计算机网络发展的新环境、新应用和新课题——代前言

王行刚 陈锦章 史美林 龚 俭

90 年代中期以来, Internet 在世界范围内迅速展延、用户与日剧增, 标志着计算机网络技术从研究试验(60～70 年代)到特定应用(80 年代)进而迈入公共服务的新阶段, 也可谓本世纪发展最快的通信奇迹。

在计算机网络发展的新阶段, 将面临着一系列新的通信网环境, 需要发展更具特色和吸引公众的新应用, 研究解决一批关键的网络技术新课题。

1 新环境

计算机网络发展初期, 可利用的通信网是电话网, 特别是公用电话交换网(PSTN), 无论使用交换线还是租用专线, 都只能实现低速数据传输。因此初期的广域计算机网络的信道速率, 一般为 1.2kbit/s～9.6kbit/s。随着电话网的局间传输系统数字化和交换系统程控化, 特别是 modem 技术的进步, 基于话路的数据速率不断提高, 目前已从 9.6kbit/s 提升到 28.8kbit/s 以至 56kbit/s, 传输质量也显著提高。另一方面, 数据压缩技术取得进展, 使得甚低速率网络环境也有可能实现多媒体信息传输, 因此电话网仍然不失为广域计算机网络的一种支撑环境, 特别是作为辅助性的通信环境。

80 年代计算机网络技术一跃进入高速范围(2Mbit/s 以上), 但局限于局域范围(典型地为 1～2km), 并且需要用户自己敷设专用电缆。这类局域网(LAN)的技术性能不断在提高: 基于共享介质的 Ethernet 从 10Mbit/s、100Mbit/s 到 1Gbit/s; 基于令牌环的环形网也从 16Mbit/s 到 100Mbit/s 的 FDDI; 进而发展了基于交换的 LAN, 包括交换 Ethernet 和 ATM-LAN 等。在建筑物和建筑物群范围内也不再为电话和计算机分别单独布线, 而采用"综合布线系统"兼顾两者的需要。当前, 为构造计算机、电话、电视的综合使用环境而布线, 将出现更经济有效的、"三合一"的新"用户住地网"。

数据通信网为广域计算机网的发展提供了比较理想的通信环境。数字数据网(DDN)可为计算机网提供点—点的数字信道服务, 而不像电话网中的租用线是点-点的模拟信道, 传输质量更高, 数据速率的范围很宽, 一般为 64kbit/s 至 2Mbit/s, 甚至更高。此外, DDN 的地理覆盖范围越来越广, 使计算机用户便于按需租用。当前, 计算机网的主干信道已可根据需要使用 2Mbit/s、34Mbit/s、45Mbit/s 以至更高速率的 DDN 信道。而组网的主干信道速率是计算机网吞吐能力的关键因素之一。

分组交换数据网(X.25 网)为计算机网提供"网络服务", 为一些数据通信业务量不大、地理范围比较分散的计算机用户组网提供了一种方便的通信环境。X.25 网通常可以提供闭合用户群、虚拟专用网等附加功能, 以增强计算机团体用户的信息安全和网络监视能力等。X.25 网经营管理者一般会根据网络业务量的变化及时调整 X.25 网中各信道的速率和交换机的吞吐能力, 以保证一定的网络服务质量。但是, X.25 网数据速率较低, 一般在 64kbit/s 以下, 网络

传输延迟较大,已不适宜作为高速计算机网的主干网,但仍有一定适用范围。

帧中继网(FR 网)是广域计算机网可以使用的新环境。帧中继网业务可以在普通公用分组交换数据网上开放,也可以在 ISDN 中使用帧中继承载业务开放。预计今后几年使用帧中继协议的公用数据网将大量增加,到 2000 年,80% 以上的数据传输业务量将由 NX64kbit/s 速率的网络承担(N = 1～8)。

帧中继网技术发展可分为两个阶段,先后将帧中继技术作为交换技术和接入技术使用。当作为交换技术时,帧中继技术有三种形式:纯帧交换,中继采用帧方式;纯帧交换,交换机引入 ATM 中继接口,即采用 ATM 网作中继网络,实现帧中继和 ATM 网络互通;帧中继网和 ATM 网形成同层网络,进一步实现帧中继和 ATM 的业务互通,ATM 网向用户开放 ATM 接入业务。当帧中继技术作为接入技术应用时,帧中继业务作为一种标准的适配业务引入 ATM 网,可最大限度地保证端到端的服务质量和发挥 ATM 技术的优势。总之,帧中继网正在迅速地与 ATM 网融通。

