WAP证券交易系统中间件结构及安全性策略

殷长友, 吉根林

(南京师范大学 数学与计算机科学学院, 江苏 南京 210097)

[摘要] WAP(Wireless Application Protocal)技术应用于证券交易时, 要保证证券交易能正常进行, 必须解决信息传输的迅速有效与安全性问题. 利用中间件技术实现多营业部资源共享, 通过专用中间件使各营业部均能开展移动证券交易, 而股民却不需改变其操作, 实现其操作的一致性. 对集中式交易的券商, 信息采用轮转法使中间件负载均衡, 对非集中式交易的券商, 根据券商标志进行信息转发到相应的中间件, 并采取密文传送方法成功解决了 WAP证券交易软件的安全有效性问题.

[关键词] WAP, 证券交易, 中间件, 负载均衡, 安全

[中图分类号] TP393 [文献标识码] B [文章编号] 1672-1292-(2005) 01-0047-03

Middleware Technic and Its Implementation in WAP Stock Exchange System

YIN Changyou, JI Genlin

(School of Mathematics and Computer Science, Nanjing Normal University, Jiangsu Nanjing 210097, China)

Abstract When WAP (Wireless Application Protocal) technique is used in stock exchange, the rapidity and effectiveness of information being communicated must be solved to ensure the normal process of stock exchange. Besides other internet technologies adopted in WAP Stock Exchange System, middleware technique is used not only to guarantee the security but also to realize the source share among many sales departments, and a special middleware ensures various departments to develop mobile stock exchange, while stock holders do not necessarily change their operation, thus realizing the consistency of their operations. SSL(Secure Socket Layer) is used to translate information between WAP server and middlewares. The above method is feasible in WAP Stock Exchange System.

Key words WAP, stock exchange, middleware, balance, security

0 引言

我国资本市场的迅猛发展使家庭的理财理念发生了很大的变化, 投资股市已成为较普遍的选择, 交易方式的多样性又对证券市场的发展起着促进作用. 移动证券商务就是在股票交易处理手段上符合需求潮流、贴近投资者个性化需要的一种新型证券交易方式, 采用这一方式首先必须解决信息传输的迅速有效与安全性问题. 证券交易行情和交易数据源自证券公司内部网络, 为保证内网不被攻击, 它必须和外部的 Internet隔离开来. 应对这一需求, 现提出基于 WAP的证券交易系统的框架结构以及中间件在交易系统中的作用和实现方法, 基于在以上思想基础上开发出的移动证券商务在南京市证券公司进行了实际应用, 达到预期的效果.

1 WAP证券交易系统结构

系统以 Brower/Server方式设计, 如图 1所示. 股民使用 WAP手机上网, 通过内置微浏览器, 连接至 WAP服务器, 即可进行股票的查询、委托, 完成股票交易. 系统采用 WML, WMLScript和 JAVA开发, 具有高效、安全、易扩展的特点. 采用多层次的设计, 实现界面、通信和业务接口的分离, 使交易得到最大限度地保证. 采用 Servlet技术提供股东进行证券交易的动态用户界面, 动态用户界面在接受股东资料时对关键数据进行加密. 客户与交易系统的联系通过中间件完成, 保证证券公司的内部网络免受外部的非法侵入.

收稿日期: 2004-08-18
基金项目: 国家 211工程学科建设基金资助项目.
作者简介: 殷长友(1963-), 讲师, 主要从事计算机网络的教学与研究. E-mail yinchangyou@njnu.edu.cn

