# 移动终端及其证券服务网络的架构和实现

张邦廉 柳 晶 (中国科技大学 100040)
肖 波 (中央民族大学 100081)

**摘要：本文在移动终端和证券网络服务系统的架构与安全运行等方面作了较详细规划；该证券POS网络系统比其他证券服务系统有明显的优势，它能很好地满足股民个性化的需求；终端POS机便携小巧，经济可靠，能实现个股查询、交易、存储等。**

**关键词：网络 POS终端 安全 证券**

## 1 移动终端及证券服务网络架构的目的

随着社会发展，居民的个人收入有了较大增长，富余的现金逐渐增加，股票已成了众多投资者的选择。为了方便股民交易，市场上出现了股票BP机、图文电视、计算机股票系统等，它们各有优点，也各有不足，均未能很好地满足股民的需求。规划移动POS终端及证券服务网络目的是为了多方面地满足现今股民的个性化需求。

及时了解股市行情与各类相关的政治、经济、金融信息，各公司的经营业绩；及时进行技术分析，综合历史和当前数据，预测未来股票大盘与个股的走势，从而决定如何对股市中的股票进行买卖操作；查询自己帐户上的资金与股票情况，进行各种股票交易；同时股票终端产品应便捷、可靠、经济。正是围绕着股民的需求进行了移动POS终端及证券服务网络的规划研制。

## 2 移动终端及证券服务网络规划

### 2.1 系统的整体规划

该系统可设计成由以下各分系统组成并分别进行规划布局：

(1) 实时/历史信息数据库系统。该系统通过卫星地面站实时接收实时数据信息并存入数据库，数据库中存储大量的历史数据和用户资料，作为应用商向用户提供各类信息的中转库；数据库迅速、可靠，自动记录各类信息的访问频度（记帐功能），提高服务质量。

(2) 委托、查询系统。该系统进行用户身份验证、鉴权，POS机中数据的加密，鉴权过程中密钥产生，委托、查询数据的透明传输。

另外证券移动POS系统还包括POS访问服务系统、应用商通信接口系统、网络管理系统、数据通信线路备份系统、智能IC卡发放系统、卫星数据通信网系统、调频付载频数据广播台/或智能寻呼台、数据专线接入网络中心系统（数据通信线路有：DDN/ISDN/X25/PSTN等）、个人寻呼和短消息服务系统等，对它们分别进行规划布局。

### 2.2 系统安全运行设计

证券POS网络及终端系统作为证券网络，其系统的安全是十分重要的，因而在系统整体设计的各个环节，都要遵循严格的网络设计规范，有效地阻止来自外部和内部的非法侵入，保证了网络的安全性，其安全性作如下的设计。

(1) POS安全性设计。POS终端的安全设计是系统安全性设计的基础，智能IC卡单元的设计遵循数据安全的国际标准，IC卡中密钥设计成具有如此的特性：密钥存储，数据加密/解密，产生随机密钥；电子签名，将改进的DES加密算法和四着色组合算法运用到数据加密中；防窃用，用户密码保证合法用户才能使用，当非法用户在一定次数输入错误密码后，IC卡自动失效。保证了客户身份验证、鉴权，拒绝非法用户，数据传输、存储安全性和源点及接收的不可抵赖。

(2) 网络安全性设计。网络安全性设计遵循国际安全标准体系，与POS安全性综合设计实现了系统的整体安全策略；非法用户无法冒充用户利用网络及其资源，无法篡改、替换、扰乱系统数据；数据交换的各种活动及发生时间均有精确、完整的记录和审计；保证数据不丢失，防止因自然灾害、人为原因和机器故障而导致的拒绝服务。

