电子商务安全管理和支付

第九章 移动支付

上海理工大学 管理学院
管理科学与工程系 郭强
guoqiang@usst.edu.cn

目录

前言

移动电话拥有用户数量、互联网宽带介入用户数的巨大和不断上升，随着3G的到来，手机上网技术已经过数年的发展，给移动电子商务提供发展的沃土。

2008

•淘宝手机网开始运行，手机网站的推出，将推动移动商务的开展，可以看出，移动支付将迎来广阔的前景。

2007

•移动悄然在广东、湖北推出名为“移动影音书刊俱乐部”的B2C网站，让用户手机或者互联网登录该网站，就可以购买影碟、唱片、书刊、书籍等商品通过手机花费作为支付

2006

•当当网曾携手中国移动推出“手机当当网”，试图让消费者通过手机可以上当当网购物

9.1移动电子商务的特点

移动电子商务是基于无线网络，运用移动通信设备，如笔记本电脑、手机、个人数据助手（Personal Data Assistants，PDA），进行的商品交易或服务交易。

用户至少可以从移动电子商务中享受到4个方面的好处.

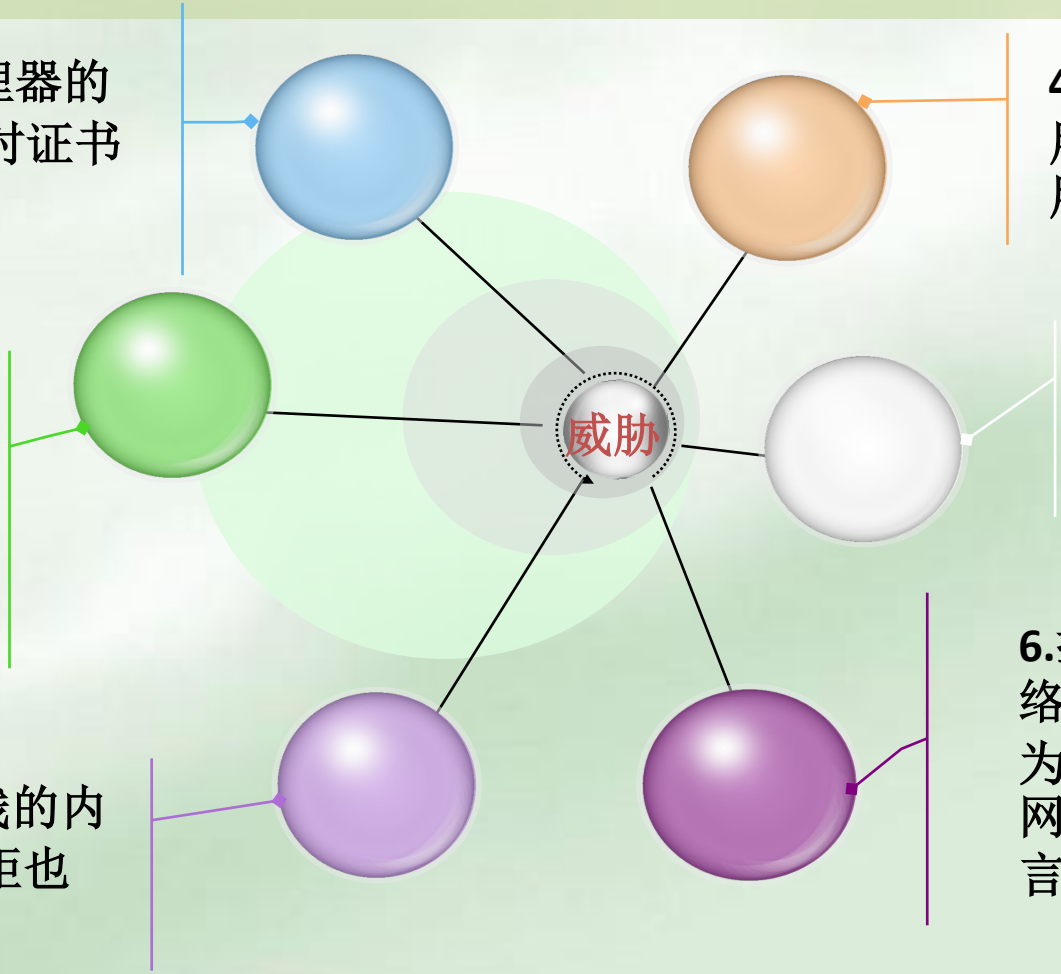
9.1移动电子商务的特点（续）

无线环境所存在的缺陷制约了移动应用的发展，特别是在考虑安全的时候。有限的资源状况对移动电子商务的安全构成了严重的威胁。

1.无线终端处理器的能力无法满足对证书事务的处理。

2.如果采用TCP/IP协议，9600比特的传输速率是无法保证稳定的网路连接的。

3.有线与无线的内存引起的差距也很大。



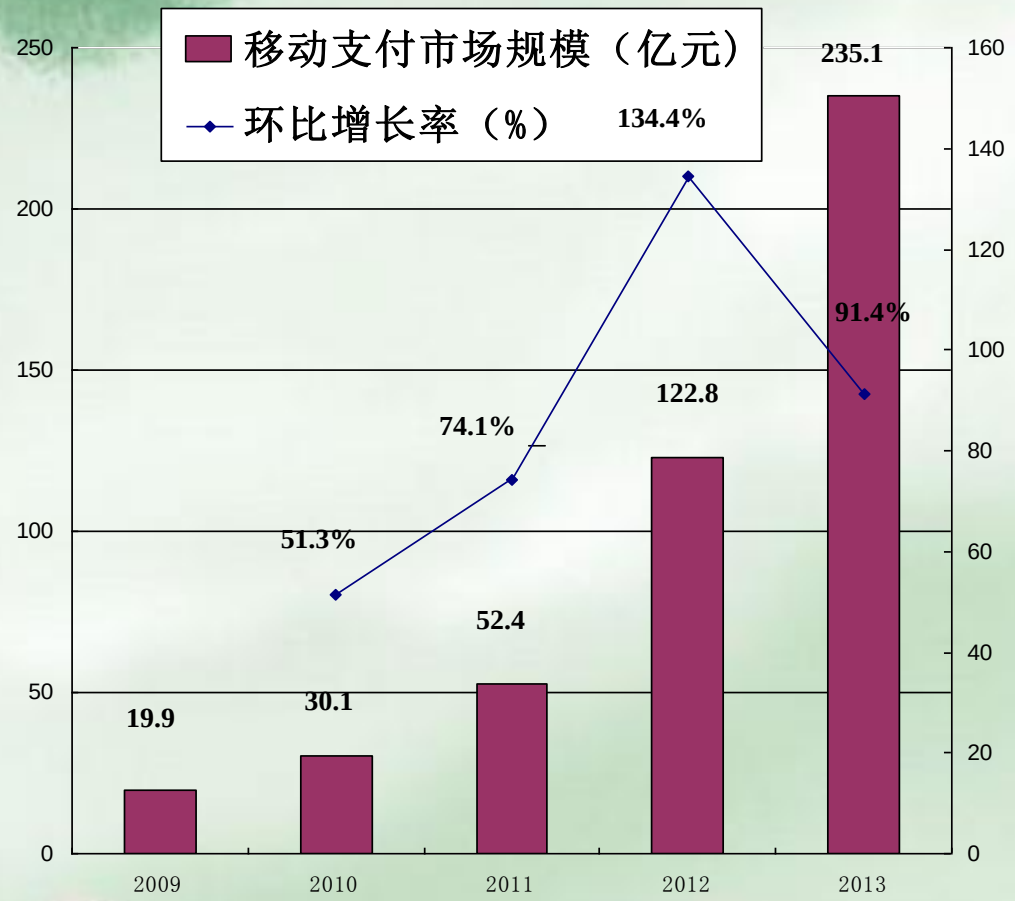
4.网路浏览器需占用大量资源，无法用于移动设备中

5.有线网络协议需要占用大量的资源，无法用于无线网络。

6.描述语言。有线网络采用HTML语言作为其描述语言，无线网路则采用WML语言来描述。

9.2移动支付的发展

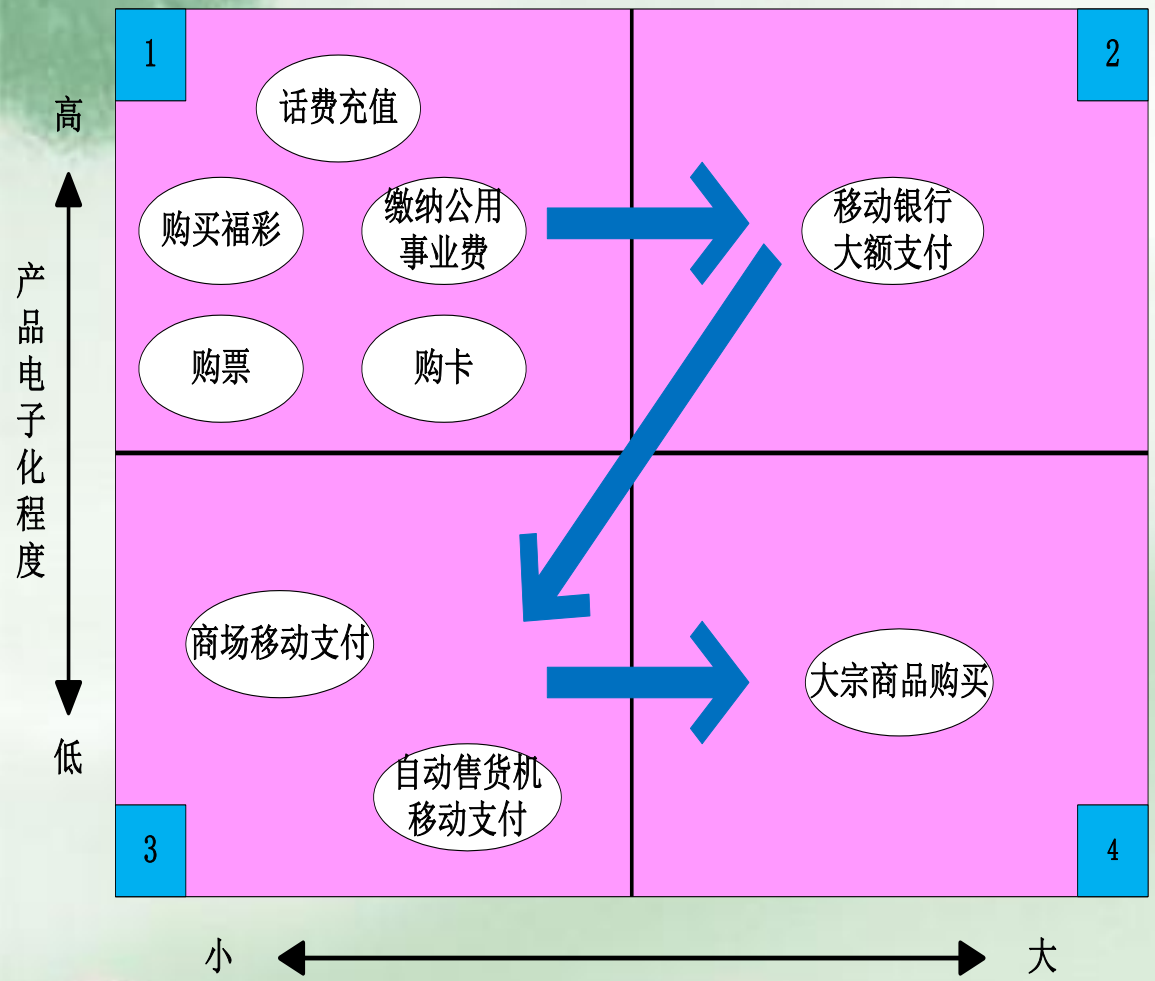
易观国际（Analysys International）预测，随着移动互联网业务的发展，远程支付将迅速发展，同时运营商和银联对近距支付推广力度也将不断增强。



2010年移动支付用户有望突破1.3亿，2011年达到2.2亿户。用户粘性的提升和更多近距支付业务的发展将使手机支付市场收入规模快速提升，预计2010年底市场规模将突破30亿元，2011年增长74.1%，共计52.4亿元，2012年则有望突破100亿元，市场收 入规模共计122.8亿元.