以 ATM 为核心交换技术的 B-ISDN 是计算机网面临的更新的通信环境,在局域范围内已经出现 ATM 网络环境,在广域范围内也即将面临实用的 B-ISDN 环境。B-ISDN 将与已有的和正在发展中的各种通信网逐步实现融通,包括 X.25 网、FR 网、ISDN 等,为计算机网络发展提供既多样化又一体化的通信环境,促进计算机网络技术的变革。

计算机网络还面临另一类正在兴起的网络环境,即有线电视网(CATV 网),CATV 网正在演变,一方面从单向的广播式网络演变为双向交互式网络,另一方面不仅提供电视业务并且提供数据业务。计算机网络如何利用双向 CATV 网的宽带环境发展多媒体业务,是促进计算机网络技术发展的又一积极因素。

此外,无线通信网还为计算机网提供了无线接入手段,为发展移动计算、移动检索信息等新应用创造了条件。总之,计算机与通信的结合是非常广泛的,任何新通信环境都会及时地被计算机网络所利用,开创网络新应用。

2 新应用

传统的电信网在扩大基本电信业务(电话、数据)的普遍服务的同时,不断推出电信智能业务和扩展业务。广播电视网在扩大覆盖率的同时,正在实施数字化变革,推出双向、交互式新业务。计算机网络在发展网络应用方面有其独特的优势:无论网络节点还是网络终端都是基于计算机的系统,可以将信息的传输、交换、处理、存储和利用集成一体,可以方便地将声音、数据、图形、图像等多种媒体信息集成一体。计算机网络有条件在发展先进的新应用方面领先于其他业务网,或者说可以网络新应用为特色在信息基础设施建设中占据重要地位。

传统的计算机网络应用主要有电子邮件、文件传输和远程登录,在 Internet 中这些网络应用协议分别是 SMTP、FTP 和 Telnet。近几年在 Internet 上风行全球的网络应用主要是“万维网”(World Wide Web,WWW)信息服务。正在发展中的网络应用有电子商务、远程教育、远程医疗、电子图书馆、计算机协同工作、虚拟实验室、移动计算等等。以下摘要说明计算机网络应用技术的一些新发展或新设想。

2.1 WWW 信息服务技术

WWW 起源于改进信息资源的访问方式,采用“超文本标识语言”(HTML)作为在计算机网上进行信息查询和共享的手段。Java 语言的出现进一步丰富了 WWW 的表现形式。HTML 和 Java 的一个重要特征是它与操作系统平台的独立性。WWW 所提供的信息交流手段是独特

的, 它是一种不同于广播电视网的广播工具、浏览工具, 允许人们选择和控制所接收的信息。

WWW 建立在浏览器/服务器(Browser/Server)模式上, 以HTML 和 HTTP(超文本传输协议)为基础。其中 WWW 服务器利用超文本链路来链接各信息片段, 这些信息片段既可以放在同一主机上, 也可放在不同地理位置的不同主机上, WWW 客户浏览器负责如何显示信息和向服务器发送请求。HTTP 是 WWW 客户浏览器和 WWW 服务器之间的应用层通信协议。HTML 用于组织 WWW 服务器上的文档。建立文档间的连接。WWW 服务的特点在于高度集成性, 它能把各种信息(如文本、图像、声音、动画、录像等)和服务(如电子邮件、文件传输、远程登录、网络新闻等)完美地连接起来, 提供生动的、一致的图形用户接口界面, 并且能与已有的信息系统结合。WWW 的迅速广泛应用, 还得益于它支持既成事实标准, 使大量的已有工具可用于创建WWW 服务器的信息资源; 它使用的新标准具有简单、开放、充分利用已有标准等特点, 如 HTML 是基于电子文档交换国际标准 SGML(广泛标准标识语言), HTTP 的编码方法与电子邮件类似; WWW 软件具有开放、跨平台和可扩展性, 它不依赖于任何厂商或平台, 而且很多厂商都提供 WWW 产品等。

WWW 的发展并未结束, 正如正在不断增多WWW 服务节点一样, 它仍在迅速发展中。值得注意的是, WWW 将作为一种新的网络应用平台, 利用它再直接支撑各种应用系统, 将会给计算机网络应用带来巨大的变化。

