中国科学 E 辑：信息科学 2008 年 第 38 卷 第 10 期：1540 ~ 1564
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

新一代互联网体系结构理论研究进展

吴建平[①②③*]，刘莹[②③]，吴茜[②③]

① 清华大学计算机科学与技术系，北京 100084;
② 清华大学信息网络工程研究中心，北京 100084;
③ 清华信息科学与技术国家实验室(筹)，北京 100084
* E-mail: jianping@cernet.edu.cn

收稿日期: 2008-06-03; 接受日期: 2008-09-11
国家重点基础研究发展计划(批准号: 2003CB314800)和国家自然科学基金(批准号: 90704001)资助项目

摘要 互联网已成为支撑现代社会经济发展、社会进步和科技创新的最重要信息基础设施. 30 年前发明的互联网面临着越来越严重的技术挑战. 文中介绍了国内外新一代互联网主要研究计划的进展情况; 分析了新一代互联网的基本特征及其发展所面临的主要矛盾; 详细介绍了国家“973”计划项目“新一代互联网体系结构理论研究”围绕新一代互联网体系结构中的关键科学问题所开展的研究和已获得的研究成果; 面对近年来新一代互联网体系结构基础研究的新形势和互联网许多创新应用对体系结构的新需求, 展望了未来该领域的研究重点.

关键词
新一代互联网
网络体系结构
多维可扩展

20 世纪发明的互联网为人类搭建了前所未有的信息通信、技术和资源共享环境, 深刻地改变着人们的生产、生活和学习方式, 成为支撑现代社会经济发展、社会进步和科技创新的最重要的基础设施. 互联网及其应用水平已经成为衡量一个国家基本国力和经济竞争力的重要标志之一.

随着超高速光通信、无线移动通信、高性能低成本计算和软件等技术的迅速发展, 以及互联网创新应用的不断涌现, 人们对互联网的规模、功能和性能等方面的需求越来越高. 30 年前发明的以 IPv4 协议为核心技术的互联网面临着越来越严重的技术挑战, 主要包括: 网络地址不足, 难以更大规模扩展; 网络安全漏洞多, 可信任度不高; 网络服务质量控制能力弱, 不能保障高质量的网络服务; 网络带宽和性能总是不能满足用户的需求; 传统无线移动通信与互联网属于不同技术体制, 难以实现高效的移动互联网等等.

为了应对这些技术挑战, 美国等发达国家从 90 年代中期就先后开始下一代互联网研究. 我国科技人员于 90 年代后期开始下一代互联网研究. 经过 10 年时间, 人们越来越深刻地认识到下一代互联网研究的重要性、复杂性、艰巨性和长期性. 目前, 虽然基于 IPv6 协议的新一

代互联网络的轮廓已经逐渐清晰, 许多厂商已开始提供成熟的 IPv6 互联设备, 大规模 IPv6 网络正在建设, 并在迅速发展. 但是互联网络面临的基础理论问题并不会随着 IPv6 网络的应用而自然得到解决, 相反, 随着信息社会和正在逐渐形成的全球化知识经济形态对互联网络不断提出新的要求, 更需要人们对现有的互联网络体系结构的基础理论进行新的思考和研究.

2003年, 清华大学、国防科技大学、北京邮电大学、东南大学和中科院网络信息中心 5 个单位共同承担了国家“973”计划项目“新一代互联网体系结构理论研究”. 该项目开展了新一代互联网体系结构基础理论、新一代互联网路由交换理论、网络动态行为和传输控制理论、可信任的互联网安全体系结构和安全监控理论、新一代互联网服务模型和服务管理理论、新一代互联网技术综合实验验证及演示平台等 6 个方面的研究工作. 经过近 5 年的研究, 项目在探索新一代互联网体系结构所面临的基础问题上, 取得了一些重要理论研究成果, 并且进行了技术实验验证, 推广应用和产业化 [1], 其中两项重要成果推动国际互联网标准组织IETF成立了专门的工作组SAVI和SOFTWIRE, 负责研究制定该技术的系列国际核心标准. 项目先后提交了近 10 项IETF标准草案, 目前已经有两项获IETF批准, 分别是: RFC4925[2]和RFC5210[3], 使中国参与IETF国际标准方面实现了新的突破, 产生了重要的国际影响. 项目研究成果的推广应用和产业化, 已获得国家科技进步二等奖 3 项.

本文首先介绍了国内外新一代互联网主要研究计划的进展情况, 分析了新一代互联网的基本特征及其发展所面临的主要矛盾; 然后详细介绍了“973”项目“新一代互联网体系结构理论研究”的研究成果; 最后, 面对近年来新一代互联网体系结构基础研究的新形势和互联网许多创新应用对体系结构的新需求, 提出了未来本领域的研究重点.