(3) 安全管理体制的规划。系统安全性管理体制参照相关的证券网络安全管理规范，围绕安全性技术制定，有效的阻止来自外部和内部的侵入。

## 3 证券 POS 网络系统的设计

### 3.1 网络系统整体构架

系统由全国统一频点的无线寻呼网和有线网组成，共同为手持 POS 终端机服务。其结构如图 1 。

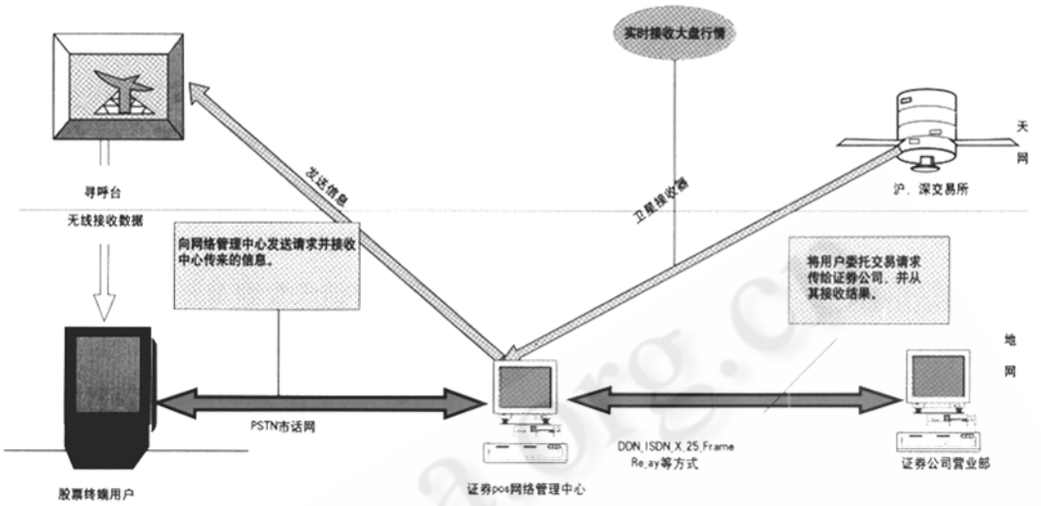


图 1 证券 POS 网络系统架构模型图

### 3.2 POS 网络管理中心的布局

网络管理中心集中管理 POS 终端用户，它存储大量的股市资料和股票实时行情，是 POS 用户的信息源，交易时它又是用户和证券交易所的纽带，因此它是系统中的关键部分。其布局的结构简图如图 2 。

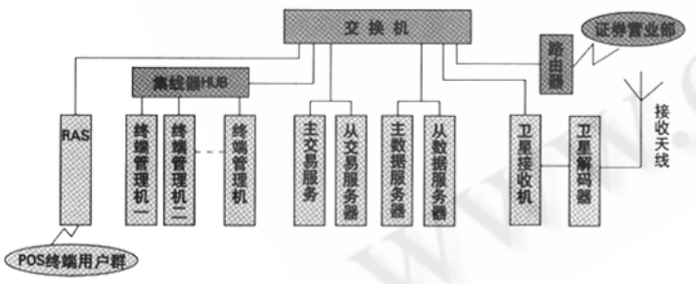


图 2 布局结构简图

### 3.3 POS 网络管理中心作业流程设计

POS网络管理中心处于终端用户和证券交易所之间，通过卫星接收器与沪、深证券交易所相联接，实时接收两地的股票行情与业界信息，如果网络中心附近有营业部，在经对方许可后可接入营业部的局域网，从营业部的行情服务器获得实时行情数据，供用户查询。以有线方式接收用户请求，并与所在城市的证券公司服务器相联接，将用户的委托工作传递给他们，完成用户的请求后，可以有线或无线方式传递给用户。流程图如图 3 。


图 3 作业流程图

### 3.4 POS 终端机作业流程初步设计

手持终端内置或外置MODEM，进入网络时，自动拨号连接网络管理中心。用户首先到与证券POS网络管理中心相连接的证券公司注册登记，获得用户上网登录密码、IC卡，并购买股票机终端。手续完毕后，用户便可以通过终端 POS 机，以有线或无线方式和证券 POS 网络管理中心相联接，查询股市行情，并可进行委托交易。手持终端可以无线或有线接收实时行情、资讯信息，有线接收历史信息、进行股票委托服务，可保存部分信息于手持终端的电子盘中。手持终端进入有线服务时，必须经过基于IC卡的身份认证。所有委托服务的数据在手持终端和进入营业部柜台接口机的所经通信途径间是加密的。

