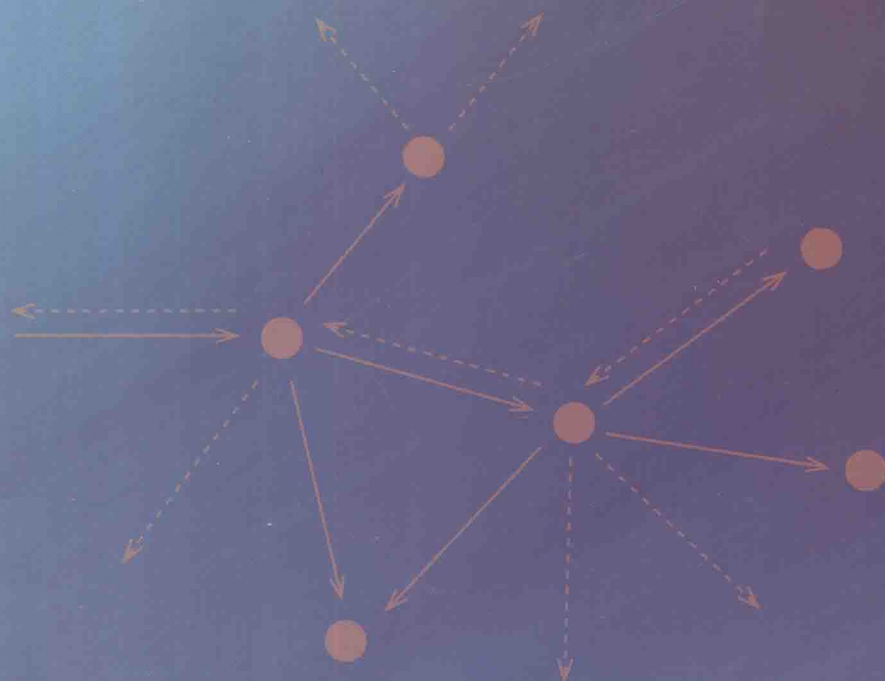


P2P网络中的 信任管理

高迎 著

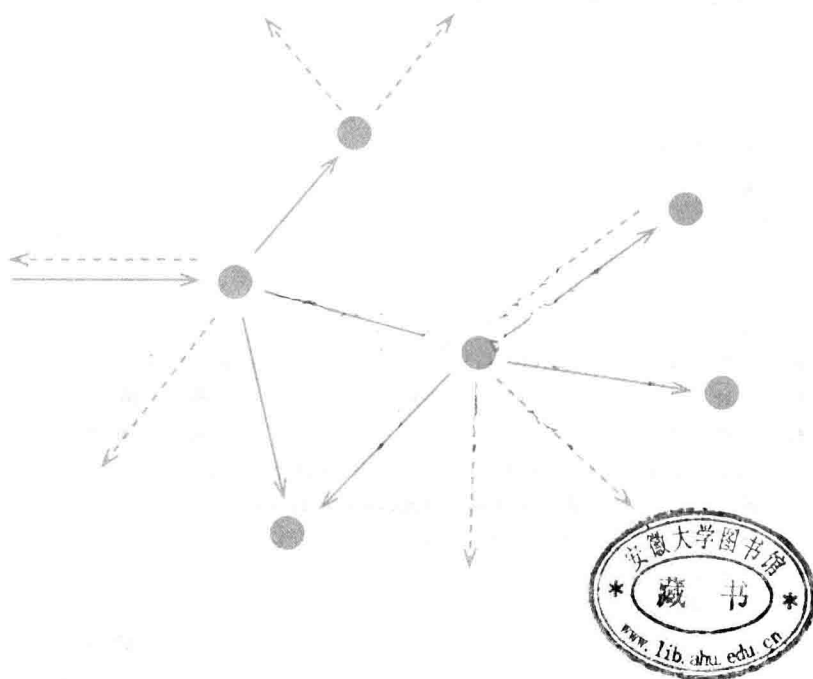


清华大学出版社



P2P网络中的 信任管理

高迎 著



清华大学出版社
北 京

内 容 简 介

本书总结了国内外有关 P2P 安全问题的研究工作进展,详细介绍了作者近年来取得的研究成果。从信任管理的角度介绍了 P2P 环境下的安全控制解决方案。本书共分 8 章,主要包括 P2P 发展概述、P2P 典型应用、P2P 网络拓扑结构、P2P 信任管理问题、基于信任值的 P2P 信任模型、基于信任值的 P2P 信任信息发布方法、分布式存储系统中基于确定性理论的 P2P 信任模型和基于动态规划的 P2P 激励机制。

本书的读者对象为高等院校计算机专业的本科生、研究生、教师、科研机构研究人员及相关领域的开发人员等。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

P2P 网络中的信任管理/高迎著.--北京:清华大学出版社,2013

ISBN 978-7-302-34031-7

I. ①P… II. ①高… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆 CIP 数据核字(2013)第 234302 号

责任编辑:梁 颖 李 晔

封面设计:何凤霞

责任校对:李建庄

责任印制:王静怡

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质量反馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:11.75

