分类号_____ 密　级 公开

UDC _____ 学校代码 10497

武漢理工大學

学 位 论 文

题　目 移动电子商务安全研究

英　文

题　目 Research On Mobile Electronic Commerce Security

研究生姓名 王大飞

指导教师 姓名 赵宏中 职称 教授 学位 博士

单位名称 经济学院 邮编 430070

副指导教师 姓名 _____ 职称 _____ 学位 _____

单位名称 _____ 邮编 _____

申请学位级别 硕士 学科专业名称 计算机科学与技术

论文提交日期 2010 年 4 月 论文答辩日期 2010 年 5 月

学位授予单位 武汉理工大学 学位授予日期 _____

答辩委员会主席 钟珞 评阅人 佘名高

周彩兰

2010 年 05 月

独 创 性 声 明

本人声明，所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得武汉理工大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

签 名：王大飞 日 期：2011.5

学位论文使用授权书

本人完全了解武汉理工大学有关保留、使用学位论文的规定，即学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权武汉理工大学可以将本学位论文的全部内容编入有关数据库进行检索，可以采用影印、缩印或其他复制手段保存或汇编本学位论文。同时授权经武汉理工大学认可的国家有关机构或论文数据库使用或收录本学位论文，并向社会公众提供信息服务。

（保密的论文在解密后应遵守此规定）

研究生（签名）：王大飞 导师（签名）： 日期：2011.5.15

摘要

随着移动通信技术的发展以及移动终端的普及，一种崭新的电子商务模式应运而生---移动电子商务。移动电子商务随着电子商务发展起来，是电子商务发展的新形式，并日益成为电子商务发展研究的热点，已经成为国民经济和社会信息化的重要组成部分。移动电子商务发展迅速，但安全问题是制约其发展的重要因素，关系到商务系统能否正常运行。因此，如何建立安全、便捷的商务应用环境，保证整个商务活动中信息的安全性，对于促进移动电子商务健康发展具有重要理论价值和实际意义。

本文首先介绍了课题的研究背景，总结了国内外移动电子商务安全研究现状，说明了本论文的研究内容和方法。接着对移动电子商务安全进行概况，分析了移动电子商务安全的特点，对移动电子商务实现技术、所存有的安全威胁和安全需求等方面进行了阐述，从技术方面分析实现商务安全的加密、数字签名和身份认证等技术机制，接着对移动电子商务的三种支付模型进行了分析和介绍。重点分析了实现移动电子商务安全的两种解决方案：基于 SMS 的移动商务解决方案和基于 WAP 的商务解决方案，针对不同方案分别分析存在的安全风险，提出安全解决方案，并就方案实现特点进行分析；重点就 WAP 承载方案进行分析，从信息加密和数字签名着手实现端到端传输安全；最后从安全管理角度阐述移动电子商务管理制度和法制建设，指出仅依靠技术手段不能完全保证安全性能，针对我国国情提出有关移动电子商务安全立法的建议。在总结和展望中，对于移动电子商务业务的安全现状以及本论文分析提出的安全解决方案进行了总结，对未来移动商务的发展和研究趋势进行了展望。

关键词：移动电子商务　移动电子商务安全　SMS　WAP

Abstract

With the development of mobile communication technology and the popularization of mobile terminals, mobile E-commerce model come into being. Along with E-commerce development, this new model is increasingly becoming a hot research, and has become an important part of national economy and information society. Mobile e-commerce develops fast, but its security is a key factor that restricts its development and normal operation of business systems. Therefore, studying how to create the safe--convenient environment for business applications and ensure the security of information in business activities, has important referring value and practical significance to promoting the healthy development of mobile E-commerce.

This article describes the research background, summarizes the status of domestic and international mobile E-commerce security research and paper's contents. Then, the paper outlines mobile commerce security, analyzes the characteristics of mobile E-commerce security, overviews its implementation technology,its security threats and security needs, etc. From technical perspective, it describes E-commerce security encryption, digital signature technologies and authentication mechanism, And then, three mobile e-commerce payment models are introduced and analyzed. There are two solutions in solving mobile-Ecommerce security: business solutions based on SMS and WAP-based business solutions. The paper analyses the two different options ,describes their security risks, security solutions proposed, and analyzes the characteristics of program implementation; it focuses on WAP –based solution, proposes a method using encryption and digital signature to realize end to end transport security; Finally, from the perspective of safety management systems and mobile e-commerce law construction, the paper points out only rely on technical means can not guarantee security, so it comes up with mobile e-commerce security legislative proposals based on our national conditions. In the summary and outlook for the mobile E-commerce business, this paper analyzes the security status of security solutions proposed, and summarizes the security solution, in the last, discusses the future development of mobile commerce and research trends.

Keywords: Mobile Commerce Mobile E-commerce Security SMS WAP

目录

第1章 绪论

1.1 选题背景

电子商务[1](Electronic Commerce)是上世纪九十年代发展起来的企业经营方式，最初是在美国等发达国家，作为一种最新的企业经用方式，利用现代网络信息技术，快速有效开展各种商务活动。包括有两方面的内容：通过电子方式和在此基础上进行的商务商贸活动。电子商务作为在全球范围内开展的商务活动，以信息技术服务为支撑，并且随着现代信息技术的发展，内容和概念也在不断的发展变化，电子商务的本质是知识经济。

随着移动通信技术的发展以及移动终端的普及，一种崭新的电子商务模式也应运而生-----移动电子商务，也日益成为电子商务发展的热点。移动电子商务是指人们通过移动电话、掌上电脑和移动手持电脑等移动通信终端设备通过无线技术接入互联网而进行的电子商务交易活动。移动电子商务通过移动终端接入互联网，省去了传统意义上的网络接入，而移动终端方便灵活，用户可以随时随地安排所需商务活动。移动设备制造商、运营商、业务应用提供商共同参与消费者商务行为，而进行商务活动则必然会给这些相关企业带来利润，作为交易行为的双方，消费者和商家需求都得到满足，因而移动电子商务有着广阔的发展前景，也是未来电子商务发展的方向趋势。

移动电子商务因其方便、灵活的特点，不受时间和地点的限制，打破了原有电子商务技术的局限，通过互联网开展网上交易活动，商家也以此作为新型的销售与促销渠道，推广各种业务。用户根据个人需求和喜好，自由选择终端设备以及服务供应商和信息服务，随时随地获取所需服务和娱乐项目。目前移动商务可以提供类似基于位置服务(LBS)、银行交易、网上购物、网上订票和无线远程医疗等应用服务[2]。

无线通信过程中，所有通信信息都是通过无线网络传递，这些信息内容包括用户身份信息，交易密码等重要安全数据信息；无线信道和有线通信相比，它是一个开放的通信通道，任何具有适当通信设备的人都可以通过技术手段，窃听到无线网络通道上传递的数据信息。无线通道信息传递安全性此时就显得

极其重要。

信息交换过程中，移动网关和应用服务器之间通过有线网络传递信息，因此存有有线网和无线网同时被窃听的双重风险。安全性事移动商务中十分重要的核心问题，需要有安全可靠的通信网络和安全解决方案来保障。因此如何保障通信过程中的信息安全性、数据完整性和可靠性，有效防御外界攻击和截取，就成为发展移动商务需要解决的迫切问题。

由于移动商务本身的特点，其商务应用环境是迅速变化的，用户需求也是多种多样，因此移动商务系统需要提供一个安全环境。随着新技术的不断发展以及新技术标准的采用，在保证商务系统正常运行的前提下，还得考虑商务系统的可扩展性和兼容能力，保证新技术标准可以对原系统兼容，保证系统能够正常运营。

移动电子商务对于信息交换的安全性要求包括有：数据信息的保密性，信息的正确性，数据可靠性，能检测重传攻击，较强的容错能力，以及对于用户身份的认证等。保密性主要体现在交易过程中需要的用户身份信息、密码、货品价格数量和银行等信息，这些信息应是秘密的，保密性就是保证这些信息的有效性，保证信息不被非法用户窃取和使用。信息正确性是指接收方所接收到的内容是发送方的原始数据，这些信息没有在网络传输中丢失或是出错，也没有被外界篡改。交易数据的可靠性主要体现在交易双方对于交易过程中所涉及的内容进行有效确认，保障当事人的切身利益，防止交易双方对自己行为的抵赖，防止欺诈和造假。

商务系统应可以检测出重传攻击，保证信息接收方可以识别出信息的传送状态，确认信息的重传原因；商务系统应具有较强的容错能力，数据信息在网络中传输难免会出现问题，当出现问题故障时，系统的安全机制应该具有一些处理机制，保障系统的可靠性，进而可以保障通信双方交易的正常进行。除此之外，还应包括系统的可操作性和安全合理的加密保障和简装的数据存储机制。

移动电子商务健康发展需要有较高的安全技术来保障。现实中经常出现一种现象，就是在商务交易过程中，商家很难赢得客户的信任，任何一个环节上的漏洞就可以导致交易失败，所以安全问题是制约移动商务发展的一个瓶颈。由于移动电子商务是在电子商务基础上发展而来，所以移动商务的安全也要考虑到电子商务本身。移动电子商务是传统电子商务与信息网络技术的结合，其安全威胁也是在电子信息技术和网络数字技术发展的背景下产生，传统意义上的安全方案不能够满足移动商务安全需要。另外，商务交易活动是国民经济的

重要组成部分，如何保障交易的安全性也很大程度上影响到国家经济安全，随着更多通信技术手段的应用，电子商务的安全问题更是得到广泛关注。

1.2 国内外移动电子商务的研究现状

1.2.1 国外研究现状

电子商务最初是在美国兴起，国外研究移动商务安全方面主要是依据移动数据的加密技术理论。“信息安全”的概念最初是由美国科学家 Claude Shannon(香农)在《保密系统信息理论》中提到。W.Diffie 和 M.Hellman 在 1976 年，发表了《密码学新方向》[3]，建立了“数据加密”的概念，后来随着美国政府颁布实施数据加密标准(DES),DES 是一种加密算法，后来被广泛应用。1983 年 8 月，美国 NSA 国家计算机安全中心颁布了官方标准，即“受信计算机系统评量基准”。此基准被认为是当时很有权威性的计算机安全标准，此标准对于可信任系统进行定义：系统由完整的硬件和软件共同组成，在遵守访问权限的前提先，可以同时为多个用户提供服务，并行处理多种秘密级别的信息。此标准将安全性能进行了四大分级，当前此标准被多个国家的计算机系统所参考使用。

到 1997 年，Rivest,Shamir 和 Adleman 共同提出了名为 RSA 的密码体制[4]，这是第一个比较完善的公钥密码体制，RSA 以数论中的欧拉定理为基础，RSA 相比 DES 更加安全。除此之外，也有其它的一些数据加密算法，例如 Merkle 和 Helman 提出的背包算法，Muller 和 Noballer 提出的基于 Lucas 的公钥密码算法，还有基于 ECC(椭圆曲线)的公钥密码体制。

随着对网络安全研究的不断深入，越来越多的电子商务安全问题也日益严重和突出，主要是由于网络系统本身的脆弱性以及相关研究技术的滞后，不能够满足系统的正常运作。网络的脆弱性即健壮性不强原因在于：网络一方面存有漏洞和安全缺陷，易受到外界攻击；另外就是安全系统在设计的时候，故意植入了“后门”程序，这些程序在关键时候可以对于网络系统以致命性的打击。

现实生活中，新的黑客攻击手段对于现有的安全技术系统造成了很大损失，范围广、危害大的电脑病毒感染等网络安全事件经常见诸报端。美国政府对于信息安全投入巨资，增强信息技术安全观念，加强各部门和政府的信息安全基础设施建设，加强信息技术安全方面的研究工作，其研究重点在于防御计算机病毒和黑客的攻击，通过设置新型防火墙，建立安全保密网络等方面，进行网

络技术创新。

像美国一样，世界很多国家也是对于本国移动商务安全高度重视，相对而言，发达国家由于信息技术和科技实力比较强，在这方面的研究也走在前沿。目前比较有代表性的解决方案有日本的 i-Mode 和无线应用协议(WAP)。

日本蜂窝电话营运商 NTT DoCoMo1999 年开展了 i-Mode 服务。i-Mode（Information-Mode）是一种移动电话服务，提供移动电话与 Internet 网的持续连接，i-Mode 服务是通过使用一种在 NTT 的主干线上附加一种包通讯的网络来实现，此传送技术允许持续的连接。

WAP（Wireless Application Protocol)是无线应用协议，是一项全球性的网络通信协议。WAP 使移动因特网有了一个通用标准，WAP 定义了可通用的平台，把目前 Internet 网上 HTML 语言标记的信息转换成用 WML（Wireless Makeup Language)描述的信息，显示在移动电话等终端设备显示屏上。WAP 仅需要移动电话和 WAP 代理服务器的支持，不需要现有移动通信网络协议做任何的改动，可以广泛地应用于 GSM、CDMA 和 3G 等多种网络。

1.2.2 我国研究现状

我国电子商务发展相对于国外而言，起步较晚，直到 1995 年我国才开始发展，并逐步蓬勃兴旺起来。移动电子商务安全方面研究方面，各种标准和法律不够完善，但政府部门和企业也都很重视网络信息安全问题，国内科研机构和大中专院校以及相关行业的企业都纷纷加入信息安全领域。

国家对信息安全成果产业化基地进行建设[5]，并且成立了国家信息安全工程技术研究中心，在 863 计划中规划了信息安全基础设施研究中心和反计算机入侵和防病毒技术研究中心，在一些有实力的高校开展了信息安全、密码学专业等国家和部队家重点学科。2002 年，国家 863 计划中规划了“系统安全风险分析和评估方法研究”课题，拉开了信息安全问题研究的序幕。2003 年 7 月国家信息化办公室完成了两项草案，包括《信息安全风险评估指南》和《信息安全风险管理指南》，并通过试点工作进一步完善。十五期间，国家进行基础理论研究和高新技术研究，开展了科技攻关项目，把信息和网络安全作为国家发展的重点任务。

目前我国的移动电子商务体系也取得了一些成果，对今后的研究提供了理论基础，但总体来讲还不是很完整，安全技术也不是很成熟，很多技术都是从

国外引进，自主推行的解决方案较少，没有形成行业标准规范。另外与国外移动电子商务发展相比，我国在互联网和电子商务的法律还不够完善，需要加强相关法律的制定和实施，来保障电子商务的正常运行。

综上所述，尽快解决移动电子商务的安全问题，尽快建立相关安全基础保障设施，推动信息技术等相关产业的发展，增强技术创新能力，对于推动移动商务安全健康发展有着极其重要的意义，同时也可以推动我国信息化产业的建设，对国民经济做出贡献。

