应用如金融交易、支付交易、售票业务等。MET 就是要建立一种以个人移动设备为核心的,能满足 PTD 的特殊需求的,适合移动商务市场的通用开放核心规范。它尽可能的符合现在的工业标准如 WAP 规范中的 WTLS, WIM, WPKI,以及 Bluetooth 无线技术等。

这是一个通用的参考模型,在许多情况下,认证服务发行者(Service Certification Issuer)、捕获者(Acquirer)和内容服务者(Content Server)可以合并为两个甚至是一个实体。MET 的最大特点就是相同的模型可以在远程(Remote)、局部(Local)和个人(Personal)环境中重用。

(1) PTD: 用户的移动电话就是一个 PTD,它主要用来认证用户的 ID 和对事务的授权(使用数字签名)。PTD 被包含在移动电话的安全元件(Security Element)内,如 SIM/WIN 混合卡、单独的 WIM 智能卡、其他的 WIM 功能的可移除设备、内建于移动电话中的硬件设备或内建于移动电话中的硬件设备。

(2) Content Server: 内容提供者通过内容服务器向用户提供内容。在远程和局部环境中用户需要通过代理(如: WAP Gateway)才能访问内容服务者。内容服务器上应用程序的执行,需要 PTD 通过服务执行接口(Service Execution Interface)执行指定的用户

认证命令。

(3) Acquirer:捕获者在内容服务器和服务认证发行者之间建立联系,在交易环境中,它为多个内容服务器与服务认证发行者之间提供商务规则和建立它们之间的联系。它不是必须的。

(4) Service Certificate Issuer:服务认证发行者为一个特定的帐户提供服务认证。被发行的服务认证是服务认证发行者用来标识用户的一种方法。

(5) Service Execution Interface:服务执行接口被用来在用户和内容服务器之间执行一个安全的事务。主要有以下几个功能:在两者之间建立一个安全的会话;内容服务器进行用户身份认证;确认用户的授权。

(6) Service Registration Interface:服务注册接口被用来将服务认证加载到 PTD 上,它可以使服务提供者将用户身份与用户的服务帐号联系起来。

(7) User Interface:用户接口被用作用户与 MET 事务之间的交互,它包括在 PTD 表达用户信息,提醒用户输入,接受用户输入并将其以合适的方式传递。

(8) Security Element Interface:安全元素接口规定了如何与 WAP WIM 规范中定义的用户校验、加密处理等方法进行交互。

MET 可应用于远程、局部和个人 3 种环境中。

在远程环境中 PTD 和 Content Server 通过 PLMN (Public Land Mobile Network) 如 GSM 网络,建立连接。WAP 网关被用来建立 PLMN 于 Internet 之间的连接。

在局部环境中 PTD 通过短程无线技术如 Bluetooth 执行 MET 交易。PTD 使用 WAP Over Bluetooth 协议于局域网中的 Bluetooth 访问节点建立连接。

在个人环境中 PTD 仅用来进行认证和授权,它通过 Bluetooth、IrDA、USB 等技术和 PC 建立连接,与 Internet 的通信工作交给 PC 来完成。

### 3.4 移动中间件(Mobile Middleware)

随着无线通信技术的发展,移动应用的开发必须面对的问题,主要有:

(1)移动设备的多样性,从 GSM 电话、具有小屏幕的 PDA 到具有多媒体功能的便携式电脑等;

(2)移动操作系统的多样性,如 EPOC, WindowsCE, PalmOS, EmbeddedLinux, JavaPhone 等;

(3)各种不兼容的网络标准,如 GSM、GSCSD (High Speed Circuit Switched Data)、GPRS、EDGE (Enhanced Data Rates for Global Evolution)、CDMA、WCDMA、TD-SCDMA 等;

(4)无线网络带宽的变化和网络连接的不连贯性。

移动中间件的使用,很好的解决了这些问题。

它将各种无线网络和电子商务服务联系在一起,屏蔽了底层网络的复杂性,为移动应用的开发提供了一个良好的支撑环境,使应用程序获得良好的响应时间和性能。移动中间件主要的功能表现在:

安全(Security)管理:安全性是所有事务中间件所必须提供的内在特性,它是实现移动电子商务的一个重要方面。当前有很多供应商(如 Certicom, Diversinet, and Verisign)为移动市场提供加密和公开密钥的技术和服务。

位置(Location)管理:它通过使用 GPS、GSM 位置服务器等设备使服务商获得用户的位置信息,从而可以为用户提供更合适的服务。如 Geo Java 就是通过使用 Oracle 空间数据库,获得用户位置信息并向用户提供服务。

事务(Transaction)和会话(Session)管理:事务管理是为了保证数据的完整性;会话管理在网络连接不可靠条件下,为应用屏蔽底层连接断开,并提供在单个或多个数据访问网上数据流复用的方法。724 Solutions、W-Technologies、Aether Systems 等公司已经在此方面取得了很大成果。