9.2移动支付的发展（续）

迄今为止的移动支付业务开展情况表现出如下特点。



(1)由于操作简便，运营商代收费成为移动支付推广的利器。

(2)以安全级别要求较低的小额支付为主。

(3)业务以无需与商户终端相交互的方式为主，所购商品大多为电子形式的商品，系统建设成本低。

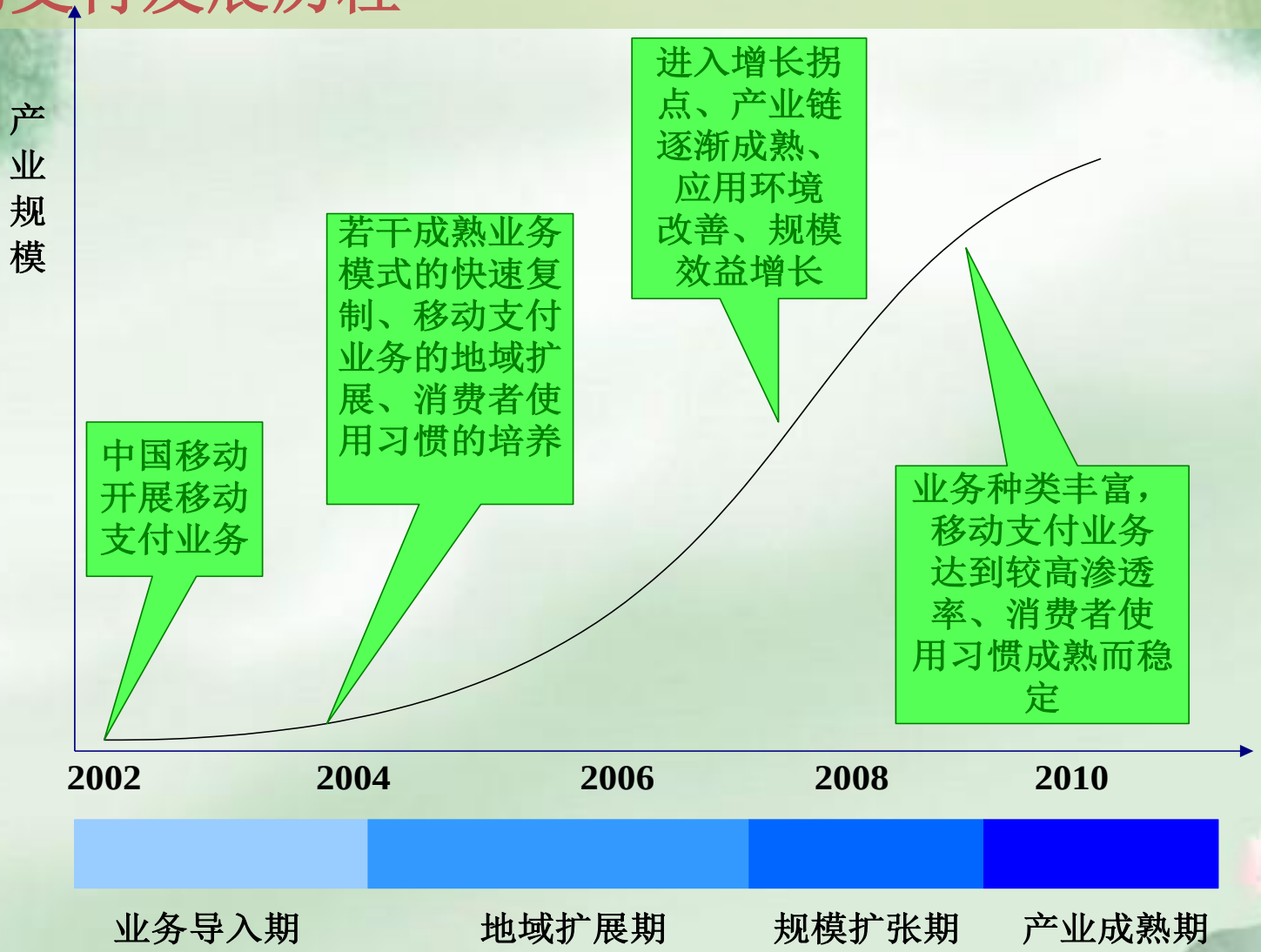
(4)大多采用短信接入方式，安全性低，仅适合小额支付。

(5)业务的推出呈现地区割据状态，地区差异较大。

(6)仅有彩票购买、话费购买等少数亮点业务，大多数业务的规模很小，处于初期的试点状态。

9.2移动支付的发展（续）

移动支付发展历程



9.3移动支付的系统架构和流程

移动支付系统是一个完整的信息系统，包括网络、数据库、分析工具等，涵盖了事务处理、中层决策、战略决策等功能。移动支付系统机构可以分为四层。

(1)负载层：这一层是整个移动商务的基础，它包含了所有移动商务的网路通信技术和底层基础结构，例如GPRS、GSM、3G等等。