1.3 本文的研究内容及方法

为了解决移动电子商务的安全问题，本论文应用移动电子商务安全的相关理论，详细分析移动电子商务当前所存在的安全问题，强调安全问题对于移动商务健康发展的重要性；分析移动电子商务的安全需求和存在的安全问题，对安全性进行一个概括性的介绍；重点介绍目前用于支付的两种安全协议安全套接层(SSL)协议和安全电子交易(SET)协议；详细介绍开展移动商务的两种主要的业务承载方式：基于短消息(SMS)方式和基于 WAP 方式，分析各自的特点和实现技术。基于短消息的方式，是移动商务开展运用的简单模式，应用系统结构相对比较简单，基于 WAP 方式是目前主流，对 WAP 架构进行了分析，理论上实现了交换数据的安全传输；最后在移动商务的管理和立法方面进行了分析和探讨，并对未来移动商务的前景进行了展望。

1.4 本章小结

移动电子商务是在电子商务发展的基础上发展而来，是电子商务发展的新阶段，逐步并已经成为电子商务发展的新方向。本章介绍了移动商务的国内外发展现状，国内由于起步较晚和国际发展程度相比，起步较晚，同时也在不断取得进步；最后介绍了本论文的研究方法和思路。

第2章 移动电子商务安全

2.1 移动电子商务内容

移动电子商务是随着电子商务发展起来，是电子商务的一个新分支，是电子商务发展的新形式。作为对有线电子商务的补充与发展，移动商务继承了电子商务的特点，并与互联网络集合起来，使得电子商务的各种业务流程从有线转向通过无线网络进行，大大发展了电子商务的概念。移动电子商务一般是指利用手机或掌上电脑等终端设备和互联网络结合起来所构成的电子商务体系。终端设备通过无线连接技术和网络互联，在这个过程中，移动运营商、移动服务提供商和手机制造商共同参与消费者的商务行为，用户可以随时随地进行商务活动。

移动电子商务是随着移动通信技术和互联网应用为前提发展起来的，全面支持移动业务，基于无线移动网络，可以实现通信、娱乐、网上浏览等服务；移动商务不仅可以在网上进行买卖货物活动，更重要的是提供了一种全新的销售和促销渠道，商家和消费者都可以从中受益。移动商务可以满足消费者个性化需求，用户可以根据自己的实际需求选择上网设备和服务项目，获得所需产品或服务。目前移动电子商务主要包括移动支付、网上股市、移动银行等，可以提供个人信息服务、股票交易、网上购物和银行业务等服务项目。相比电子商务，移动商务方便快捷，可以随时随地根据自己需求来进行商务活动；移动商务不存在距离和空间的限制，用户是通过无线接入互联网络，适合大众化应用。

随着移动用户数量的迅速增加，以及移动通信技术在信息化领域的纵深发展[6]，我国移动电子商务发展开始步入快车道。据统计，2007 年底我国移动通信终端已达 5.48 亿，手机数量已远超个人电脑，2010 年手机用户数量将近 7.4 亿，无线互联网市场空间巨大。电信运营商、终端厂商、银行和服务提供商等产业链内成员都开始逐步进入无线电子商务领域。无线商务借助于短信和 WAP 等承载方式得以实现。运营商领域，中国移动“商信通”软件，用友移动的移动电子商务平台“移动商街”，这些无线商务平台都得到很好普及推广。

随着3G的应用和推广，电信基础设施不断提升，窄带无线逐步向宽频无线过渡。WAP产业国内发展迅速，用户关注度也不断得到提升。WAP资源随着用户需求数量的则加，也将得到丰富扩充，服务内容也向多元化转变。

2.2 移动电子商务实现技术

移动电子商务飞速发展，随着互联网技术和移动通信技术的发展，实现移动商务的手段越来越多元化，主要技术有以下几类：

2.2.1 无线应用通信协议 WAP

无线通信协议标准WAP，是在数字移动电话、因特网、计算机应用之间进行通讯的开放全球标准，基于在移动中接入网络的需要，目标是将互联网中的丰富信息及业务内容引入到移动电话等无线终端中。由于WAP采用二进制传输，可对传输数据进行压缩，其优化功能可以满足低带宽通信；WAP定义了一种通信终端连接因特网的标准方式，将移动网络和万维网以及公司内部网紧密连接起来。同时，WAP提供了一种应用开发和运行环境，支持当前主流嵌入式操作，支持多数无线终端设备。WAP是移动商务开展的主要承载技术，可以不受时间地点限制随时随地接入网络。

WAP无线网络由移动终端、服务器以及网关三者组成，即无线网应用模型框架，本模型可以支持无线网多种WAP应用。WAP手机相比电脑而言，具有体积小和操作简单等特点，可以接入无线网络浏览新闻等信息，但不适用于数据流太大的通信应用；随着3G网络的迅速发展，越来越多支持WAP浏览器的智能手机出现，使得移动通信速度得到迅速提高。

移动网络运营商提供WAP网关，WAP服务器则是由因特网内容提供商来提供，移动终端则是由手机厂商或是电脑厂商提供。WAP应用定义了包括客户端、WAP代理和源数据服务器三种实体。移动终端常见的是手机、PDA或是平板电脑，终端有显示屏，可以运行微型浏览器，显示网页内容。终端使用无线标记语言WML显示网页内容，现阶段最新的平板电脑更是可以支持flash，使得显示内容更加丰富。WAP代理内容涵盖WAP协议栈，协议网关等；源数据服务器中包括了使用WML Script脚本语言编写的各种WAP应用。

WAP手机可以浏览网上信息，省时方便。随着3G网络的开展和普及，以后手机上网速度会更快，支持的应用也是更加多样。

2.2.2 通用分组无线业务

通用分组无线业务(GPRS)是一种基于GSM系统的无线分组交换技术，打破了GSM网络仅提供电路交换的定式。GPRS业务将分组交换模式引入到GSM网络中[7]，通过增加相应的功能实体和对现有基站系统进行部分改造来实现分组交换。GPRS无线电子商务平台把行业用户终端和企业内部网以及互联网连接在一起，进行电子交易和电子采购等业务，高效实现企业业绩增长，推动企业电子商务应用的发展。

GPRS拥有高于10倍于GSM网的速度，具有较高的数据传输速度，可以比较方便传输大容量文件；用户可以随时保持和网络间的联系，通过GPRS接入建立无线连接几乎不需花费多余时间；通过数据流量多少来计算所需费用，而非按照上网时间长短计费。

以后网络发展的确实便是将有线网和无线网以及互联网结合起来，形成综合的数字化网，从而更多应用得到推广使用。基于GPRS的无线商务是建立在通信网和因特网平台上的应用，涉及以下产品技术：GPRS无线Modem和无线终端；VPN虚拟专用网；安全中间件以及嵌入式OS等。企业和集团用户是最早使用GPRS无线网开展商务应用的，主要解决保险、银行以及税务等方面需求；通过GPRS实现无线IP接入，利用VPN专用网技术在公共网络上构建虚拟专用网，是的远程接入用户能安全访问内部网络，基本上实现了把行业用户的终端设备和企业内部网以及公共网连接在一起，从而实现电子交易、管理订单以及电子采购等流程。

2.2.3 移动网络协议

移动网络协议即移动IP技术[8]，使得移动节点以固定网络IP地址，实现跨越不同网段的漫游功能，并保证基于网络IP的网络权限在漫游过程中不发生任何改变。移动IP技术是移动通信和IP的深层融合，为移动节点提供了一个高质量的实现技术，可应用于用户需要经常移动的所有领域。

移动IP技术使结点进行无线链路切换时不需要改变其IP地址，也不需要中断

正在进行的通信连接，在一定程度上满足移动商务的应用开展。移动IP技术满足了普遍计算时代的需求。随着基于移动IP技术的3G通信时代的来临以及和因特网的进一步结合，可以为用户提供高速和高质量的多媒体业务。移动IP技术并非移动通信技术和互联网技术的叠加，而是移动通信和IP技术的深入结合，真正实现语音业务和数据业务的结合。

目前移动IP技术是业内研究的热点，把移动IP技术的实施过程分为三个阶段：第一是实现移动业务IP化；第二是向移动网络的分组化发展；第三即在3G网络中实现。

2.2.4 蓝牙技术

蓝牙(Blue Tooth)是一种短距离无线通信连接技术，旨在提供一个成本低、可靠性高并且可以进行高质量语音传输的无线网络。

蓝牙是一种支持设备短距离通信(一般10m内)的无线电技术，采用分散式网络结构以及跳频技术，支持点对点及点对多点通信[9]。采用时分双工传输方案实现全双工传输，工作在全球通用的2.4GHZ频段，数据速率为1Mbps，能在包括移动电话、PDA、无线耳机、笔记本电脑和相关外设等众多设备之间进行无线信息交换。

蓝牙技术使得不同厂家设备间可以在无线连接的状态下，进行信息交换和操作。目前主要应用在汽车电子，办公打印设备和医疗设备等领域；蓝牙技术是一种全球规范，并且是开放性的，用于无线数据和语音通信，实质内容是在设备间通过建立无线接口，使通信技术和计算机技术有效结合，近距离实现数据信息传递。蓝牙技术最初是在1998年被提出，作为一种短距离的无线连接标准，目的是替代原有的有线连接实现无线数据通信；蓝牙技术具有成本低和功率小的特点，能在手机、PDA和打印机等设备间近距离传输信息，也广泛应用于汽车蓝牙免提。

蓝牙共有六个版本，目前通用的是V2.1版本，业内正在推动V3.0版本新规范的实施，设备制造商也开始研究对应蓝牙版本的解决方案。3.0新版本传输速度很快，包括运用了无线802.11协议，可以传输更大数据量的内容信息，并在功耗方面加入了对于电源耗电量得控制，蓝牙设备的耗电功耗会降低。

2.2.5 第三代通信系统

第三代移动通信系统(3G)，是相对于一代模拟制式手机和二代GSM数字手机而言，将无线网络和多媒体技术有机结合的新一代系统，可以处理有关图像、视频和语音等媒体信息，能提供高速数据业务。

3G主要特点是能够实现全球无缝漫游，是可以在全球范围内使用的系统。支持统一标准，使用相同频段进行通信。当前移动通信主要是进行语音电话业务，真正把多媒体和高速传输效率服务于用户则是3G时代所体现的特点。全球范围内的3G标准有WCDMA，CDMA2000和TD-SCDMA[7]。其中WCDMA和CDMA2000是已经比较成熟的技术标准，TD-SCDMA是我国具有自主知识产权的标准，特点是可以节约频带资源，升级成本较低，相对WCDMA，CDMA2000而言，通信质量会差一些。

3G时代通信系统更加关注数据信息的传输速率，而非传统的通话质量和通信网络稳定性的问题。3G移动上网速度基本可以和当前移动带宽相当，相比先前2G和2.5G时代而言，可以提供更丰富的视频和图像。

3G服务通过无线通信和互联网等多媒体通信结合，能同时传送语音和数据信息。3G手机具有移动支付、手机银行等功能，手机变成了移动电子钱包，通过话费直接可以支付，不需要第三方支付平台；同时随着3G上网资费的下降，会吸引更多的客户参与到整个的电子商务活动中来。

2.3 移动电子商务安全威胁

移动电子商务是传统电子商务和无线互联网技术的结合，所以分析移动商务存有的安全威胁，须从电子商务和无线网络所存有的安全问题进行分析。传统电子商务交易双方通过网络开展业务，其安全性需要计算机安全网络和安全交易过程来保障。商户主要是采用防火墙技术来保护商务交易系统，防火墙是软硬件相结合的系统，在内部网和外部网之间、专用网与公共网之间构造一种保护屏障，保护内部网免受非法用户的侵入，起到一个安全网关（Security Gateway）的作用。但是防火墙有时会被黑客通过非法手段进入内部系统，计算机病毒也可以通过防火墙感染计算机。

电子商务系统一般存在以下安全问题：

1、计算机管理不当。一些电子商务系统内部人员有一定的管理系统权限，

若对计算机设备管理不当，很可能会被一些别有用心的人员非法进入，为自己牟利，造成损失。

2、外部攻击。网上电子交易会吸引黑客进行网络攻击，截取或是盗取商户的交易信息，冒充正常用户进行非法登录，侵害交易当事人的正当权益。

3、病毒或木马。对电子商务系统而言，病毒是常见的威胁，而且电脑并脑病毒种类繁多，由病毒侵入造成损失的例子也是经常看到。木马对商务系统的威胁最大，木马利用计算机程序漏洞侵入系统并窃取文件资料。

4、拒绝服务。拒绝服务通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务。

无线通信网络作为开展移动电子商务的必要技术，由于无线线路的开放性，同样面临多种安全威胁。终端系统、服务网络系统和无线链路共同组成了无线通信系统，其威胁也来自于以上三部分，攻击位置的不同造成的破坏也不同，攻击方式也不同。

2.3.1 终端威胁

目前手机等终端的安全威胁主要来自于病毒，手机通过蓝牙、手机多媒体信息服务和手机缺陷(Bug)等方式传播病毒。手机病毒是一种以手机为攻击目标的电脑病毒，通常以手机为感染对象，以手机网络和计算机网络为感染途径，通过发送病毒短信等形式，是手机系统得到破坏，造成手机状态异常。每年全球手机病毒数量也不断增加，其攻击途径主要有以下三种：

1、以“病毒短信”方式攻击手机本身系统。

2、通过信息传播感染其他手机，对手机主机造成破坏。

3、攻击和控制“网关”，向手机发送垃圾信息，致使网络运行瘫痪。

手机病毒可能会自动拨打电话、盗取电话本名单或者删除手机上的资料，并产生金额庞大的电话账单，致使用户损失巨大。

另外，终端设备可能会丢失、被借用或是被超权限使用，系统资源收到非法访问；攻击者可以修改或是删除终端上的应用软件和其他资料，破坏系统完整性；近年来随着技术的发展，可以通过复制手机 SIM 卡来监听正常 SIM 卡使用者信息，或是伪装成真是用户进行权限操作。

2.3.2 网络服务系统威胁

网络服务系统的威胁主要存在以下几种：

1、非授权数据访问。系统入侵者没有访问权限，非法访问或是窃听系统数据信息；或是伪造身份冒充合法用户进行系统网络接入，对系统进行访问。

2、完整性威胁。系统入侵者通过相关手段修改或是删除系统数据信息，对系统完整性形成破坏。

3、拒绝服务。通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务。

4、抵赖否认。用户可对业务费用和数据来源进行否认；网络单元否认发出信令或者否认接收到了其他数据信息。

2.3.3 无线网络威胁

无线网络因其开放性，与有线传输网络相比，安全性稍微差些。与网络服务系统威胁类似，无线网络所存在的安全威胁也分为三种情况：对于数据的非授权访问，对于无线传输信息的完整性威胁和拒绝服务。入侵者利用相关技术手段可以窃听无线链路上的数据信息，可以修改或是删除信息，破坏其完整性。可以进行插入攻击[10]，布置一些非授权的设备或创建新的无线网络为基础，这种部署或创建往往没有经过安全过程或安全检查。有些用户可以通过临近无线网络访问互联网，占用大量网络带宽，影响网络性能。另外，还有一些其他隐患，如客户端对客户端的攻击(包括 DOS 拒绝服务)，对加密系统的攻击或是进行错误的配置等，都会对无线网络带来风险。

