主动式路由器操作系统TH-AOSR的设计与实现*

马洪军 张尧学 陈 桦

(清华大学计算机科学与技术系 北京 100084)

E-mail: {mhj,zyx,chua}@sun475.cs.tsinghua.edu.cn

摘要 传统网络存在着自身难以克服的弊端,如新的网络协议、新的用户服务在现行网络上实施、推广困难.而主动网络计算则是解决这一问题的一个可行方案.文章设计并实现了一个主动式路由器操作系统——TH-AOSR(Tsinghua active operating system for router),它在兼容传统路由器功能的同时,还具有主动网络互连和计算能力,可以方便地为用户或应用提供定制服务.

关键词 主动式网络,路由器,操作系统,资源管理,安全管理.

中图法分类号 TP393

路由器操作系统是网络互连关键设备——路由器的核心软件.它主要负责路由器系统资源的管理与分配、数据包的寻址与转发、数据传输的安全与保密以及不同物理网络(PSDN,DDN,ISDN和以太网等)间的无缝连接.

路由器操作系统大致可以分为两类:一类是Cisco,Bay,3Com等网络公司为自己的路由器产品推出的专用路由器操作系统,如Cisco公司的IOS(internet operating system),另一类是强化了路由、转发等功能的通用路由器操作系统,如UNIX+gated(gated是Cornell University为UNIX平台开发的寻径程序).前者一般基于专用总线结构和硬件平台,具有很高的数据包转发速度.后者则由于受原通用操作系统体系结构的制约,数据包的转发速度相对较低.但在功能上,二者并无本质不同.

近年来,随着计算机网络应用技术的迅速发展,以转发数据包为主的传统网络逐渐暴露出一些自身存在的弊端.新的网络技术、标准、服务在现存网络上实施困难便是其中之一.如多播(multicast)、资源预约协议(RSVP)、IPv6、IP移动服务(IP mobile)等虽已出台,但至今仍不能在因特网上推广应用.主动网络技术将是解决这一问题的一个可行方案.

本文在清华大学和桑达公司联合开发成功的SED-08路由器操作系统[1]的基础上,设计并实现了一个用于清华主动网(Tsinghua active network)实验床的主动式路由器操作系统——TH-AOSR(Tsinghua active operating system for router).该系统除了具有SED-08路由器操作系统的功能外,还具有"主动"功能,即用户或应用可根据需要对它进行编程,使之实现用户或应用的定制处理.

1 主动网络

主动式网络(active network)是为了解决传统网络所存在的新服务实施困难这一问题而提出的一个新的网络概念[2].在这一概念下,网络不只是在终端系统间"被动"地转发数据包的通道,而是一个可编程的网络计算平台.它允许用户或应用在网络内部定制自己的数据包处理方法.同样地,数据包也不再只是一个仅包含用户数据的数据单元,而是一个既包含用户数据又包含数据处理程序的主动包(类似于OOP技术中的对象).当主动包到

---

* 本文研究得到国家自然科学基金和国家863高科技项目基金资助.作者马洪军,1966年生,工程师,主要研究领域为主动网,操作系统.张尧学,1956年生,博士后,教授,博士生导师,主要研究领域为网络互连,QoS,操作系统.陈桦,1972年生,博士生,主要研究领域为计算机网络,QoS,多媒体通信.

本文通讯联系人:马洪军,北京 100084,清华大学计算机科学与技术系

本文1998-08-20收到原稿,1999-01-15收到修改稿

达各节点时,主动节点下载并执行主动包中的程序,以实现对数据包的定制处理,如修改包头、处理用户数据、重定向包等.图 1 是一个简单的主动式网络(由主动式节点和传统节点构成的混合网络)的数据包处理过程示意图.

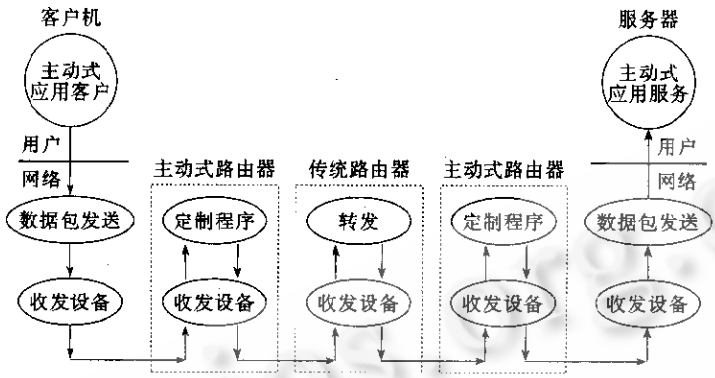

图1　主动式网络数据包处理过程示意图

与传统的网络相比,主动式网络具有两方面的优点:(1) 新技术、新标准、新服务实施容易,使得网络可以根据用户的需要迅速进行功能升级、换代;(2) 应用和网络可以实现充分的信息交流,使网络成为应用感知网络(application-aware network),使应用成为网络感知应用(network-aware application).