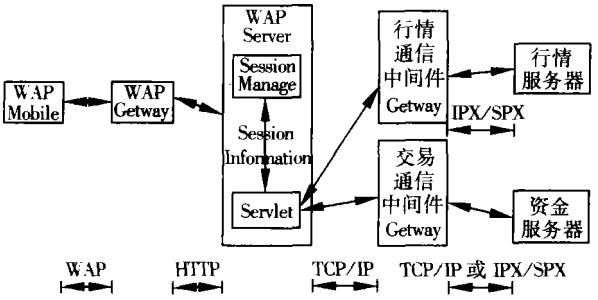

图 1　WAP证券交易系统框架

2　中间件的实现

2 1　中间件的概念

中间件是指能够屏蔽操作系统和网络协议的差异, 为异构系统之间提供通信服务的软件. 从逻辑上讲, 它把原来的二层结构分离开来形成逻辑上的三层结构或多层结构, 可以是处于操作系统和应用程序之间的软件, 也可以是处于应用程序与后台数据库之间的软件. 中间件的适用范围极其广泛, 形式多种多样, 小到一个函数, 大到一个系统. 中间件技术是一种对信息进行中间加工的技术, 还可以对信息进行中间校验、过滤和转换等, 并可起到防火墙的作用. 中间件可分为过程调用、面向消息、对象请求代理、分布式事务处理、数据访问等类型, 针对不同的应用采用相应的方式.

2 2　基于WAP的证券交易中间件安全设计框架

为保证系统的安全性须将证券公司的内部网络与 Internet隔离开, 设计通信中间件传递两者的信息, 可有效防止内部网被非法侵入. 通信中间件根据WAP服务器的请求负责将该请求传给内部网络的相应服务器, 并将结果反馈给 WAP服务器. 由于证券公司普遍采用资金与行情分开的三层结构, 因而本系统的通信中间件分别采用基于对象请求的行情传输通信中间件和交易数据通信中间件 (如图 1所示). 通信中间件的网关中仅开放与WAP服务器之间的专用通信服务, 确保柜台交易系统的安全. 为达到营业部共享, 设计专门的中间件, 它判断该股民属于哪个营业部, 并将其请求由WAP服务器通过 Internet发到相应营业部的交易数据通信中间件完成相应的证券交易.

2 3　以信息流负载均衡为基础设计通信中间件

证券公司的内部行情通常是基于 Novell的网络操作系统, 通过 IPX /SPX 协议进行信息的传输, 资金系统又与行情系统隔离, 通过交易系统的中间件进行信息交换, 其拓扑结构是硬三层. 通信中间件通过 IPX /SPX协议与证券公司的行情服务器进行通信, 通过 TCP / IP协议与资金服务器进行通信.

2 3 1　中间件管理

为了最大限度地节约成本, 共享资源, 同时使本系统具有较好的可扩展性, 对中间件采用集中式管理方法, 即无论是本地还是外埠, 所有中间件开启时均向 WAP服务器以自己的编号进行登记, 从而形成一种树型结构, 如图 2所示.

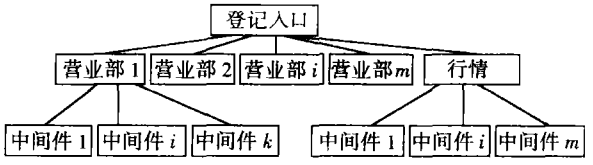

图 2　中间件登记形成的树型结构

由于加入的营业部是静态的, 而每个营业部的中间件个数则是动态的, 各营业部仅提供交易中间件, 行情中间件由主站提供. 建立下列符号表, 每个中间件登陆时形成动态链, 符号表中各单元的指针指向这个动态链中的第一个目前未向它发消息的中间件. WAP服务器根据消息头判断出应将该信息发到营业部 x 所指向的中间件, 由该中间件的管理队列进行相应的管理, 如图 3所示.

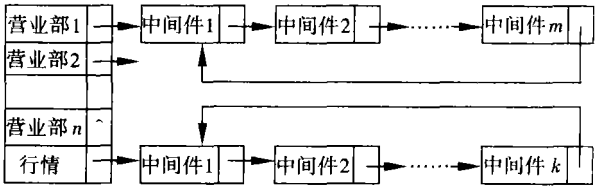

图 3　中间件管理符号表

采用循环链表, 将符号表指针指向动态链中的第一个目前未向它发消息的中间件, 这样可保证消息的分配均衡, 同时也很容易实现.

2 3 2　优先队列的管理方式

基于消息的中间件有消息、队列和队列管理等要素. 所谓消息是在应用之间交换的所有数据以消息形式实现, 它包括消息头和消息正文两部分, 消息通过队列进行交换. 队列是一个被命名的目标用于存放系统和用户信息, 对队列的存取可采用先进先出或按优先级进行. 队列管理负责消息排队服务.