2.4 移动电子商务安全需求

通过分析移动商务系统各部分所存有的安全威胁，便可以看出安全性对于移动商务重要性。从安全性上讲，一个完整并且安全的移动商务系统应该有以下特点：

(1)数据机密性需求

数据机密性要保证数据在传输过程中不被泄露，并不能被未授权访问，更不能对信息进行修改。可以使用加密技术或是采用安全信道来实现数据保密性；

加密技术分为对称密钥和非对称密钥技术，一般采用对称密钥算法。对于移动商务还得在传输层和应用层上进一步采用加密措施。

(2) 数据信息完整性

保证数据信息在传送和存储过程中未受到非法更改、删除或是重放，防止非法入侵者伪造信息替代正常合法信息。可以使用消息摘要技术和加密技术(HASH 函数)来实现，而支付信息的完整性可由支付协议来保证实现。

(3)防抵赖性

保证接收方对于自己以接受的信息内容不能进行否认，发送方对于已经发出的信息进行抵赖否认；保证交易数据的正当保留，维护双方当事人的合法利益。可以通过数字签名技术来实现。

(4)身份认证

系统要确保使用者是合法用户，具有授权权限，确定信息接收方或是发送方的真实身份，防止身份被伪造。可采用一些认证技术来实现，包括有：公钥技术、数字签名技术和口令等，常用的是口令技术。

(5)重传攻击检测功能

重传攻击是对网络信息安全有很大威胁的攻击方式，系统要能够接收方能识别所收到信息的状态，确定是否是信息重传。

(6)容错能力

信息在网络中传输，设备和线路经常会发生故障，要保证在故障产生时，系统不会长时间出于停滞状态，要有备用方案去处理；还要保证更新系统时对于原有软硬件的兼容能力。

另外，移动商务对于系统的经济性也得适当考虑，希望在增强系统安全性的同时，能够尽量降低所花费用；合理的加密技术是增强安全的最有利措施，目前以有不少加密算法可以实现，要从算法的可实践性上来适当选择。

综上，移动电子商务由于是通过无线接入互联网络，和电子商务通过有线网络传输相比，安全性降低。移动商务系统要实现安全解决方案应从终端、无线传输网络以及网络服务系统三部分共同实现。无线网络是信息传输的通路，需要保证传输安全，终端设备和服务器系统要有较强的业务处理和纠错兼容能力。

2.5 安全技术

移动电子商务是电子商务技术的继承和发展，作为电子商务和移动互联技术的结合，移动商务安全实现技术包括了电子商务安全技术，还有移动接入安全性需求。主要包括的安全技术包括有加密技术、身份认证技术、防火墙技术、数字签名和电子安全协议等。

2.5.1 加密技术

为了保证数据的安全传输和交易信息的安全，确认交易双方的真实身份，从技术层面上常用到加密技术。加密技术是用加密算法把传输数据信息变成密文进行传输，到达目的后再进行解密还原。加密技术包括两个元素：算法和密钥。加密算法[11]就是将普通文本信息与一串随机字符结合产生密文，这个随机字符就是密钥，密钥是对数据进行编码和解码的参数信息。通信过程中，通过适当的密钥加密技术和管理机制来保证网络的信息通讯安全。明文信息 M 通过加密算法 E 得到密文 C，过程即 C=E(M，Ke)。参数 Ke 是密钥，密文 C 经过解密算法 D 变为 M 过程称为解密。加密过程用图 2-1 表示。

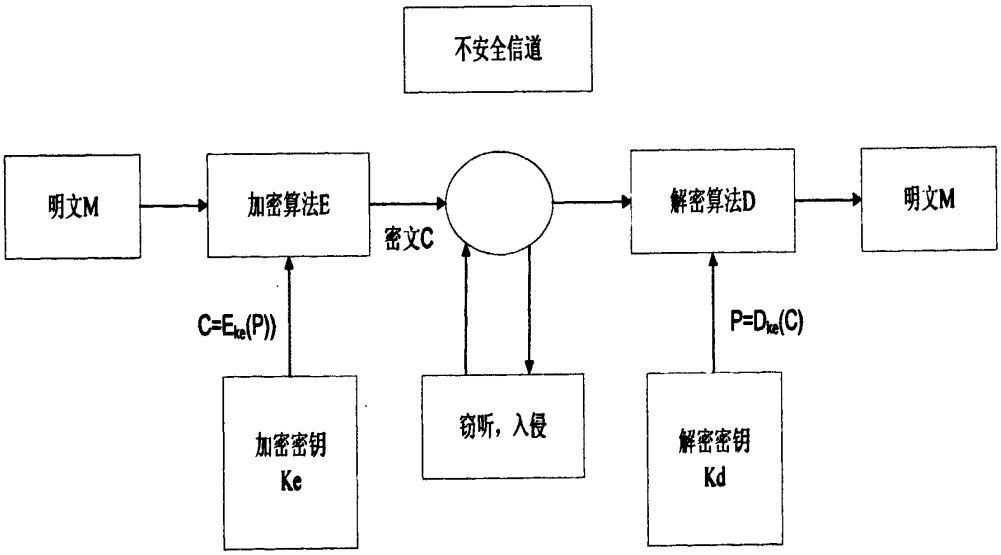

图 2-1

密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。对称密钥指加密和解密过程中使用相同密钥，非对称密钥即加密密钥和解密密钥不相同。对称密钥安全性取决于加密算法强壮性和密钥的秘密性，

而非算法的秘密性，算法可以公开。

对称密钥算法中加密和解密速度比较快，制造商可以开发出低沉本的芯片实现数据加密。常用对称算法有 DES，AES 等。非对称加密体制又名公开密钥体制，比较流行的有两类：一种是基于大整数因子分解，代表是 RSA 算法；另一种是基于离散对数问题，代表是椭圆曲线公钥密码(ECC)。

RSA 是麻省理工学院的 Riverst、Shamir 和 Adleman 共同提出来，作为第一个比较完善的公钥密码体制，其安全性基于大素数的因式分解难题。RSA 算法过程如下：

RSA 密钥生成阶段有：

1.随机选取两个素数 p、q.

2.计算 N=p*q，以及欧拉函数 $\varphi(N)=(p-1)*(q-1)$.

3.任意选取整数 e，满足 $1<e<\varphi(N)$，且 $\gcd(e, \varphi(N))=1$.

4.计算 d，满足 $e*d\equiv 1 \bmod \varphi(N)$.

其中 p、q、$\varphi(N)$、d 需要保密，d 是密钥，(e，n)是公钥。

RSA 加密过程如下：

当发送者需发送消息 m，对其加密得到密文 c，使得 $c=m^e \bmod N$。

RSA 解密过程如下：

当接受者接收到密文 c 时，进行解密，以便得到明文 m，且 $m=c^d \bmod N$。

椭圆曲线密码(ECC)体制如下：

密码学中的椭圆曲线是定义在有线域上的。即对于素数 p，p>3，有线域 Fp 上的椭圆曲线 E 有这样的公式：

$$y^2 \equiv x^3 + ax + b \pmod p$$

这里 p 是素数， a 和 b 为两个小于 p 的非负整数，它们满足：

$$4a^3 + 27b^2 \pmod p \neq 0$$

椭圆曲线 ECC 密钥生成过程如下：

首先，选取 Fp 上定义的椭圆曲线 E，在 E 上取点 P，其中 P 的阶是素数，设为 n，n 为素数，设定一个集合{0，P，2*P...(n-2)*P ，(n-1)*P }，此集合是由 P 生成的椭圆曲线循环子群。

其次，素数 p，E，P，n 构成公开参数组。

第三，选取 d，使得 $1<d<n-1$。

最后，计算 Q=d*p。Q 是公钥，d 是私钥。

ECC 加密过程如下：

1、发送者发送消息 m，表示为 E(FP)上的某点 M。

2、选取 1<k<n-1，计算 K=k*P。

3、进行 H=M+k*Q。(K，H)即为密文。

ECC 解密过程如下：

1、进行 M=H-d*K。

2、在 E(FP)上的点 M 上，取出 m，得到原有明文信息。

2.5.2 认证技术

认证技术[12]包括有身份认证、数字签名、时间戳、数字信封和数字证书等方式。身份认证是比较简单的认证方法，可通过密码验证，生物学特征(指纹识别、虹膜识别)，动态口令和 USB KEY 认证等方式。数字签名用来保证信息传输过程中信息完整并可以提供对信息发送者的身份认证。数字信封是用加密技术来保证信息内容只能够特定的收信人打开的技术；时间戳[13]则提供对于电子交易文件日期和时间的安全保护。数字证书是由证书中心颁布，用于标记通讯各方身份信息。

数字证书是经过证书认证中心即 CA 中心数字签名的，并包含有公钥持有者信息和公钥的证书文件，CA 中心是第三方的认证机构，具有权威性和可信赖性，负责对各种认证需求进行服务。目前数字证书已被广泛应用，遵循 X.509 标准。

一般数字证书中包括有用户的身份 ID 信息，所持有公钥信息以及 CA 签名数据，经 CA 签名能保证证书的真实可信，用户所持公钥也能保证所发送信息完整性。证书验证过程包括有单向验证和双向验证过程。单向验证即单向通信，通过对通信 A 和 B 双方身份的证明来保证传输信息完整性；双向验证是在单向验证的基础上，加入了对于接收方 B 的应答信息。

单向验证过程如下：

1、发送方 A 产生随机数 R_1。

2、A 构造消息 M1=(R_1，T_1，I_2，m)。T_1 是 A 时间标记，I_2 是 B 身份证明，m 是任意一条数据。

3、A 将(C_1,D_1 (M_1))发给接收方 B。C_1 为 A 证书，D_1 是 A 私钥。

4、B 确认 C_1 得到 A 公钥 E_1，解密 D_1 (M)，并检查 M_1 中 I_2，确保信息。

双向验证是单向基础上加入了对于接收方回执信息的确认，包括有一个单向验证过程以及一个从接收方到发送方的相仿的单向验证。以单向验证中的数

据传递过程为例，从 A 到 B 的双向验证除包括有上述的单向过程外，还包括有以下几个步骤：

1、接收方产生一个随机数 R_2，构造消息 $M_2=(I_2, I_1, R_2, R_1, m)$，$T_2$ 是 B 的时间戳，I_1 是 A 身份。

2、加密 M_2，把 $D_2(M2)$发送至 A。

3、A 收到信息后，进行 $E_1(D_2(M_2))$，确认 B 的签名以及发送信息的完整性。

4、A 收到信息后，可以检查 M_2 中 T_2，验证信息的时效性。

2.5.3 防火墙技术

防火墙[14]其实是一种形象说法，是计算机软硬件的组合，在互联网和内部网之间建立起一个安全网关，此网关能够保护内部网络避免受到外界非法用户的侵入。实际上防火墙技术是一种隔离技术，在网络间通信时执行访问控制，最大限度的组织网络黑客访问内部网。防火墙可分为硬件防火墙和软件防火墙，通常是硬件防火墙，通过软硬件结合达到隔离目的，软件防火墙则是纯软件方式通过一定访问规则来控制网络访问。防火墙主要具有以下功能：

1、隔离危险区域：防火墙在内外网之间，对于相对稳定的内部网而言，外部网络存有很多安全问题，只有经过筛选的数据包才可以通过。

2、加强网络安全

建立以防火墙为核心的安全方案，将安全软件集成配置到防火墙上，安全管理更加经济。

3、限制访问内网

防火墙通过相关策略对于内网信息实行访问控制，只有被允许的访问才可以进入内部网。

2.5.4 数字签名

数字签名可以保证信息在传输过程中的完整性，并可以提供对信息发送者身份的验证。在电子商务中数字签名是最普遍应用且可靠性最强的一种方法。

数字签名是公钥加密算法的应用，信息发送方用私钥加密报文摘要，并与原始信息内容附加在一起。使用时，报文发送方在报文中生成 128bits 或 160bits 的单向 hash 值，即报文摘要；然后用私钥对此摘要进行加密，形成数字签名。

然后数字签名和原有报文一起发送过信息接收方，接收方从接收到的原始报文中计算机出 128bits 的 Hash 值，用发送方的公钥对数字签名解密，若计算出的两个 Hash 值相同，则报文接收方就能确认此报文时签名者那里发送，并且报文在传输中保持了完整。

数字签名应该实现：

1、信息的接受者能验证发送者对于信息的签名。

2、签名者不可以对已签名内容进行否认。

3、数字签名不可以被伪造。

数字签名和消息认证不一样，消息认证可以使得信息接收方验证信息的发送者以及所发送信息的完整性，若接收方和发送方产生冲突矛盾是，仅仅靠消息认证是不能解决矛盾，就需采用数字签名技术。

2.5.5 电子安全协议

安全协议分为安全套阶层协议(SSL，Secure Socket Layer)和安全电子交易协议(SET，Secure Electronic Transaction)。SSL 协议是 Net Scape 开发，可以对于通信内容进行加密，而且这种加密强度比较高；可以提供对于用户以及服务器的认证，保证数据信息在传输过程中的完整性。

目前主流的 Web Browser 都集成有 SSL 技术，在浏览器运行过程中只需对证书进行加载就可以，当浏览器指向一个安全域时，SSL 会同步确认客户端和服务器端，采用相同加密方法和会话密钥，保证建立会话的私密性。

SSL 会话产生时，SSL 证书由服务器传送给客户端，由客户端对证书进行自动分析，并根据用户浏览器版本产生密钥位数不等的会话密钥。一般密钥位数是 40bits 或是 128bits，这个会话密钥用于对传输的交易信息进行加密，且这个过程是透明的，从而在客户端和服务器间建立了安全通道。密钥长度越长，破译的难度越大，并且 128bits 的服务器证书可产生 128bits 以上的会话密钥，加密程度更强。

本协议通过对应用程序进行数据交换前交换 SSL 初始握手信息来实现有关安全特性的检查。SSL 握手，采用 DES 加密来实现信息机密性。图 2-2 是 SSL 在网络间的位置。