2. 2　远程教育技术

在发达国家, 随着计算机网络的普及, 通过 Internet 已运行着多种学科、多种层次、数量庞大的教学系统, 其中最著名的有美国 PLATO 系统、加拿大的 CAL 系统、欧洲的 DELTA 工程和日本的"多用联机教育系统"等。经过 20 多年的努力, 仅 PLATO-IV 系统就存储了 150 多个专业 7000 多学时的教学内容, 美国国内已有 300 多所大专院校使用该系统进行教学, 并已出口几十套系统。目前世界上一些发达国家和地区十分重视交互式远程教育系统, 正在积极展开这方面的试验工作, 已出现以下一些形式。

(1) 远程访问(Tele-access): 通过联机访问远程信息资源进行学习, 如访问电子图书馆、数据库、博物馆、卫星数据以及远程教室。

(2) 远程体验(Tele-presence): 借助于通信网络和其它电化教育手段, 学生可以从远程来体验和感受一些事件的发生过程和结果, 这些经验在传统的教学环境中只能间接的获得。

(3) 远程辅导(Tele-mentoring): 学生可通过电子公告牌、电子新闻组、电子论坛等多种交流和辅导形式获得专家的辅导。这种远程辅导形式对于教师进修和成人教育也有积极的意义。

(4) 远程共享(Tele-sharing): 这种源于电子邮件系统的远程教育方式可推动学生之间的交流和教师之间的合作, 共享数据、经验、主意、发现等信息资源。这种教育模式将改变传统的垂直结构的师生关系, 提高参与者的平等性。

(5) 虚拟出版(Virtual Publishing): 借助于 WWW 等工具, 信息的发表不再受印刷工具的限制, 丰富了信息的表现形式, 同时也增强了学生的学习积极性。

过程教育技术对教学的影响是多方面的, 初期是作为教师的课外活动内容, 取得经验后作为正常课堂教学内容的补充; 然后修改课程设置, 增加远程教育的内容, 使远程教育技术完全进入教学环境, 教师在学习过程中的作用从传统的"站在舞台中央"转变为"幕边指导"。传统的学校和教室的概念将被打破, 而出现虚拟学校和虚拟教室。

2. 3　虚拟实验室技术

"没有围墙的实验中心"的设想是, 试图利用各种网络技术和网络工具, 为科学家们提供一

种环境,使他们更有效地利用现有的科技条件和资源而不受地域的限制,形成所谓的网络“科研协作体”(collaboratory)。

例如,位于美国华盛顿州 Richland 的太平洋西北试验室(PNL)正拟实施一项环境和分子科学虚拟实验室计划,将把分散在全美各地的不同学科领域的 250 多位专家通过 Internet 组织起来,共同研究环境科学的一些重大问题。参加协作的科学家们甚至可以通过网络共享科研协作体内的一些尖端仪器设备,研究土壤与水源污染、废物的分析、处理、存储及其对生态和人类健康的影响,研究成果也通过网络让其它学术机构共享。

网络“科研协作体”的形成将是当代科学发展的需要,它将优化研究资源的分布和利用;密切同一学科研究人员之间的联系;促进不同学科的科学家间的合作,加速基础知识的更新和传播;缩短从发明到实际应用之间的时间。

2.4 计算机协同工作技术

计算机协同工作(Computer Supported Cooperative Work, CSCW)的概念最早是在 1984 年由美国 MIT 和 DEC 的两位研究人员提出的,用于描述如何用计算机支持交叉科学的人们共同工作。一般,CSCW 指地域分散的一个群体(group)借助计算机网络技术来共同协作完成一项任务。通常,将支持协同工作的计算机软件称为群件(groupware)。

群体协作方式的多样性,为 CSCW 研究提供了丰富的内容。CSCW 系统中支持的协作方式,按时间划分为同步方式和异步方式。在同步方式时,群体各成员在同一时间进行同一任务的协作。在异步方式时,群体各成员在不同时间进行同一任务的协作。按群体成员的地理分布,协作又可分成本地协作和远程协作。典型的 CSCW 应用如下:

(1) 多媒体计算机会议:这类应用可将不同会场的与会人员活动情况,会议内容以及各种会议资料及时传递给每个与会者,实现实时多媒体信息交互,进行实时讨论和共同设计。例如,美国 Cornell 大学的 Cu-SeeMe 系统和欧洲的 MICE 系统就是典型的多媒体计算机会议系统。

(2) 协同编著和协同设计:这类应用为在不同时间和不同地点的用户提供以协作方式完成多媒体文档编著和产品设计的工具。例如,美国 Michigan 大学的 DistEdit 就是一个典型的协同编著系统。