内容适配(Content Adaptation)管理:它负责使传输内容适宜于访问设备的带宽和终端特性,并可为用户提供个性化的服务。

数据通信(Data Communication)管理:它负责为用户提供 SMS(Short Message Service)和 E-Mail 的数据服务。

当前为了占领日益扩大的移动电子商务市场,各大软件公司纷纷推出自己的移动中间件平台。这些平台主要可以分为:移动门户平台(Mobile Portal Platforms)、移动商务平台(Mobile Commerce Platforms)、移动支付平台(Mobile Payment Platforms)、移动银行平台(Mobile Banking Platforms)。

这些中间件平台的使用,简化移动电子商务的组建过程,使应用服务商可以快速构造适合自己的移动电子商务平台,有力的推动了移动电子商务的发展。

### 3.5 移动电子商务的安全

安全性是移动电子商务能否取得成功的关键。移动电子商务的安全性的功能主要包括以下几个方面:

私有性(Private)确保通信是私有的,不能被任何可能侦听到它的中间者理解。

确认性(Authentication)能够对进行通信的各个部分进行确认。

完整性(Integrity)确保通信的是未改变的和无误的。

不可否认性(Non-Repudiation)确保通信的各个部分不能否认通信的发生。

通过认证技术和合理的组织策略使移动用户和他的通信伙伴之间建立一种信任关系在移动电子商务中是一个至关重要的问题。这需要建立一种被全球广泛接受的安全体系结构。在 WAP 2.0 中规定了一套在无线环境中应用的安全策略。它主要包括以下几个方面:

WAP 标记语言脚本加密库(WML Script Crypto Library)它允许 WAP 应用程序对库中的基本加密函数进行调用,通过它可以方便的实现信息的加密。这个库提供的主要功能有:

- (1) 密钥对的生成;
- (2) 数字签名的生成和校验;
- (3) 数据的加密和解密。

无线应用协议识别模块(WIM; WAP Identity Module)是一个独立的安全模块,主要用来存储和处理用户身份认证与授权所需的信息,一般无线终端内的智能卡(如 SIM 卡)上实现。它同时作用于安全层和应用层,主要用于增强安全层和应用层某些功能的安全性。通过使用 WIM, WAP 可以提供对电子商务所必须的身份认证和不可否认的支持,同时它还增强了在 WTLS 中实现的消息的私有性和完整性。

WTLS 是与因特网上的 SSL 相类似的一种规范,主要用来保证移动设备和 WAP 网关之间消息的私有性和完整性。应当注意的是由于移动设备计算能力的限制,WTLS 使用了较弱强度的加密算法,如椭圆曲线加密法(ECC; Elliptic - Curve Cryptography),所以在与 Internet 通信之前必须将 WTLS 信息转换为使用强加密算法的因特网上使用的 SSL 信息。

公开密钥体制(PKI; Public Key Infrastructure)是一项重要的网络安全技术,它采用证书管理公钥,通过第 3 方的可信任机构——认证中心(CA; Certificate Authority),把用户的公钥和用户的其他标识信息(如名称、E-Mail、身份证号等)捆绑在一起,在 Internet 网上验证用户的身份。无线公开密钥体制(WPKI; Wireless PKI)是将公开密钥体制运用于无线应用协议网络从而保证无线应用协议应用安全的重要手段。

(1) 用户应用程序向 PKI 门户(PKI Portal,它与 WAP 网关类似,是一个网络服务器,负责为 WAP 客户向 RA 和 CA 传输请求,一般可将 RA 的功能内建在 PKI Portal 之中)发出在注册中心(RA; Registration Authority)进行注册认证的请求。

(2) RA 通过认证请求并将其传送给 CA。

(3) CA 生成用户认证并经过认证 URL 传给用户。

(4) CA 向数据库提交认证。

(5) 内容服务商接受到认证消息并调出相关信息。

(6) 移动用户与 WAP 网关使用 WTLS 协议根据数字签名进行通信。

(7) WAP 网关与内容服务商利用 SSL 进行通信。

## 4 机遇与挑战

根据 GartnerGroup 的研究,到 2004 年全球 B2C 市场的 40% 将是由移动电话来完成。一份基于无线数据和计算服务(Wireless Data and Computing Service)的报告指出,2004 年全球的移动市场份额将达到 2 000 亿美元。

虽然移动电子商务有着巨大发展潜力,但我们必须认识到,要使它成为一种理想的电子商务平台,必须解决好网络处理和存储、应用开发、兼容性、互操作性、安全性及适应用户需要的功能特性等一系列方面的问题。同时也应该意识到移动电子商务平台的建立并不仅仅是一个技术问题,它还包括相关政策法规的制定,人们意识的提高,支付手段的配套等。这就需要计算机和通信专家、经济学家、社会学家以及商务管理者一起来为它制定一个开放的、基于标准的结构平台,来促进移动电子商务的发展。