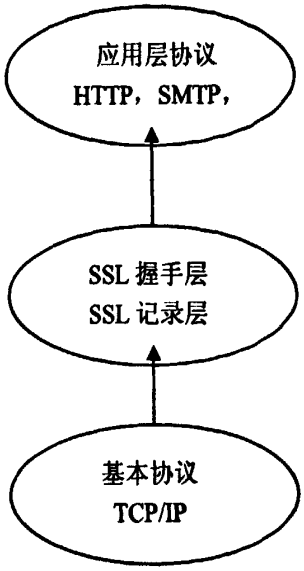

图 2-2

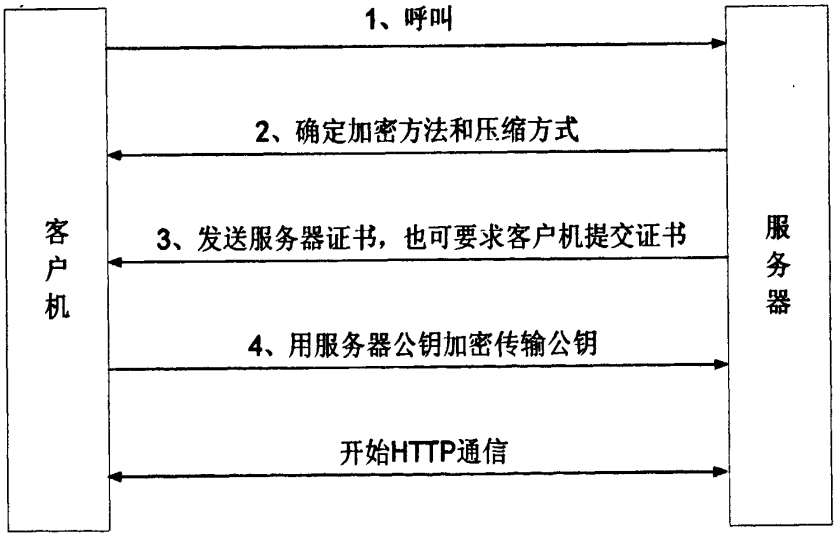

图 2-3

SSL 协议采用公开密钥和专用密钥两种加密方式：在建立会话时，使用公开密钥，会话进行过程中使用专有密钥。根据图 2-3 握手过程[15]，可分为五个阶段：

1、建立连接：客户呼叫服务器。

2、交换密钥：客户和服务商间确定加密方法，交换双方认可密钥。

3、发送证书：服务器向客户机发送服务器证书。

4、检验：检验服务商取得的密钥，用服务器公钥加密传输密钥。

5、通信过程：验证客户可信度，进行 HTTP 通信，结束时交换信息。

SSL 协议提供有以下几种服务：用于认证用户和服务器；进行数据加密，保证传输中信息安全；保持数据完整性。

SET 安全交易协议是美国 VISA 和 MasterCard 两大信用卡组织推出的电子商务行业规范，实质是一种应用在网络上以信用卡为基础的电子付款系统规范，目的是为保证网络交易安全。本协议采用公开密码体制和 X.509 电子证书，通过软件和数字签名以及机密技术，使得在交易过程中保证安全进行。

SET 协议定义了四种实体：持卡人，商户，支付网关和发卡行。持卡人即持有信用卡的用户；商家是提供商品服务的；支付网关是由金融机构等第三方控制，用于处理用户和商家之间的交易；发卡行即发放信用卡的金融机构。SET 交易中，持卡用户与商家和支付网关共同参与交易过程。

SET 采用公钥和私钥加密共用的办法来保证信息的私密性，公钥采用 RSA 算法，私钥加密算法则采用 DES 数据加密标准。SET 协议通过数字签名技术来保证信息完整性并确认信息源，数字签名方案则采用和信息加密相同的加密方案[16]。

SET 安全协议包括有：SET 通信协议，支持 SET 标准的电子钱包，证书中心取得的电子证书，发卡机构对于消费卡的认证和管理，参与交易实体等内容。

SET 协议得到了不错应用推广，但仍存有一些漏洞问题：包括协议本身没有提供对于“非拒绝行为”的保证，网上卖家不能证明订单是否是客户发出；无法解决消费者对商品不满意时的责任归属问题；交易数据的处理问题等。

SET 协议相对于 SSL 有较高的安全需求，SET 要求交易实体需申请数字证书来认证身份，SSL 则只需获得卖家服务器端得认证即可，对于用户则无强制认证；若消费者将进行 SET 交易，则需申请证书并安装 SET 标准的软件，而进行 SSL 交易则不用安装。

2.6 移动商务安全支付业务

2.6.1 移动支付概述

移动支付是移动电子商务中的重要组成部分，也是移动商务实现的必要途径。类似于移动电子商务衍生于电子商务，移动支付也是从电子支付发展而来。所谓电子支付，是指从事电子商务交易的当事人，包括有消费者、商家或是金融机构，通过信息网络并使用安全的信息传输手段，采用数字化方式进行的货

币支付或是资金流转。移动支付是在电子支付基础上的扩展，指的是当事双方通过移动设备进行货币价值交换以获得所需商品和服务的过程。

移动支付借助于银行系统和移动通信网络实现电子商务支付。基于 SMS 的移动商务方案中，用户使用 SIM 卡，通过 STK 预先设定的菜单，和银行服务进行绑定，个人有关银行交易业务可以同银行进行及时沟通。目前国内淘宝网上已经开展电子支付，用户可以通过淘宝网推出的“支付宝”，来实现购物、手机充值以及水电费缴纳等业务。

移动支付有几种分类模式。按照数额大小可以分为微支付、小额支付以及宏支付；按照时间信息分为预支付、在线支付和离线支付等；根据交易对象的不同，可以分为 C2C 支付、B2B 支付以及 B2C 支付等。移动支付的领域和范围也越来越大，已经从传统意义上的电子购物范围向包括有无形商品交易以及基于 LBS(Location Based Service)的位置服务等方向发展。

移动支付体系需要一些实体参与，包括有消费者、商户、金融机构和一个可信第三方。消费者和商户是参与交易的主题，消费者向商家购买产品或是获取相应服务，商户提供产品和服务给消费者用户，金融机构(主要指银行)在当中充当一个“桥梁”作用。银行收到商户所接收到的购买请求时，进行交易金额的处理工作，完成付费操作，当支付进行完毕后，反馈给商家和消费者一个交易成功信息，商家在收到付费成功消息后，把商品或是服务发给消费者，完成交易过程。可信第三方是形象说法，指的是一个因特网服务器，连接互联网和银行支付系统的一个工具。

移动支付的安全问题是网上电子银行能正常开展的前提和保障，也是移动商务交易完成的关键，当前网上交易可以通过对用户身份认证，签发和安装证书，SSL 加密传输以及安装网站安全插件来实现支付系统安全。

移动支付主要技术有 SMS、WAP 和 STK，主要支付协议有 SSL 和 SET 协议，前面章节已有介绍。

2.6.2 移动支付安全业务模型

移动支付业务模型[18]，主要有 Mobey 业务模型、PayCircle 业务模型和 SeMoPS 业务模型等。

2.6.2.1Mobey 业务模型

Mobey 业务模型定义了一个价值链，其中各个部分可以自由选择服务和技术标准，同时各部分又相互独立。该价值链各部分包括有：用户、银行、商家、安全组件提供商和运营商等。安全组件提供商是提供安全组件的研发和发行，并针对各种平台进行个性化定制，保证系统安全运行；移动运营商则是负责提供网络服务，保障网络的正常运营以及服务的正常提供。

2.6.2.2 Pay Circle 业务模型

Pay Circle 是移动电子商务支付系统标准化组织，目的是建立一个统一、易用并且安全的移动支付标准。和 Mobey 业务模型不同，该模型省去了不少单元，仅仅保留有消费者、商户和支付服务供应商。其中，支付服务供应商是为消费者提供支付服务的第三方，涵盖购物网站和零售商店。

Pay Circle 模型支付流程中，对于用户支付和商家提款环节进行了定性限制，当用户买下商品并付款后，款项不会直接汇至商家账户，而是由支付服务供应商对本款项进行暂时收管，等用户确认收到产品或是对应服务项目时，本款项才到达商户账户，本次交易才完成。国内的知名购物网站淘宝网所采用的支付宝业务就是利用这一机制，很好的保障了消费者正当利益。

2.6.2.3 SeMoPs 业务模式

SeMoPs 模型中，由银行和移动运营商作为支付机构，同样包括有传统模型中的参与实体，不同的是重新在基础上加入了数据中心(Data Center)部分，数据中心作为一个关键实体，可对数据信息进行短暂存储，在各支付机构中起到连接作用，尤其是跨境交易的产生时，作用更为重要。

本模型中，SeMoPs 模型将银行引入，联合网络运营商结合组成移动支付处理机构。

2.7 本章小结

本章节对于移动商务内容进行了介绍分析，包括有移动电子商务概念，实现移动电子商务的几种主要技术途径，目前所存在的安全威胁，移动商务运行的安全要求和实现移动商务安全的技术方法，最后介绍了移动支付的相关理论和三种业务模式。只有针对性的分析移动电子商务安全需求和安全威胁，才能

得出完整有效的安全解决方案。本章中对于移动商务所存有的安全威胁和实现技术方法进行了着重分析，其中加密技术和身份认证技术是保证传输信息完整性和机密性的重要实现手段，为以下章节实现移动商务安全方案打下基础。

第3章 基于SMS移动电子商务方案

随着移动通信技术的发展和手机用户的增多，移动服务的范围也是愈来愈广泛。运营商除提供语音服务基础业务外，短信息服务(SMS)也是被广泛运用，其特点是方便实惠。目前基于手机短信息的服务诸如：手机证券，网上银行，位置服务和手机支付等越来越多，消费者使用短信息用于日常信息交流和定制移动服务也很普遍；并且随着手机功能的增多以及智能手机的使用，手机目前可以利用短消息进行金融转账、电子商务和网上股市等业务。用手机短消息来进行例如电子商务和网上股市等交易服务时，交易安全是消费者用户很关心的事情。

基于短消息的移动商务是以手机短消息为承载工具开展，即直接在手机短消息系统上开发出各种应用。基于SMS的安全方案应该有以下几方面考虑：

1、系统能具有身份认证功能，在短消息网关和服务提供商之间安全接入服务器，使得服务器能够确认短消息来源，对信息状态进行确认。

2、能保证数据信息传输的完整性和有效性。通过增加一些软件模块，通过加密技术来实现对短信息完整性的检验。

3、检测重传。能保证消息的接受者能识别出所接收到信息的状态。

4、保留证据。保留证据防止发送方和接收方对于所发生行为的抵赖和否认。

通信安全有两种实现模型：点对点安全模型和端到端的安全模型。点到点模型，即链路加密方式，在数据进入到物理链路之前进行信息加密，可以工作在网络的物理层和数据链路层。点到点模型对网络上相邻结点之间传输数据进行保护，使用密钥相同进行加密和解密工作。报文在OSI七层模型中的第二层至第七层间以明文形式出现，在物理层和数据链路层间进行加密，随之以密文形式在物理链路上进行传输。当报文传输到通信通路间某结点时，对报文进行解密，然后再次加密以密文形式传输给后面结点。

端对端模型是直接建立通信双方之间的模型，直接通过双方间的保密通信，整个过程中信息始终是被加密，仅在最终结点用户才被解密；此加密方案是在表示层和应用层上进行，在表示层上容易实现，可以避免物理层中的加解密问题，仅在最终结点才可以被解密。

由于底层的加密技术仅能保护通信传输安全，不能提供对于上层应用数据

的安全，基于短消息的移动商务模式不能采用点到点模型，须采用端到端加密，才能避免交易数据在传输环节中被窃听或是修改。

3.1 SMS 网络与实现

SMS 服务通过短消息服务中心 SMSC 实现，SMSC 是短消息存储转发中心。网络在 SMSC 和移动终端间定义了移动电话发起服务(MO)和终止服务(MT)。SMS 网络结构如图 3-1 所示。

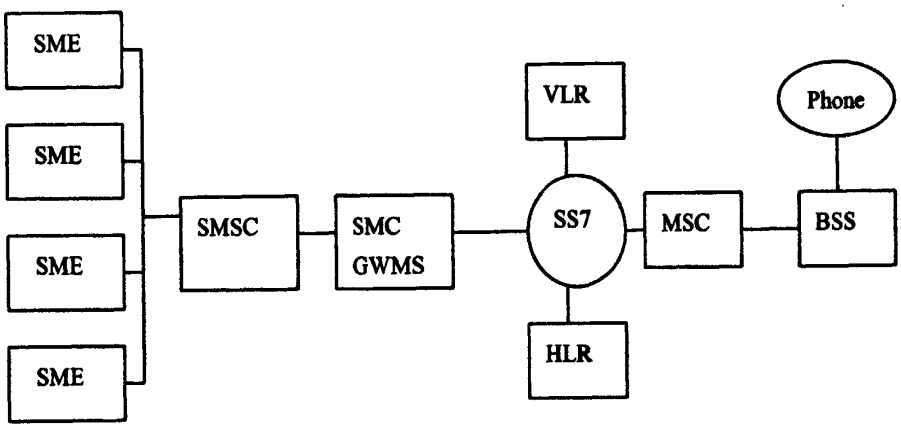

图 3-1

图示中所包含的实体：SME，SMSC，SMSGWMS，VLR,HLR，MSC

SME：Short Messaging Entity，短消息实体。用于接收或改善短消息，位于固话系统、移动基站或其他服务中心内。

SMSC：Short Message Service Center，即短消息服务中心，负责在 SME 和基站之间对短消息进行中继、储存或转发；移动台（ME）到 SMSC 的协议能传输来自移动台或朝向移动台的短消息，协议名为 SMTP（Short Message Transmission Protocol）。

SMCGWMS 或 SMCGMSC：SMS-Gateway MSC，SMS 网关。接收由 SMSC 发送的短消息，并向 HLR 查询路由信息，然后将短消息传送给接收者所在基站的交换中心。

HLR：Home Location Register，归属位置寄存器。用于永久储存管理用户和服务记录的数据库，由 SMSC 产生。SMS 网关与 HLR 间协议使可网关通过 HLR 搜索到用户地址。SS7 是信令系统 7 号电信协议，采用公共信道信令技术为信令服务提供独立分组交换网络。

MSC：Mobile Switching Center，移动交换中心。负责系统切换管理，控制电话和数据系统间连接服务。

VLR：Visitor Location Register:，访问位置寄存器。VLR 是含有用户临时信息的数据库。

当 SMS 向短信息中心 SMSC 发送消息时，SMSC 将该消息发至短消息服务交换网关 SMS-GMSC，然后网关查询 HLR 寄存器得到路由信息，再发至相应交换中心 MSC，最后发至目的移动台。应用服务器对于收到用户业务请求进行处理，然后把处理结果发至短信息网关，短信息网关将结果传送给短信中心 SMSC，最后由 SMSC 经 GSM 网发至用户手机上。

3.2 STK 原理

STK 是用户识别应用开发工具 SIM Tool Kit 缩写，是一组用于开发增值业务的命令，实际上是一种小型编程语言，它允许基于智能卡的用户身份识别模块 SIM 运行自己的应用软件。STK 卡是一种智能卡，用于存储移动用户和运营商相关信息。