(2)网络交互和核心应用平台：这一层在用户以及服务商和金融组织间建立数据库，部署和传输数据，使信息流通畅。

(3)商业层：这一层包含了在移动商务层面的所有商业活动，比如移动彩票、移动银行等，支持事务处理功能。

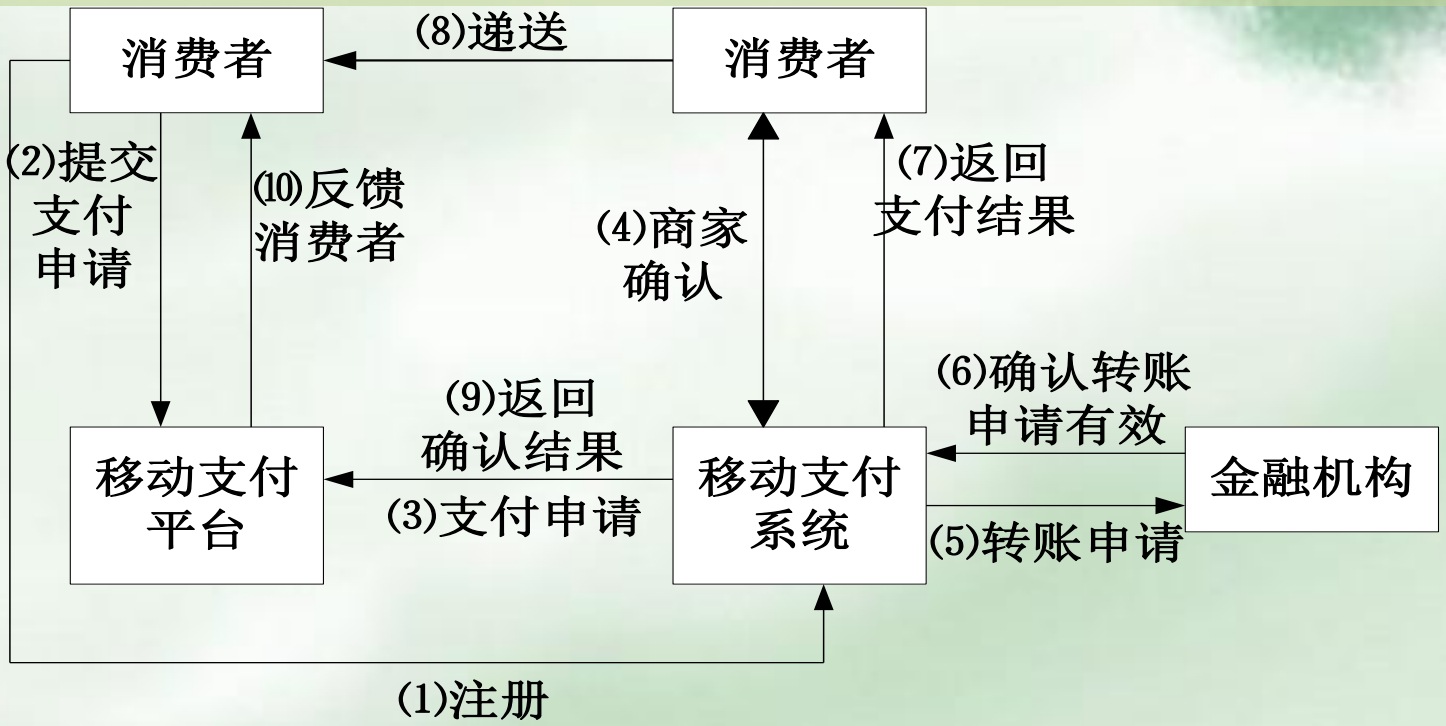
(4)决策层：在整个框架中位于最高层，这一层运用多种数据分析和数据挖掘软件来分析移动支付的市场从而做出决策。

9.3移动支付的系统架构和流程（续）

在移动支付协议中，主要的参与者有四个：用户、商家、金融机构和支付网关。

9.3移动支付的系统架构和流程（续）

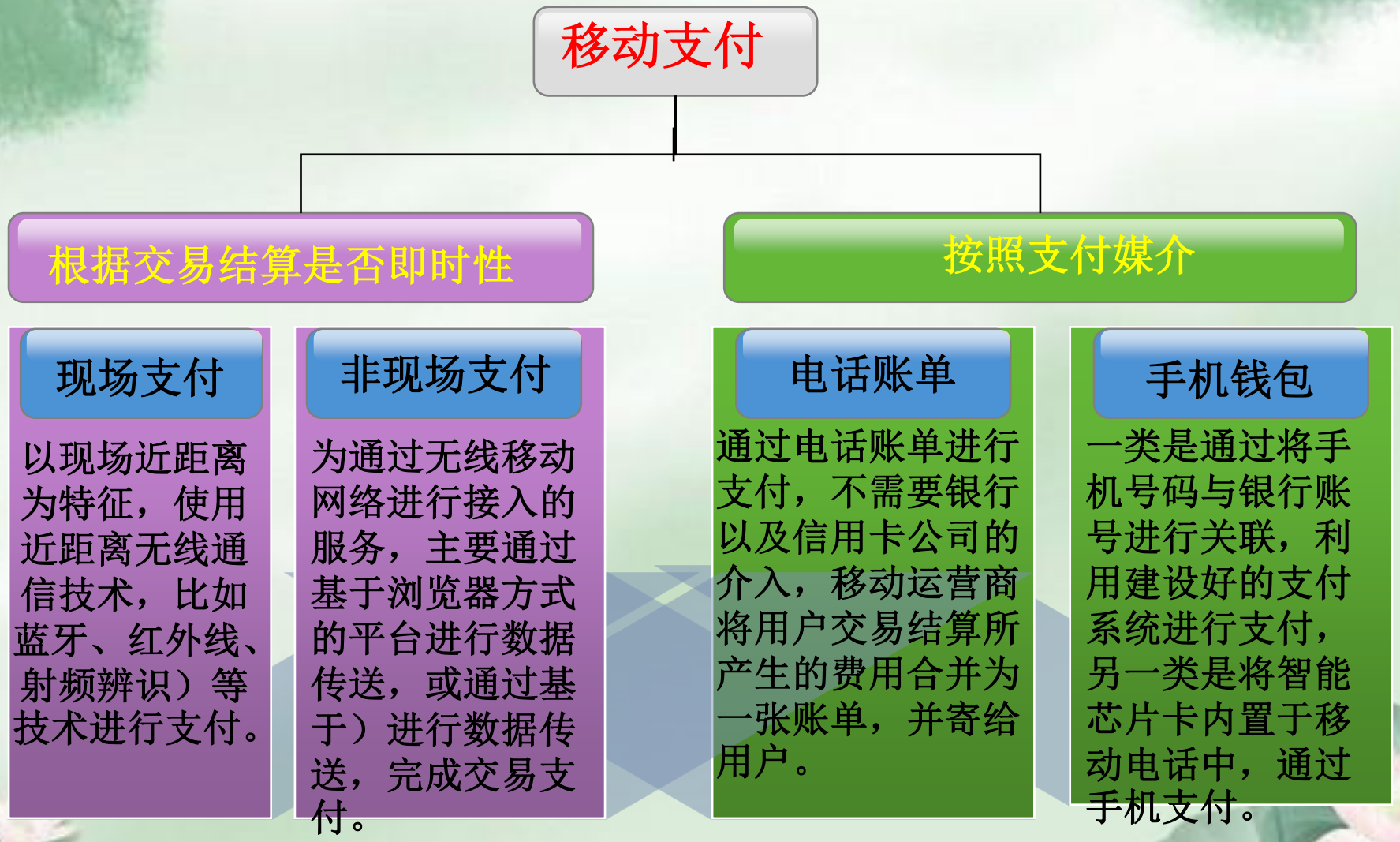
假设用户和服务商都在金融组织拥有账户，那么其支付的一般流程如下。



图中的流程是一种消费者、商家、金融机构都能在支付网关的支持下进行移动支付的流程。如果在其中某一部分发生错误，整个流程就会停滞，并且系统会立刻向用户发出消息。随着移动技术的不断发展以及移动运营成本的不断降低，这一流程还会得到完善。