### 参考文献:

- [1] 董燕举,富钢. 移动电子商务的发展与支持技术研究[J]. 沈阳航空工业学院学报,18(1).
- [2] 耿志刚,尚海忠等. 移动中间件:移动无线 Internet 的将来[J]. 计算机工程,27(11).
- [3] Upkar Varshney, Ronald J Vetter, Ravi Kalakota. Mobile Commerce: A New Frontier[M], 2000.
- [4] Amit Vyas, Peter O'Grady. A Review of Mobile Commerce Technologies[M]. Internet Lab Technical Report TR, 2001.
- [5] UMTS Report - An Investment Perspective, Durlacher Research Ltd.
- [6] WAP Architecture, WAP - 210 - WAPArch - 20010712.
- [7] WKPI, WAP - 217 - WKPI - 20010424.
- [8] MeT Core Specification Version 1.1.

作者简介:姜志(1977-),男,湖北黄陂人,本科,武汉大学计算机系在读硕士。

(下转第 42 页)

(9) 监控网络的设计,完全依据邮电部电信总局的监控系统技术规范要求。全面支持中国移动通信集团公司规范要求的 FSU、LSC、CSC、LMNMC 网络组织架构。

## 5 环境监控网络的发展方向

随着环境监控网络新技术以及软件工程理论的进一步发展,环境监控网络的硬件和软件也将不断的发展。

### 5.1 硬件的发展方向

环境监控网络包含基础节点、监控传输网和监控中心 3 大部分。

基站节点部分监控硬件随着工业技术的发展,将能提供更多的模拟量和智能设备的接口,诸如机房湿房、窗户开关状态,射频泄漏值等环境参数将纳入监控网络中。

监控传输网随着如无线局域网、民用频段无线通信等新的通信技术的引入,将逐步采用新的通信模式,逐步摆脱主网传输的束缚,自成传输体系,从而更好的达到监控的目的,更好的为主网服务。

监控中心随着局域网技术和计算机技术的发展,配置和扩容更灵活,更好的满足监控节点不断增多的需要,更好的发挥监控网管作用。

### 5.2 软件的发展方向

随着软件工程理论的进一步发展,环境监控软件将逐步沿着模块化、Web 化的方向更加成熟,数据库的同步技术也将更加成熟。

#### (1) 模块化

在软件模块划分上,将采用前置处理软件、中心通讯服务器和显示控制软件的划分方式。

前置处理软件主要功能:负责与下位机的通讯,报文的分析,向中心通讯服务器传送告警等信息,通信信道的管理、备份。

中心通讯服务器的主要功能:联结显示控制程序、前置处理软件和上、下级的中心通讯服务器;负责数据的分发,命令的转发;完成对数据库的读写,保证数据库的完整和一致。

显示控制程序的主要功能:是面向用户的一个图形界面 GUI,将所监控的数据以各种方式显示给用户,接受用户的命令,并向中心通讯服务器发送,告警的处理显示。

在将来的程序设计中,将把前置处理软件和中心通讯服务器开发成一个 NT 的服务(Service),这样可以提高前置处理软件和中心通讯服务器的工作效率。显示控制程序将采用一些可视化编程方面较好的编程语言,方便以后在界面上的修改。

#### (2) Web 化

通过提供 Web 服务,用户可以在任何时间、任何地点通过 Internet 浏览器看到所管辖范围内监控设备的运行情况。可在浏览器上实现监控的基本功能,包括遥信、遥测、遥控和遥调功能、告警功能等。

#### (3) 数据库的同步

将来可能会采用一些大型数据库提供的数据库同步功能来取代现有的通过系统自身软件传送消息进行数据库同步的方法。

#### 参考文献:

- [1] 中国移动通信动力及环境集中监控系统技术规范[S]. 2000.
- [2] 湖北省移动通信动力及环境集中监控系统技术规范书[S]. 2000.
- [3] 赵玉峰. 动力设备及环境集中监控系统[M]. 北京:北京邮电大学出版社.

作者简介:王 琦(1975-),男,湖北武汉人,2000 级华中科技大学工程硕士在读。

(上接第 4 页)

# Mobile Electronic Commerce and its Key Technologies

JIANG Zhi<sup>1</sup> NIE Zhi-feng<sup>2</sup>

(1. Wuhan University, Wuhan 430070, China; 2. Hubei Mobile Communication Co., Wuhan 430030, China)

**Abstract:** We give a introduction of the framework of Mobile Electronic Commerce, and expatiated on some key technologies in this field. First, we introduce the infrastructure of Mobile Electronic Commerce - Wireless Network, and explain two key technologies in Mobile Electronic Commerce - WAP 2.0 and MET, then analyze the importance of mobile middleware in Mobile Electronic Commerce, and expound its security, finally we discuss the problem and prospect of Mobile Electronic Commerce.

**Keywords:** Mobile Electronic Commerce; WAP; MET; Mobile Middleware; WPKI