(3) 工作流管理:工作流是指在多人参与的办公事务中所使用的一系列操作或步骤,这些步骤的发生可以是顺序的或并行的。工作流管理系统对工作流的管理提供辅助支持,自动完成有关信息交换,从而加速与事务有关的电子文档的处理速度,提高工作效率。例如,Lotus 公司的 Lotus Notes 就是一个典型的工作流管理系统。

CSCW 的发展和应用将为人们提供越来越有效的信息交流和协作工具,必将深刻地影响人们的工作和生活方式,促进经济发展和社会进步。

2.5 其他

计算机网络的重要应用领域还有电子商务、远程医疗、电子图书馆、电子出版物等,真可谓日新月异,不胜枚举。未来,“网络经济”、“网络竞争”、“网络扩张”、“信息战争”等等,都有可能从概念到现实。正是在这样广泛、深刻的网络应用需求驱动下,计算机网络技术(包括网络应用技术和组网技术)的研究开发一直是非常活跃,硕果累累,并且极快地转化为产品、商品面市。

3 新课题

计算机网络正向高速化、实时化,实现大规模互连和群体通信,加强信息安全和网络管理等方向发展。相应地引发了一批网络技术新课题,以下仅选择若干课题略加介绍。

3.1 IP 网与 ATM 网结合

通常将采用 TCP/IP 协议的计算机网简称 IP 网。IP 网具有面向无连接、分组较长等特点; 而 ATM 网具有面向连接, 以定长短信元为单位进行传输、交换等特点。为了使这现两类存在显著差异的网络结合, 已发展了以下一些方法。

(1) IP 封装(IP Encapsulation)方法, 如 IP 封装在 ATM 适配层(AAL3/4 或 AAL5)内, 这种方法不够灵活, 效率也较低。

(2) 叠加方式(Overlay Model), 类似于在以太网上叠加 IP 层一样, 可在 ATM 上叠加 IP 层。由于两者的地址空间和路由选择是分离的, IP 路由器与 ATM 交换机在功能上也是分离的, 因此这种方式需要地址解析机制。属于这类方式的有 Classical IP Over ATM 和 MPOA (Multi-Protocol Over ATM), 其中 MPOA 1.0 版已被 ATM 论坛批准。

(3) 同等方式(Peer Model), 具有同一地址空间和路由选择, 采用综合的 IP 路由器和 ATM 交换机, 形成 IP 交换网络。

IP 交换网络一般由两部分组成: 具有路由功能的交换机(IP 交换机); 外围的边缘路由器(或称IP 交换网关)。从功能上看, 路由功能在网络层实现, 交换功能在链路层实现。通过网络层的路由选择对链路层交换的映射, 使路由技术与交换技术紧密结合, 以便提高网络性能。

路由选择一般只在边缘路由器和与其相连接的 IP 交换机之间进行。边缘路由器接收到 IP 分组后, 根据目标 IP 地址按路由协议确定目标交换机, 选用已建立的源 IP 交换机与目标 IP 交换机之间的虚电路, 或者通过逐个 IP 交换机逐步建立虚电路的方式, 建立起源边缘路由器和目标边缘路由器之间的快速通道。

例如, Cascade 公司的 IP Navigator 采用前一种方法, 即在网络中任意两个交换机之间一般都预先建立了虚电路。Ipsilon 公司的 IP Switching 采用后一种方法, 即只需在第一个 IP 分组通过逐个交换机建立的临时虚电路后, 后续 IP 分组都可在该虚电路上传送。这两种方法都无需 IP 交换机对每个分组都进行路由选择, 而且采用 "切入"(cut-through)方法, 进一步减少网络延迟。

属于这类 IP 交换技术的还有 Cisco 公司的标记交换(tag switching)技术, 3Com 公司的快速IP 技术(fast IP)等。它们各有特点, 但相互之间很难互通。为了解决互通问题已在制定一种统一的标准, 即 Multi-Protocol Lebal Switching (MPLS), 预计将在一、两年内公布。

(4) 基于 ATM 网的新型计算机网络体系。这类课题研究的前提是, 计算机网并不一定基于 TCP/IP 协议。在局域和/或广域范围存在 ATM 环境的条件下, 可考虑发展新型的计算机网络体系, 以便充分利用 ATM 网的特点, 克服目前 IP 网存在的缺点, 实现具有服务质量(QoS)控制的多媒体通信业务等新目标。例如, 可考虑在计算机网络应用软件与 ATM 之间设计一种 "中间件", 它向上为应用软件提供多种不同的应用编程接口(API), 向下直接利用 ATM 信令。

