国家科学技术学术著作出版基金
NFAPST

对等(P2P)网络安全技术

王汝传 徐小龙 韩志杰 王 杨 李致远 吴 敏 徐 鹤 编著

科学出版社

国家科学技术学术著作出版基金资助出版

对等(P2P)网络安全技术

王汝传　徐小龙　韩志杰　王　杨
李致远　吴　敏　徐　鹤　编著

科学出版社
北京

内 容 简 介

本书首先深入分析了P2P网络系统中的安全问题，然后设计了P2P网络系统安全模型及组成部件。在此基础上，对P2P网络系统中的身份认证机制、信任与激励机制、访问控制机制、流量检测与控制机制、安全路由机制、公平交易机制、病毒防御机制进行了深入的分析，并提出一系列关键技术、机制和解决方案。本书最后还给出了P2P网络系统安全软件平台及应用示范。

本书可作为计算机、电子信息及信息安全等专业的高年级本科生、硕士及博士研究生的教材，对从事分布式计算、网络信息安全技术、信息网络应用系统研究和开发工作的科技人员也同样具有重要的参考价值。

图书在版编目(CIP)数据

对等(P2P)网络安全技术/王汝传等编著. —北京：科学出版社，2012.4
ISBN 978-7-03-033874-7

Ⅰ.①对… Ⅱ.①王… 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(2012)第047535号

责任编辑：余 丁 杨 然 / 责任校对：钟 洋
责任印制：赵 博 / 封面设计：耕 者

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销
*
2012年4月第 一 版 开本：B5(720×1000)
2012年4月第一次印刷 印张：26 3/4
字数：522 000

定价：80.00元

(如有印装质量问题，我社负责调换)

前　言

对等(peer-to-peer,P2P)计算的思想改变了 Internet/Intranet 原来的客户/服务器(client/server,C/S)计算或是浏览器/服务器(brower/server,B/S)计算这样不对称的计算模式,网络中的每个对等节点(peer)地位对等,可以同时成为服务的使用者和提供者,这就为大规模的资源共享、直接通信和协同工作提供了灵活、可扩展的计算平台。

P2P 技术已经受到学术界和产业界的关注,与网格计算(grid computing)和普适计算(ubiquitous computing)一同成为当前网络计算领域的三大研究热点。目前本领域的研究者和研究机构已经在 P2P 网络拓扑结构、资源管理、数据索引、资源查找、资源定位以及路由机制等方面取得不少重要的研究成果。同时,诞生了一批实用并受到广泛欢迎的 P2P 系统,如用于文件共享的 Napster、Gnutella、BitTorrent 等,用于语音通信的 Skype 等,目前已经被 Internet 上数以百万计的用户使用。另外值得关注的是 California 大学发起的一个大规模的 P2P 项目 SETI@home,试图聚集 Internet 上数以万计的个人计算机(personal computer,PC)所拥有的计算能力来分析无线电望远镜拾取的信号,从而寻找外星智能生物。这是利用 P2P 技术来实现计算能力的共享的典型案例。

但是,目前 P2P 技术仍然没有能够真正充分地挖掘出 Internet 所蕴涵的巨大计算能力和海量的各类资源,即真正方便、稳定地共享各种资源以解决需要大计算量、大存储空间的有价值问题。用于共享文件的 P2P 系统(如 BitTorrent)一般也只是为用户用于共享或是交换音乐、电影等娱乐性资源,这类系统中交换的大量数据甚至还会造成 Internet 等网络拥塞,进而严重影响 WWW(World Wide Web)、E-mail 等传统业务和其他关键应用的普及;SETI@home 项目也仅仅是少数的几项利用 P2P 共享计算能力的个案,一般只有这类少数有权威影响力的机构能够吸引较多数量的节点来参与其的科研项目,大多数单位或个人难以号召和聚集大量的对等节点来贡献自己的计算能力。其本质原因在于,目前的研究和系统开发主要关注于对等节点所能够提供的各种资源和 P2P 网络的构成,而忽视了 P2P 网络系统所包含的大都是 Internet 上的边缘节点——而这些节点所有者(即人)的意愿、需求、行为等才是影响 P2P 各种活动的根本因素——因而所构建的系统缺乏必要的信任、激励、协作和安全等保障机制,产生了机密信息泄漏、搭便车、公共悲剧、路由欺骗、分布式拒绝服务攻击,以及虚假文件、共谋、不合作等一系列安全问题。这样的系统难以得到持续的、良性的发展,对于复杂的任务也难以稳

