计算机科学2001Vol.28№.7

证券网与IBM ES-9000大中型机互联应用
——并发实时银证联网系统

The Application of Internet between the Bond Network and the Big or Middle Computers of IBM ES-9000
——The concurrent real-time bank bond internet system

周琪云　黄明和
（江西师范大学计算机科学技术学院　南昌330027）

Abstract　Concurrent real-time nonuniform network is the developing trend of today's network-constructing technology. In this paper the composition, structure, function and implementation technologies of the bank bond network system in the concurrent real-time state based on the client/server model are introduced, which are developed by us with Jiangxi Huitian science-technology limitted company and the Jiangxi branch of China Industrial-commercial Bank. And the important effects of isomerization to the network application system's currency, flexibility, expandancy are also analyzed. At the same time the new compound variable-length, Eor, multiple encipher/decipher means and check means are given.

Keywords　Concurrency, Real-time, Nonuniform network, Internet system, Multiple encipher/decipher means

一、引言

网络互联是当今网络发展的必然趋势，各商业银行为了开拓新业务和吸收更多资金，加速开展了与各主要用户的互联。我们将以IBM ES 9000大中型计算机为中心将工行内部金融网同证券局域网相联，构成一个复杂的综合型的异构互联网络系统。基于安全可靠因素，我们在中心机房建立银行网（一个独立的NT网），通过通信机4700仿真卡与IBM ES 9000机相联，向下通过中心前置机与证券商网络相联，并在银行网中设立管理机，实现系统维护。

二、硬、软件环境

1. 工行证券中心：① 服务器P Ⅱ 128M内存10G以上硬盘一台；② HP pc网关机gateway，加天刚卡一块；③ 前置机P Ⅱ 64M内存一台；管理监控机64M内存一台；④ LQ1600打印机一台；CISCO 3640 16口路由器一台；MODEM若干。

2. 证券方：MODEM一个；CISCO 2610路由器一台；PC Ⅱ 64M的PC机一台。

3. 系统软件：① MS SQL 7.0数据库；FOXPRO 2.6；② MS NT 4.0 SERVER中文版；MS NT WORKSTATION；WINDOWS 95/98；③ VB 6.0，VB 4.0(16位)；CGS 3270。

4. 开发应用软件：① 与大机做交易应用软件HOSTS。协议和编码转换，发送和接收IBM ES 9000的数据。② 与证券方通信软件STOCKCOMM，验证、记库、解密、接收请求和发送处理结果。③ 证券方接口及其与证券中心通信软件STOCK。通用数据库接口、发送请求和接收处理结果。④ 证券中心实时监控软件MONITOR。实时监控、查询历史日志。⑤ 证券中心开户、销户、修改及其打印的管理软件MANAGE。柜员管理、证券商资料管理和股民资料管理。

以上是我们自己开发的应用程序，采用的编程语言是VB6.0，对其中核心部分在第四节中论述。

三、功能及其实现方式

1. 功能　实现股民的银行帐户与股民的保证金帐户间的对转。股民的银行帐户可以是灵通卡、专用卡、信誉卡、甚至活期存折。股民的证券方帐号可以是上海股东代码，深圳股东代码或保证金账号。

2. 实现方式　发起方由证券方开始，证券方通过证券系统来接收股民的电话委托或自助下单委托，把这一请求委托纳入指定的缓冲池中，本系统将自动从缓冲池读取数据，并发实时与银行大机完成交易（要求全过程<10秒）。

四、计算机网络体系结构

1. 网络体系结构

网络体系结构如图1所示。

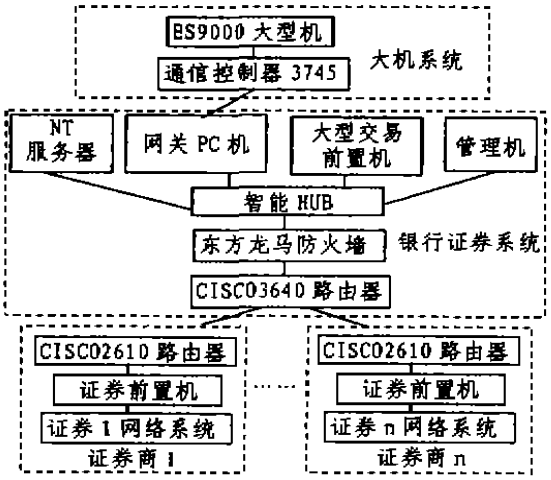


图1 网络体系结构

2. 网络结构分析

本系统所采用的网络结构是多协议并存的综合型网络结构，即在ES-9000大、中型计算机、银行方证券中心机房的NT网络和证券方网络中异种机、异种协议、异种字符编码的综合型网络体系。从图1中可了解到，网络通用性、扩展性以及安全可靠性是解决银行方的主要任务，银证网络的建设在协议上必须多样化，在与证券方相联中可采用最流行client/server方式的TCP/IP协议，而与大机ES-9000联接则必须使用SNA协议。银行方证券中心NT网与证券方采用的字符编码是ASCII码，而IBM-ES 9000大中型计算机所采用的字符编码则是EBCDIC码。