3.2 多媒体通信

多媒体通信是一种新的通信业务, 它是基于群体通信(group communication)的尚待在发展中逐步界定其内涵的新业务。多媒体业务(multimedia service)的特征是, 在一次单一的通信会话(communication session)期间, 可以有多个参与方, 多条连接, 而且通信资源和用户数可以增减。

多媒体业务可分为交互型业务和分配型业务两大类。交互型业务包括会话型(如会议电视、可视电话等)、电子信函型(如声、图、文电子信箱, 文本传递等)和检索型(如可视图文, 文件

检索, 视频检索等) 业务。分配型业务按用户能否进行单独演示控制分为两种: 用户不能控制的分配型业务是广播型的, 用户不能控制广播信息的起始时间和顺序; 用户能够进行单独演示控制的分配型业务是点播型的, 用户可以控制节日的起停和顺序等。

在计算机网络上实现多媒体业务, 有的已经实现(如电子信函型业务) , 有的正在研究开发和试验。从总体上看, 现有计算机网络技术尚不能满足多媒体业务的需要, 面临着发展具有服务质量控制的、实现实时通信的群体通信技术。

群体通信要解决的关键问题包括群体管理、资源分配、群体通信的 QoS 控制等。群体管理涉及群体的建立、地址分配、关闭, 群体成员的动态加入和退出, 错误恢复等群体的管理功能。为了保证实时多媒体信息的有效传送, 需提供相应的资源预留机制, 确保有足够的可用资源, 如传送带宽、路由器的转发能力、用户机器的处理能力等。网络拥塞和缓冲区溢出会导致数据丢失, 需要通过群体通信的流控和重传等机制有效地减少拥塞和重发, 实现 QoS 控制。

群体通信体系结构, 可考虑划分为四个层次(其参考结构示于图 1) : 主机及路由扩展; 资源预留: 可靠传输; 协同应用通信支持。

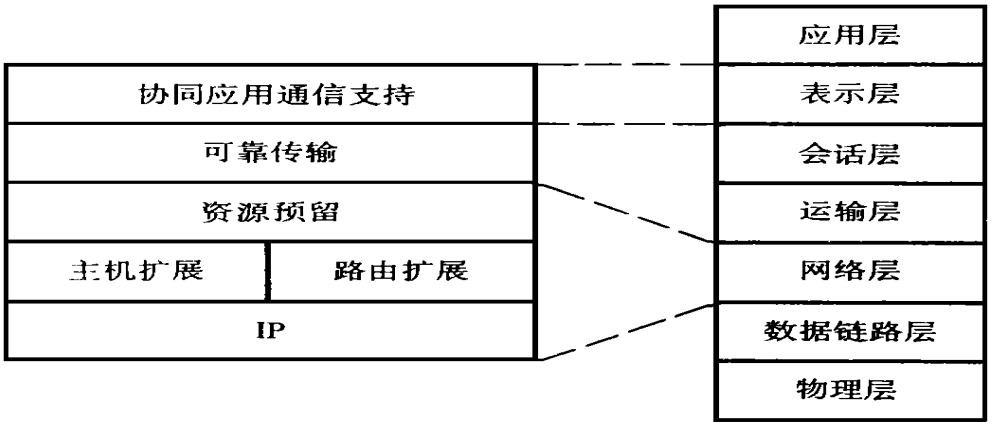

图 1 群体通信体系结构

(1) 主机扩展, 其目的是使主机具有多目标分组发送(multicast) 和接收功能, 包括群体地址管理、群体成员管理、多目标分组的发送和接收等。

发送多目标分组与发送一般IP 分组的主要区别在于: 目标地址是 D 类IP 地址; 需指定发送分组的生存期(Time-To-Time, TTL) ; 当一台机器同时有多个网络接口时, 需指定发送多目标分组的网络接口; 当发送方同时是该群体成员时, 应向本机高层回送该多目标分组的一个副本。接收多目标分组则与接收一般 IP 分组基本类似。

路由扩展, 即扩展群体通信的路由控制, 确定从多目标分组的发送方到接收群体各成员的多目标分组分发树。

多目标分组发送范围的限制方法有两种: 通过路由算法来尽量使多目标分组只向接收群体成员分发, 即 “修剪多目标分组分发树 ”方法; 通过设置每个转发端口(downstream interface) 和转发节点(downstream neighbor) 的 TTL 值, 限制生存期短的分组不向远处群体成员转发, 即 ‘限制分组生存期 ”方法。