定、高效、便捷地协作完成。

恶意代码的泛滥是P2P网络系统中存在的另一个严重的安全问题。P2P优秀的资源共享和通信能力使得P2P网络系统成为恶意代码滋生和传播的天然温床。P2P网络系统中存在的海量的节点,使得在P2P计算环境中的恶意代码传播速度更快,波及范围和覆盖面更大,造成的损失也更为严重。在P2P网络系统中,每个节点防御恶意代码的能力不同,只要有一个节点感染恶意代码,就可以通过内部共享和通信机制将恶意代码扩散到附近的邻居节点。因此,P2P网络系统中的恶意代码可以在短时间内造成网络拥塞甚至瘫痪、共享信息丢失、机密信息失窃,甚至完全控制整个网络。目前已经有不少研究者意识到P2P网络系统存在的上述问题,对问题原因及其解决方案展开了多方面的研究。

在学术界,P2P计算现已成为分布式系统方向最活跃的研究领域之一,国内外的很多高校和研究机构都成立了从事P2P计算研究的团队,并有一系列成果面世。对P2P的研究历程可简单描述为:2002～2003年,P2P处于理论研究阶段,DHT等理论、算法是研究热点;2003～2005年,P2P的研究开始从纯理论中走出,强调总结经验,切合实际,并且开始关注其中所包含的经济学原理及模型,由此开始对P2P中的信任、激励机制进行研究;2003年后,一些研究人员将P2P与Grid结合,代表作是Foster的一篇对比P2P与Grid的文章;2004年以后研究P2P应用的渐多,方向包括文件共享、组播、计算及存储资源共享、流媒体等方面,并开始着手研究P2P系统建模与实际性能评估,特别是P2P安全性、可靠性保障技术。可以看出,目前国内外的研究者已经从P2P技术的方方面面对其展开了深入的研究,许多研究人员都对P2P技术、P2P安全及其应用表现出极大的研究热情和研究兴趣。总之,P2P网络安全是保障P2P业务安全的关键技术,是P2P网络能否真正得以应用的关键。由于国外对P2P网络安全技术的研究起步较早,国内起步较晚,对P2P网络的安全问题的研究还不足够,也没有提出一个对于各种上层应用具有普适性的、完善的安全对等计算环境系统。

本书作者在P2P网络和信息安全技术领域已经有了多年的研究经历,具有扎实的理论基础和实践经验。本书的内容主要来源于作者所领导的科研团队承担的国家高技术研究发展计划(863计划)项目"新型对等计算网络安全关键技术"(编号:2006AA01Z439)以及国家自然科学基金项目"基于安全的移动Agent的新一代分布式网络管理关键技术研究"(编号:70271050)和国家自然科学基金项目"移动代理安全机制关键技术研究"(编号:60173037)的研究工作和相关成果。

针对目前国内对P2P及安全技术的研究需求,本书是取材国内外最新资料,在认真总结作者主持的863计划项目和国家自然科学基金项目的相关科研成果的基础上,精心组织编写的。本书详细、深入地分析了P2P技术、P2P网络安全问题、P2P安全保障机制和关键技术,集中反映了P2P安全技术的新思路、新观点、

新方法和新成果，具有较高的学术价值和应用价值。本书首先深入分析 P2P 网络系统中的安全问题，然后设计了 P2P 网络系统安全模型及组成部件。在此基础上，对 P2P 网络系统中的身份认证机制、信任与激励机制、访问控制机制、流量检测与控制机制、安全路由机制、公平交易机制、恶意代码防御机制进行了深入的分析，并提出一系列关键技术、机制和解决方案。本书最后还给出了 P2P 网络系统安全软件平台及应用示范。