STK[19]卡是基于 Java 语言平台的 32K 卡片，可以固化在 SIM 卡中。可以接收和发送 GSM 短消息数据，作为 SIM 卡与短消息之间的接口，允许 SIM 卡运行自己的应用软件。这些功能常被用在可通过软件激活的电话显示屏上，用菜单界面代替传统"拨号-收听-应答"方式，用户可以通过按键进行复杂的信息检索操作。目前无线交易系统中常采用 SIM 与 STK 相结合的方案，该方案采用 3DES 加密和 MAC 校验，且拥有友好交互界面，所以程序菜单被写入 STK 中。方案模型如图 3-2 所示。

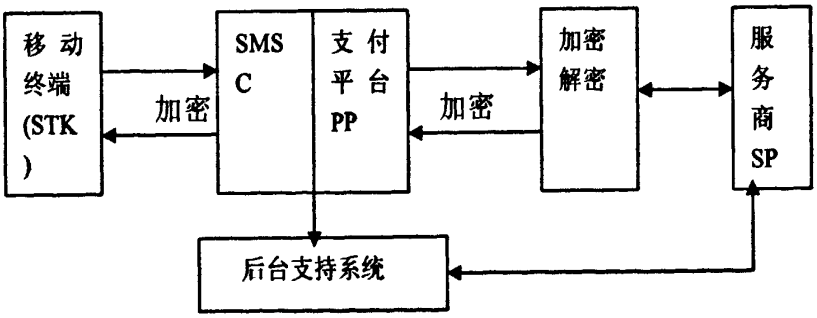

图 3-2

对于一种具体的短消息业务而言，信息数据需要经过 GSM 网络和互联网进行传输。在传输过程中，互联网有安全传输协议 SSL，GSM 也有安全规范，只要能保证短信息中心和短信网关之间采用点对点协议就可以解决问题。SSL 协议主要为应用层提供安全服务，而 GSM 规范主要是在于用户和网络间的认证，负责识别用户所用网络，认证用户是否是本网安全用户；点到点方案无法保证信息传输过程中安全性，所以基于短消息的解决方案应该使用端到端解决。

短消息系统由接入部分、短信息处理中心和短信网关三部分组成，所以分析短信系统安全须从此三部分着手。

(1)接入部分

短信息接入信息中心有两个阶段：移动用户和移动基站之间的无线通路和基站与 MSC、SMSC 间的有线网。短信息在无线通路中传输以明文形式，存有被窃听的危险，攻击者可以将信息窃听并截取，或是进行伪造。有线网间短信息传输也是明文形式，虽然 MSC 和 SMSC 间是内部网，有一定安全系数，但也不能完全保证短信息安全性。

(2)短信息中心

短信息中心安全性依靠短信息中心和外界间信息传递连接的安全和短信息中心数据库的安全。短信息中心和短信息网关之间通过 SS7(信令系统 7)连接，短信网关和短信中心则是 TCP/IP 连接。目前安全措施已比较成熟，主要威胁是 SMSC 数据库，数据库管理是数据库安全中很重要环节，数据库管理要保证不能非授权访问，同时数据库操作人员不能把信息数据非法使用。

(3)短信网关

短信网关是短信息中心和外部服务商 SP 之间连接媒介，一方面将 SP 提供给用户的内容交给 SMSC，另外用户的点播服务由 SMSC 经短信网关传给服务提供商。这两方面的网络通信都是基于 TCP/IP 网络，各采用不同协议，数据机密性和完整性仍存有威胁。

对于短信息系统总体而言，在短信息中心和短信网关间存在连接的弱保护，攻击者使用网络监听便可以记录下短信网关到短信息中心的登录口令字段。事实上，在短信网关和短信息中心间，往往会有防火墙存在，但是短信息中心和网关并非运行在防火墙之后，入侵者便可以利用此漏洞伪造原有网关，进入短信息中心进行短信息处理。

3.3 安全解决方案研究

传统的短信息服务中，短信息服务器系统会根据客户的实际服务请求，来提供各种相应服务。在提供服务时需要进行身份认证，对用户身份进行确认。一般身份认证采用口令方式，即用户将自己身份信息与口令发给服务器，然后服务器查看数据库中用户身份信息是否存在以及验证用户口令是否正确；对于正确且通过验证的口令，则可以对用户请求进行响应，反之，则拒绝对用户服务。

用户将自己身份和口令信息发至服务器过程中，存有被黑客窃听和截取的危险，黑客通过相应技术手段窃听到用户信息。防止被截取和窃听的方法就是对用户的口令信息进行加密，以密文形式进行传输；这种方式不能抵御重传攻击，黑客仍然可以截获到口令密文，仍然可以重新冒充合法用户身份请求服务。对于重传攻击可以采取一种认证方式，即当服务器响应用户的请求服务时，给用户发送一个随机数或是时间戳，用户在收到随机数后，利用本身口令信息对随机数进行计算，然后把结果回执给服务器；服务器收到回执结果后，也利用口令函数对随机数进行计算，若计算结果和收到的回执结果相同，则可以确认用户的真实性。

设计思想中提到对于随机数的计算结果，就是计算机消息验证码。因为用户端和服务器端使用相同的认证方式，就是口令函数，对于相同的随机数而言，计算结果肯定是相同的。系统结构框架引入短信安全服务器，框架模型如图 3-3 所示。

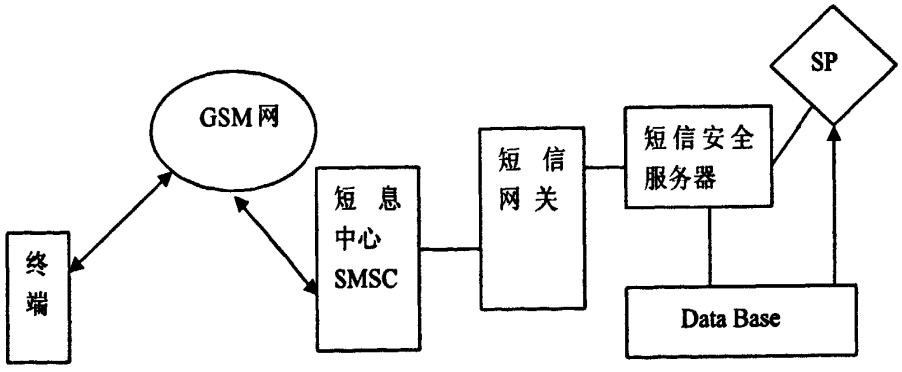

图 3-3

如上图所描述，短信安全服务器连接短信息网关和内容服务商 SP，对传输的内容信息进行加密。除加密功能外，短信安全服务器还可以进行短信息 Mac

值校验，对 Mac 值进行验证，保证数据信息完整性。用户向服务器发送的请求报文和服务器回执给用户的报文格式中，都有序列号，安全服务器采用基于序列号同步确认技术，来确认用户真实信息。随着 SIM 卡存储容量的扩增，且多支持 OTA (Over the Air)下载机制，可以对菜单实时更新。

短信息安全系统能完成对于用户发送数据的加密和认证功能，还可以对服务商发送给用户的回执服务信息进行封装加密。按照同客户端约定的加密算法对通信消息进行加解密工作，提供对于用户身份的验证，通过校验阶段对数据内容的完整性和有效性进行分析。

用户和服务商进行通信时，通过选择 SIM 卡中预制的菜单,从终端上输入信息请求内容；终端设备上的 SIM 卡经过加密认证，用户通过 SIM 卡向短信息服务器发送被加密的短信息内容，信息内容经过 SMSC，经过短信息网关最后发送至短信安全服务器。当短信安全服务器收到信息内容时，对信息内容进行解密操作，确认信息有效性，并完成对于用户身份的确认。短信息被短息服务器认证后，存在数据库 Data Base 中，传送给服务商。服务商收到用户的请求信息并为用户提供信息服务后，短信安全服务器便可以对服务商提供的内容进行认证和加密工作，保证用户收到信息的完整性。

认证过程如下：

1、用户在手机上输入请求内容，暂存与 SIM 卡中。

2、手机 SIM 卡进行密钥分散，产生会话密钥 K1。.

3、SIM 卡用 K1 对 SIM 卡内请求内容加密。

4、加密后，SIM 卡进行认证封装计算数据 MAC 值。

5、手机用户向安全服务器发送信息 Data。

6、服务器收到 Data 后，对主密钥进行分解得到会话密钥 K1，检验用户请求数据 MAC 值，对两 MAC 值校验，相等则进行协议步骤，不相同则转为错误处理。

7、服务器进行解密，存入数据库中，等待 SP 应用处理，将结果发至用户。

除外，安全服务器对于所提供的交易内容等信息，由于信息的重要性，需要服务器有备份功能，可以采取计划事务方式来进行对内容信息的安全备份，并可以进行升级扩容。

上述方案模型具有以下特点：

1、具有身份认证功能。收发双方都是有约定的口令密钥，能确认身份。

2、通过 MAC 值校验，保证信息完整性。

3、信息传输过程中对信息加密。

4、可以抵御重传攻击。采用 MAC 值校验和同步序号状态判断，可以有效识别并防止重传攻击，避免资源浪费。

3.4 SMS 商务方案特点

基于 SMS 移动商务方案中需要实现对于移动终端、SMS 网关以及服务器端得认证。对于移动终端的认证是通过对于终端本身安装的 SIM 卡实现，交易实现时由运营商服务器来获取终端 SIM 卡中的密钥信息，来确认此身份是否合法；系统中同时存有很多种服务内容，短信息系统通过对内容服务器进行 CA 认证进而可以确保用户可以收到请求内容信息。

对于 SMS 商务方案，虽然可以有相对比较安全的交易方案，但是由于 SMS 以及终端本身的限制，例如手机内存不够、不能支持复杂的算法、存储能力有限和 SIM 卡容量有限等缺点，本方案更加适用于一些小额数目的商务应用。

短信息安全平台系统应具有很多功能实现，包括有加密功能、认证功能、防止重传功能和日志功能等。系统在终端和短信服务器间传输的信息进行加密工作，实现消息内容的私密性，在认证过程中，采用序列号同步双向认证机制，保证消息请求时由合法用户发出；对于重传功能的防止则是通过对于两个 MAC 值结果的校验以及判断同步状态，来防止重传；系统的日志功能用于对于交易相应信息的查询和记录功能。

基于 SMS 的移动商务方案，也具有自己的独特优势。首先是成本较低，且服务内容多样化，所需各种服务功能均可由 SMS 服务系统自动实现；其次，由于手机终端的便携性和移动性，使得用户更加容易获取到相应商业信息，进行商务活动，方便易行；最后，用户和运营商之间定制各种服务，可以根据自身需求以及喜好来实现个性化定制，由用户自己提出需求，消费者心理容易得到满足。

另外，移动商务系统对移动终端实现认证时，涉及到密钥信息的交换，密钥信息存在于终端 STK 卡中，用户须不断进行更换 STK 卡，而 STK 在容量方面始终存有不足，相应存有一些问题制约移动商务交易发展。

3.5 本章小结

基于 SMS 的移动商务方案是移动电子商务安全解决方案之一，是一种比较简单的实现模式，目前而言，多适用于小额数目交易费用。基于 SMS 业务方便、简单并且价格比较低廉；同时，基于 SMS 的移动电子商务的安全性也是一个不可忽视的问题。由于手机等移动终端相对于计算机终端而言，处理能力和存储能力有限，并且基于互联网的安全协议和一些复杂加密算法很难在上面实现。

第 4 章　基于 WAP 移动电子商务方案

4.1 WAP 介绍

WAP 即 Wireless Application Protocol 缩写，即无线应用协议，是应用于无线通信网络的工业标准，具有开放性和可扩展性。1997 年 9 月，WAP 论坛[20]上发布了第一个 WAP 标准框架结构，并于 1998 年 5 月份推出 1.0 正式版本，包括了 WAP 协议栈和 WML 等，2000 年发布了 WAP1.1 版本，并在 2001-2002 年间发布了 WAP1.2 和 WAP2.0 版本。其中 WAP1.2 版本在原有基础上增加了诸如 Push 和用户代理结构以及 WIM (WAP ID Model)等功能，WAP2.0 为加强 WAP 实用性而设计，适应了当前高宽带和高速传输的行业要求。

WAP 是一种与平台无关的协议，用户可以利用无线设备通过无线网络方便地访问网上信息。作为移动通信技术和互联网技术相结合的产物，WAP 使得用户能突破网络制式和运营商间的差别限制，根据自己需要访问网络资源。作为新兴的网络接入模式，WAP 技术的应用和发展为电子商务提供了一个广阔平台和发展空间。

4.2 WAP 协议结构

典型的 WAP 模式应用系统由三部分组成，即移动终端，WAP 网关以及 WEB 服务器。

移动终端即客户端，可以包括有移动手机或是 PDA 等终端设备。

WAP 网关是连接用户以及服务器的桥梁，实现 WAP 协议和互联网协议间的信息转换，并且可以进行压缩编码，可以优先减少网络间传输的数据量。

WEB 服务器是互联网上的服务器，可以提供用户所请求内容。

WAP 网关从服务器上将请求下载的内容进行转换并传送至 WAP 终端设备上，WAP 可以提供一个包括有浏览器和脚本解释器的终端应用环境，这个环境可以使得客户端上能显示出所接受到的内容。WAP 浏览器可以处理 WML 语言，可以运行脚本，解释 Wml Script 编写的内容信息。

WAP 应用的工作模式[21]如下：

1、首先 WAP 终端向服务器发送访问请求，用户代理将编码后的 Http 请求无线接口传输给 WAP 网关；

2、网关接到终端的请求信息后，对信息进行编码处理，读取其中信息，经解析后把标准的 Http 请求通过网络发送给 WAP 服务器。

3、服务器将所请求内容反馈给 WAP 网关，网关则把接收到的信息内容进行压缩处理再发至用户手持终端上，内容由显示屏进行显示。

WAP 包括 WSP(Wireless Session Protocol)，WDP(Wireless Data Protocol)，WTP(Wireless Transaction Layer)，WTLS(Wireless Transport Layer Security)，WAE(Wireless Application Environment)。