字 数:293 千字

版 次:2013 年 10 月第 1 版

印 次:2013 年 10 月第 1 次印刷

印 数:1~2000

定 价:23.00 元

产品编号:046709-01

前言

互联网技术目前正深刻改变着人们的生活和工作方式,而它的起源与一对夫妇密切相关。波萨克是斯坦福大学计算机系的计算机中心主任,勒纳是斯坦福商学院的计算机中心主任。两位计算机主任联姻成就了一段佳话。但更重要的是,他们设计了一种新型的联网设备,这种设备用于斯坦福校园网络,将校园内不兼容的计算机局域网整合在一起,形成一个统一的网络。这种设备叫“多协议路由器”,它标志着联网时代的真正到来。而这对夫妇正是 1984 年于美国硅谷的圣何塞成立的思科公司的创始人。这样一个充满着传奇和浪漫色彩的故事拉开了互联网技术发展的大幕。从此,网络技术就像具有魔力一样,以惊人的速度开始了它的发展历程,并从根本上改变了人类的工作和生活方式。

P2P 技术具有与生俱来的对等特性,在以集中的中心服务器为主体的网络发展遭遇困境之时,P2P 借助一个小小的 MP3 音乐文件的共享系统重新走入人们的视野。如今,P2P 无论在学术领域还是应用领域都获得了极大的关注,并被美国《财富》杂志称为改变互联网发展的四大新技术之一。P2P 技术在资源共享、即时通讯、分布式计算、搜索引擎、流媒体等领域起到了不可替代的作用。

虽然目前的 P2P 应用日益广泛,然而与传统的安全由服务器集中进行控制的客户端/服务器(Client/Server)系统相比,开放、自治是 P2P 系统的特点。P2P 系统中不存在中心控制节点,节点是不可靠的。这种结构在安全方面是一把双刃剑:一方面有利于隐私保护和健壮服务;另一方面在知识产权、拒绝服务等方面存在明显的漏洞。David Streitfeld(《纽约时报》撰稿人)将 P2P 描述成“对当前 Internet 的无政府主义威胁(an anarchistic threat to the current Internet)”,Marc Andreessen(网景通讯公司创始人)则把 P2P 软件称做“慈善病毒(benevolent virus)”。

面对 P2P 技术在安全方面存在的上述挑战,本书从信任管理的角度出发,提出了一系列的解决方案。本书共分 8 章,主要包括 P2P 发展概述、P2P 典型应用、P2P 网络拓扑结构、P2P 信任管理问题、基于信任值的 P2P 信任模型、基于信任值的 P2P 信任信息发布方法、分布式存储系统中基于确定性理论的 P2P 信任模型和基于动态规划的 P2P 激励机制。其中,P2P 发展概述和典型应用介绍了 P2P 的定义、发展历史和现状及 P2P 主流应用。P2P 网络拓扑结构部分介绍了目前 P2P 网络主要的拓扑结构,包括集中式拓扑、全分布式非结构化拓扑、全分布式结构化拓扑、半分布式拓扑,并详细分析了各种拓扑结构的特点和信息检索方式。P2P 信任管理问题部分则分析了 P2P 环境下网络面临的各种安全问题,并介绍了目前基于 P2P 网络的信任管理研究现状。基于信任值的 P2P 信任模型介绍了 P2P 环境下基于信任值的信任管理模型的主要模块结构及功能。P2P 信任信息发布方法部分给出了一种高效的 Gnutella 和 DHT 混合的广播算法实现证书状态发布。基于确定性理论的 P2P 信任模型部分提出了分布式存储系统 Peerstore。运用确定性理论中的不确定推理模型建立了一个 P2P 存储系统信任模型。基于动态规划的 P2P 激励机制一章提

出了动态副本管理机制——DynRM,并在此基础上给出了一种建立在激励机制上的存储资源分配算法。

本书是作者及其 P2P 信任管理研究团队近些年在这个领域努力工作的研究成果。书中分布式存储系统中基于确定性理论的信任模型研究和基于动态规划的 P2P 激励机制研究部分的编写工作得到了侯孟书教授的大力支持,在此深表感谢!此外,研究团队在 P2P 信任管理的相关研究工作受到了国家自然科学基金项目 No. 71240002、No. 60703007,北京市自然科学基金项目以及北京市人才强教计划"青年拔尖人才培养计划"等的资助。

限于作者水平,书中一定存在缺点和不足,恳请读者和专家指正!

作 者

2013 年 8 月

目 录

第 1 章 P2P 发展概述	1
1.1 P2P 技术的出现	1
1.2 P2P 与 Web 比较	6
1.3 P2P 应用	8
1.4 P2P 的特点及未来发展	14
1.4.1 P2P 的特点	14
1.4.2 P2P 的未来发展趋势	16
1.5 小结	16
参考文献	16
第 2 章 P2P 典型应用	18
2.1 资源共享领域	18
2.1.1 P2P 文件共享软件分类	18
2.1.2 P2P 资源共享系统的特点	20
2.1.3 P2P 资源共享系统的优势	21
2.1.4 典型资源共享系统介绍	22
2.2 即时通信领域	24
2.2.1 即时通信类型	24
2.2.2 即时通信软件	25
2.2.3 IM 的安全问题	27
2.3 分布式计算领域	29
2.3.1 SETI@home 项目	29
2.3.2 寻找梅森素数项目	32
2.4 搜索引擎领域	33
2.4.1 搜索引擎的发展	33
2.4.2 P2P 搜索引擎	34
2.4.3 典型工具	35
2.5 P2P 流媒体	36
2.5.1 P2P 流媒体现状	36
2.5.2 P2P 流媒体应用	39
2.6 小结	41
参考文献	41