### 3.5 无线系统部分的设计

(1) 无线系统的结构。无线系统是用来发送和接受股票实时行情和资讯信息，信息的来源是 POS 网络管理

中心和沪深交易所的实时行情，它由三部分组成：信息源、无线发射系统、无线接收终端。结构模型如图 4。

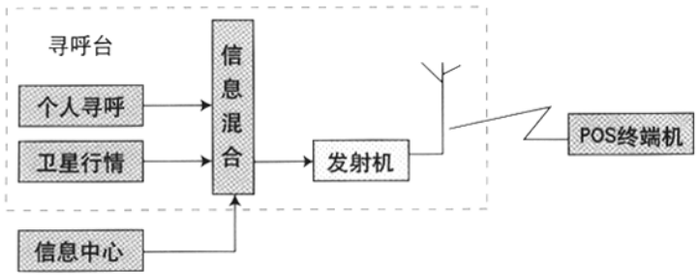


图 4　结构模型图

(2) 无线信息流模型如图 5。

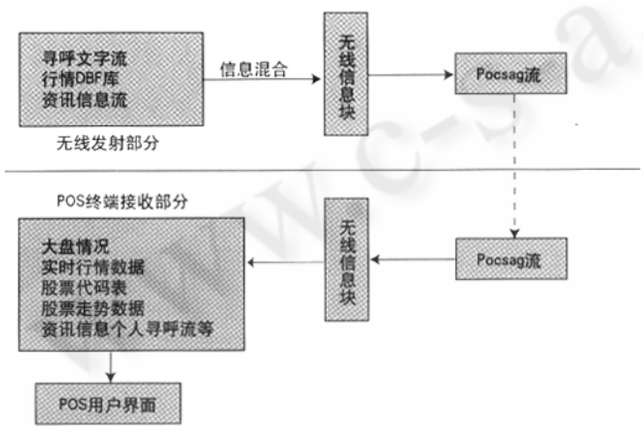


图 5　无线信息流模型

### 3.6 POS 终端结构和接收协议的规划

(1) 终端机结构如图 6。

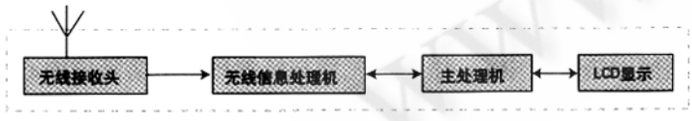


图 6　终端机结构

(2) 终端机接收协议布局如图 7。

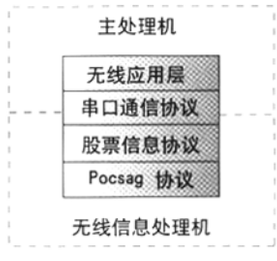


图 7　终端机接收协议布局

### 3.7 证券公司网络对请求处理的流程设计

证券公司网络信息系统：接受处理证券 POS 网络管理中心发出的用户委托请求，并将处理完毕的用户请求返还给证券 POS 网络管理中心。营业部柜台系统的局域网与网络中心设计成隔离的，营业部柜台与网络中心的委托服务不能直接进行，必须通过运行在营业部柜台接口机上的特定程序来实现。

该程序的工作流程如下：

(1) 从网络中心获取委托请求数据；

(2) 将请求数据加密，并确定是合法用户；

(3) 将请求数据写入交换文件，并等待营业部柜台系统的处理结果；

(4) 从交换文件中读回执数据；

(5) 将回执报文加密，发送回 POS 网络中心。

流程如图 8。

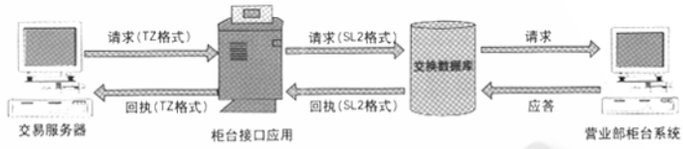


图 8

### 3.8 系统达到的主要质量标准与技术定性指标要求

网络架构：Client/Server；操作系统：NT/SQL Server；通信协议：TCP/IP；访问速率：33.6Kbps--56Kbps；交易速度：<8s；系统容量：>300000 用户；无线编码格式：FLEX/pocsage；系统可靠性：双机热备份、冗余等；系统安全性：智能 IC 卡、安全网络、安全管理体制。