1 国内外新一代互联网体系结构研究现状

与人类历史上的绝大多数重大技术发明和工程不同, 作为人类 20 世纪最伟大技术发明之一的互联网, 人们多年来仅仅对其局部问题进行有限的数学描述, 却无法从整体上进行全面、准确的数学描述. 长期以来, 互联网基础研究的薄弱, 给人们了解互联网的基本机理, 解决它的技术难题带来了极大的困难. 例如: 传统的通信网络理论在处理互联网流量的高度突发性和自相似特性、大规模网络系统的复杂性和可控性、网络可信性等问题时已显得无能为力. 面对互联网存在的重大技术挑战, 单靠一般的技术发明和工程实践, 很难找到理想的解决方案. 因此, 基础理论在新一代互联网研究中具有重要的指导作用.

1.1 国外新一代互联网研究计划

1.1.1 美国新一代互联网研究计划 FIND 和 GENI

美国自然科学基金会NSF于 2005 年启动了两项新一代互联网研究计划: 未来互联网设计FIND[1)]和全球网络创新环境GENI[2)].

FIND 计划的目的是让研究人员发挥自己的创新与能动性, 设计一个全新的满足未来 15

1) Future Internet Design, http://find.isi.edu
2) Global Environment for Networking Innovation, http://www.geni.net

年社会需求的网络. 该项目最大的特点在于从草图设计开始, 探讨所需的网络结构及其设计, 而不是增量式地逐步改进现有网络. FIND 在网络体系结构各个方面的研究和设计都尽量做到不受以往的研究思维的影响和束缚, 即“clean slate process”. FIND 每年召开两次项目工作会. 第 4 次 FIND 工作会议于 2007 年 11 月在美国华盛顿召开, 会议分 4 个主题研讨: 信息层联网、灾害期间联网、高可靠性和限时传递的网络, 以及易于管理的网络. 此次会议还特邀中国、日本、韩国和欧洲代表参加会议, 并探讨进行国际合作研究的可能性.

GENI 计划的目的则是构建一个全新的、安全的、能够连接所有设备的互联网, 以促进互联网的发展, 并刺激创新, 促进经济增长. 其目标是发现和评估可以作为 21 世纪互联网基础的新的革命性概念、示范和技术, 建立一个用于研究未来互联网体系结构、服务和过渡的一个实验环境, 提供更多数量和更好质量的研究平台, 并能将研究成果迅速转化为实际的产品和服务, 使这些产品和服务能够提高国家未来的经济竞争力和国家安全, 并且能够让当前的网络较快过渡到新的网络体系结构. GENI 计划所设计的未来互联网将具有的特征包括: 值得社会信任、激发科学和工程革命、支持新技术融合、支持普适计算、成为物理世界和虚拟世界的桥梁, 以及支持革命性服务和应用.

GENI 由两部分组成: 研究计划(research program)和实验设施(experimental facility). 其中“研究计划”的重点是, 研究创造新的核心功能, 包括要超越现有的数据报、分组和电路交换框架, 设计新的命名、寻址和身份识别体系结构, 构建内置的网络安全机制和新的网络管理机制, 使下一代互联网具有高度安全性和可管理性. “实验设施”的重点是, 研究能够提供包括传感器和无线移动通信设备等在内的多种接入技术, 并能够部署和验证新的体系结构(例如, 新的无线技术和光技术、传感器网络、移动无线通信、RFID 等).

2007 年初, 美国自然基金 NSF 委托 BBN 技术公司进行 GENI 工程设计, 历时 4 年.

1.1.2 欧盟新一代互联网研究计划 FIRE

2007 年初, 欧盟在其第七框架FP7 中设立了“未来互联网研究和试验”(future internet research and experimentation)FIRE[1)]项目. FIRE是一项长期的试验驱动的原创性研究, 涉及了未来互联网的概念、协议和体系结构、相关的科技、工业和社会经济学等方面. 其主要研究内容包括: 网络体系结构和协议的新方法; 管理未来互联网日益增长的规模、复杂性、移动性、安全性和通透性; 在物理和虚拟结构的大规模测试环境中验证上述属性.

同为未来互联网研究计划, FIRE 和 GENI 有着很多的相同之处, 它们都关注如何搭建真实试验环境, 从而为理论研究提供证据支持. FIRE 希望通过螺旋式的部署方案, 冲出地理上的限制, 建立全球性的大规模试验环境. FIRE 同样采用虚拟化技术, 该技术将独立存在的资源和设施联系起来, 不仅使多个组织协同合作, 还能降低能耗和成本. 另外, FIRE 同样也具有联盟和跨学科等特点.

2007 年 2 月在布鲁塞尔成立了 FIRE 专家委员会, 2007 年 6 月发布专家委员会第一次报告, 确定了 FIRE 的目标、内容和发展轨迹, 并启动了 FIRE 实验设施的公告.