第3章 P2P 网络拓扑结构	42
3.1 计算机网络概述	42
3.2 计算机网络拓扑结构	42
3.2.1 星状拓扑结构	44
3.2.2 总线型拓扑结构	44
3.2.3 环状拓扑结构	45
3.3 P2P 网络模型概述	46
3.4 集中式拓扑结构	47
3.4.1 集中式 P2P 网络的原理	48
3.4.2 集中式 P2P 网络的优缺点	49
3.4.3 集中式 P2P 网络应用实例	49
3.5 全分布式非结构化拓扑	50
3.5.1 非结构化 P2P 网络原理	50
3.5.2 非结构化 P2P 网络应用实例	51
3.5.3 非结构化 P2P 网络的优缺点	52
3.6 全分布式结构化拓扑	53
3.6.1 分布式散列表(DHT)原理	53
3.6.2 Tapestry 项目	54
3.6.3 Pastry 项目	56
3.6.4 Chord 协议	58
3.6.5 CAN 项目	61
3.6.6 DHT 类 P2P 网络应用实例的性能比较	63
3.7 半分布式拓扑	63
3.7.1 半分布式 P2P 网络原理	63
3.7.2 半分布式 P2P 网络优缺点	64
3.7.3 半分布式 P2P 网络应用实例	64
3.8 P2P 网络拓扑结构综合对比	65
3.9 第四代 P2P 网络	66
3.10 小结	66
参考文献	66
第4章 P2P 信任管理问题	68
4.1 P2P 网络安全问题	68
4.1.1 面临的主要安全问题	68
4.1.2 P2P 安全问题的特点	70
4.2 信任管理研究现状	72
4.2.1 PKI 信任模型	73
4.2.2 信任管理系统	74

4.2.3 主观信任值评估模型	76
4.3 P2P 网络中信任管理研究	79
4.3.1 P2P 信任管理中的基本概念	79
4.3.2 P2P 信任管理中的关键问题及现有模型的不足	82
4.4 小结	83
参考文献	84
第 5 章 基于信任值的 P2P 信任模型	85
5.1 P2P 环境中信任管理问题特点	85
5.2 基于信任值的信任管理模型	85
5.3 支持信任度的安全凭证与策略描述语言	87
5.3.1 相关概念	88
5.3.2 语法	89
5.3.3 综合用例	90
5.4 P2P 信任信息存储方法	91
5.4.1 安全凭证链查找机制中存在的问题	92
5.4.2 Hilbert 空间填充曲线	92
5.4.3 分布式动态哈希表	95
5.4.4 安全凭证信息的映射	97
5.5 基于部分关键字的信任信息查找方法	98
5.5.1 存储均衡设计	100
5.5.2 构造最小凭证图的信任链发现方法	100
5.5.3 算法性能分析	103
5.6 小结	107
参考文献	108
第 6 章 基于信任值的 P2P 信任信息发布方法	110
6.1 P2P 网络主观信任度值的计算	111
6.1.1 实体间信任关系及分类	111
6.1.2 实体直接信任值的度量	113
6.1.3 实体全局信任值的度量	116
6.1.4 信任值的存储	117
6.2 P2P 信任信息发布方法	119
6.2.1 凭证状态信息发布中存在的问题	119
6.2.2 P2P 信任管理系统中 CRL 发布方法	120
6.2.3 P2P 网络中高效的广播算法	121
6.2.4 基于 Bloom Filter 的 CRL 压缩方法	122
6.3 小结	127
参考文献	128

第 7 章 分布式存储系统中基于确定性理论的 P2P 信任模型	130
7.1 P2P 分布式存储系统	131
7.1.1 P2P 存储系统分类	132
7.1.2 典型 P2P 存储系统介绍	133
7.1.3 Peerstore 原理简介	136
7.1.4 Peerstore 文件组织	138
7.1.5 Peerstore 路由算法	139
7.1.6 Peerstore 典型文件操作	145
7.2 确定性理论	146
7.3 节点可信度	147
7.3.1 节点可信度的放置要求	148
7.3.2 节点可信度的放置	149
7.3.3 节点可信度的计算	150
7.4 安全性考虑	151
7.4.1 改变身份	151
7.4.2 冒名	152
7.4.3 虚假评价	152
7.5 性能分析	153
7.6 小结	155
参考文献	156
第 8 章 基于动态规划的 P2P 激励机制	158
8.1 动态副本管理机制	159
8.1.1 DynRM 的基本原理	160
8.1.2 DynRM 模型表示	163
8.1.3 DynRM 模型分析	164
8.2 具有激励机制的存储分配算法	165
8.2.1 具有激励机制的存储分配原则	167
8.2.2 动态规划	167
8.2.3 存储分配算法描述	168
8.2.4 节点贡献值的放置和计算	171
8.3 安全性考虑	172
8.3.1 协同作弊	172
8.3.2 诋毁	174
8.4 性能分析	175
8.5 小结	176
参考文献	177

第 1 章

P2P发展概述

1.1 P2P 技术的出现

P2P,即 Peer-to-Peer 的缩写,由于可被理解为“端对端、点对点”,所以经常被大家称为对等网。P2P 技术最早起源于联网通信方式,已经有了较长的历史。P2P 有着广泛的应用,比如被大家所熟知的 USENET(产生于 1979 年)和 FidoNet(产生于 1984 年)。随着 P2P 技术的发展,现在已经有了更新的应用以及全新的定义。