9.4 移动支付的分类

移动支付的分类

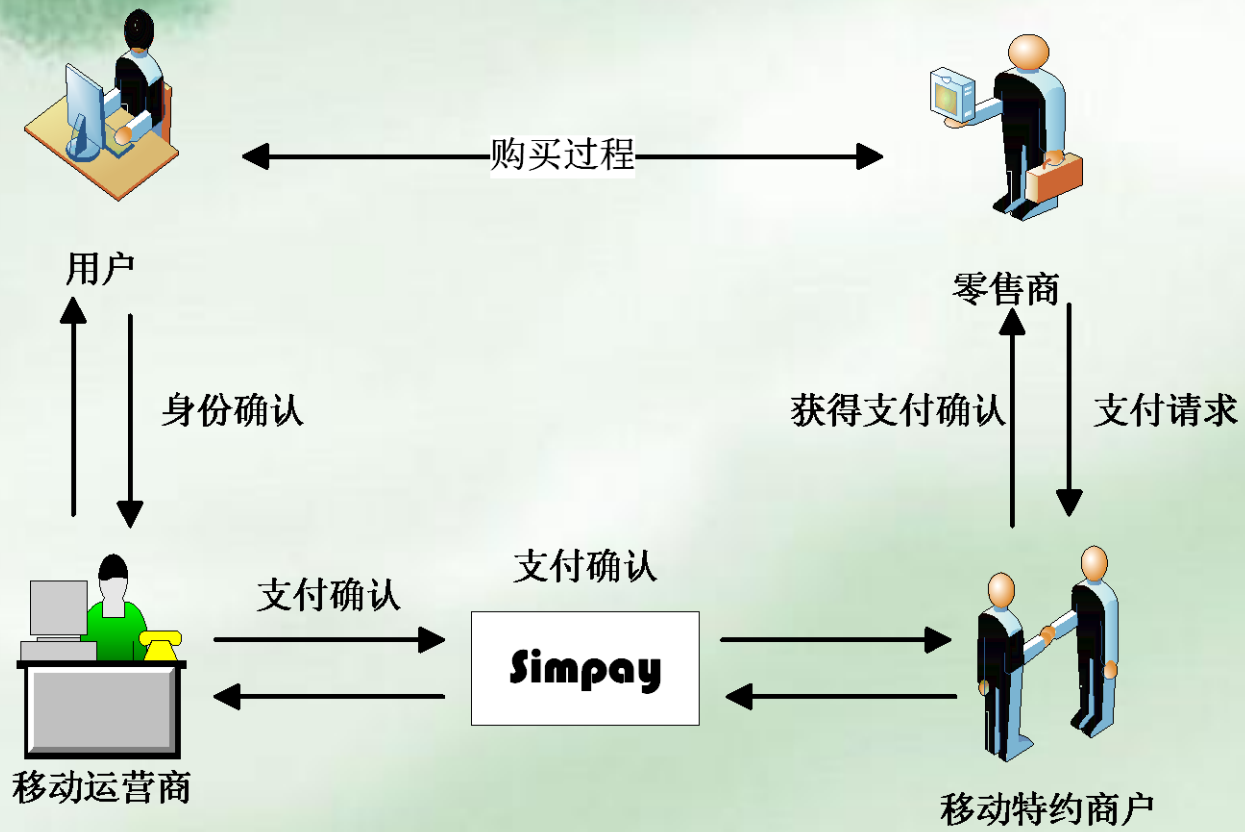


9.5移动支付的组织经营模式

- 9.5.1 移动运营商独立或联合经营
- 9.5.2 金融机构独立经营
- 9.5.3 移动运营商与信用卡组织合作经营
- 9.5.4第三方机构独立经营

9.5.1移动运营商独立或联合经营

无论是移动运营商独立还是联合经营，实质上移动支付都是以移动运营商为主体的。移动运营商为主体比较典型的系统是SimPay。

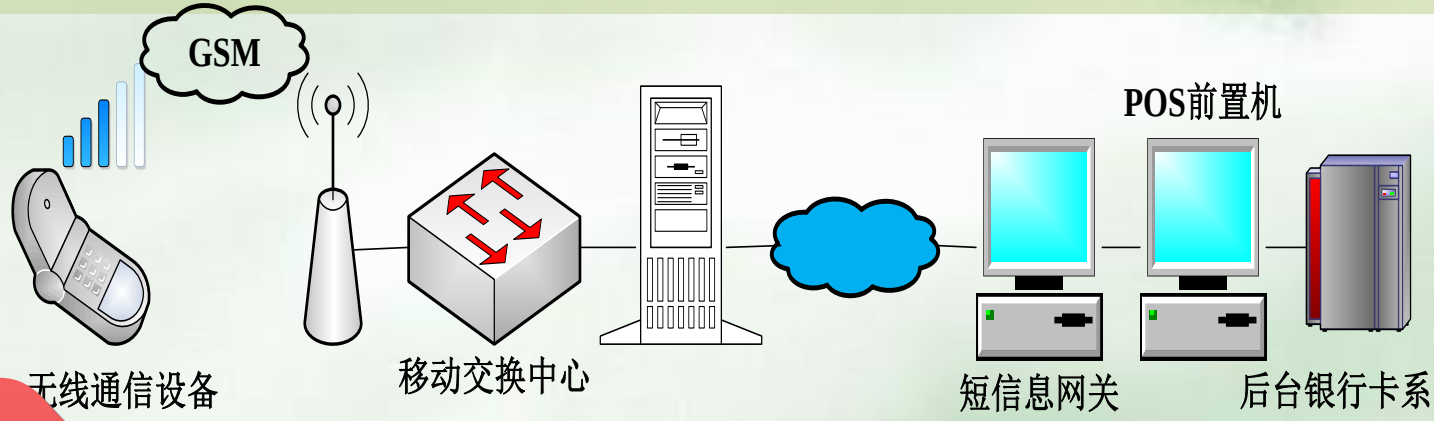


SimPay商业模式的特点

(1)多个移动运营商共同经营；
(2)规模效应，拥有庞大的用户群；
(3)由来自不同国家的虚拟团队组成；
(4)拥有极高的商业信誉；
(5)多领域专业服务的整合
(6)法律方面严格的约束。

9.5.2金融机构独立经营

该模式下通过专线与移动通信网络实现互连，将银行账户与手机账户绑定，用户通过银行卡账户进行移动支付。



由银行等金融机构主导经营的移动支付流程

其优点

1. 在移动网络覆盖以及漫游地区均可使用此项服务。
2. 功能强大，操作便利
3. 申请简短，手续方便
4. 系统加密，安全可靠

9.5.3移动运营商与信用卡组织合作经营

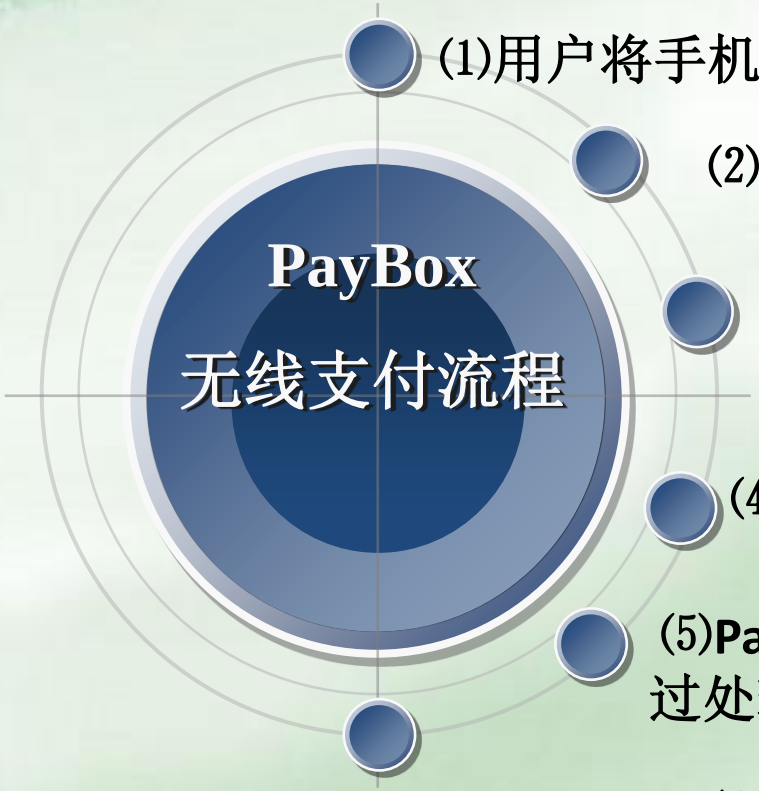
移动电信运营商与卡类组织联合运营，此种方式下，网络运营商和卡类组织同时为用户提供服务,最成功的是日本的I-mode Felica。

I-mode Felica的应用领域

I-mode Felica是NTT DoCoMo于2004年中期开始在日本推出的手机钱包，是RFID技术与其PDC和FOMA相融合而产生的技术，支持Felica业务的手机（含第二代手机和第三代FOMA手机）采用内置RFID芯片，将手机变成了移动钱包

9.5.4第三方机构独立经营

第三方服务商独立于银行和移动运营商，利用移动通信网络资源和金融机构的各种支付卡，实现支付的身份认证和支付确认。典型的例子是瑞典的PayBox，PayBox无线支付以手机为工具，取代了传统的信用卡。



(1)用户将手机号告诉提供商品的商户.

(2)商户将手机号和支付金额发送给PayBox.

(3)PayBox系统自动拨打用户手机，并用语音提示用户进行支付确认.

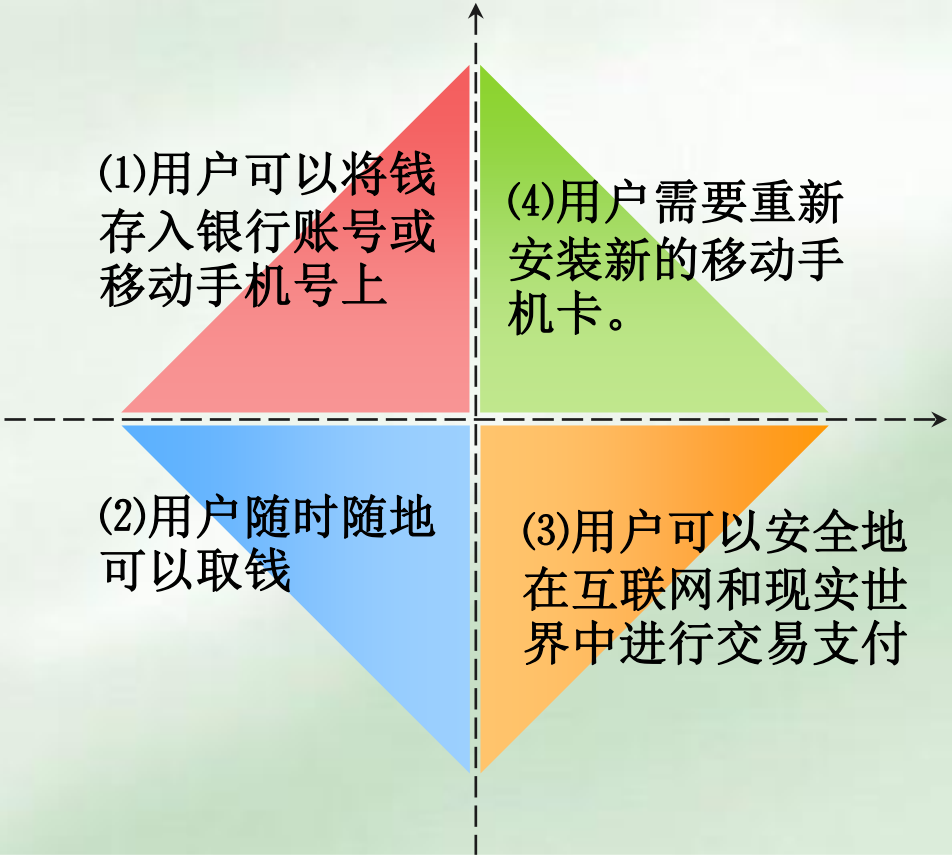
(4)用户输入4位的PIN码以确认支付.