2　主动数据包格式与主动节点数据包处理机制

主动包的格式到现在还没有一个统一的规定.当前,各研究机构采用的格式主要有两种.

(1) IP 数据包格式的变种[3].这种格式对 IP 包进行了简单扩展,为其增加了一个携带程序主动选项.由于是与传统数据包格式兼容,因此可以简化主动网实现的复杂度.但由于受 IP 选项长度的限制,主动包携带的数据包处理程序不能大于 40 个字节.

(2) 专用主动包格式.宾西法尼亚大学主动网研究小组根据主动式网络的计算特点定义了一种全新的主动包格式[4].它打破了格式(1)中 IP 选项域长度的限制,因而可以携带功能更为强大的定制处理程序.

THAN 实验网采用的是格式(1)包格式.为了打破 IP 选项长度的限制,IP 选项只携带定制程序的名称及必要参数(即指定处理数据包的程序).当主动包到达各节点时,各节点加载、执行主动包指定的程序.主动包指定的程序(以下简称定制程序)可能存在于本地(本地提供的或先前缓存的),也可能存在于远程(与数据包同源或其他服务器).

与由 IP 选项直接携带处理程序相比,上述机制具有以下优点:(1) 数据包开销少;(2) 定制程序不受 IP 选项长度限制;(3) 可以较好地控制定制程序来源,以保证程序的安全性、可靠性以及用户对网络使用的非随意性.其缺点是,程序加载时间较长.但这一缺点可以通过增加节点缓存空间加以解决.

3　TH-AOSR 的实现

TH-AOSR 是在 SED-08 路由器操作系统基础上为 THAN 实验床所使用的路由器设计的主动式路由器操作系统.它一方面增强了原操作系统所支持的一些功能,如安全管理、网络接口;另一方面增加了一个全新的主动网处理机,以实现主动网络计算.图 2 是 TH-AOSR 的结构框架示意图.

3.1　微内核

微内核的基本功能是系统资源管理.其中的内存管理、进程(线程)调度、时钟管理、文件管理等功能与传统的多任务操作系统基本类似(事实上,TH-AOSR 这几部分功能的实现借鉴了 LINUX 系统的实现技术),在此不再赘述.下面重点介绍它的数据包缓冲区管理、链路资源管理和安全管理.

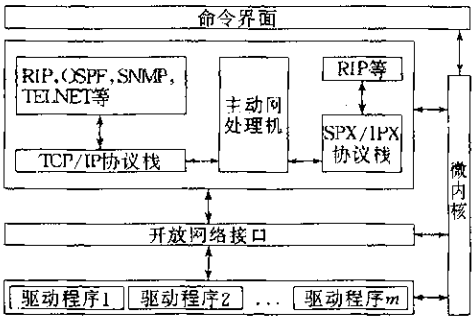

图2　TH-AOSR结构图

3.1.1　数据包缓冲区管理

为了提高路由器的性能，加快数据包的收发速度，TH-AOSR在LINUX系统的段页式内存管理基础上，创建了一个动态自适应数据包缓冲区.

缓冲区采用链栈方式管理.系统在初始化时为每一类型的网络接口创建一个数据包缓冲区链栈.每个缓冲区的大小由网络接口的最大传输单元(MTU)决定.某类缓冲区的数量由系统的可用内存空间和这类缓冲区的使用情况共同决定.

TH-AOSR根据会话的性质或服务质量协商结果来管理会话对资源的使用.

3.1.2　链路带宽管理

带宽一直是网络通信的瓶颈.因此，为了保证数据传输的质量(QoS)，必须对链路带宽资源的使用进行控制.首先，带宽资源的使用必须预约.没有进行资源预约的会话的数据包将被丢弃，或者按照"尽力传输"的方式进行传输.其次，进入的数据包将按照资源预约时的协商结果进行分类、过滤、整形，并被送入相应接口的相应队列中进行传输.最后，在各网络接口上，发送函数采用加权公平队列(weighted fair queueing)技术实现对待发送包的调度发送.

3.1.3　安全管理

TH-AOSR提供了本地认证、远程认证等安全机制，以防止用户对系统重要信息、资源等进行非法访问、占用、修改，甚至破坏.

本地认证将用户输入的帐号和口令与本地路由器中的数据库中的值作比较.如果一致，则认证通过，并授权用户的操作范围.如果不一致，则拒绝登录.

远程认证将用户输入的帐号和口令经路由器转发给安全认证服务器，由认证服务器进行确认，并给出授权的操作范围.TH-AOSR的远程认证实现了用户拨入服务远程认证协议(RADIUS).

3.2　主动网处理机

主动网处理机根据主动网络计算的需要，一方面提供了一组与主动网络计算相关的功能函数，如数据包操作函数、节点环境访问函数、数据包控制函数等，用于用户或应用定制程序运行时调用；另一方面实现了定制程序的安全加载和调度运行机制.