P2P 应用最初来自互联网,有些应用至今仍然在使用^[1]。P2P 技术虽然是这些早期网络应用的核心,但是大部分使用者并没有直接感觉或接触到,所以通常情况下这些应用没有被看做是基于 P2P 技术。

1969 年,当 ARPANET 作为因特网的前身刚刚出现的时候,P2P 就是当时的网络应用模式^[2]。为了实现在全美国范围内计算资源共享这一目标,ARPANET 诞生了。综合当时已有的各种局域网(比如 Utah、UCLA、UCSB、和 SRI 等大学计算机系统),使它们尽可能地形成一个完全通用的网络,并把各个主机设计成网络上的平等成员,是这个项目当时所面临的主要挑战。之后,深受大家欢迎的应用程序,诸如 FTP 和 Telnet 逐渐出现在因特网上。尽管采用了客户端/服务器方式,但在整体的使用模式上,各个主机是对称的。在这些应用中,出现在网络上的每个主机,既可以作为客户端 FTP 或远程登录到另一台主机;也可以作为服务器,提供自己的资源共享。新闻组,即 Usenet 或 Newsgroup,是一种分布式新闻组系统,它诞生于 1979 年。简言之,它是一个基于网络的计算机组合,新闻服务器就是这些计算机的统称。任何一个用户都可以借助一些软件的帮助,登录到新闻服务器上,查看消息并进行讨论。由于新闻组有着可以让任何一个网络用户都能进行相互交流的特性,所以经常被称为完全交互式的超级电子论坛。它通过 UUCP(UNIX TO UNIX Copy Protocol)协议,实现在各个计算机间完成文件复制的操作。得益于这一协议,通过拨号连接,任何一台 UNIX 计算机都可以访问另一台 UNIX 计算机,并在文件交换后自动断开。

DNS(Domain Name System)即域名系统,是因特网的一项核心服务。它的实质是一个分布式数据库,具有把域名与 IP 地址相互映射的功能,方便人们更好地访问因特网,省去记录复杂烦琐的 IP 地址的麻烦。域名系统也是当今 P2P 应用的经典实例,把域名映射成 IP 地址是它最大的功能。

起初,因特网的整体规模并不大,一共仅有几百台主机。当时,网络信息中心(NCI)作为中央权力机构,保存着一张由域名到地址的平面表 host.txt。NCI 通过邮件的方式向网

络中站点发送并更新主机的域名/地址对。随着因特网整体规模的不断扩大,DNS 最终取代了 host.txt。与 host.txt 的平面存储不同,DNS 使用的是层次的名字空间,并把该名字空间的绑定表划分成了不相交的、分布于因特网中的各个子表,并用于查询整个网络。由于每一个 DNS 的功能都完全相同:既可以被当成服务器,接受其他 DNS 的请求;也可以被当成客户端,对其他 DNS 发出请求;所以 DNS 是属于 P2P 的^[3]。

1995 年以后,越来越多的计算机使用和接入因特网,发送电子邮件、浏览网页和网上购物成为人们热衷在网络中做的事情,这些用户行为的改变深刻而长远地影响了网络架构的发展方向。由于安全和信任等原因,网上协作的崩溃随之而来、防火墙被大量的使用、非对称的网络连接方式开始流行。这些直接限制了 P2P 应用的发展。

一个非常显著的变化就是网络的主流使用方式变成了客户端/服务器(C/S)和浏览器/服务器(B/S)模式。由于受早期计算机性能、资源等因素的限制,随着互联网规模的迅速扩大,大多数连接到互联网上的普通用户并没有能力提供网络服务。随着万维网(WWW)应用方式的推行,C/S 的结构开始成为互联网中的主流。C/S 模式形成互联网上信息资源向同一方向集中,这样的模式符合一对多、强对弱的社会形式,满足了计算机网络的发展需求。运行网络客户端的计算机只是下载数据,并不需要发布或上传信息,所以它不需要一个固定的地址,也不用一直连在互联网上,它唯一需要做的就是提问并接受响应。在 B/S 模式中,客户机节点使用浏览器访问存储在网站上服务器中的内容,出现了不对等的模式。一些处理速度快、计算能力卓著、存储容量大的节点渐渐变成了共享资源的中心,它们为其他节点提供资源请求服务,而其他的普通节点由于自身处理能力、计算速度和存储能力的限制只拥有少量的资源,通过请求服务器完成自己的需求。在 C/S 模式中,服务器需要安装高性能的服务器软件。信息的交互是通过集中上传、分别下载的方式进行。C/S 模式这种集中的特点在网络构架形成的相当长时间内是一种主流的计算模式,能够满足用户的需要。

与此同时,平等协作作为互联网的本质也逐渐发生了改变。在早期,互联网是对称的,每一台因特网中的主机,都是平等的参与者;若一台计算机能够连接网络,其他计算机就可以访问它。但是随着防火墙、动态 IP(Internet Protocol,网络协议)地址以及网络地址转换技术(NAT)的发展,尤其是 20 世纪 90 年代末期非对称网络连接的发展,对 P2P 应用带来了巨大冲击。越来越多的 SIP(The Session Initiation Protocol,会话启动协议)开始提供非对称的带宽,以此获取效率的提升,而这些非对称带宽通常有着“下行带宽很大,上行带宽却很小”的特点,例如大家常用的 ADSL(Asymmetric Digital Subscriber Line,非对称数字用户环路),它的下行与上行带宽相差了 3~8 倍。由于 TCP(Transmission Control Protocol,传输控制协议)控制着速度的大小,如果上行通路带宽很小,下行通路即使带宽再大仍会受到影响。因此,如果一台计算机正在通过小带宽的上行通路将文件传送给其他计算机,那它就无法同时在大带宽的下行通路上进行文件下载;这就是大部分的 SIP 限制 P2P 程序的根本原因。