WAP 体系结构[22]如图 4-1 所示。

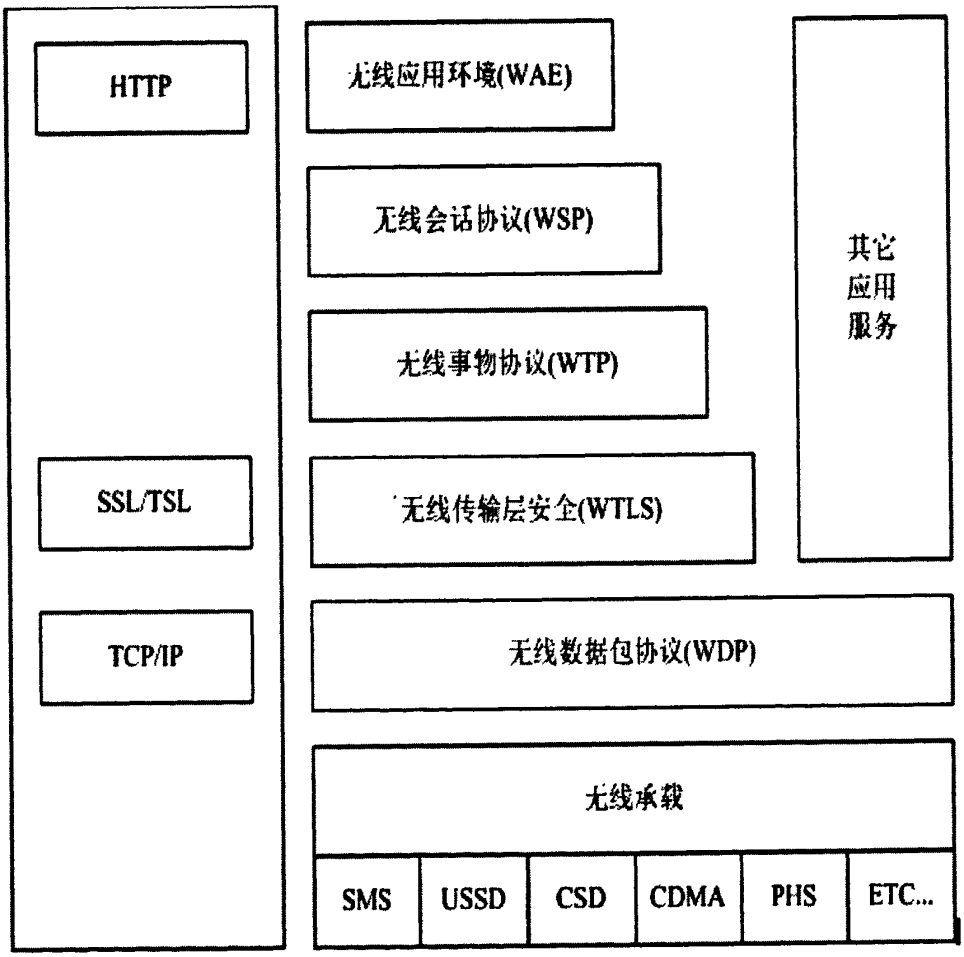

图 4-1

WAE 是 Wireless Application Environment 的缩写，即无线应用环境。WAE 具有浏览器、解释器等功能，提供一个可以供用户和服务提供商之间互操作的安全环境。

WAE 包括有微浏览器、WML 和 WML Script 功能[33]，其中微型浏览器将终端接收到的信息内容显示在设备上，是和 WAP 应用系统进行信息交互的软件环境；WML 和 WML Script 解释报文形成 WAP 内容，最大限度利用小屏幕进行显示；WML 和互联网标记语言 Html 类似，都是具体运用 XML 语言，可以进行处理和输入输出的功能，WML Script 是应用程序接口，可以允许 WML 加密数据库给出相应安全特性，这些特性内容包括密钥对的产生以及数字签名和密钥管理相关信息，在 WML 基础上增加了计算功能，使得终端设备更加智能。

WSP 在用户客户端和服务期间进行信息交换，在用户端和服务器端建立释放连接。相对于 Http，增加了相应的"PUSH"功能，此功能可以方便服务器直接将信息内容发至用户端；WSP 使用经过压缩编码的二进制 Bit 流在用户端和服务器间传输，传送效率相比 Http 提高不少。WSP 还可以基于相同的借口提供 WTP 层上基于连接的服务以及相应的 Push 功能，Push 是信息推送功能，该功能最主要的是在于信息的主动性以及信息的及时性。

WTP 是无线事务处理协议，运行在数据报服务之上。事务可被解释为一个用户端向服务器端请求并收到服务器返回信息的整个过程，本协议和 TCP 协议相仿，可以提供可靠连接，并可在无线网上高效运行。WTP 总共定义了三种事务服务[34]：

1、Class 0：提供不可靠且无应答的请求。

2、Class 1：提供可靠且无应答的请求。

3、Class 2：提供可靠且有应答的请求。

WTP 有以下特点[38]：

1、提供上述三种级别的事务服务。

2、对收到的每条信息确认，保证用户间信息可靠性。

3、可以进行协议数据单元级联并能延迟确认。

4、通过重发和确认机制为上层协议提供可靠连接。

WTLS 是无线传输安全层，在 TLS 协议基础上发展而来，可以为上层提供完整性校验和身份鉴别等安全功能。WTLS 可以保证信息在用户终端和服务器间传递过程中的数据完整性，并且可以保证传输中的信息安全性，保证数据不会被截取和攻击。WTLS 定义了 3 中服务类别：

1、Class0：提供安全通信通道，采用非对称密钥算法来交换公共密钥，再利用对称算法对数据进行加解密操作，但不能鉴别通信双方，不能抵御中间人攻击。

2、Class1：可以提供 Class0 中的服务，并且比第一类服务多了对于服务器的鉴别。

3、Class2：能提供包括有 Class1 的功能，还能对服务器和用户进行鉴别，防止对于用户身份的冒用。

WTLS 是 WAP 安全模块，为 WAP 提供包括有加密和数据完整性鉴别服务。服务主要可以分为四部分：使用数字签名和公钥证书实现对于移动终端和内容服务器的鉴别,；在移动终端和服务器间保证传输数据信息保密性；保证信息在传输中的完整性，包括信息包不被更改或是删除；最后可以对 DOS 服务进行有效保护，能检测重传。

WDP 是无线数据报协议，在 WAP 协议栈的最底部，可以支持不同网络类型，可以适配不同网络载体，进而实现和底层无关的特点，可以运行在 SMS、USSD、GPRS 等不同承载之上；作为一个通用传输服务，WDP 对上层提供了通用的数据接口，提供对于上层协议不可见的独立的网络技术平台。WDP 可以服务上层协议，提供有地址服务和数据管理服务，并可以对下层网络数据包拆分进行重组和分段，有长格式和短格式两种。

SMS 承载方式中，接受和发送短信息仅需要通过信令通道，不需要通过短信业务通路；短信息系统中，在上节中基于 SMS 方案中已介绍，短信息中心 SMSC 作为短信息处理中心，当 SMS 作为 WAP 承载方式时，SMSC 便成为无线数据报网关。SMSC 通过接受发送短信内容和 GSM 网络中的用户设备交换数据信息，在和 WAP 服务器通信时，则是通过 SMPP，即短信息对等协议。不过，SMS 不支持 IP 协议，传输能力也有限，只是作为 WAP 承载方式的一个补充。

利用 GPRS 作为 WAP 的承载方式比较方面。GPRS 即通用无线分组业务，是 GSM phase2+阶段引入的基于分组的数据业务，在原有 GSM 网基础上叠加了一层网络，组成 GSM/GPRS 网，增加了相应实体，诸如：GPRS 服务支持结点 SGSN，GPRS 网关支持结点 GGSN 和计费网关等。

GPRS 可以实现空中接口至外部网络间的分组数据传输。GPRS 无需拨号连接，采用分组交换模式，与网络保持实时连接，可以实时通过网络进行信息收发和传输，并且具有高达 177.2kbits/s 的无线接入速率，在线时间长短不是此项业务收费依据，收费依据是所花费流量的多少。GPRS 数据业务交换传输速度相

对于 GSM 网快了 9 倍，相对于 SMS 和 CSD 承载方式而言，所需耗费较少。

另外，GPRS 网连接 GSM 和因特网，在用户设备和 WAP 服务器间提供 IP 通路。若是通过 GPRS 提供 WAP 业务，需在用户终端和 WAP 服务器间建立 WAP 协议栈，如图 4-2 所示。

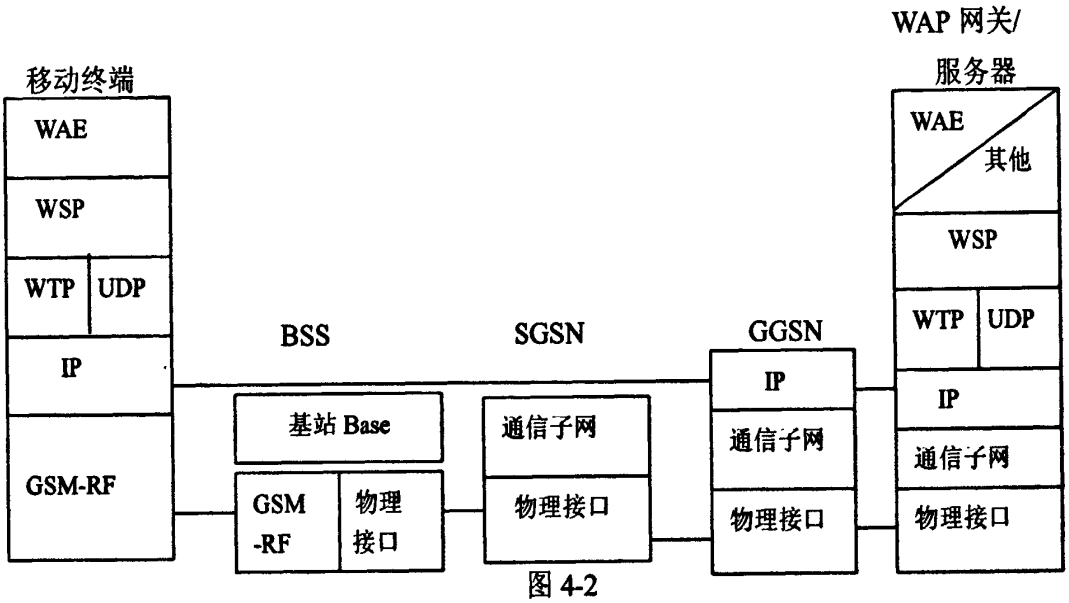

图 4-2

此时当 GPRS 可以支持 IP 协议，数据包协议不是 WDP，变为 UDP/IP 协议。

4.3 WAP 协议分析

WAP 协议标准分为 WAP1.x 和目前的 WAP2.0 版本，WAP2.0 实现了对于 WAP1.x 版本的兼容。WAP 各版本推出时间和特性如图 4-3 所示。

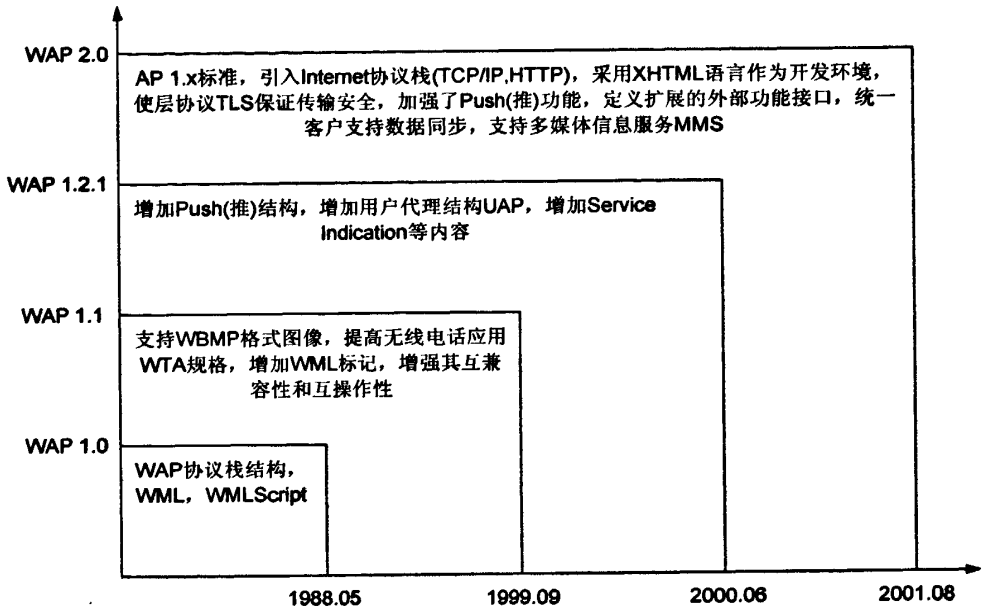

图 4-3

WAP1.1 安全性依赖于协议中的无线传输安全层协议，可以保障传输层数据的机密性以及信息内容的完整性。WAP1.1 中支持 WBMP 格式图像，提高了无线电话应用 WTA 规格，并增加了 WML 标记，增强了互操作性和兼容能力。WAP1.2 中对版本 1.1 进行了改进，加入了 WIM 规范和 WMLScript 作为 WML Script 的应用开发库。

基于 WAP 的移动电子商务模式，在设计上通过 WTLS 安全传输协议将移动终端和 WAP 网关连接起来，服务器系统提供对于用户身份验证和数据签名功能。WAP 网关负责 WAP 终端与网关以及网关和内容服务器间信息交互，具有协议转换和编解码功能，是终端设备和万维网链接的桥梁。

WAP1.x 协议中，存在端到端的安全问题。WAP 接入方案具有较为较强安全机制，但由于数据在移动终端和网关之间采用 WTLS 信道传输，而在网关和服务器系统之间采用 TLS 信道[35]，因此在 WAP1.X 协议中存有端到端(P-P)的安全问题。用户设备上仅适用于二进制信息数据作为交互形式，服务器上是以超文本标记语言 HTML 作为格式，所以在二者间的数据传输在 WAP 网关中需转换为明文形式，而未经加密的明文则存有被第三方攻击或篡改的安全隐患。

目前对于这种端到端的安全隐患，主要是尽量避免数据以明文形式出现在网关中，可以通过建立具有 WAP 网关的 WEB 服务器，使得原本作为中间媒介的网关作为运营内容服务器的一部分，不需要数据作为明文出现，数据被加解

密后直接提交给服务器；或是通过保证数据明文信息不再磁盘中读写，快速在内存中完成信息的加密和解密工作，使得被占用的内存空间可以在释放前被覆盖，在软管理上为保证网关安全，可以加强对系统访问权限的控制。

WAP2.0 中实现了对于 WAP1 版本的兼容，可以完成在 WAP1 中的安全操作，并在原有基础上增加了新的安全规范。对于 WAP1 中的网关隐患的问题，进行了改进。WAP2.0 加入了对于 TCP/IP 和 HTTP 等互联网协议的支持，使得互联网协议可以在用户终端和因特网间能互相运行。WAP2.0 协议结构如图 4-4 所示。