多目标路由算法已经提出以下一些主要算法: 扩散(flooding) 算法, 分发树(spacing trees) 算法, 逆向路径广播(Reverse Path Broadcasting RPB) 算法, 修剪的逆向路径广播 TRPB (Truncated RPB) 算法, 逆向路径多目标发送(Reverse Path Multicast, RPM) 算法, 以及核心

分发树(Core-Based Tress, CBT) 算法等。

目前主要的群体通信路由协议有: 距离矢量多目标路由协议(Distance Vector Multicast Routing Protocol, DVMRP), 它扩展 IP 路由器支持多目标分组的转发, 采用 RPM 算法; 开放的最短路径优先多目标路由协议(Multicast extension to the Open Shortest Path First routing protocol, MOSPF), 它扩展 OSPF v2 以支持群体通信; 与下层协议独立的多目标路由(Protocol-Independent Multicast, PIM) 协议, 它在 Internet 上提供具有可扩展性的多目标路由, 当群体成员分布比较集中且网络带宽足够时采用 RPM 算法, 当群体成员分布比较分散且网络带宽不充足时采用类似于 CBT 算法的路由算法; CBT 协议, 它采用 CBT 算法, 核心路由器的设置由人工进行。

由上述群体通信路由算法实现的群体通信, 还存在着如何提高转发效率、尽量减少人工参与、各多目标路由协议的互连等问题。

(2) 资源预留, 其目的是为了保证数据传送所需要的网络资源。对于群体通信, 要在多目标分组分发树经过的各主机和路由器上预留相应的资源, 保证多目标分组的有效传送, 已经提出的资源预留协议(Resource reSerVation Protocol, RSVP) 是主机及路由扩展子层上的一个子层, 通过网络把有关资源预留的 QoS 要求传送到分发树经过的各路由器节点及收发各方, 在每个节点为多目标分组申请资源预留。

RSVP 程序要与路由器的资源管理模块(确定在路由器是否有足够的可用资源来保证要求的 QoS) 和权限控制模块(确定用户是否有相应的资源预留权限) 联系(参见图 2), 当这两个控制模块的检查都通过了才进行相应资源预约。RSVP 通过分组分类(packet classifier) 模块(确定每个分组的 QoS 类型) 和分组发送安排(packet scheduler) 模块(通过调整分组的发送顺序来实现对每个数据流的 QoS 承诺) 中的参数设置得到要求的 QoS。

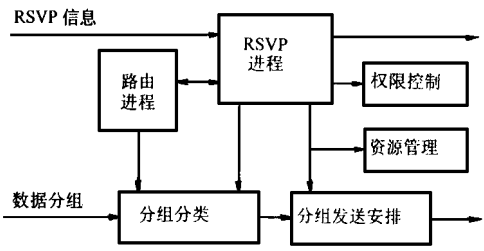

图 2　路由器中的 RSVP

当数据流从高速网络向低速网络转发、带宽无法满足最高要求时, 为了保证实时性只能丢弃部分次要信息。信息过滤(filter) 就是在这种情况下针对信息特点选择最优的信息丢弃和变换算法, 以便保留尽可能多的有效信息, 达到优化带宽利用、协调接收群体成员的不同环境、优化资源分配等。

信息过滤机制的研究目前集中在音频、视频等实时多媒体信息的压缩算法。已提出的信息过滤方法主要有: 丢弃信息片段, 如丢弃视频流中的一帧信息; 丢弃信息流中的次要特征, 如丢弃视频信息流中的彩色信息, 仅保留灰度信息; 信息压缩方式变换, 如低压缩比方式到高压缩比方式的变换。

(3) 可靠传输, 这一子层采用的可靠多目标发送协议(Reliable Multicast Protocol, RMP) 对应于运输层和会话层协议, 提供多发送方到接收群体各成员的可靠、容错、有序的信息传送。RMP 的错误恢复对于应用程序是透明的。

RMP 提供的 QoS 有以下几类: 无确认多目标发送(unreliable), 收方可能收不到、收到一份或收到多份; 有确认多目标发送(unordered), 收方至少能收到一份, 但不保证接收顺序; 有确认有序多目标发送(source ordered), 收方能且只能收到一份, 同一发送方的分组发送和接