随着计算机软件的更新速度高速发展以及硬件成本的不断降低,整个 Internet 的用户量成几何级数增长,用户的需求量也不断增大,这种客户端/服务器和浏览器/服务器模式网络构架的弊端越来越明显:少数拥有快速处理能力或存储能力的节点成为系统的瓶颈——大量资源聚集在少数服务器上,使服务器的负载越来越大,即便本身具有快速处理能力也不能满足这种强大的流量需求。此外,由于大量节点中资源分布的不均匀,存在计算资源和存

储资源的剩余、计算资源的浪费。如果能将这些资源加以利用,整个网络的性能将会得到很大提高,对计算和存储资源利用率的改善也是大有裨益的。因此,人们感到有必要直接控制、改变和共享资源。20世纪90年代后期,PC的性能在速度和处理能力上突飞猛进,人们开始意识到可以将服务器软件放在单独的PC上,而且可以在PC之间初始化全双工的信息流,随着新的P2P应用技术的开发,这一“古老”的思想开始焕发出新的光彩。

当对等计算机在C/S模式下作为客户机进行操作时,它还包含另外一层可使其具有服务器功能的软件,对等计算机可以响应其他计算机发出的请求,而请求和响应范围以及方式都取决于具体的应用程序。P2P技术让人们通过互联网直接交互,把人们联系起来,使得网络上的沟通变得更加容易、更直接;任何人都可直接连接到别人的计算机进行文件交换。P2P网络中,没有所谓的中心服务器;每一个节点既作为客户机,又充当服务器;既享用其他节点提供的服务,又为其他节点提供服务。P2P中的节点都是对等的,节点之间进行直接连接与共享,C/S模式和P2P模式的结构差别如图1-1所示^[4]。

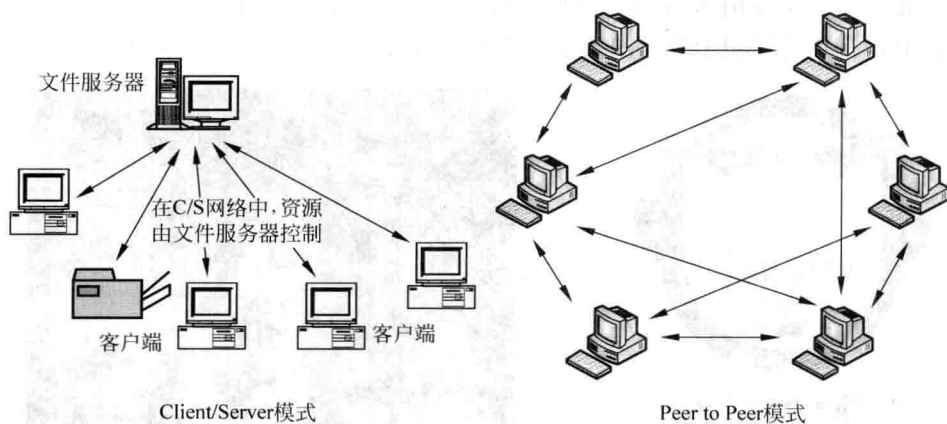


图 1-1 C/S 系统与 P2P 系统结构差别

P2P 应用可以被看做不同技术和流行趋势的产物,现在的 P2P 应用和最初已经发生了很大的改变。以下两个趋势对 P2P 技术的发展产生了决定性的影响:

(1) 把新技术结合于软件工程之中,这就形成了把工作分散的趋势。作为这种趋势的自然结果,P2P 计算产生了。

(2) 站在工程的角度上看,过去的十年来,由于企业应用集成等因素驱动,用分布式系统替代集中的单机系统已经成为一种趋势。集中式应用具有容易控制的优点,尽管这一点在某种程度上限制了分布式潮流的发展,但随着互联网的发展以及 B2B(Business To Business)商务模式的兴起,分布式计算已经成为一种强烈的商业需求。这种趋势的两个最大的影响因素就是对功能强大的网络计算机的需求和昂贵的带宽开销的需求。

P2P 计算由许多互相连接的同位体(Peer)组成,这极大地提高了效率。除此以外,社会因素也不容小觑。毫无疑问,人们对 P2P 计算的高度关注与诸如 Napster、Gnutella 这样的程序密不可分。

随着互联网的普及、网络带宽的增加以及基于互联网的端系统计算能力的增强,P2P 网络应用模式逐渐发展起来。以前在其他网络计算模式中广泛存在却又通常被忽视的客户端用户设备成为了真正具有价值的计算资源。相比于传统的客户端/服务器模式,P2P 技术的

优势是显而易见的,它能非常有效地利用现有网络上普遍存在的大量闲置信息资源、存储空间以及处理器周期,这样既避免了服务器的瓶颈问题,又降低了服务器的总成本。归功于P2P技术,网络资源从原本的集中走向现在的分散,每一个用户都能真正地参与到网络计算和应用中来,体现了自身的价值。因此,“Harness the edge of Internet”这句口号已经成为了当今一个新的研究目标。其中,“Edge of Internet”指的就是那些在传统的应用模式中广泛存在却又通常被忽视的计算设备。