(5)PayBox通知Deutsch银行处理此支付，银行通过处理普通支付一样的系统处理此支付.

(6)PayBox通过短信或语音通知商户，进行支付确认.

9.5.4第三方机构独立经营（续）

PayBox的优势在于：银行、移动运营商和第三方支付运营商都可以采用PayBox方案。其特点如下：



PayBox与SimPay有着共同的特点，就是通过短信或电话语音进行身份认证和支付确认。

9.6移动支付的“空中交易”模式

9.6.1 “空中交易”的短信系统结构

9.6.2 “空中交易”的网络系统结构

9.6.3 “空中交易”的系统特点

前言

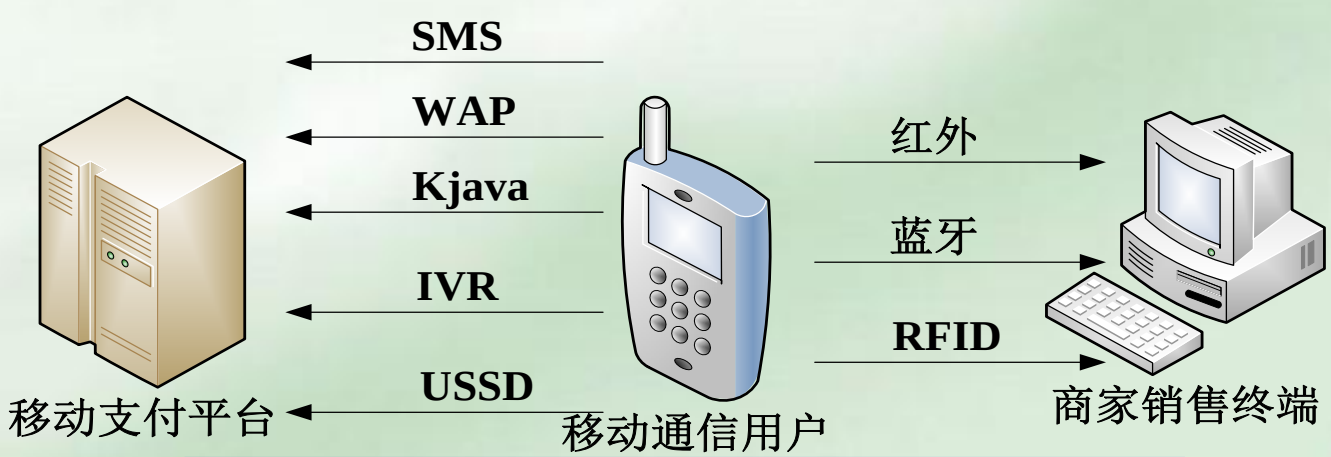
按照传输方式不同，手机支付可以分为空中交易和WAN（广域网）交易两种。WAN方式在日本和韩国得到比较广泛的应用，我国普遍使用的是空中交易模式。

空中交易

空中交易是支付需要通过终端浏览器，或者基于SMS/MMS等移动网络系统，主要特点是以手机为信息载体

WAN交易

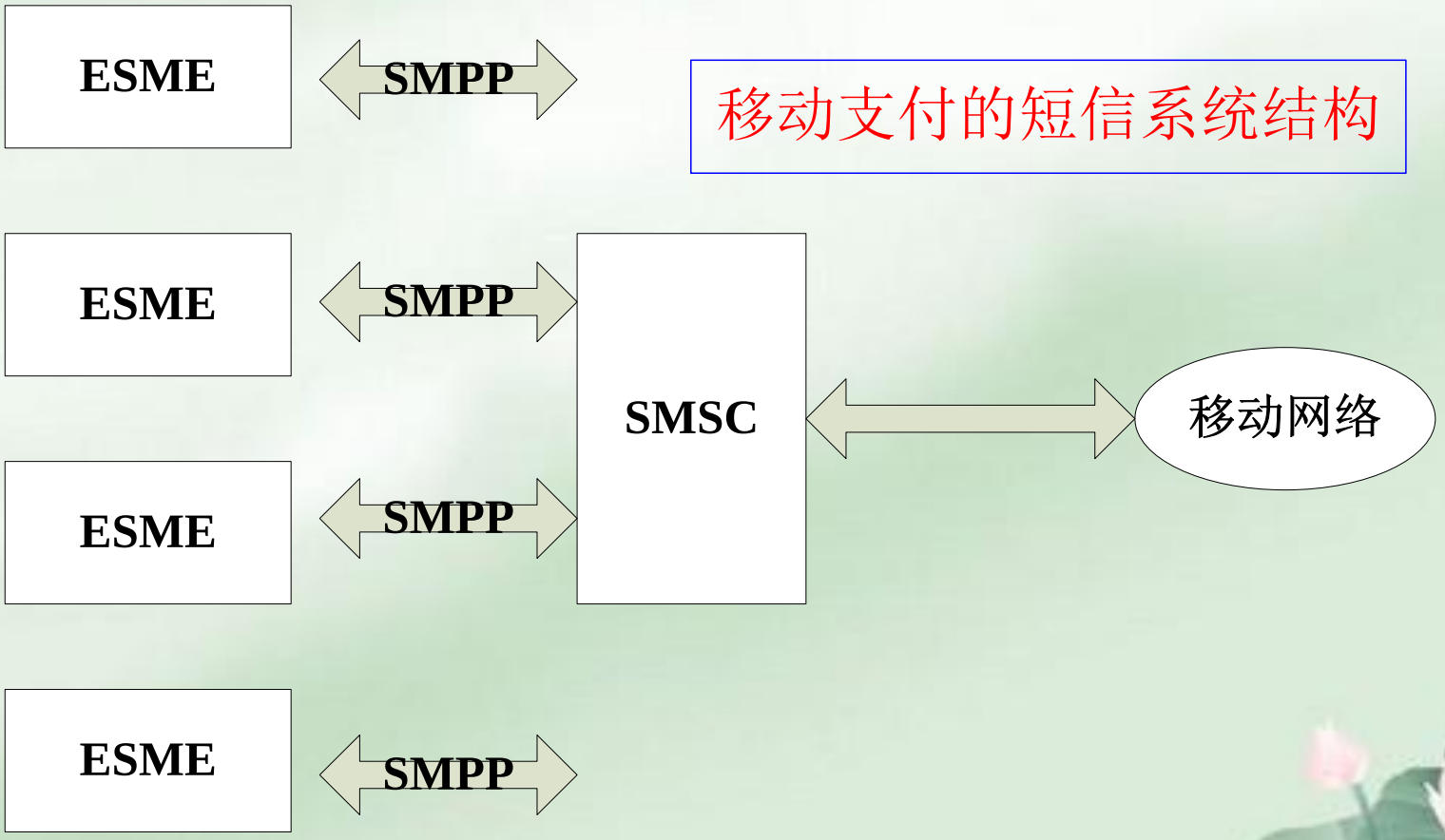
WAN交易则主要是指移动终端在近距离内交换信息，而不通过移动网络，更贴近于用户自身目前的支付方式