本书注意从实际出发，采用读者容易理解的体系和叙述方法，深入浅出、循序渐进地帮助读者把握 P2P 及安全技术的主要内容，富有启发性。与国内外已出版的同类书籍相比，本书具有鲜明的特色：①选材新颖、学术思想新、内容新；②体系完整、内容丰富；③范例实用性强、应用价值高；④表述深入浅出、概念清晰、通俗易懂。本书可作为计算机科学技术专业、电子信息专业以及信息安全专业的大学高年级学生、硕士及博士研究生的教材，同样对从事分布式计算、网络信息安全技术、信息网络应用系统研究和开发工作的科技人员也具有重要的参考价值。

研究生支萌萌和饶元等参加了部分章节的编写工作，南京邮电大学计算机学院孙力娟、李玲娟教授和中国科技大学熊焰教授对书稿进行认真审阅并提出宝贵的意见，同时针对书稿与作者进行了有益的讨论，对本书的完成给予了很大的帮助，在此衷心感谢他们。

由于编写时间仓促，加上作者水平有限，书中不妥之处在所难免，敬请读者批评指正。

目　　录

第 1 章　P2P 网络技术概论

顾名思义，P2P 网络[1]中的每个节点的地位都是对等的，每个节点既充当服务器，为其他节点提供服务，同时也享用其他节点提供的服务。在互联网领域，P2P 模式是作为 C/S 模式的对立面出现的。P2P 技术以其特有的自组织性、分布性等优势在互联网上迅速发展，已成为互联网络不可分割的部分，P2P 网络与其他C/S、B/S 网络相比具有健壮性好、可扩展性强的特点。P2P 技术的应用更是层出不穷，包括内容共享、分布式计算、协同处理、即时通信等领域。

1.1　P2P 定义和特点

各个研究机构关于 P2P 技术给出了不同的定义。Intel 工作组认为“……P2P 是通过在系统之间直接交换来共享计算机资源和服务的一种应用模式……”。A. Weytsel认为“……P2P 是在 Internet 周边以非客户地位使用的设备……”。R. I. Granham 通过三个关键条件来定义 P2P：具有服务器质量的可运行计算机，具有独立于 DNS 的寻址系统，具有与可变连接合作的能力。根据 Clay Shirky 的定义，P2P 技术是在 Internet 现有资源组织和查找形式之外研究新的资源组织与发现方法，P2P 技术最大的意义在于不依赖中心节点而依靠网络边缘节点自组织对等协作的资源发现(discovery，lookup)形式。Kindberg 认为“P2P……是独立生存的系统……”。D. J. Milojicic 认为“P2P……给对等组提供或从对等组获得共享，对等端向组给出某些资源，并从组获得某些资源……例如节点把音乐供给组内其他人，并从其他人处获得音乐，或者捐赠计算资源用于外星生命的搜索或战胜癌症，获得帮助其他人的满足”。

我们认为比较全面完整的是 Ian Foster 对 P2P 计算技术作出的定义：“……P2P 计算技术为加入 Internet 的各种资源的使用主体和提供主体提供了非中心化的、自组织的、所有的或大部分联系是对称的分布式环境，在广域的范围内实现了对数据信息、存储空间、计算能力、功能组件、通信资源的充分利用。”

我们可以通过以下几个关键词，进一步阐明上面的定义。

关键词一：行为。P2P 所涉及的是一种交互行为，这种行为是实时动态而非静止的。

关键词二：双向交互。P2P 扩大了交互的方式和范围，每个参与交互的用户都可能同时成为产品的生产者和消费者，交互是双向的；P2P 的价值就在于服务

和资源的交换,整个网络像一个物品丰富的繁荣的集市,令每个进入 P2P 网络的主体都可能受益。

关键词三:信息。提供信息的方式、质量和数量是 P2P 系统中的又一亮点。在 P2P 中,所有的信息都是由数量巨大的 Peer 创建的,这些信息将存放在 Peer 自己的计算机上,而无须像传统的 Web 方式中那样需要"发布"在某个特定地点(网站)。Peer 依靠自己的资源,无须在服务器上申请和分配空间,这样就可以提供实时更新的信息。