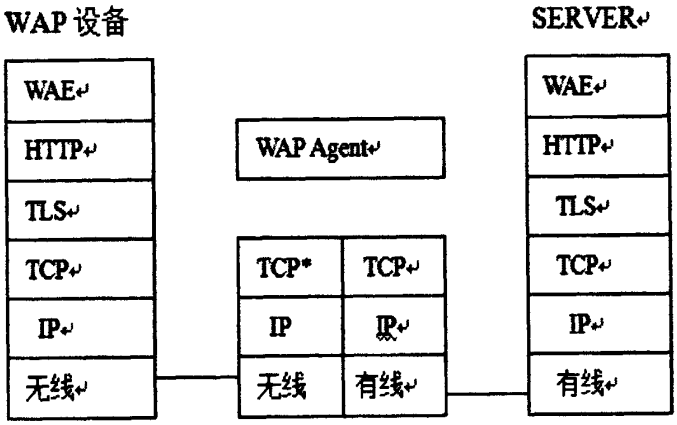

图 4-4

WAP2.0 中，支持 TCP 协议，可以在终端 WAP 设备中使用，安全套接层 SSL 和 TLS 传输安全层可以保证传输层的安全，相比 WAP1 中存有的端到端的安全问题，2.0 版本便可以解决。

TLS 协议中有几种协议，包括握手协议、记录协议和警告协议等；握手协议和警告协议相对记录协议，在 TLS 中处于上层。记录协议可以封装多种应用层协议，握手协议则在用户和服务器传输信息时服务，建立握手连接。

WAP 引入了无线 HTTP，即 Wireless HTTP[36]和 TLS 以及无线 TCP，即 Wireless TCP，目的是通过引入 TCP 协议来实现对于大容量数据的传输和传输层的安全，还用于和国际标准 IETF 保持一致。

无线型 TCP 可以实现和标准 TCP 协议的互操作，无线 TCP 优化包括大窗口长度和窗口比例以及环回时间测量等。WAP2.0 中 TLS 替代了 WTLS，可以解决 WAP1 版本中存有的安全问题。

TLS 握手协议中，和 TCP 三次握手类似。客户端和服务器端进行握手建立会话连接，首先是用户端向服务器端发送连接请求，建立 TLS 安全链接，然后

在此链接上进行信息通信，最后链接关闭，释放通道。若是在建立通信连接的过程中，发生了错误，需要把错误信息反馈并进行记录，通知建立连接的双方，称作是警告协议。

TLS 建立安全连接过程具体如下：

1、客户端 Client 向服务器 Server 发送 Client_Hello，包括有协议版本，随机数，客户端支持的加密算法以及压缩方法等内容信息。

2、服务器回执 Server_Hello 内容包括有版本，从客户端加密算法选择的加密算法，压缩方法等；Certificate 证书，用于认证服务器需要；Server Key Exchange 作为对服务器证书信息的补充，用于客户端对于证书信息的确认；Certificate Request 用于对客户端证书的请求需要。

3、客户端若收到证书请求，则发放客户端证书；与客户端密钥交换信息，然后对完成对证书的确认。

如上述过程，整个 TLS 中的 Handshake Protocol 用于完成以下几个功能，包括客户端和服务器间的密码算法的选择、算法中随机数的选择以及对于双方的认证。

4.4 WAP 安全结构

WAP 安全架构包括 WTLS、WPKI、WIM、WML Script 四部分，其中 WIM 是无线身份模块，WML Script 是无线标记语言脚本。WTLS 是无线环境下的传输协议，可以保证移动终端和无线网关间的安全传输，有线传输环境中的 SSL/TLS 可以使得 WAP Gateway 与服务器间的安全传输，二者联合 TCP/IP 协议共同构成安全协议结构。WAP 安全架构如图 4-5 所示。

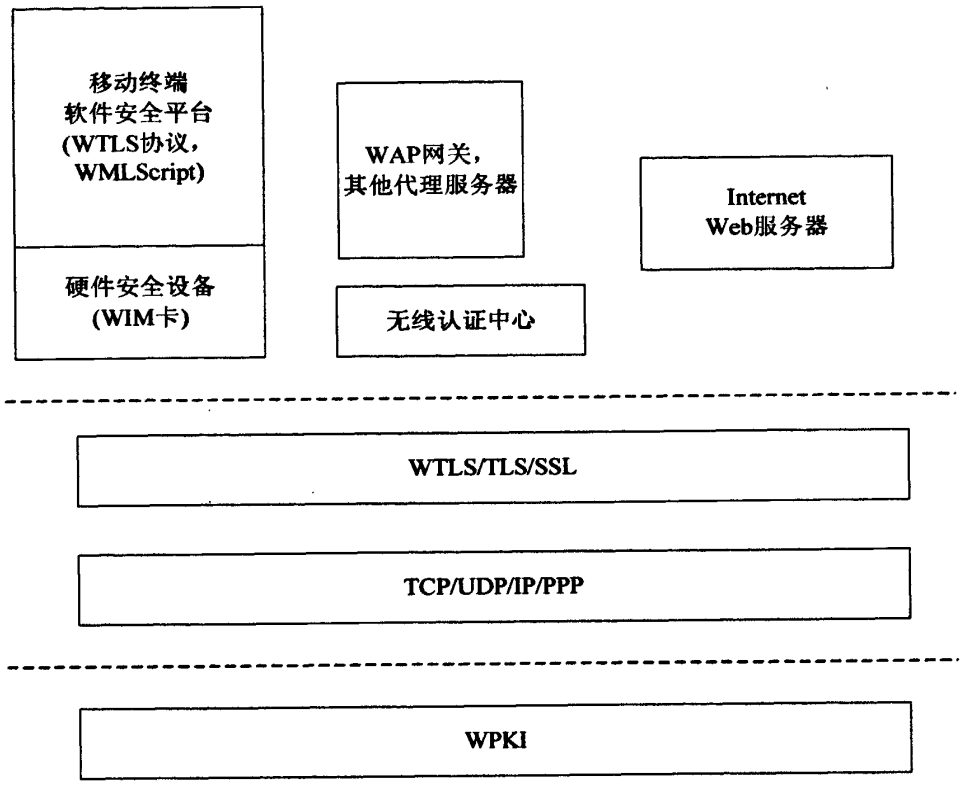

图 4-5

WPKI 是无线应用公钥基础设施，全称是 Wireless Public Key Infrastructure。WPKI 是在 PKI 基础上的优化扩展，PKI 是公钥基础设施，是一种遵循既定标准的密钥管理平台，可以为网络应用加密和进行数字签名，所包含的基础技术有加密、数字签名、数字信封以及双重数字签名机制等。

和 PKI 相仿，WPKI 也可以实现对于电子商务应用中的关于证书的管理以及加密等方面的机制和策略。WPKI 系统包括有 PKI 客户端、证书注册中心和一个认证中心 CA 以及证书库等部分，其中 CA 是签发证书的机构，是第三方部门，在整个 WPKI 系统中出于核心位置；用户向 CA 中心申请证书，通过 RA 进行注册验证，RA 还可以实现对于用户身份的认证。

WIM[37]是无线应用身份模块，作为安全平台的一部分，作用在安全层和应用层，在这两层上起到增强安全的作用，主要用于存储和处理用户的身份信息，用于对用户身份的识别以及对身份的验证等。WIM 通常是被集成在用户终端的智能卡上，具有 WIM 功能的智能卡以 ISO 7816 标准为基础，采取了类似 ISO 7816 的标准接口，也适用于非 WAP 方面。另外 WTLS 协议运行在 WAP 网关与用户终端之间，WIM 可以通过嵌入与智能卡上的密码算法(RSA 或 DSA)来实现

对于双方的验证。

Wml Script[38]是一种脚本程序，可以运行在用户移动终端设备上，与脚本语言 JavaScript 类似。JavaScript 可以嵌入到超文本标记语言 Html 里，而 WmlScript 在被无线设备采用前就已预先编译。Wml Script 基于 JavaScript，是 JavaScript 的一部分，并且在 JavaScript 基础上进行了相应扩展。

4.5 WAP 应用模型实现

前面对 WAP 协议分析中指出，WAP 系统是由用户终端，WAP 网关以及 WEB 服务器组成，WAP 会话的建立就是在上述三部分之间进行。整个 WAP 会话过程包括两个部分：用户终端和 WAP 网关之间的信息传输和 WAP 网关与 WEB 服务器间的信息传输。WAP 会话过程如图 4-6 所示。

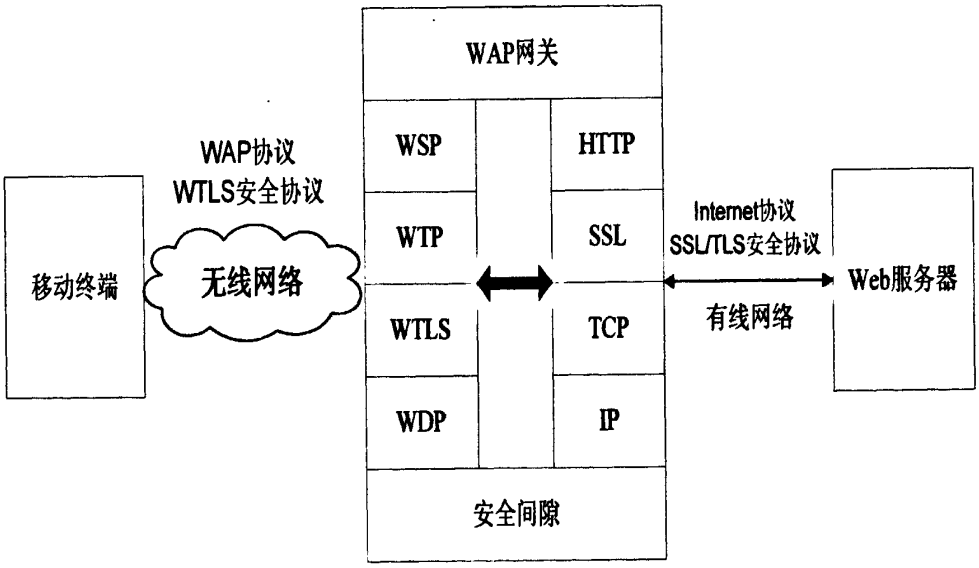

图 4-6

由上图可以看出第一部分即用户终端和网关间会话，经由无线网络传输，由 WTLS 协议来保障传输安全；第二部分在网关和服务器间则由安全套阶层协议 SSL 和传输安全层协议 TLS[39]来保证信息安全。

数据在用户终端和服务间间进行传输，由网关来实现对于 WTLS 和 TLS 协议保护的数据的转换功能。数据在上述两部分间的传递通路是相对安全的，但是在 WAP 网关处由于数据信息需要被提取，以明文形式被显现，存有“数字鸿沟”问题。对于“数字鸿沟”问题，前面已有相应解决方案。下面介绍一种端

到端的安全模型方案：WTLS 隧道模式。

类似于 VPN 模式，把需要通信的链路以“隧道”的封闭模式来保证安全传输。在 WTLS 隧道模式[40]中，用户终端仍然完成对于数据信息的加密工作，不同的是当 WAP 网关收到经 WTLS 加密的消息之后，并不进行转换提取，而是直接经 TLS 对加密信息进行重复加密。当服务器接收到信息后，首先对 WAP 网关的 TLS 加密信息进行解密，再进行 WTLS 解密。当 WAP 服务器将信息回传给用户时，也是经过两次类似加密和解密过程。

基于上述隧道模式来保证数据信息传输过程，下面给出一种利用加密算法和数字签名技术来保证信息安全传输的方案研究。

数字签名[41]过程如下：报文发送方用散列函数在报文文本中生成报文摘要，称为散列值。发送方用私钥对散列值加密形成报文附件与报文一起发送给接收方。接收方用与发送方相同的散列函数从接收到的原始报文中计算出报文摘要，再用发送方的公用密钥来对报文附加的数字签名进行解密。最后对两个散列值进行验证是否相等，若相等则可以确认该数字签名是发送方的；若不相等，则确认信息被篡改，从而来保证消息内容的完整性和安全性。

方案实施如下述过程：

设定 K_a 为服务器端公钥，K_b 为用户端会话密钥，Kc 为服务器私钥，终端发送的信息内容为 M。

1、服务器端将 Ka 发给用户端。

2、用户端使用加密算法生成 K_b。

3、进行 $E_{Ka}(K_b)$，发给服务器。

4、服务器用私钥 Kc 解密，$D_{Kc}(E_{Ka}(K_b))= K_b$。

5、用户端进行 HASH(M)=m，m 作为消息摘要。

6、用户端进行 $E_{Kc}(m)$，即数字签名。

7、将此数字签名附加至原信息内容上。

8、用户端进行 $E_{Kb}(M)$，经 WTLS 协议发至 WAP 网关，再经 TLS 协议发至 WAP 服务器。

9、服务器端进行 $D_{Kb}(E_{Kb}(M))$，即得到 M 文件内容。

10、服务器端进行 $D_{Kc}(E_{Kc}(m))$，即得到消息摘要 m。

11、进行 HASH(M)，验证所得值与 m 是否相同。

经过以上步骤，通过数字签名来验证原有发送过来的信息是否经过修改，

从而保证原有信息完整性。

4.6 WAP 模型特点

基于 WAP 的移动商务安全方案，即是解决通过 WAP 模式实现移动商务安全问题。由于无线链路通道相比有线链路安全性较差，所以基于 WAP 的安全解决方案有着更高的安全需求，需要保证对于用户身份的认证，同时又能保证数据信息的私密性和完整性。WAP 模式下开展电子商务，需考虑基于 CA 认证[42]和数字签名以及加密等安全技术，还有 WAP 网关的安全性，信息在用户端和服务器端传输过程中，存有端到端的安全问题。上述给出的基于 WAP 解决方案可以在一定程度上实现端到端安全。

4.7 本章小结

基于 WAP 的商务方案是本论文的重点。本章 WAP 实现方案，进行了详尽分析，里面包括了协议分析、加密技术、安全问题分析以及所存有的安全问题，并对可行的安全方案进行了研究。基于 WAP 模式的方案是现阶段发展的重点。

上述电子商务解决方案，在设计时需考虑到方案所要达到的安全目标，需要满足对于用户和服务器的身份认证问题，确保非正常用户介入；都需要保证信息传输的安全性，一般是对数据进行加密，保证信息完整性和有效性。

基于 WAP 商务方案，分析了 WAP 协议栈的相关内容，对于其安全机制进行了分析，主要是依靠 WTLS 来实现。WAP 系统安全需考虑到各个参与实体的安全性，WAP 网关在系统中是个中间角色，起着“翻译器”[43]的作用，但是也存有“数字鸿沟”安全问题，文章中给出了相应分析，包括存在问题的原因以及可行解决办法。

第5章 移动电子商务安全管理

5.1 移动商务安全管理制度

移动电子商务是伴随着信息网络技术和通信技术发展起来的，作为一个时代的产物，其产生带着强烈的时代标记。移动电子商务的发展[44]也在逐步走向成熟和完善，安全性能也在不断得到加强和改进；作为社会经济活动的一部分，在推动社会经济不断增长和保证经济安全方面，发挥了重大作用。