让P2P思想深入人心的是美国的Napster公司^[5],它的LOGO如图1-2所示。Napster的开创者是Shawn Fanning,如图1-3所示。早在1998年,美国波士顿东北大学的一年级新生、18岁的Shawn Fanning为了帮助他的室友在网上找到喜欢的音乐而编写了一个简单的程序。这个程序能够搜索音乐文件、提供检索,并将所有的音乐文件地址存储在一个服务器上集中管理。这种处理方式极大地简化了大家搜寻自己想要歌曲的过程。出乎所有人的意料,在1999年,Napster成为炙手可热的应用程序——音乐爱好者从此梦想成真,无数人在一夜之间开始使用Napster。8000万,这是Napster在最高峰时的注册用户人数,也是一个让其他网络应用望尘莫及的数字。从此,P2P软件正式进入了人们生活。



图 1-2 Napster LOGO 图



图 1-3 Napster 创始人 Shawn Fanning

通过Napster,用户可以在网络中下载任何自己想要的音乐文件。与此同时,Napster能够让你的机器成为一台“服务器”,其他用户可以从其中下载想要的音乐。在这个网络中,实际上它提供的仅仅是音乐文件“目录”,并不提供MP3文件的下载。MP3文件实际存储在联网的每一台用户机中,下载时是从别人的机器中进行下载的,当然传输速度也非常惊人。Napster具有极其强大的搜索功能,可以将当前所有在线的用户机器上的MP3音乐信息进行自动搜寻,并进行分类管理,以备其他用户查询使用。只要输入喜欢的歌曲名称或歌手名称,就可以和全世界乐迷一起分享这音乐的饕餮大餐。也可以选择自己要与其他人在网上共享的音乐文件的目录,并且可以与喜欢同样风格音乐的人聊天、在论坛讨论、互相交流。

但是,“Napster”的出现却吓坏了美国的唱片公司,因为很多网民都能熟练地使用这类软件,在计算机上分享新出的单曲或者怀旧的老歌,昂贵的CD则有卖不出去的危险。它的出现,使音乐爱好者间共享MP3音乐变得容易,却也因此招致音像界对其导致大规模侵权行为泛滥的指控。

为此,1999年12月,代表环球、华纳、百代等七大唱片公司利益的美国唱片工业协会,以违反版权保护法为由将Napster告上法庭。2001年2月,Napster败诉,网站不得不修改

程序框架和服务流程,同时将涉及版权问题的海量音乐文件统统删除。在 Napster 上诉案的宣判中,美国第九巡回联邦上诉法院裁定:将具有版权的数字音乐制作成容易进行大量交换的集中型目录的做法是违法的;同时该法院还驳回了 Napster 公司提出的不监视该公司音乐目录的要求;同时法院还判定,虽然依据“公正使用”的原则,个人出于自身使用的目的将受著作权保护的数据复制下来是合法的,但是通过互联网将这些副本与他人交换却是违法的;而且还认定,根据“家庭音频录音法(Home Audio Recording Act)”的规定,使用计算机对音乐进行再录音也属于被禁止的行为。

尽管在法庭的责令下 Napster 已经终止,它却给点对点文件共享程序,如 KazaA、Limewire 和 BearShare 的拓展铺好了路,对这种方式的文件共享的控制,也变得愈加困难。如今 Napster 靠付费服务生存着,免费的 Napster 的流行使之在计算机领域和娱乐业成为一个传奇的符号。

P2P 这种分布计算的模型,象征着分布式运算系统的一种新体制,被很多人形象地称为“民主化体制”。自 C/S 模式广泛应用以来,在互联网上,无论是与别人连接,还是获取信息,都必须要有个中央服务器,以此作为数据聚散点并起到指挥调度作用。然而 P2P 对这种固定套路的系统进行了一次“民主革命”。P2P 技术废除了曾经的“中央集权制度”,真正实现了“人人平等”,即每个计算节点都是同等的——每台机器既是服务器,又是客户端。

惠普实验室将 P2P 定义为“利用分布式资源以非集中的方式完成特定功能的一类系统或应用”,该定义强调的是 P2P 网络的分布式特点。其中的分布式资源具体指的是计算能力、数据、存储资源、网络带宽、其他计算机和人力等资源^[6]。特定功能包括了数据或内容共享、分布式计算、交流和协作以及平台服务。非集中的方式会应用于算法、数据、原数据或者以上所有这些。当然在某些需要的时候,也包括在系统或应用的某些部分保存集中的方式。Intel 将 P2P 定义为“通过系统间的直接交换所达成的计算机资源与信息的共享”,这些资源与服务涉及处理器时钟、信息交换、缓存和磁盘空间等等。Roku Technologies 公司将 P2P 定义为“使个人与个人之间直接通信成为可能且更便捷的网络结构”。IBM 给 P2P 赋予更广阔的定义,把它看成是由若干互联协作的计算机构成的系统并具备若干特性。P2P 技术的主要特点在于充分利用分布在终端计算机上的边缘性网络资源,包括计算资源、带宽资源、内容资源等,以降低对中央服务器资源的消耗需求^[7]。