手机支付的两种传输方式

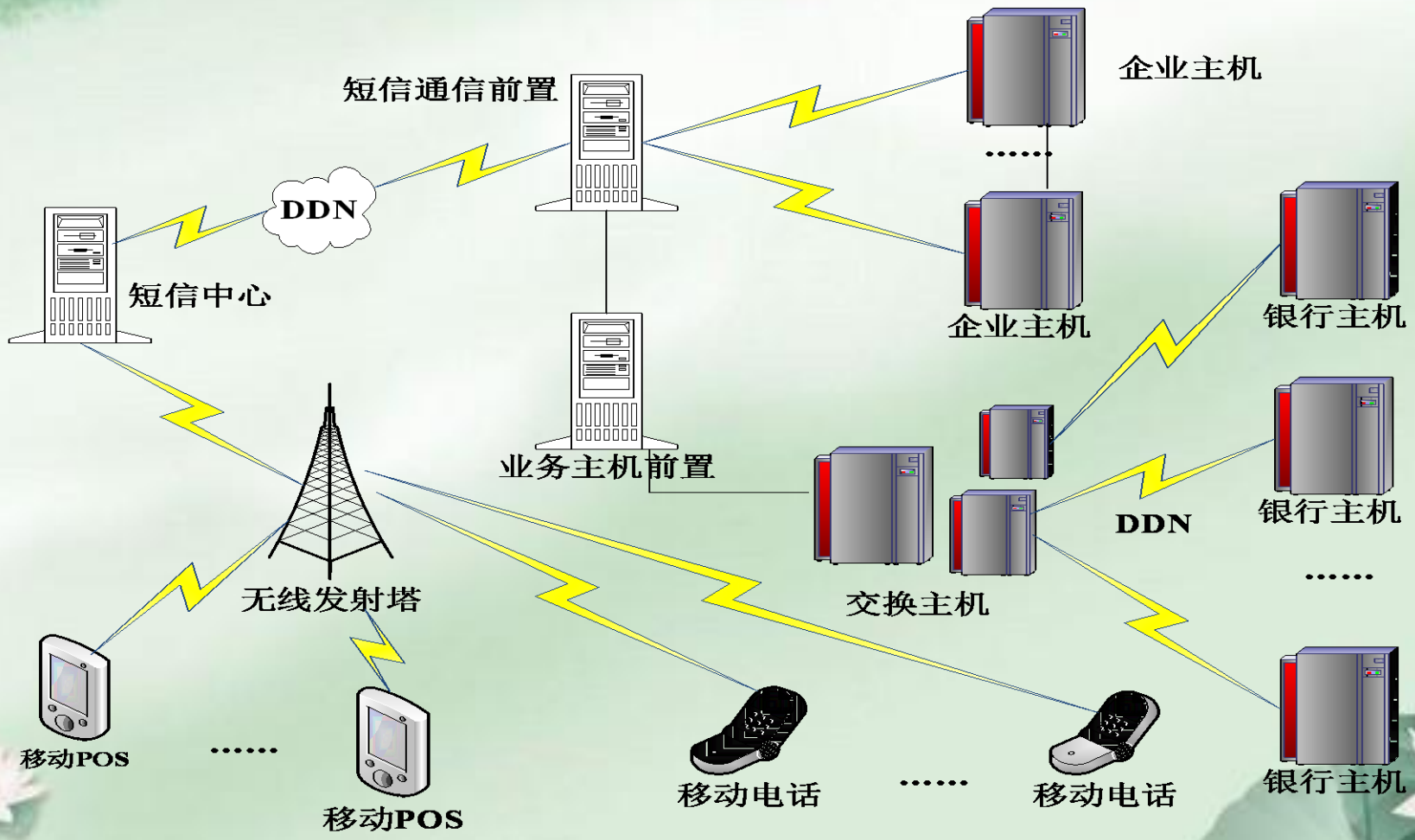
9.6.1“空中交易”的短信系统结构

目前在国内应用最广泛的短息系统是利用GSM系统中的短息业务作为媒介，利用STK卡（Sim Card Ki，SIM卡开发工具包）作为信息加密、解密工具。



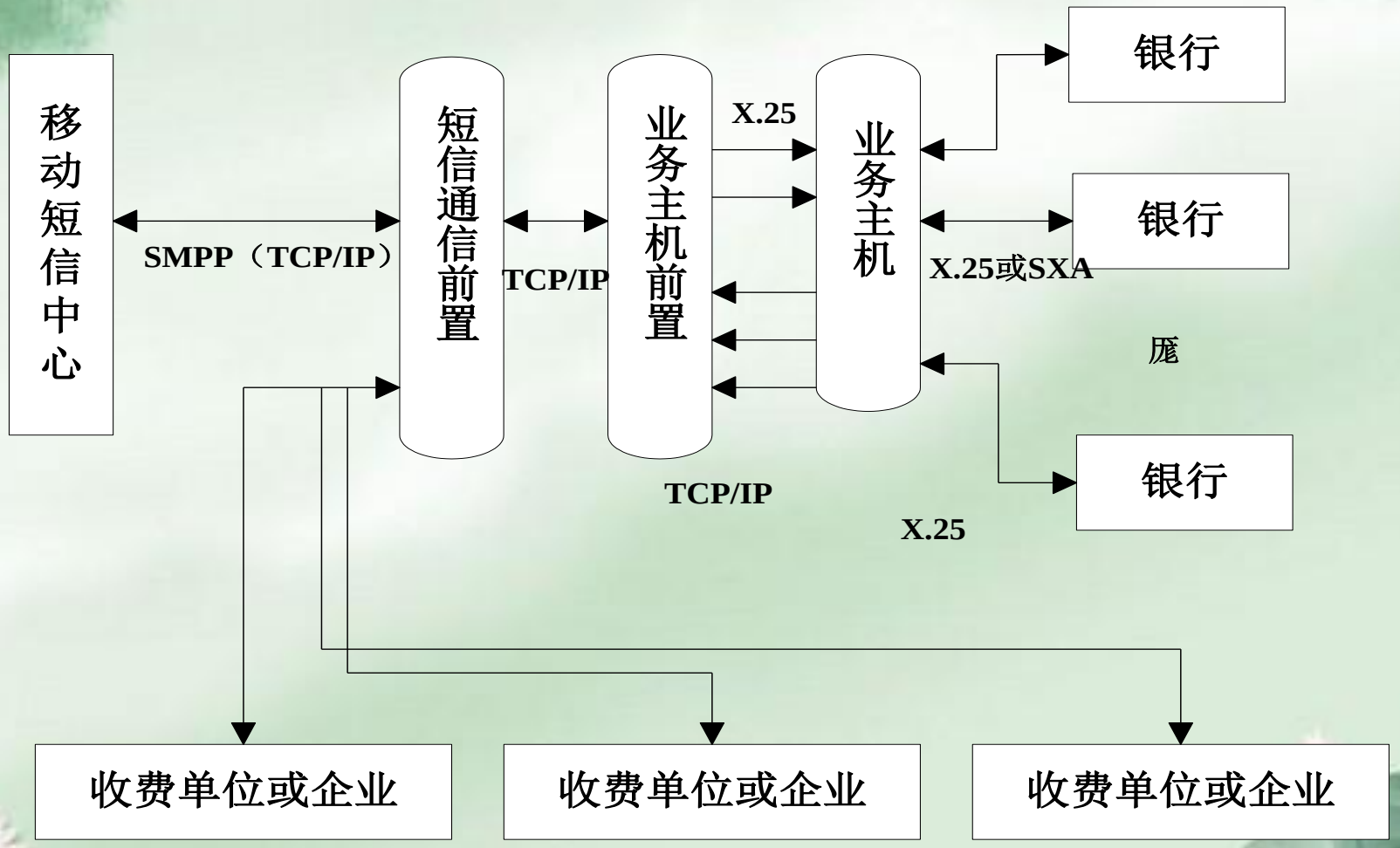
9.6.2 “空中交易”的网络系统结构

“空中交易”的网络与移动通信公司的DDN（Digital Data Network，数字数据网络）连接，网络协议采用SMPP协议（一种基于TCP/IP协议之上的网络协议）。系统网络图如图：



9.6.2 “空中交易”的网络系统结构（续）

系统拓扑图



9.6.3 “空中交易”的系统特点

“空中交易”的系统特点主要有：

1. •交易数据的传递通过移动局的短信平台实现，突破了通过有线电话实现相应功能的局限。
2. •只要一张容量更大的STK卡就能使用多家银行和多家证券商的移动理财服务。
3. •提供的移动理财服务内容丰富，覆盖银行、证券、外汇、保险等多方面，服务方式多样化。
4. •手机用户在商场购物或者其他移动付款环境下，能够使用手机通过移动POS机系统进行支付。
5. •移动POS机为城市的现代化管理带来支付系统的现代化，以极低成本实现安全快捷的远程电子支付，成为物流、资金流和信息流综合在一起的移动终端。

9.7移动支付面临的安全威胁

9.7.1 移动终端的安全隐患

9.7.2 无线网络标准中的安全隐患

9.7.3 移动支付中的病毒与黑客

9.7.1 移动终端的安全隐患

移动支付中的终端设备主要包括个人数字助理（PDA）、智能手机（smart phone）、便携计算机、GPS导航设备等，他们面临的安全威胁主要有以下几类：

1.加密和认证问题

2.移动终端中机密资料的泄露

3.通信内容被窃听或偷看

4.用户自身的麻痹大意

5.安全制度漏洞

9.7.2无线网络标准中的安全隐患

移动商务涉及的网络标准很多，其中应用最广泛的是手机访问互联网的WAP标准、无线局域网的802.11标准和构建个人网络的蓝牙技术。WAP环境的安全机制包括4个安全标准，这些标准应用于无线环境中的应用层、传输层和管理层。