3. 安全保证措施

不管是证券方还是银行方，数据的安全、可靠是最重要的问题之一。本系统设计的网络结构提供多处安全防卫措施。

①虚拟技术 将银行内部网、银证互联网、证券网分成独立的VLAN，相互间只能在路由器所允许的控制范围内进行访问。

②防火墙技术 采用东方龙马公司的防火墙，进行IP地址转换，端口地址转换，隐藏内部网络，过滤非法请求，监控网络上的非法用户，提供较强的防御攻击能力。

③入侵监测技术 提供实时的入侵检测及采取相应的防护手段，如及时报警、记录证据，用于跟踪、恢复和断开网络连接等。

④数据打包技术 在广域网中使用数据打包技术，保证数据在传输过程中的安全性和完整性。

⑤认证技术 AAA(鉴定、授权和计帐)对各种网络设备进行集中管理，并做到有据可查。

4. 扩展性、灵活性和备份性

路由器采用与硬件无关的IP协议作为支撑协议，加上路由器本身接口的多样性，使得路由器可以构造各种结构复杂、介质各异的网络，网络结构设计极为灵活，有利于扩展，路由器支持TCP/IP网上传送SNA网络节点延伸至任意一个TCP/IP节点，因而极大提高了SNA网络构造的灵活性，每增加一个证券商都可通过DDN线或远程拨号方式连接远地的银行方网络，这就极大地加强了网络的可扩展性。若出现线路故障，可采用电话拨号方式连接，做为DDN线备份线。

五、应用程序的软件技术

1. 软件功能总体流程

软件功能总体流程如图2所示。

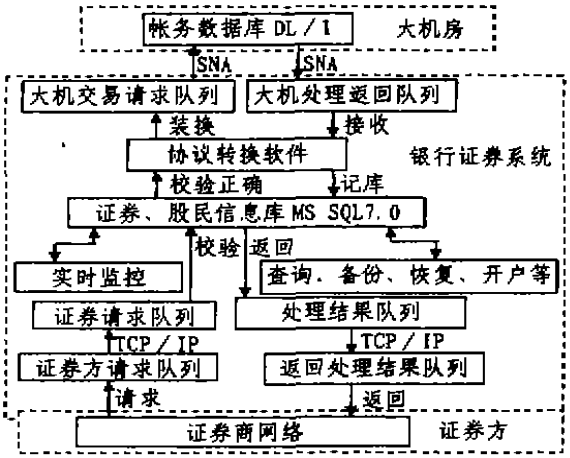


图2 软件功能总体流程

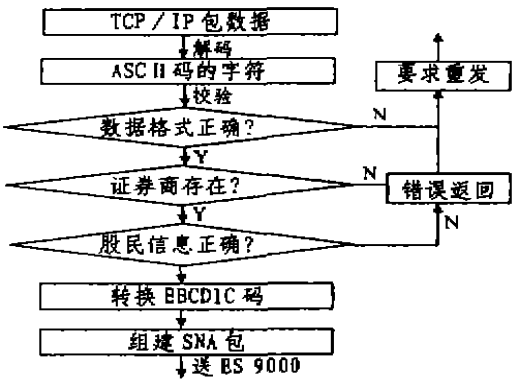


图3 协议编码转换

2. 模块分析

从图2可知，一共有3对消息队列，分别是证券中心机房与ES-9000交换的消息队列、证券中心机房与证券通信的消息队列，与证券商接口的消息队列，所有消息队列都可同时多进程和多线程进行读取，而stock-

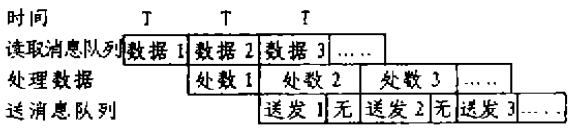
comm 是多进程的应用程序，每一个证券商连接就产生一个进程与之对应。而 Hosts、stock 程序是多线程的程序。