从 21 世纪开始,以 Napster、BT 为首的一些 P2P 应用程序迅速引起大家的广泛关注^[8]。与此同时,OICQ 和 MSN 等国内外即时通信应用程序也迅速风靡^[9]。其中 QQ 的运行机制和 Napster 颇为相似,即用户运行客户端,客户的账号和地址会被登记到服务器上。用户通过服务器查找其他在线用户的账号和地址,然后就可进行直接聊天。其中,对等计算方面不乏很多著名的案例,在 Distribute(). Net 案例中^[10],利用 100,000 台联网的计算机对 56 位 DES 数据加密算法实施了强力攻击;在 SETI@Home 项目中^[11],使用一个屏幕保护程序占用约 100 万台 CPU 的空闲时间,通过循环分析以寻求探索外太空生命过程中所产生的大量数据。在协同工作方面:作为 Intel 内部处理器开发工具,Netbatch 允许工程师们利用未被使用的一万台遍布全球的 Intel 公司工作站,对芯片设计进行计算机仿真,这种做法在过去十年中已累计为 Intel 公司节约了高达 5 亿美元。

纵观 P2P 的发展史,可以看到这样一个发展趋势:在互联网发展初期,“内容位于中心”。这一模式更适合当时的情况,受限于当时的技术。由于 PC 的性能很低,因此需要有

一个专门的服务器进行数据收集和处理。由于带宽太窄,PC 不得不进行被动浏览。然而随着科技的飞速发展,尤其是计算机技术和网络技术的飞速发展,高宽带互联网、高性能 PC 的出现让我们有理由相信,随后的时间将被“内容位于边缘”的模式所主导。

“资源在哪里创建,就到哪里访问”的愿望促进了因特网进入分布式计算的发展阶段。P2P 技术正在引导网络计算模型从集中式走向分布式。网络应用的核心正在由以前的中央服务器转向网络边缘的各种设备终端:从服务器到服务器、服务器到个人计算机、个人计算机到个人计算机、个人计算机到 WAP 手机……几乎每一个可以上网的设备终端都可以进行点对点的对话。这种方式把人们在互联网上的实时共享提高到了一个前所未有的高度,大家可以更自主地融入网络中去。正像第二代互联网之父 Doug Van Houweling 所说的:“下一代互联网网民们将真正参与到网络中来,每个人都能为网络的资源和功能扩展做出自己的贡献”。它改变了人们使用网络的方式,也为未来网络的发展提供了一种新的思路,财富杂志更将对等网络列为影响 Internet 未来的四项科技之一。

1.2 P2P 与 Web 比较

当 P2P 再一次摆在人们面前的时候,大家对 P2P 的含义有着各式各样的理解。从字面上看,P2P 作为 Peer-to-Peer 的缩写,其中 peer 在英语中有“(地位、能力等)同等者”、“同事”和“伙伴”的意思。由此可见,P2P 就可以被理解为“伙伴对伙伴”、“同等者对同等者”的意思,或被称为对等联网。抽象地看,P2P 就是为了达到某一既定目标而进行的生产者和消费者之间直接的信息与服务双向交换的一种行为。

定义 1.1 P2P 是一种分布式网络,网络的参与者共享他们所拥有的一部分硬件资源(处理能力、存储能力、网络连接能力、打印机等),这些共享资源需要由网络提供服务和内容,能被其他对等节点(peer)直接访问而无须经过中间实体。因此,网络中的参与者既是资源(服务和内容)提供者(服务器),又是资源(服务和内容)获取者(客户端)。

从上面的定义可以看出:

- P2P 系统是一个分布式系统,大量的节点汇集在一起共享彼此的资源(如文件、存储和 CPU)。
- P2P 是一个分散的系统,系统中不存在中心服务器,任何节点都可以充当服务器,向其他节点提供服务。
- P2P 系统是一个动态的系统,节点可以随时加入和退出。

和传统的 C/S 模型相比,P2P 系统具有如下特点:

(1) **非中心化**。网络中的每一个节点既是服务器,也是客户端。P2P 网络不像 C/S 模式那样具有权力集中的服务器,而是“全民皆兵”,整个网络的资源和服务都是分散的,其非中心化的特点在可扩展性和健壮性等方面优势突出。

(2) **可扩展性**。由于 P2P 是一个分布式系统,不存在所谓的中心服务器,所以可以更容易地对系统进行扩充。系统的处理能力会随着新节点的加入而不断增强,资源共享也会愈加丰富。

(3) **鲁棒性**。P2P 与生俱来就有抗攻击、高容错的特点。这归功于 P2P 的运行机制:它没有中心服务器,每个节点都被当成是无差别的,这样一来即使某些节点或局部网络发生

了故障,也不会对整体网络产生毁灭性的影响。P2P 网络通常都是以自组织的方式建立起来的,节点被允许自由地加入或离开网络。此外,P2P 网络还能够根据网络带宽、节点数和负载的变化随时做出相应的调整。

(4) **可用性**。系统可以复制一个内容的多个副本并将其储存到网络的多个节点上。这样即使某一个节点的内容发生了丢失,还有其他的节点可以弥补。

(5) **自适应性**。P2P 网络采用动态的拓扑结构。根据当前的运行状况,节点可动态调整拓扑结构,大大提高了使用效率。

(6) **负载均衡**。P2P 网络环境下由于每个节点既是服务器又是客户机,减少了对传统 C/S 结构服务器能力、存储能力的要求,同时因为资源分布在多个节点上,更好地实现了整个网络的负载均衡。