(1)WIM（WAP identity module）

WIM是安装在WAP设备（如手机、PDA等）里的微处理器芯片，能够保存一些关键信息（如PKI的公钥和用户的私钥信息），WIM通常使用智能卡实现。

(2)WMLScript（WAP Script Crypto API）

WMLScript是WMLScriptLip库提供的应用编程接口，包含密钥产生、数字签名，以及处理一些常用的PKI对象（如密钥、证书等）的函数。

(3)WTLS（Wireless Transport Layer Security）

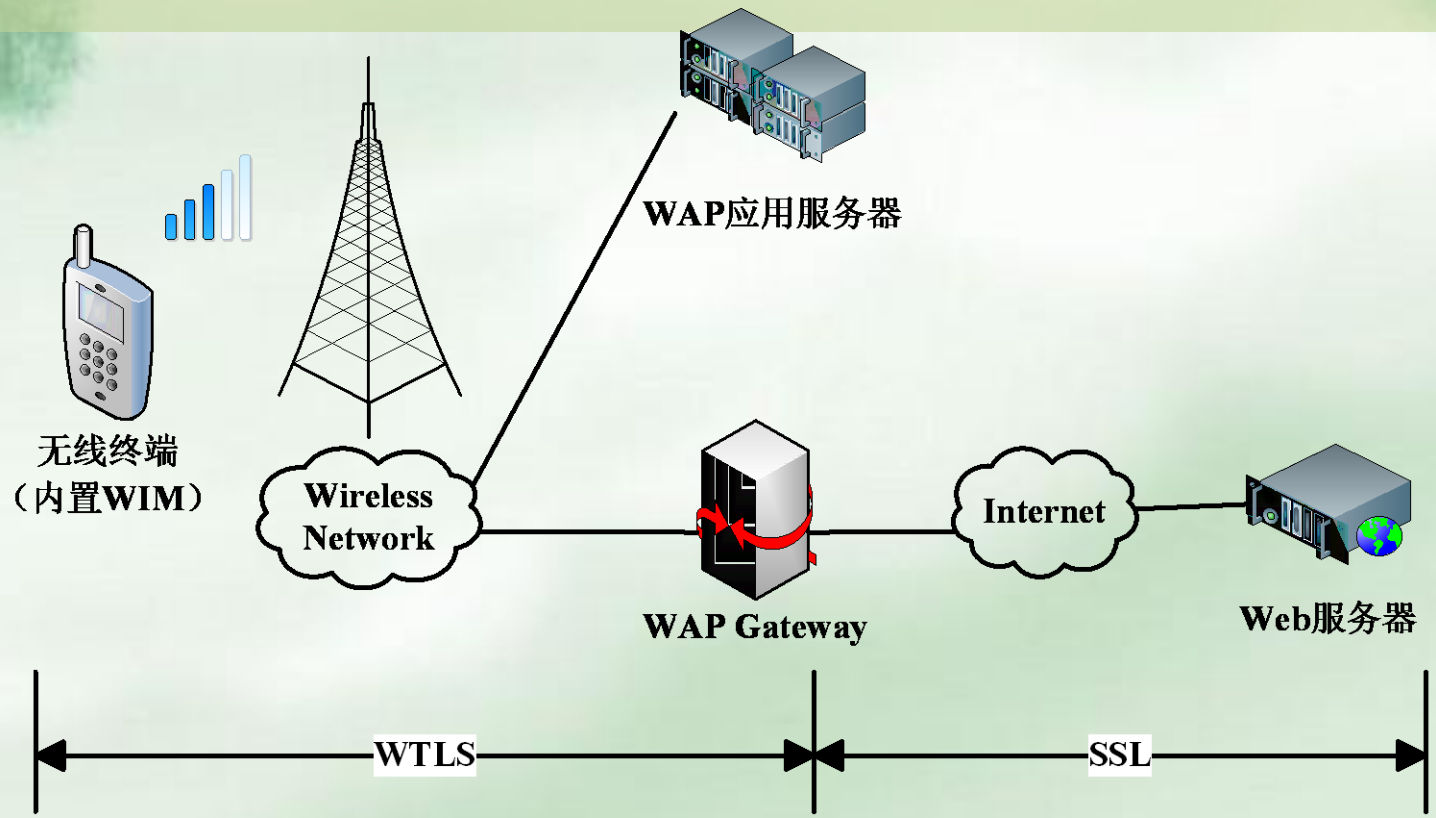
WTLS是基于互联网中的TLS（Transport layer Security）的传输层安全协议。WTLS能够实现对通信参与方的认证，对WML数据加（解）密，并能保证WML数据的完整性。

(4)WPKI（Wireless Application Protocol PKI）

无线应用协议的PKI（WPKI）是传统PKI在无线应用环境中的优化扩展。

9.7.2无线网络标准中的安全隐患（续）

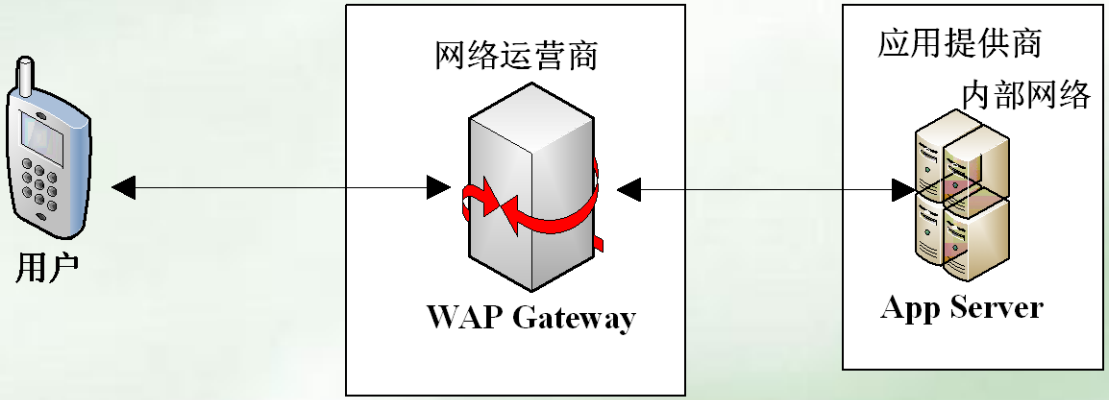
Client与App Server之间就建立了一个间接的安全连接。WAP环境中的安全模型如图



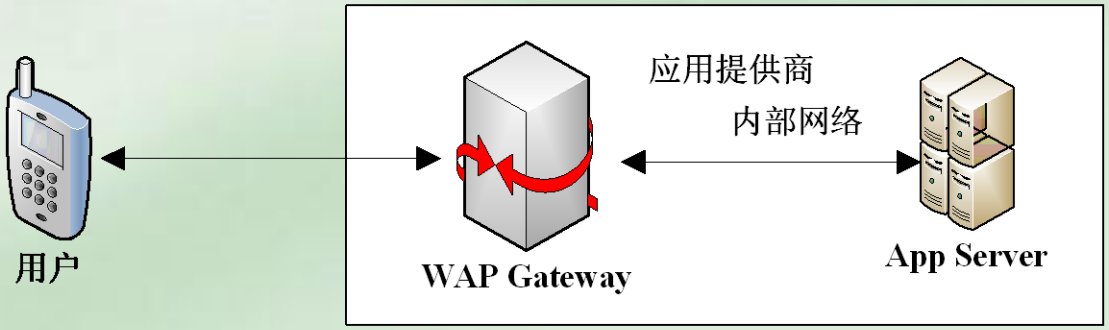
在WAP安全机制中，Client与WAP Gateway之间采用WTLS连接，保证Client与WAP Gateway之间的双向身份认证和加密传输；WAP Gateway与App Server之间采用SSL连接，保证WAP Gateway与App Server自己的双向身份认证和加密传输。

9.7.2无线网络标准中的安全隐患（续）

WAP Gateway可以按照其在整个应用系统中的位置分为两种类型：电信级的WAP Gateway和用户级的WAP Gateway，如图



电信级的WAP Gateway



用户级的WAP Gateway

9.7.2无线网络标准中的安全隐患（续）

WLAN（Wireless Local Area Network）是指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。其安全隐患如下

1

802.11标准使用的WEP（有线等效加密）安全机制存在安全缺陷，公用密钥容易泄露而且难以管理，容易造成数据被拦截和窃取。

2

WLAN的设备容易为黑客所控制和盗用，向网络传送有害的数据。

3

许多WLAN在跨越不同子网的时候往往不需要第二次的登录检查。

4

网络操作容易受到堵塞传输同调的拒绝服务攻击。

9.7.2无线网络标准中的安全隐患（续）

WLAN目前主要通过在不同层次采取相应措施来保证通信的安全性，已有的主要安全机制如下：

(1)通过在物理层采用适当的传输措施，如采用各种扩频技术，利用其很强的抗干扰性来满足安全性要求。.

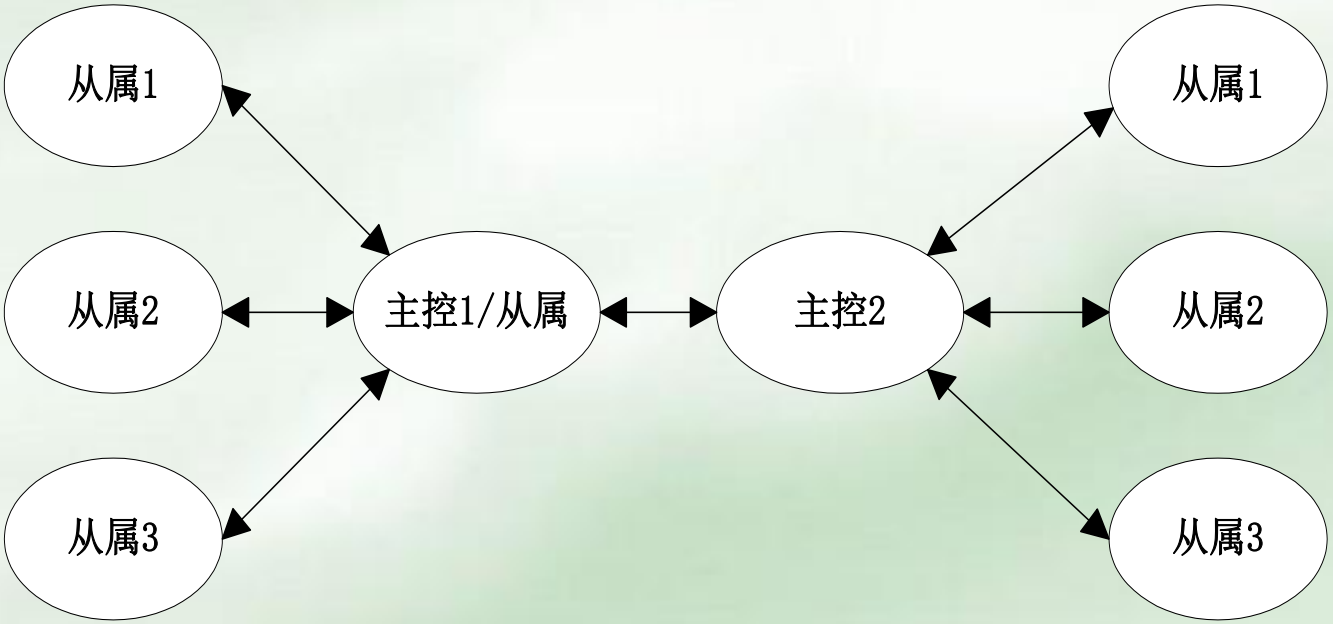
(4)对用户所发送的数据进行加密，WLAN最关键、最独特的保密措施是在网络的媒体访问控制层使用802.11b定义的WEP加密算法。