## 4　系统安全运行与可靠性的设计

安全性是证券 POS 网络系统能正常运行的重要保障，也是股民们普遍关注的问题。

### 4.1 网络系统中安全及可靠性保证的一般措施

按照 C2 级安全标准进行设计；磁盘系统由盘控卡、SCSI 电缆及硬盘驱动器组成，为了防止故障而死机可采用磁盘镜像、双工技术，也可在阵列卡上实现RAID1，可采用 RAID 5 技术，将奇偶校验后的数据分配到多个硬盘，增强其可靠并提高速度；采用多 CPU 处理(SMP)提高服务器的处理速度；利用多重 PCI 将阵列卡和网卡合理地分配 PCI 总线上，可提高服务器的吞吐率；采用 $I^2O$ 技术(智能的输入输出体系)减轻服务器的负担；采用冗余

网卡(NIC)、冗余热插拔电源、ECC冗余内存和热插拔PCI提高系统的可靠性；采用结构化布线和网管软件监视设备的运行从而提高整个系统的可维护性；服务器采用主从双机热备份形式（可用NOVELL的NetWare SFT Ⅲ 或VINCA的Standby server）保证服务的安全运行。

4.2 加密技术的运用

（1） DES（Data Encryption Standard）是使用较广泛的一种加密方法，3DES是DES的替代物，它可以使用3种不同的密钥，只能使用在ECB模式中，它是在速度和更加安全的算法之间的一个折中。可将该加密方法加以改进后运用到证券POS网络系统IC卡的数据加密和认证之中。

(2) 不对称加密。不对称加密也称“公开密钥加密”，可以使用两个不同的但是相关的密钥值：公钥和私钥。共钥的用途：数据完整性，数据的保密性，发送者不可否认，发送者认证等，为了防止第三者伪装成发送者，可以使用公钥和私钥进行双重的加密，任何人将能够解密第一个报文，获得内嵌的加密文本，但是只有接收者使用自己的私钥才能对加密文本解密，必须保证每个公钥/私钥对的唯一性和私钥保持为私有。证券POS用户可采用该种方式进行认证。

(3) 数字签名。数字签名是将一个加密的消息摘要附加在一个文档后面，可以确认发送者的身份和该文档的完整性，它没有提供消息的内容的机密性，但它隐含了消息的内容。制作数字签名并运用到POS网络系统的数据加密中。用于POS用户发送信息和证券公司发布信箱公告。

(4) 密钥管理。证券POS网络系统的最终用户的数量是巨大的，每个用户都有自己的密码，为了有效地管理，创建密钥分配中心KDC来进行密码的分发和管理以及用户注册。保证公钥/私钥对是唯一的，公钥的分发可以采用数字证书进行，建立在ITU-TX.509标准基础之上，提供唯一登录能力的机制。使用分布式创建秘密会话密钥，提供了一种为双方建立一种共享密钥。

4.3 证券网络系统中遭到常见攻击威胁以及预防

（1）未授权访问是指未经授权的实体获得了访问网络资产，并有可能篡改资源的情况。它是通过在不安全通道上截取正在传输的信息或利用相关技术及产品中固有的弱点来实现。为了防止未授权访问对通过不安全的通道的通信量必须加密编码，使之在传输过程中不能被修改。

（2）假冒攻击是指通过出示伪造的凭证来冒充别的事物或别人而攻击对方，如:盗窃私钥、访问明码形式的用户名/口令，或者记录一条授权序列并在以后重放。使用多重有效认证可防范假冒攻击。

（3）拒绝服务（DoS — Denial of Service）是指服务的中断，中断原因可能是系统被毁坏或暂时性不能用，如：摧毁计算机硬盘、切断物理结构和耗尽所有的可用内存；许多常见的DoS攻击都是由网络协议引发的（如IP协议）。因此为IP的应用添加一些补丁程序，从而防止入侵者利用IP的重装配错误，限制系统的可接受的TCP连接个数以及缩短连接保持在半开状态的时间，降低或消除TCP SYN溢出攻击所带来的影响，同时在基础设施的入口和出口点限制TCP连接的个数来控制。

通过一系列网络规划和安全措施的使用，证券移动POS网络系统一定能设施并安全运行，为广大股民提供多方面个性化的主动服务。■

*参考文献*

1 《数据通讯与计算机网络》，杨心强，邵军力，电子工业出版社

2 《实用软件工程》，郑人杰等，清华大学出版社

3 《网络安全性设计》，美 Merike Kaeo 人民邮电出版社