(7) **高性能/价格比**。性能优势是 P2P 被广泛关注的一个重要原因。随着硬件技术的发展,个人计算机的计算和存储能力以及网络带宽等性能高速增长。采用 P2P 架构可以有效地利用互联网中散布的大量普通节点,将计算任务或存储资料分布到所有节点上。利用其中闲置的计算能力或存储空间,达到高性能计算和海量存储的目的。通过利用网络中的大量空闲资源,可以用更低的成本提供更强的计算和存储能力。

目前已经出现了大量的 P2P 系统,并且 P2P 系统的数量还在迅猛增长。可以从功能、分散度、和网络结构的特点等角度对其进行分类。这里分散度表示 P2P 系统中节点在多大程度上依赖于中心服务器;网络结构指 P2P 系统的覆盖网络是受某种机制的制约还是完全动态的、即时的。

拓扑结构不同,即两个系统中节点的连接方式不同,是 P2P 技术与 C/S 模式的根本区别所在。分布式网络拓扑结构有四种基本形式:环状拓扑、集中式拓扑、树状拓扑和分散式拓扑。除此以外,将这四种基本拓扑结构进行相互结合,还可形成各种混合式的拓扑结构。只有一小部分的 P2P 是属于纯分散式拓扑的,其余绝大部分都属于带有服务器的混合式拓扑;然而 C/S 模式则为集中式拓扑。当今,互联网的技术模式还是以 C/S 模式为主,这就要求计算机拥有及其强大的处理能力和足够大的带宽支持,再配合高性能的服务器软件,服务器上不得不集中放置大量的数据,而且还需要安装各种可能会用到的服务软件,并且在集中处理数据的同时要随时应对突如其来的发自互联网客户机的各种请求,进行相关数据的发送和接收,提供处理能力和其他相关服务。与强大的服务器形成鲜明对比的是,对与之联机并接受服务的客户端的性能要求就弱小很多了。与 C/S 模式完全不同,P2P 技术的最大特点就是弱化对服务器的要求,甚至是取消服务器,实现任意两台联网的计算机机互为服务器,同时互为客户端。

在 C/S 模式下,服务器集中了互联网上的绝大部分信息和成本资源,这样的集中模式优点突出:即便于管理、安全性高,并且符合一对多、强对弱的社会关系形式,因此 C/S 模式是符合市场需求的。与之形成鲜明对比的是 P2P 技术会导致大量信息和成本资源都分散到互联网的各个终端,这也就是所谓“边缘化”。其优点是:交互性、即时性好,同时这也符合“一对一”的特点,以及彼此等同的社会关系形式,因此 P2P 技术也是符合市场需求的。正因为 C/S 模式和 P2P 模式都是符合市场需求的,且各有各的好处,所以这两种方式能够共存,而有关 P2P 替代 C/S 模式的说法是不能成立的。作为当今互联网应用的补充,P2P 技术有其独特的市场。表 1-1 从几个方面对 P2P 技术与 C/S 模式进行了比较。

表 1-1 P2P 和 C/S 模式主要指标对照表

指 标 类 型	Peer-to-Peer	Client-Server
数据发布	好	差
数据接收	中	好
数据互动性	好	差
传输速度	好	差
数据安全性	差	好
数据更新	好	差
成本控制	好	差
数据管理方便性	差	好
资源定位方便性	差	好

P2P 与 C/S 模式在对称性、耦合性等方面的对比如表 1-2 所示。通常来讲, P2P 系统的特征主要体现在: 网络中每一个节点同时具有客户端和服务器的特点, 加入 P2P 网络的每一个节点都能提供资源共享。P2P 系统还有一些其他特性, 比如: 没有中心数据库服务器、没有中心协作机制、任何一个节点都没有这样一张全局视图用来存放整个网络系统数据的位置等。除此以外, 作为 Peer 组中的成员至少需要具备这些基本特征: 服务质量可操作、能处理复杂多样的网络连接(要求拥有一套地址系统且不同于域名系统)。

表 1-2 P2P 与 C/S 架构比较

	Client-Server		Peer-to-Peer
	Session-based	Web-based	
耦合度	紧密	松散	非常松散
通信方式	不对称	不对称	对称
客户端数目	适中(1000)	高(1,000,000)	高(1,000,000)
服务器数目	很少(10)	较多(100,000)	没有(0)

1.3 P2P 应用

P2P 引导网络计算模式从集中式向分布式偏移, 也就是说, 网络应用的核心从中央服务器向网络边缘的终端设备扩散: 服务器到服务器、服务器到 PC、PC 到 PC、PC 到 WAP 手机……网络应用的核心正在由以前的中央服务器转向网络边缘的各种设备终端, 几乎每一个可以上网的设备终端都可以进行 P2P 对话。这种方式把人们在互联网上的实时共享提高到了一个前所未有的高度, 大家可以更自主地融入网络之中。

目前, P2P 主要应用和研究领域分布在以下几个方面。

1. 文件共享

BitTorrent 简称 BT, 是一种在互联网间把文件进行共享和传输的协议^[12]。它依赖于 P2P 技术, 有多款软件支持, 如 BitTorrent、BitComet 等。由于其使用极其方便, 因此被广大用户所使用。BitTorrent 共享文件的步骤如下: 首先文件将被分割成若干个分片, 并且