收顺序是相同的, 但不同发送方的分组在不同接收方的总体顺序可能不同; 完全有确认有序多目标发送(totally ordered), 它把所有发送的分组排成一个顺序, 按相同的顺序送到每个接收方, 使多个发送方的分组在接收方的总体接收顺序相同。

(4) 协同应用通信支持, 这一子层针对各类信息的特点, 对各类信息的群体通信给出相应的分组格式和各字段意义约定, 反映具体信息传送的需求。实时传输协议(Transport Protocol for Real-Time Application, RTP) 就是针对实时视频和音频信息传输给出的一组分组格式, 分组中不仅有压缩的视频和音频数据, 还包括压缩格式、发送时间、分组序号、发送方信息(发送方标识、机器名、用户名、地理位置、电子邮件地址等)。这些约定对于不同类型系统间的群体通信是很重要的。

日前, 群体通信技术研究工作主要集中在群体通信路由算法和协议, 而对资源预留和可靠传输的研究还很不成熟。要较好解决群体通信问题, 尚有待不断扩展现有的计算机网络概念、方法和技术。

3.3 网络安全技术

Internet 的全球化和商业化, 引发了 Internet 技术在企业、部门、领域范围内计算机网络中的推广应用。这种基于 Internet 体系结构和技术的 "内部" 网络, 简称为 Intranet (内联网)。当 Intranet 与 Internet 互连时或在 Internet 上开展电子商务等应用时, 网络信息安全问题尤为突出。

网络安全问题涉及三个方面: 端到端安全; 端系统安全; 网络基础设施安全。

(1) 端到端安全, 涉及用户(包括代理) 之间的数据加密、鉴别、完整性维护等方面。

数据加密在于防止网络中存储和传输的数据内容被泄露, 采用的方法包括: 通信双方使用相同密钥的对称密钥体制(如 DES、IDEA 等方法); 通信双方使用不同密钥的公开密钥体制(如 RSA、离散对数方法等)。通常, 加密是根据需要在特定用户之间采取的措施。

鉴别技术用以验证用户的身份, 传统的方法是使用用户标识和口令, 还可以使用基于各种信息摘录(message digest) 算法, 如 MD5 的数字签名技术。通常, 鉴别功能可在整个网络范围内使用。

数据完整性技术用来保护网络中的数据不被非法修改, 通常使用数据签名技术来实现。

Internet IETF 有几个工作组在同时从事上述几个方面的研究工作, 例如, CAT 工作组研究开发了一组支持各种 Internet 协议开发的分布式通用安全服务和程序库(GSS-API v2, RFC2078), 包括鉴别、加密和完整性维护等功能, 以方便新协议的开发和增强互操作性, 同时还可以使这些协议不受安全技术变化的影响。

再如, OTP 工作组基于 Bellcore 的 S/KEY 技术开发了一个一次性口令鉴别系统(RFC1938), 可用于防止窃听口令的被动式攻击。

SECSH 工作组正在改进 SSH 协议, 使其为传输的数据提供自动的加密、鉴别和压缩功能, 从而增加远程登录、文件传输以及 TCP/IP 的安全性。TLS 工作组也在进行类似的工作, 开发主机之间运输层之上的安全传输通道。

WTS 工作组在研究 WWW 应用的安全性问题, 已提交两个 Internet 标准草案; HTTP 安全需求规范; HTTP 安全协议规范(SHTTP v1.1)。此外, Netscape 公司也提出了一个有关 WWW 安全的技术方案 SSL, 并已得到 Micorsoft 和 IBM 等公司的支持。

对于群体通信, 现有的加密、鉴别和完整性技术对支持其整体是合适的, 但对于群体中个别成员的安全性要求尚不能满足。

(2) 端系统安全, 主要涉及防火墙(fireware) 技术。防火墙对网络中传输的数据提供过滤功能, 可分为三类: 安全通道(通常为加密的 TCP 连接); IP 级防火墙; 应用级防火墙。

在大型 Intranet 中一些主机(如中心主机) 的安全水平可能高于防火墙, 另一些主机的安全水平则低于防火墙, 因此防火墙仅对后者有益, 而使前者损失效率。可见, 是否设置防火墙, 要视两者的比例, 还取决于所保护组织的性质(网络用户之间是否有共同利益), 以及防火墙所增加的网络开销等因素。此外, 防火墙还无法阻止内部使用合法的程序和手段向外泄漏信息, 或外部用户向内传送有害信息。总之, 防火墙技术的作用是有限的, 要避免由于设置了防火墙产生虚假的安全感, 反而使内部人员放松了警惕。

