电子邮件过滤检测系统的设计与实现

王庆波，方滨兴，云晓春
(哈尔滨工业大学，　黑龙江 哈尔滨 150001)

摘　要：电子邮件给人们的通信带来了快捷与方便，其安全性与可靠性倍受关注。介绍了一种采取拦截过滤检测方式的电子邮件过滤检测系统的设计与实现方案。该系统能够根据预先设定对邮件服务器所收到的电子邮件拦截并依据过滤规则集进行过滤检测，根据不同的处理结果可采取正常接收、拒绝接收、发送警告信息等相应的处理措施，应用此系统可大大加强电子邮件服务的安全性与可靠性。

关键词：电子邮件；代理；SMPT；CORBA/IIOP
中图分类号：TP393.098　TP393.08　　**文献标识码**：A　　**文章编号**：1001-3695(2000)10-0105-02

1　引言

随着Internet技术的发展，各种网络应用服务越来越多。特别是网络中广泛应用的电子邮件服务，由于在传送信息方面具有快捷、方便、高效等优点已经成为了现代通信技术方式的重要组成部分之一。目前多数电子邮件系统所采取的服务方式是多个用户共享同一电子邮件服务器，一般这种电子邮件服务器没有必要的安全性与可靠性检查。威胁电子邮件的安全性与可靠性的主要问题有以下几种：骚扰性电子邮件、恶意破坏性电子邮件、用户不愿意接收的电子邮件。同时电子邮件系统管理员也希望禁止用户使用电子邮件进行非法信息传递。为此我们设计了电子邮件过滤检测系统，该系统能够根据用户需求对邮件内容、邮件发出者、邮件标题及邮件长度进行设定，根据设定方案可采取相应的处理措施，邮件系统管理员也可以对用户的通信内容进行检测。

2　电子邮件的报文格式及其相关协议

电子邮件的报文内容分为会话部分、邮件头、邮件体等部分。简单电子邮件传输协议SMTP(Simple Mail Transfer Protocol)、扩展电子邮件传输协议MIME(Multipurpose Internet Mail Extensions)是电子邮件传输中的主要传输协议(具体可参照RFC821、RFC822、RFC1521、RFC1522等)。由于在电子邮件的传输过程中只能传送ASCII码格式的文字信息，所以在传送过程中一般都要对报文进行编码，报文传输编码方式(Content-Transfer-Encoding)又分为Base64、Quoted Printable等多种方式。

3　系统设计方案

电子邮件服务器一般是在UNIX系统平台下运行的，而绝大多数UNIX系统都是英文操作系统。这样就很难恰当地显示电子邮件的非英文内容部分，然而本邮件过滤检测系统的基本目标之一就是使该系统的管理员可以查看过滤系统的运行情况以及不合格电子邮件的内容等相关信息。所以本系统采用UNIX与Windows相结合的分布式系统设计方案，采用JAVA语言及CORBA技术共同实现。CORBA是由OMG组织提出的一种基于对象的软构件标准，IIOP协议定义了在此标准上异构系统中对象之间的互操作规范。本系统的拦截过滤部分设置在UNIX邮件服务器上，而人工检查部分、规则集设定部分、邮件处理代理、邮件记录代理等运行在中文Windows操作系统上。它们之间的互操作采用CORBA/IIOP这种中间件技术实现，CORBA技术与JAVA技术的结合大大加强了本系统的健壮性、安全性。同时采用代理的机制使功能模块化，便于软件工程的实现。

收稿日期：2000-04-05

4　系统的实现

系统主要由电子邮件拦截接收模块、自动过滤检测模块、处理及记录模块、检测规则设定模块、人工检测管理模块组成。

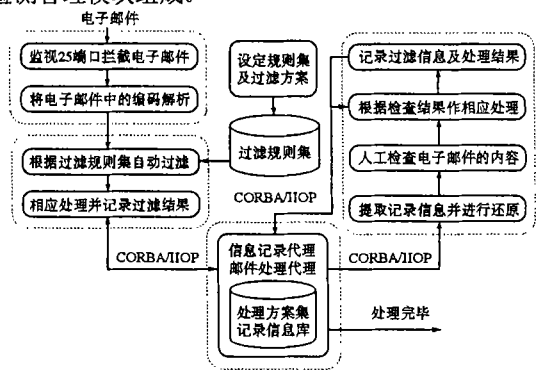

图1　电子邮件过滤系统处理流程图

拦截接收模块：本模块运行在所需检测的电子邮件服务器上，由于此模块要对电子邮件进行拦截，所以需要将原电子邮件服务器的正常接收邮件的25号IP端口更改为其它某一闲置的IP端口。此模块将对发送到25号IP端口的电子邮件依据SMTP协议规范完成与电子邮件发送端的正常邮件接收功能。此模块取代原电子邮件服务器接收功能，同时依据电子邮件的传送编码方式对编码后的电子邮件进行解码，得到正常的电子邮件信息。