关键词四:服务。用户计算机中存在大量的被闲置的计算和存储等资源。众多 Peer 可以共同参与和协作完成一项大规模的计算任务,聚集并提供单个 Web 服务器无法提供的服务和计算、存储能力。

关键词五:直接。P2P 的用户可以享受最直接最迅速的交互活动,纯粹的 P2P 网络环境中不需要中心节点,不存在中介。

关键词六:差异与对等。虽然 P2P 系统中 Peer 的能力、资源、行为存在差异性,有时这种差异是巨大的,但每个 Peer 的角色和地位在服务的提供和消费方面是对等的。

P2P 的思想改变了 Internet 原来的 C/S 计算或是 B/S 计算这样不对称的计算模式,每个节点地位对等,可以同时成为服务的使用者和提供者,这为大规模的信息共享、直接通信和协同工作提供了灵活的、可扩展的计算平台。

1.2 P2P 特点

P2P 的特点体现在以下几个方面。

(1) 非中心化:网络中的资源和服务分散在所有的 Peer 上,信息的传输和服务的实现都直接在 Peer 之间进行,而无须中间环节和服务器的介入,避免了可能的系统瓶颈。

(2) 可扩展性:在 P2P 网络中,随着节点的加入,不仅服务的需求增加了,系统整体的资源和服务能力也在同步地扩充,始终能较容易地满足用户的需要。整个体系是全分布的,不存在瓶颈。理论上其可扩展性几乎可以认为是无限的。

(3) 健壮性:P2P 网络架构天生具有耐攻击、高容错的优点。由于信息存在冗余,且服务是分散在各个 Peer 之间进行的,部分节点或网络遭到破坏对其他部分的影响有限。很多 P2P 网络都是以自组织的方式建立起来的,并允许节点自由地加入和离开,在部分 Peer 失效时能够自动调整整体拓扑,保持其他 Peer 的连通性。P2P 网络能够根据网络带宽、节点数、负载等变化不断地做自适应调整。

(4) 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,计算机的计算和存储能力以及网络带宽等性能依照摩尔定理高速

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高的计算和存储能力。

可见，与传统的分布式系统相比，P2P 技术具有无可比拟的优势。P2P 理念及技术的发展影响整个计算机网络的概念和人们的信息获取模式，某种程度上实现网络就是计算机，计算机就是网络的梦想。实质上，从狭义层次来理解，P2P 是一种技术、一种系统、一种网络结构；而从广义层次来理解，P2P 是由任何地位对等的实体构成的计算环境，是一种基于实体对等思想的计算模式。P2P 具有广阔的应用前景，Internet 上各种 P2P 应用软件层出不穷，用户数量急剧增加。尤其是 P2P 文件共享软件和即时通信软件的用户使用数量分布从几十万、几百万到上千万骤增，节点间互相交换的信息甚至给 Internet 带宽都带来巨大冲击。

1.3　P2P 与其他网络技术的对比

P2P 技术与 C/S 技术都能运行在 Internet/Intranet 平台上，也都能服务传统或新的应用，如 eBusiness、eServices 等；但在结构和构成上又有着很大区别，我们可以从管理能力、构态能力、功能模块、组织结构、资源定位等几个方面来比较 P2P 技术与 C/S 技术，具体如图 1.1 所示。