通信中间件采用优先队列的管理方式, 为保证证券交易的及时性, 采用优先队列可使客户的委托具有较高的优先性, 而相关查询则优先级较低, 根据数据包的消息头描述就可得知业务的类别, 定义它的优先级, 提交处理. 实现优先队列需要 3种操作容器: Insqueue将对象插入容器, Searchpri返回容器中的最优先对象引用, Delquepri将最优先对

象从容器中删除.本系统用二叉树的结构方式排列优先队列,故上述 3种操作实际为对二叉树的操作.例如插入队列 Insqueue,由于完全二叉树的底层必须从左到右填充,插入点必须加在底层下可获得的位置上,同时结构树又必须有正确的形状,而且仍然保持有序状态.

通信中间件的接受进程从 WAP服务器获得消息,并根据消息头判断出该请求是要获取行情信息还是交易查询或委托,以决定是查询行情服务器中的沪深行情数据的请求还是向证券公司的交易系统的中间件发一条相关交易请求,然后将该请求插入队列中的相应位置等待处理;通信中间件的处理进程根据消息队列的请求或向行情服务器取数据或向交易系统取数据,通信中间件的发送进程将对用户的响应形成新的消息发送给 WAP服务器,并通过 WAP服务器传给用户,然后从队列中删除该请求,从而完成消息的处理.

2 4 中间件的安全策略

由于 WAP服务器与中间件可能分布在不同的地方,因而它们之间通信的安全性问题必须考虑.采用 SSL(Secure Socket Layer)进行信息传输是一种较好的选择,它可节约开发时间,减少成本,SSL是 netscape公司设计的主要用于 Web的安全传输协议. SSL可以用于保密的传输,这样,中间件与 WAP服务器之间传输的消息便是"安全的".这种协议在 Web上获得了广泛的应用.

SSL是一个介于 HTTP协议与 TCP之间的一个可选层. SSL层:借助下层协议的信道安全协商出一份加密密钥,并用此密钥来加密 HTTP请求. TCP层:与 web server的 443端口建立连接,传递 SSL处理后的数据.接收端与此过程相反. SSL在 TCP之上建立了一个加密通道,通过这一层的数据经过了加密,因此达到保密的效果.

SSL缺省只进行 server端的认证,客户端的认证是可选的. SSL客户端(也是 TCP的客户端)在 TCP链接建立之后,发出一个 Clienth* lb来发起握手,这个消息里面包含了自己可实现的算法列表和其它一些需要的消息, SSL的服务器端会回应一个 Serverh* lh,这里面确定了这次通信所需要的算法,然后发过去自己的证书(里面包含了身份和自己的公钥). Client在收到这个消息后会生成一个秘密消息,用 SSL服务器的公钥加密后传过去,SSL服务器端用自己的私钥解密后,会话密钥协商成功,双方可以用同一份会话密钥来通信了.其流程大致如下:

Client Server
Clienth* lb- - - - - - - - →
Serverh* llo
Certificate*
ServerKeyExchange*
CertificateRequest*
← - - - - - - - - Serverh* lbDone
Certificate*
ClienKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished- - - - - - - - →
[ChangeCipherSpec]
← - - - - - - - - Finished
Application Data ← - - - - - - → Application Data

3 结束语

无线网络通信是一个具有广泛应用前景的领域,在其应用中特别需要考虑其安全、有效、快捷,尤其是应用于金融领域、电子商务等.利用中间件技术将核心数据与外界隔离开来,可有效地防止核心数据遭受攻击.在中间件等基于 Internet网上的站点间的通信采用目前较成熟的 SSL技术可减少研发周期,同时也有效提高了系统的安全性.随着无线通信设备速率的提高,对 WAP开放的业务种类、内容的组织和策划更加重要,它决定能否吸引更多客户,是决定 WAP业务成败的关键.对不同的应用领域应用 WAP技术有助于 WAP的推广,从而提高我们的工作效率.

[参考文献]

[1] 殷长友, 宋震. WAP技术应用于证券交易的一种安全措施[J]. 计算机应用与软件, 2003, 20(8): 30-31.
[2] 舒华英, 胡一闻. 移动互联网技术及应用[M]. 北京:人民邮电出版社, 2001.

[责任编辑: 刘健]