3. 协议转换和编码转换

由于从证券上送来的数据请求是 TCP/IP 打包的数据和非常熟悉的 ASCII 字符集，而大机 IBM ES-9000上要使用的协议和字符编码是 SMA 和 EBCDIC 字符集，这样就必须进行协议和字符编码的转换。具体流程如图3所示。

4. 消息队列时间片的安排

多进程、多线程的程序关键在于时间片的安排，为了实现并发功能，进程或线程对消息队列读取时间的设定可由配置文件中来配置。假设配置时间为 T，针对多进程多线程的程序而言就是如下时间表示：



5. 变长异或多级加解密方法和校验方法

为确保系统的安全可靠，本应用软件创造性地提出了新的加解密方法，即变长、异或、多级加解密方法。由于银证业务对实时性要求较高，本加解密方法不仅安全可靠，而且运算速度快，其具体方法如下：

所谓多级是指把要加密的数据分成若干组，而组的长度是根据传送数据的不同而变化的，异或特点是两次对同一数据位异或结果不变。

假设有一串要加密的数据 $s=x_0x_1\cdots x_{n-1}$（长度为 n 个字符），则第一级加密数据长度为 m_1，即 $s=x_1x_2\cdots x_{m_1-1}$（$m_1<n$）这里 m_1 可以在配置文件中设定，一般小于10。具体加密方法为：

$$y_i=\mathrm{chr}(\mathrm{ASC}(x_i)\oplus(0XFF)$$

其中：$0<i<m_1$，这里⊕表示异或运算，0XFF 表示十六进制数据 FF。由此得到一级加密数据：$s_1'=y_0y_1y_2\cdots y_{m_1-1}$，且得出第二级加密长度：

$$m_2=(\sum_{i=0}^{m_1-1}y_i \bmod 10)+1$$

从而又得到第二级加密字符为 $s_2=x_{m_1}x_{m_1+1}+\cdots+x_{m_1+m_2-1}$，这时我们把 s_2 分为 $L_2=m_2/m_1$（取整）个 m_1 长度的组和一个小于 m_1 长度的组，共 L_2+1 个组，最后一组字符个数为 $m_2'=m_2 \bmod m_1$，对于每一组均采用：$y_{i+ml+1,k}=\mathrm{chr}(\mathrm{ASC}(x_{ml+i+j,k})\oplus y_i)$ 方法加密，其中：$0\leqslant i<m_1\ 0\leqslant j<L_2+1\ k=m_1$ 或最后一组 $k=m_2'$。由此得到二级加密数据 $s_2'=y_{m_1}y_{m_1+1}\cdots y_{m_1+m_2-1}$，且得出第三级加密长度：

$$m_3=(\sum_{i=m_1}^{m_2+m_1-1}y_i \bmod 10)+1$$

如此类推可得到后面各级加密数据以及各级加密数据长度。若 $m_1+m_2+m_3+\cdots>n$，则整个数据加密完毕，加密后的数据为 $s'=s_1'+s_2'+s_3'+\cdots$。解密方法和加密方法在处理思想上完全一样，这里不再赘述。

在数据传送过程中仅仅加密并不能判断数据是否正确和完整，线路状况千变万化，总会出现一定的差错，为了判定数据的正确性和完整性，我们采取如下方法对数据进行校验，实践表明它比奇偶校验更优，而这只需增加2位标准字符，即校验位为：$P=\sum_{i=0}^{n-1}(y_i) \bmod 100$ 把这2位的数值转化成2位字符，与加密数据一起传送，即现在传送的数据为 $s'=s_1'+s_2'+s_3'+\cdots+P$，在校验过程中通过把计算所得的校验位与传送上来的校验位进行比较即可得出数据的正确性和完整性。

6. 通用数据库接口程序

鉴于证券方数据库的多样性，为了实现数据接口的通用性，我们采用了基于面向对象 ODBC 和 ADO 连接方式来编写数据接口程序，现可连接 FOXPRO、VFP、MS SQL、Orcale 等众多数据库。

结束语 本应用程序已在中国工商银行江西省分行营业部投入运行，在运行过程中，系统具有稳定、安全、可靠和处理速度快等特点，具有极大的推广应用价值。

参 考 文 献

1 Garms J 著(美) WINDOW NT SERVER 4 大全. 北京：机械工业出版社，1997

2 冯青. 银行计算机系统的安全与对策. 中国金融电脑，1997(12)：55～56

3 余成、周琪云、常晓虹. 陶瓷产品的计算机系统造型和花面设计系统. 软件学报，1993，4(4)：44～50