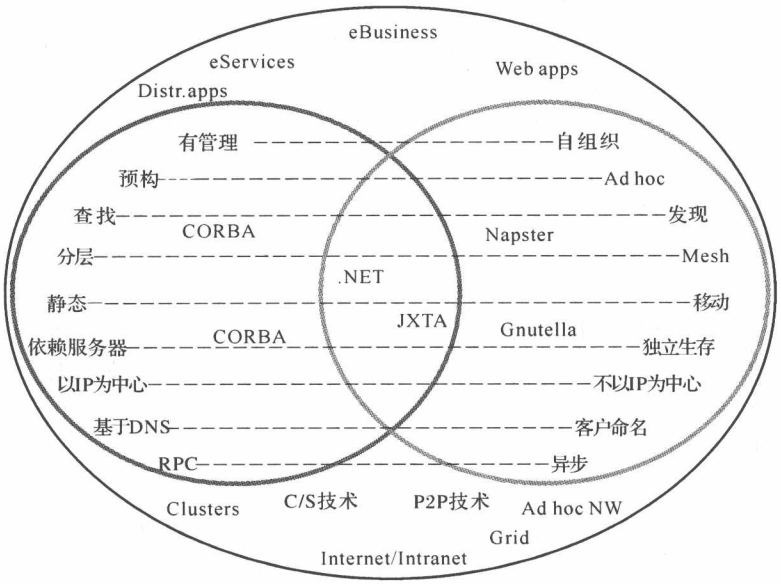

图 1.1　P2P 技术与 C/S 技术对比图

网格计算系统作为一个集成的计算与资源环境，能够吸收各种计算资源，将它们转化成一种随处可得的、可靠的、标准的且相对经济的计算能力，其吸收的计算资源包括各种类型的计算机、网络通信能力、数据资料、仪器设备甚至有操作能力的人等各种相关资源。网格是借鉴电力网的概念提出的，网格的最终目的是希望用户在使用网格计算能力解决问题时像使用电力一样方便，用户不用去考虑得到的服务来自于哪个地理位置，由什么样的计算设施提供。也就是说，网格给最终的使用者提供的是一种通用的计算能力。

对网格计算理论做出巨大贡献的 Ian Foster 等认为网格是“在缺乏中央控制、全局信息和严格信任关系的情况下能够协同使用地理分布的资源”。一般认为：将地理分布、系统异构、性能各异的高性能计算机、计算机机群、大型服务器、贵重科研设备、大型通信设备、可视化设备等，通过高速互联网络连接并集成起来，形成一个广域范围的无缝集成和协同计算环境，这个计算环境称为网格计算系统，一般称为网格。

网格计算系统是一个集成的计算资源环境，或者说是一个计算资源池，它能够集成各种计算资源，将这些计算资源转化为可靠的、标准的、抽象的计算能力。网格计算系统给最终使用者提供的是与地理位置无关、与具体的计算设施无关的通用的计算能力。组成网格计算系统的计算资源不仅包括高性能计算机、计算机机群、大型服务器，而且包括贵重科研设备(电子显微镜、雷达阵列、粒子加速器、天文望远镜等)、大型通信设备、可视化设备，以及连接这些资源的高速互联网络。

与由超级节点构成的稳定的网格计算环境相比，P2P 计算更关注于 Internet 上海量的边缘节点；P2P 技术的价值在于为对等节点间的资源共享、通信、协作提供平台；更为有战略意义的是使得从事有意义活动但又缺乏足够的计算或信息资源的某些组织可以聚集如此庞大数量的边缘节点的资源，从而完成大规模的计算任务。P2P 的网络大都在 Internet 边界或 ad-hoc 网内。基于 Internet 的 P2P 网络中的对等节点具有节点数量大、资源冗余、节点资源差异性大、节点活动的随机性大、网络的不稳定性大等特征。

从表 1.1 中可以看出，P2P 和网格有着许多相似之处，特别是在资源管理和查找机制上面。随着 P2P 计算技术的发展，用户对 P2P 系统安全性和稳定性的要求越来越高，用户希望得到极好的服务质量。与此同时，网络技术的发展使得网络研究不限于计算领域，已提出数据网格、知识网格等，这些都是为用户提供数据服务而不是计算服务。

由 SUN 公司推出的 JXTA 技术是为 P2P 的网络应用开发提供一个统一的平台。JXTA 技术是网络编程和计算的平台，提供了基础性的机制解决当前分布计算应用中面临的问题，实现新一代统一、安全、互操作以及异构的应用。JXTA 与著名的网格中间件 Globus 有许多相似之处。Globus 是一个研究性的项目，它的