(2)采取网络隔离和设置网络认证措施，可以防止不同局域网之间的干扰与数据泄露，如服务区标志符（SSID）。

(3)在同一网中，设置严密的用户口令及认证措施，可防止非法用户入网，如802.11b定义的开放系统认证和共享密钥认证等。

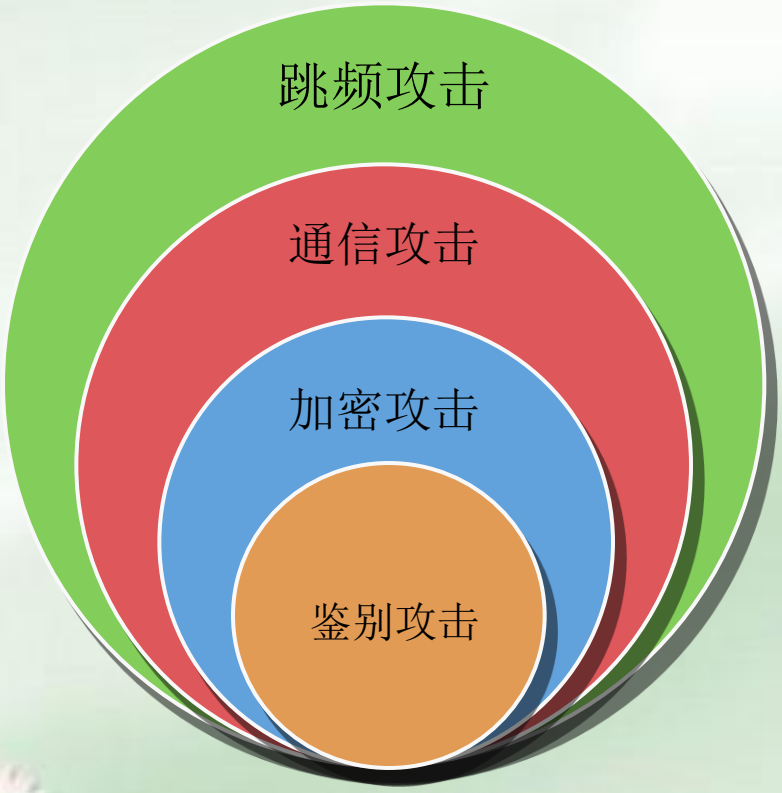
9.7.2无线网络标准中的安全隐患（续）

蓝牙网络通信是一种基于邻近组网原则的对等通信，安装了蓝牙的设备，在一定距离内形成一个自组网（Adhocnetwork），典型的结构如图，



9.7.2无线网络标准中的安全隐患（续）

这种网络有一些不同于固定网络的安全特性，它没有固定的节点和框架，网中设备能充当路由器来中转信息到发送端不能直接到达的节点上，可能会遇到以下类型的攻击：



总体来说，蓝牙技术对于比较小的网络来说是安全的，但对于讲过蓝牙微微网互连而构成的较大的网络来说，系统的安全性能是不够充分的，必须从硬件涉及、跳频算法、鉴别与加密算法等方面来完善和提高蓝牙模块的安全性能；同时增添相关协议子集，完善蓝牙中间协议组；在基本的信息安全传输问题解决之后，还必须在网络高层上实时更加复杂的安全标准。

9.7.3移动支付中的病毒与黑客

目前出现的手机病毒仍以锁定智能手机为主，但病毒越变越聪明。受感染的手机会不断地将短息传送给通讯录中的好友，而且信息夹带病毒。手机病毒基本可以分为三大类

以蓝牙为主要感染扩散方式

此类以食人鱼病毒（SymbOS.Cabir）为代表。食人鱼病毒为手机病毒始祖，至今已经出现20余只变种，并在美国加州出现店内手机交叉感染的案例

通过网路下载图片铃声等服务的方式

其中以骷髅头病毒（SymbOS.Skulls）为代表。骷髅头病毒会在使用者下载的图片铃声屏幕管理软件进入手机后，将手机屏幕上的应用图像都改成骷髅头的图片，接着让手机无法收发短信，无法读取电话簿或者日程表。

通过流行的MMS彩信及蓝牙的方式

此类则以武士病毒（SymbOS.Commwarrior）为代表。武士病毒发出的信息包括告知手机用户下载防毒软件、手机桌面管理软件、3D游戏和色情图片。

9.7.3 移动支付中的病毒与黑客（续）

从现有的情况看，手机病毒主要有三种攻击方式

主要通过发送“病毒短信”来攻击手机，使手机无法提供某些方面的服务。

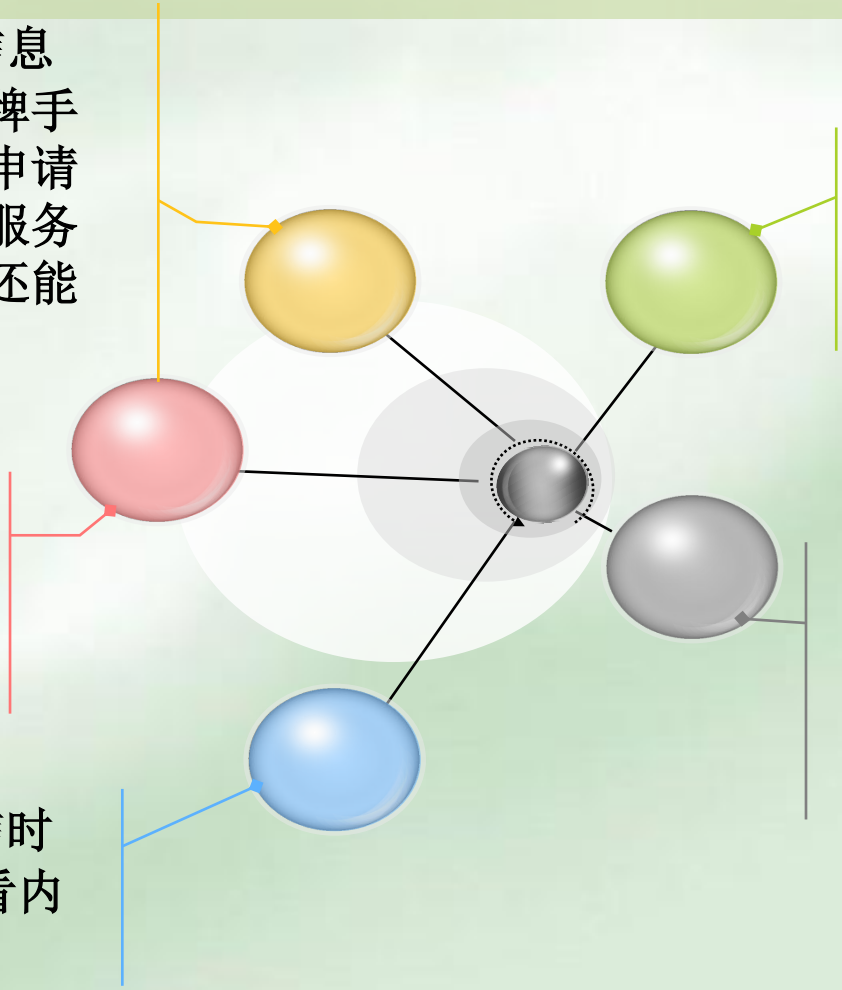
当病毒作者找到网关的漏洞后，就可以利用这种漏洞来编写攻击网关的病毒。一旦病毒攻击成功，将会对整个手机网络造成影响，使手机的所有服务都不能正常工作。

黑客可以利用服务器的漏洞编制能够攻击服务器的病毒，通过病毒来影响服务器的正常工作，使手机无法接收正常的网络信息。

9.7.3 移动支付中的病毒与黑客（续）

对付手机病毒的最好方法是防患于未然，预防手机病毒、减少病毒危害可以通过以下几个方法：

1在手机里存放有重要信息的用户，可以在各大品牌手机生产商的官方网站上申请有偿“电话号码管理”服务，这样，手机中毒后，还能有几乎备份恢复。



4.平时做好备份，手机一旦中毒，立即关机并拿到维修点恢复，不然会传染更多的手机。

2.蓝牙手机的蓝牙功能，不用时一定要关闭或设置为隐形状态。 business

5.在接电话时，发现来电显示带有不正常的乱码、英文等，不要接听。

3.接到陌生手机彩信时，直接删除，不要看内容。

9.8 本章小结

1. 全面地介绍了移动支付的基本概念和发展的总体概况。

2. 通过案例对移动支付的四类经营模式的应用和特点进行了比较分析。

3. 系统地描述了移动支付应用中的两种传输技术—空中交易模式和广域网交易模式，并重点分析了这两类传输技术的系统结构和主要特点。

4. 描述了移动支付面临的安全威胁，特别对来自于无线网络标准的安全问题进行了深入的剖析。

同学们再见!