IETF 的 AFT 工作组为防火墙环境下的网络应用服务开发了一个安全鉴别协议, 使报文在穿越各个 IP 防火墙时能不断地得到鉴别。技术上基于 SOCKS 系统(RFC 1928) 。

(3) 网络基础设施安全, 涉及路由器、DNS 服务器, 以及网络控制信息和管理信息的安全问题。路由信息的控制包括: 相邻的路由器之间交换的路由信息的鉴别: 所有路由信息源点的鉴别; 对路由信息操作的鉴别等。

IETF 的 IPSEC 工作组通过在 IP 协议中增加鉴别报头(AH, RFC1826) 和安全负载封装(ESP, RFC1827) 功能来保护它所支撑的高层协议。这些安全功能的核心是加密安全服务(具体算法是可更换的), 它可支持鉴别、完整性、访问控制和数据安全等安全服务的组合。加密安全服务所需的密钥管理协议称为 IKMP(Internet Key Managment Protocol), 它正在改进中, 其最终目标是使 IP 协议支持密钥分配中心(KDC) 的概念。

IETF 的 DNSSEC 工作组过去几年的工作集中在增强 DNS 协议的安全性, 已提出 RFC2065 和 2137, 以保护 DNS 的动态修改操作(防止恶意地重用、错序和在传送过程中被篡改); 目前正在研究如何将 DNS 用作为密钥分配的辅助工具。

3.4　网络管理、轻型协议及其他

(1) 网络管理

Internet 的全球化使网络管理问题变得突出了, 这涉及全球的路由管理、IP 地址分配和域名注册等问题。

域名注册, 关于顶级域名的设立和管理一直是争论的焦点, 传统的管理和运行方式已被证明是不合适和不可靠的。一些国家的政府和一些国际组织要求介入顶级域名的制定和管理过程, 并希望能够建立相应机构来制定管理法规。

在 Internet 的商业化运行模式下, 每个用户都是通过某个 ISP 接入 Internet, 而在每个国家和地区都可能存在多个 ISP。按照路由的一般原则, 接入不同 ISP 的用户之间的信息交换要通过他们共同的某个父 ISP, 最坏情况下将通过第一级 ISP 之间交换。因此有可能出现在亚洲或欧洲的同一城市的两个用户之间要经过美国才能交换信息。为解决这个问题, 已提出 Internet 交换点(Internet eXchange Point, IXP) 的概念。IXP 的作用是在正常的路由交换系统中提供短路机制, 通过交换路由表实现两个特定网络之间的直接互连。IXP 的引入不能干扰原有的路由机制, 不能参与路由的决策。IXP 可大致分为两类: 基于链路层和基于网络层的 IXP。

(2) 轻型协议

计算机网络的低层协议的实现, 硬件尽量发挥了作用, 使得网络低层协议的执行速度不断高速化; 网络高层(运输层至应用层) 协议则主要基于软件实现, 执行速度较慢, 因而出现了传输速度高与网络软件处理速度低这种不相适应的局面。

为了解决上述矛盾, 可从研究设计新的高速协议入手, 对计算机通信全过程进行革新性的

简化, 减少操作开销。如果将传统的协议称为 "重型协议 "的话, 这类新的高速协议则可称为 "轻型协议 "(light-weight protocol)。

自 80 年代以来, 已经提出一些轻型协议, 如 NETBLT、VMTP、XTP、Delta-t 协议等。例如 NETBLT 协议是为高吞吐量的大容量数据传送而开发的, 将数据流与控制流分开, 允许两者独立处理。不过, 至今尚未提出有重大革新意义的高速协议。

协议的高速实现是解决上述矛盾的另一途径, 可考虑研制专用 VLSI、专用协议处理机来提高实现协议功能的执行速度, 包括引入并行处理机制等。

(3) 其他

计算机网络及其应用技术是一个相当宽广的领域。本文只涉及零星点面, 深度就更谈不上了。好在本专辑有十几篇好文章同时刊登, 内容涉及 LAN 到 Internet, 组网技术到网络应用, 以及网络安全、网络管理等热点, 这些将有助于读者了解国内的研究进展和国际动向。

为了促进我国计算机通信事业的发展, 总结几年来在计算机通信领域的研究、应用成果, 本刊组织了这期 "计算机通信 "专辑。

本专辑的责任编委有: 中国科学院计算技术研究所研究员 王行刚先生、邮电部数据通信技术研究所主任高级工程师陈锦章先生、清华大学计算机科学与技术系教授 史美林先生。