3.2.1　定制程序运行调度机

传统路由器的主要任务是转发数据包.因此，对CPU这一运算资源的管理较为松散(简单的进程调度).而主动式路由器的任务除了转发数据包外，还要运行定制程序.由于定制程序的安全性、可靠性难以保证.因此，为了防止某些定制程序大量且无谓地耗费CPU的运算资源，必须对定制程序的运行进行严格的管理和控制.

TH-AOSR在SED-08操作系统的进程(线程)调度(该调度机制和普通操作系统类似)的基础上实现了一种定制程序运行管理调度机(以下简称调度机).调度机是一个核心进程(线程).它的运行服从系统的进程(线程)调度策略.每个定制程序作为一个独立运行单位，由调度机调度运行.运行参数主要有：时间片、优先级、责任者(即定制程序所属的用户或应用)、生存期(time-to live)等.定制程序生存期的长短一般由指定程序的源、功能特性、责任者等几方面决定.调度机按照定制程序运行调度策略来管理和调度它们的运行.若有必要，如在调度机认为定制程序存在问题的情况下，调度机可以取消它的运行.调度策略可由管理员根据需要进行调整.

3.2.2　代码检查

定制程序不但要占用系统资源(CPU、内存)，而且可能会引起系统崩溃.因此，为了保证定制程序的安全性，TH-AOSR在定制程序的加载过程中采取了责任者认证和代码检查两项措施.责任者认证是对会话的认证.当处理机接收到主动包时，首先分析数据包的责任者是否有权运行相应的定制程序.如果有权，则检查定制程序是

否在本地.如果在本地,则加载运行.如果不在本地,则进行远程加载.加载时,要进行代码检查.如果无权运行,则按照系统配置情况,或者丢弃,或者转发.

代码检查用于检查定制程序的安全性.定制程序需要在一个封闭的"沙盒"(sandbox)内运行.因此,代码检查要检查以下几项内容:(1) 代码是否在运行时修改了自身;(2) 代码中的转移指令是否已转向非法区域;(3) 代码是否存取了非法区域.

3.3 开放网络接口

开放网络接口是连接低层物理网络接口驱动程序和高层协议栈(包括主动包处理机)的桥梁.它屏蔽了不同物理网络接口的差异,为高层提供了一致的链路服务.一方面,它主动识别接收数据帧的高层协议,实现对多协议栈的支持;另一方面,它将各协议栈要发送的数据包进行适当封装,送到相应接口上进行发送.

接收报文的处理过程,可简述如下:

(1) 当接收到物理网络接口驱动程序上传送的数据帧时,根据帧的类型,分析出它的上层协议.

(2) 如果上层协议是 IPX,则将 IPX 数据包抽取,上传到 SPX/IPX 协议栈.

(3) 如果上层协议是 IP,则进一步分析其 IP 选项域是否有主动选项.如果有,则上传到主动包处理机,否则,上传到 TCP/IP 协议栈.

(4) 如果上层协议既不是 IPX 也不是 IP,则将数据帧丢弃.

发送报文处理过程较简单,这里不再加以介绍.

4 结束语

主动式网络是当前网络界的一个新的世界性研究课题.它的研究刚起步不久,许多问题还有待解决,如包携带程序的安全性问题、主动网效率问题.TH-AOSR 是我们在当前研究成果的基础上实现的一个初步的主动式路由器操作系统,还存在许多不足.我们正在以下几个方面对其进行改进:(1) 增加 Java 支持环境,使指定程序可以用 Java 语言编写;(2) 增加对目录服务的支持,提高对网络资源的控制能力;(3) 将组件技术引入主动式网络,提供程序的重用性;(4) 实现更为严格的安全控制、管理机制,如定制程序数字签名.

参考文献

1 张尧学,赵艳标,盖峰.SED-08 路由器.高技术通讯,1997,7(10):32～34
(Zhang Yao-xue, Zhao Yan-biao, Gai Feng. A study on the router SED-08. High-Tech Letters, 1997,7(10):32～34)

2 Tennenhouse D, Smith J, Sincoskie W *et al*. A survey of active network research. IEEE Communications, 1997,35(1):80～86

3 Wetherall D, Tennenhouse D. The active IP option. In: Proceedings of the 7th ACM SIGOPS Europe. Workshop, Connemara, Ireland, 1996

4 Alexander D, Arbaugh W *et al*. The switch ware active network architecture. IEEE Network (Special Issue on Active and Controllable Networks), 1998,12(3):29～36

Design and Implementation of Tsinghua Active Operating System for Router

MA Hong-jun　ZHANG Yao-xue　CHEN Hua

(*Department of Computer Science and Technology　Tsinghua University　Beijing*　100084)

Abstract　In a traditional network, it is difficult to deploy new network protocols and services, and this problem could not be overcome by itself. Active networking, however, is a feasible way. In this paper, the authors introduce a new router operating system——TH-AOSR (Tsinghua active operating system for router), based on the investigation of active network. In addition to be compatible to traditional routers, TH-AOSR has active networking and active computing capacity, which enables any specific user or application to customize their services, while forwarding data packets securely and rapidly.

Key words　Active network, router, operating system, resource management, security management.