移动商务是个不断发展的概念，是电子商务发展的新形势和新阶段，当前在安全管理制度方面还是存有不少问题。

移动电子商务安全管理制度是一种行业规范和准则，目的是为保障移动电子商务的正常开展。主要范围包括以下几方面内容：人员管理制度、保密制度和系统维护制度等。

5.1.1 人员管理

移动电子商务是在电子商务基础上发展而来，是通信技术和传统电子商务的有效结合。从事电子商务的人员都是知识分子，既有专业基础知识，同时还有比较强的操作能力。商务活动参与人员是市场经济条件下企事业单位进行经济活动的主体，和商务系统的安全有着直接关系。因此，对于商务系统的参与人员的管理就显得十分必要。

1、要在商务人员的选拔上进行把关。选拔一些立场坚定、有知识、懂管理的人员来任职。

2、对上岗人员进行培训。对于相关上岗人员进行培训，内容包括理论基础培训、技术能力实践和相关管理技能培训，目的是提高商务系统参与人员的整体素质，尤其是安全意识。

3、严格落实安全责任制度。商务系统安全管理需落实到个人，实行责任惩罚制度，对于违反安全制度和规定的人员要及时教育并进行严肃处理。

4、实行激励保障措施。对于安全遵守管理规定并能很好完成安全任务的人

员实行激励保障措施，激发其工作积极性。

5、遵循交易系统安全运作的基本原则。比如对一些重要业务实行多人负责，相互制约；对于安全管理人员，要经常调换岗位；安全操作人员不得越权操作，只能在本职责范围内进行。

在本论文第二章介绍移动电子商务存有的安全威胁时，提到了非授权人员对于商务系统的非法入侵，对于这些非授权人员的管理也是属于对商务系统人员的管理方面。

5.1.2 保密制度

保密制度是为保障公司信息安全而设立的监管制度，目的是为了增强员工的安全保密意识，加强公司的保密工作。电子商务活动同样需要保密制度。

保密级别按照轻重级别不同，分为“绝密”，“机密”和“秘密”三种级别[25]。绝密是指最重要的秘密，若被泄露则会使公司利益得到特别严重损害，比如公司的专利技术和产品策略等信息；机密级别是重要的公司秘密，若被泄露则会使公司权益和利益遭受到严重损害，比如公司的财务报表和会议安排等；秘密级别指的是一般的公司秘密，若被泄露公司的权益和利益会遭受损害，比如公司的一些产品介绍或是人事档案等。

商务系统安全方案中，经常会用到加密技术[45]，因此密钥管理也十分重要。密钥管理涉及到密钥的产生、分发、更新、存储和销毁等方面。对于商务系统中用到的加解密密钥，要做好密钥管理工作。

5.1.3 系统维护制度

任何电子系统都需要经常定期维护，移动商务系统也是如此。系统管理维护人员要定期对通信基站、交换机和服务器设备进行维护，借用一些相应网关软件来完成对于一些网络设备参数的估计，判断系统是否正常工作。对于系统软件方面，则是包括对支撑软件和应用安装软件的维护。对于系统支撑软件主要是一些系统本身软件，包括有操作系统(OS)，数据库等，定期对系统进行优化，完成对数据库系统备份，最好采用双数据库系统来保障信息的安全性；对于应用软件要做好版本控制工作[46]。

对于经常出现的木马和病毒，要做好防范意识，采取必要策略，通过安装

防火墙和杀毒软件来增强系统安全级别。

以上制度对于保障商务系统的安全运行会起到很大保障，关键在于这些安全管理制度能否得到真正落实，真正得到贯彻执行。

除了上述三点之外，还应加强对于移动服务市场的安全监管工作，对于利用手机或是其他终端设备进行通信的用户，要进行实名身份认证，运营商对于用户注册信息需做好保密工作，不得利用用户信息进行其他用途。一个成熟的商务系统安全方案包含很多专业领域内容，需要各方面通力合作，需要制定并执行信息系统安全管理制度，政府和安全机构做好安全监督和审查工作。

5.2 移动电子商务安全法制

移动电子商务是在国外源起并逐步发展起来，商务活动的正常开展需要信息技术做基础，另外还需要系统的管理制度以及完善的法律法规的建设。国外对于移动电子商务安全法制方面，早已立法，通过法律来监管电子商务活动的正常开展。我国电子商务发展较晚，尽管发展很快，但是很多方面还是不健全，当前我国还没有针对移动商务安全的专门法律。

对于移动电子商务交易安全的保护包含有两方面的内容：移动通信网络载体和电子商务。对于移动通信网络，则需要加强网络基础设施以及计算机方面的安全；电子商务交易本身是通过电子支付手段实现的商品交易，本质还是商品交易，涉及到一些经济法的内容。所以对于移动商务的法律方面的考虑，应该结合发展实际，赋予传统法律一些新的与时俱进的内容。

移动支付的安全实现仅仅依靠技术手段不能够完全保证，需要相关法律法规来保障。通过借鉴参考国际标准来制定一些适合本国国情的移动商务安全标准，全国人大会议需通过制定移动电子商务安全领域的法律条文。结合本国实际情况，根据时代发展需要，审时度势，与时俱进，不断完善国内安全领域法律法规，做到有法可依、有法必依、执法必严、违法必究，这样方能保障移动商务的正常开展。

5.3 本章小结

移动电子商健康发展需要科学技术作为支撑，也需要相关管理制度和法律法规来保障，法治社会要使得行业有法可依。本章节中对商务系统管理制度方面进行了三个主要方面的介绍和分析，包括人员管理、保密制度和系统维护方面；在商务安全的法律保障方面，国内还没有直接的法律法规，指出我国应结合我国实际国情，参考国外相关经验，尽快制定相应法律法规。移动商务的健康发展需要相关法律法规的保障。

结束语

伴随着互联网技术的发展以及移动通信技术的进步，电子商务发展到移动电子商务阶段，安全问题贯穿于这两个阶段，成为制约其发展的主要瓶颈。本论文主要阐述了移动电子商务的安全问题，分析了移动商务的安全需求、目前所存有的安全威胁和实现技术等，主要是对开展移动商务的两种承载方式进行了分析，给出理论上的安全方案，最后从管理角度和法律建设方面来阐述增强移动商务安全性的措施，认为仅仅依靠技术手段是不能够完全解决目前所存在安全问题的。

移动电子商务已经成为电子商务发展的新模式，发展迅速，随着3G网络的成熟和4G网络的研究，前途无限，必定会产生很大的社会效益和经济效益。与此同时，发展过程中所存有的问题也会伴随其中，安全仍然是个主要考虑点。对于安全，我们应该有正确的认识：

首先，安全是相对的，完全绝对的安全是不存在的。其次，安全不仅是技术层面的概念，同样需要管理和法律规范的参与。最后，安全是一个发展的概念，不同的阶段对于安全要求不同，其内涵会不断得到扩充。

本论文的目的是在分析移动商务所存有的安全风险基础上，得出安全解决方案，为移动电子商务健康发展提供综合的保障体系。但是由于时间、篇幅和笔者知识结构以及写作水平有限，本文不可避免的存有不足，对于一些问题的认识和分析方面存在不足；对于移动商务的安全解决方案，是从理论层面上实现，没经过具体实际应用，这些问题有待于进一步的深入研究。

随着网络技术和移动电子商务的不断发展，密码学理论和其他相关的安全机制和安全技术也会不断得到强化和发展；除了技术研究之外，移动商务的安全还需依赖于相关政策和法律法规的建设与实施，这些课题的研究不仅具有重要理论价值和实用价值，而且对于推动电子商务的发展有重要现实意义。

致谢

在本论文完成之际，回想起这三年来的学习生活，不禁心怀感激之情！我的每一点进步都与许多人的关怀和帮助分不开。

感谢我的导师赵宏中教授，感谢赵老师平日里对我的教诲和无微不至的关怀，他在学习上和生活上对我的言传身教让我获益良多。无论是做学问还是做人，赵老师的作风都潜移默化地影响着我，我对他充满了敬佩和感激。感谢武汉理工大学计算机学院所有的老师，感谢他们三年来对我的栽培。我在学业上的每一点点进步，都是和老师们的悉心培养是分不开的。在计算机学院的学习和生活，令我感到非常地充实和愉快，这也是我人生中至关重要的经历。老师们对我的教诲，我会一一谨记。

感谢和我一起生活和学习的同学们。感谢陈敏、李登付、刘中锋、於磊等同学，以及“真情年代”交流群中的同学们，和他们的相处总是愉快和有益的，感谢他们与我在课题上的探讨和实验上的配合，他们给了我很多启发和帮助。

感谢我的父母，他们为我的成长付出了巨大的心血。我能顺利完成学业，他们在我背后，默默无闻地付出了很多。

最后，对在百忙之中评阅本文的各位专家教授表示感谢，恳请各位专家评委对我的论文进行批评和指正。

参考文献

[1] 吴志平.ERP与电子商务的相关性研究[D].湘潭:湘潭大学,2004.

[2] 李锋.移动支付安全研究[D].济南:山东大学,2008.

[3] 成杨.移动电子商务安全问题研究[D].沈阳:沈阳理工大学,2007.

[4] 董尼.基于AES与ECC的混合密码体制的研究与实现[D].合肥:合肥工业大学,2006.

[5] 王伟.基于J2EE的智能小区信息管理系统的安全性研究与应用[D].武汉:武汉理工大学,2007.

[6] Fengwu Han, Yanhui Wang. Research on PKI-Based Anonymous Mobile Agent Security in E-Commerce[C],WuHan:The Fifth Wuhan international Conference on E-Business,2006.

[7] 张晓旻.移动电子商务——电子商务的新模式[D].武汉:华中师范大学,2004.

[8] 尚庆华.移动IP中安全问题的研究[D].西安:西安电子科技大学,2007.

[9] 王安定.蓝牙车载免提系统的开发及调频算法的研究[D].杭州:浙江大学,2003.

[10] Jian Tang,Jari Veijalinen.Using agents to improve security and convenience in Mobile E-commerce[R], Hawaii:The 34 Annual Hawaii International conference on System Sciences,2001.

[11] 徐瑶等.数据加密技术及应用研究[J].科技信息,2008,(32):83-83.

[12] 凌峰.电子商务中安全技术的探讨[J].商场现代化,2008,(36):136-136.

[13] 张娟.移动电子商务中的安全支付协议研究[D]. 西安:西安电子科技大学,2006.

[14] 吴洋.电子商务安全方法研究[D].天津:天津大学,2006.

[15] 何毅俊.WAP中WTLS安全性研究[D].长沙:中南大学,2007.

[16] Manvi S.S,Bhajantri L.B,Vijayakumar M.A,Security Payment System in Wireless Environment[R],WuHan:Future Computer and Communication,2009.

[17] 江红等.短消息业务SMS[J].重庆邮电大学学报:自然科学版,2001,13(2):43-46.

[18] 宋珊珊.基于WAP的移动电子商务安全支付协议框架的研究[D].上海:东华大学,2007.

[19] 郑琦.OTA业务下载平台的设计与实现[D].成都:西南交通大学,2010.

[20] Do Van Thanh. Security issues in Mobile E-commerce[R], London:Product Line Mobile E-commerce,2000.

[21] 肖艳等.WAP网关服务器应用及其与有线网结合[J].通信与信息技术,2006,(6):59-62.

[22] 李智勇.移动电子商务安全研究与设计[D].成都:西南交通大学,2006.

[23] 朱振荣.移动电子商务安全关键技术研究[D].北京:北京邮电大学,2008.

[24] Jie Zhou, Tian rui Zhou. Mobile e-commerce characteristics and safety Analysis[R], DaLian:

International Conference on Wireless Communications, Networking and Mobile Computing,2008.

[25] Tin-Wo Cheung,SamuelT.Chanson.A PKI-based end-to-end secure infrastructure for mobile E-commerce,Tokyo:21 st International Conference on Formal Techniques for Networked and Distributed Syestem,2001.

[26] Yuanjun Dai,Lihe Zhang. A Security Payment Scheme of Mobile E-Commerce[R], Tokyo:ICCT2003,2003.

[27] 范晓晖.移动电子商务安全研究[D]. 北京:北京邮电大学,2004.

[28] 邓娟,蒋磊.3G网络时代移动电子商务安全浅析[J].电脑知识与技术,2009,5(6):1314-1315.

[29] Lu Tao,Lei Xue.Study on Security Framework in E-Commerce School of Information Management[R],ShangHai: IEEE2007,2007.

[30] Zhuo Wang, Ran Hu, JianFeng Xu. Mobile E-Commerce Security Architecture[R], NanChang: GrC 2009,2009.

[31] 王晓莉.移动电子商务模式探讨与研究[D]. 北京:北京邮电大学,2006.

[32] 肖军.移动电子商务中的信息交换安全性[D].天津:复旦大学,2005.

[33] 程震.WPKI的研究及其在移动电子商务安全中的应用[D].济南:山东大学,2005.

[34] 罗清元等.数字签名技术的研究与应用[J].计算机安全,2008,(10):72-74.

[35] Feng Tian, Xiao-bing HAN. Study of WAP Mobile E-Commerce Security on WPKI[R]. NanChang: Second International Symposium on Electronic Commerce and Security,2009

[36] Yali Mu，Changxiang Shen. Building up Active-Defending Security Assurance Framework for E-Commerce[R],HangZhou: ICWMMN 2006,2006.

[37] 殷晓虎.电子商务的安全问题及对策研究[D]. 西安:西安科技大学,2006.

[38] 洪海等.一种基于WAP网关的系统设计[J].武汉理工大学学报,2005,29(1):30-33.

[39] Jiang Yi jun. The Security Of Mobile E-business,Brazil:CAEC,2004.

[40] Hua Jiang. Study on Mobile E-commerce Security Payment System[R],GuangZhou: International Symposium on Electronic Commerce and Security,2008.

[41] 朱振荣.移动电子商务安全关键技术研究[D]. 上海:上海交通大学,2008.

[42] Gai Jian hua.System Frame For Secure End To End Mobile Commerce[R], Brazil: CAEC ,2004.

[43] Miguel Soriano,Diego Ponce. A Security and Usability Proposal for Mobile Electronic Commerce[J]. Communications Magazine, 2002,(8):62-67.

[44] 张学植.移动电子商务业务安全解决方案[D].济南:山东大学,2005.

[45] Wang Shunman, Tao Ran, WangYue. Security Analysis on Mobile E-commerce[R].Xia Men:The 8th International Conference oil Computer Supported Cooperative Work in Design Proceedings,2004.

[46] 吴洋.电子商务安全方法研究[D].天津:天津大学,2006.

攻读硕士研究生期间所发表的论文

1.王大飞，赵宏中。基于LBS的移动电子商务模式分析.中国科技论文在线，2010.7