自动过滤检测模块：在电子邮件接收过程中，此模块不断地对接收到的电子邮件进行过滤检测。主要

检测电子邮件会话部分、邮件头的如下部分：电子邮件源地址、目的地址、电子邮件主题、电子邮件的长度；同时依据过滤规则集对邮件体进行过滤检测。

处理及记录模块：检测的同时启动信息记录代理模块、邮件处理代理模块。对接收过程中的必要信息进行记录以便于统计分类等，同时根据过滤检测结果采取相应的处理措施。如果是检测通过的电子邮件则依据SMTP协议将电子邮件转发到原电子邮件服务器修改后的IP接收端口，由电子邮件服务器完成剩余的正常接收电子邮件过程。如果是不符合用户设定的邮件则可采用拒收、发送警告信息等设定的处理方案。如果不是系统管理员设定的邮件则通过CORBA/IIOP转交到系统管理员的人工检测处理模块进行人为的处理。

检测规则设定模块：该模块的主要功能是建立由电子邮件系统管理员，电子邮件客户两者共同设定的检测规则集。可对电子邮件的发送者的源地址、电子邮件主题、电子邮件内容中的关键词等进行设定，同时也可以根据设定采取如关键词的加权检测法等不同检测规则设定不同的过滤方案。

人工检测管理模块：当拦截接收模块接收到不符合邮件管理员设定的电子邮件时，处理及记录模块将电子邮件暂存、并做必要标记后转交给人工检测管理模块进行人工处理。本模块首先对电子邮件的基本信息进行还原，系统管理员可通过友好的界面查看该电子邮件的内容、标题、接收时间、邮件长度、收发信者、邮件附件等相关信息来确认电子邮件的安全性与可靠性。根据判断结果把电子邮件再次转交到处理及记录模块按处理方案采取相应措施。

5 总结

电子邮件是人们进行通信、获取信息的重要手段之一，人们十分重视其安全性与可靠性。共享型电子邮件服务器的用户经常受到病毒、骚扰、蓄意攻击以及其它非法的行为攻击。而有一些用户则可能利用电子邮件进行非法信息传递。若电子邮件服务器安装了本检测过滤系统则可以适度地解决此类问题。

参考文献：

[1] 唐征武，景宁，陈荦. 电子邮件服务的集成应用技术[J]. 小型微型计算机系统，1999,6.

[2] 肖钰，陆松年，诸鸿文. 电子邮件中的邮件狗[J]. 计算机工程与应用，1999，10.

[3] OMG CORBA/IIOP2.2 Specification.http: //www.omg.org[EB]. 1998-2.

(上接第96页)线仲裁的设计与实现。因为，在总线型的网络交换机中，各类网络交换模块及嵌入式CPU模块既可作为主设备来进行总线操作，又可作为从设备来响应总线操作。对于这样一个具有多个总线主控器的系统，就必然存在着总线仲裁的问题，其目的就是要合理地控制和管理系统中需要占用总线的数据源，在多个设备同时提出总线占用请求时，以一定的优先级算法判决哪个设备应获得对总线的占用权。例如，总线仲裁可采用循环优先级算法，而且总线的缺省拥有者总是为当前优先级最高的模块；也可采用固定优先级算法，如快速以太网模块获得总线使用权的优先级应高于以太网交换模块等。

5 高性能网络交换机的帧转发机制

图6为网络交换机帧转发机制算法。其中，CPU处理子程序1和子程序2分别用来完成CPU对单点报文和多点报文的处理。

6 高性能网络交换机的工程实现

网络交换机中，以太网的数据传输率为10Mbps，快速以太网的数据传输率为100Mbps，链路上的速率更高，可达125Mbps，这样，网络交换机的工程实现就需成功地解决高速电路的设计、布局布线、电源网与地网的分割滤波、电磁兼容和电磁屏蔽等技术难题。可采取的措施有：采用多层(4层或6层)PCB板设计；电容、电感滤波；布局要紧凑，走线应尽可能地短而直；差分信号要成队平行走线；为解决同步问题，时钟走线要尽量等长等等。

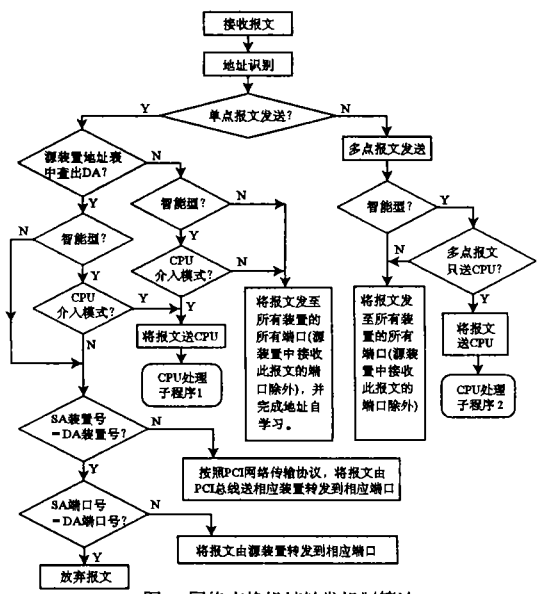

图6 网络交换机帧转发机制算法

7 结束语

目前，我们研制成功的多种型号的高性能网络交换机系列(SRswitch)性能稳定可靠，现正处于中试生产阶段，具有良好的产业化前景。

参考文献：

[1] 肖文贵，等. 交换式以太网和快速型以太网[M]. 北京：电子工业出版社.

[2] PCI Local Bus Specification (Rev 2.1)[Z]. 6/1/1995.

[3] Switched Ethernet Controller for 10BaseX[Z].

[4] Switched Ethernet Controller for 100BaseX[Z].