1) Future Internet Research and Experimentation, http://cordis.europa.eu/fp7/ict/fire/

1.2 我国下一代互联网基础理论研究现状

面对互联网的主要技术挑战和下一代互联网的重大需求, 我国较早开展了下一代互联网基础理论研究, 积极解决互联网面临的重要理论难题和技术挑战, 努力开展下一代互联网技术创新. 国家自然科学基金委员会在 2003 年前就设立了相关的课题, 支持开展下一代互联网基础理论研究. 2000 年底, 国家自然科学基金委支持启动了“中国高速互联研究实验网络 NSFCNET”项目, 在北京研制成功我国第一个地区性下一代互联网试验网络. 该网络采用当时国际上先进的 DWDM 和 IPv6 技术, 连接了清华大学、北京大学、北京航空航天大学、中国科学院、国家自然科学基金委员会等 6 个节点, 开发了一批面向下一代互联网的重大应用, 并且在国家信息产业部的协调和中国电信的大力支持下, 首先通过美国的 Internet2, 实现了我国下一代互联网试验网与国际下一代互联网的对等互联. 同时, 国家自然科学基金委员会在“十五”期间, 资助了一大批下一代互联网及其应用的探索性研究课题, 还先后启动了面向下一代互联网及其应用研究的重大研究计划“网络和信息安全”和“以网络为基础的科学活动环境研究”, 重点资助了下一代互联网体系结构、新一代网络应用平台和网络管理的基础理论和关键技术研究、网络计算环境的基础科学理论、网络计算环境综合试验平台、网格计算环境示范应用等研究项目课题. 2003 年后, 国家“973”项目陆续支持了新一代互联网相关研究.

清华大学等 5 个单位共同承担了国家“973”计划项目“新一代互联网体系结构理论研究”. 这个项目是关于互联网理论研究的“973”项目. 项目的主要目标是: 1) 在基础理论方面, 围绕新一代互联网络发展过程中的主要矛盾研究新一代互联网络的基础理论问题, 建立新一代互联网络体系结构的多维可扩展模型和分析验证理论; 建立互联网动态行为模型和分析理论; 建立互联网的资源管理与控制理论; 研究互联网的脆弱性模型并建立可信性模型理论; 建立互联网的服务模型和服务管理理论; 建立系统的互联网科学实验理论框架和多维网络行为观测模型. 2) 在网络体系结构设计和实现方面, 基于上述理论成果, 设计出面向新一代互联网络的提供多维可扩展的、可管理的、安全的网络体系结构和服务总体框架, 设计其中主要的协议机制、关键算法并实现可运行验证的原型系统. 3) 在实验平台建设和实验方面, 提出互联网基础研究的综合实验验证理论框架, 为基础研究成果的实验验证提供理论支持; 依托国家已有的下一代互联网试验平台, 建设一个新一代互联网技术的实验、验证和演示平台, 为基础研究成果的实验验证提供实验环境; 依托实验平台完成一系列典型实验和展示项目.

北京交通大学等单位承担的“973”计划项目“一体化可信网络与普适服务体系基础研究”, 针对新信息网络的体系理论问题、异质异构网络的一体化问题、新网络体系的服务普适问题、新网络体系下的可信与移动问题等科学问题, 展开研究, 希望能够创建一体化可信网络与普适服务的基础理论, 形成一系列国家与国际标准; 并创造性给出一体化可信网络与普适服务的新型体系结构, 提出一体化网络广义交换路由、服务标识和连接标识解析映射等机理与原理; 研制原型系统和验证平台, 对新型网络体系结构、理论等进行验证.

上海交通大学等单位承担的“973”计划项目“无线传感网络的基础理论及关键技术研究”, 针对国内外网络技术的发展现状和传感器件制造的发展趋势, 以建设大规模、实用化、高可靠的新一代无线传感网络系统所急需的关键技术为突破口, 围绕 3 个关键科学问题展开研究: 低

耗自组——适合于动态自组环境下的低耗节能机制; 构互连——不同传感器或传感网络互连的原理; 泛在协同——大规模部署的无线传感网络数据协同处理与控制. 希望能够实现从传统网络到新一代网络的转变, 从系统实体单元的单一同构性到泛在异构性的转变, 以能量、时间和空间复杂性最小化为目标, 提出一整套无线传感网络基础理论与关键技术的突破, 为我国无线传感网络产业的发展提供核心技术支持.

1.3 新一代互联网体系结构研究的新认识

近年来, 日本、韩国等国家也都已相继启动了未来互联网的研究计划. 可以看出, 以美国为首的发达国家已经开始新一轮新一代互联网基础研究高潮. 我们于 2003 年开始新一代互联网体系结构理论研究. 截至目前, 5 年的时间已经过去了, 相比于 5 年前, 我们目前对新一代互联网体系结构的研究又有了更深入的认识.

首先, 这 5 年国内外新一代互联网取得了新的研究进展, 主要体现在两个方面: 一是新一代互联网规模不断扩大, 研究成果不断涌现, 但是解决互联网面临的主要技术挑战进展缓慢, 急需可演进的新一代互联网体系结构扩展平台; 二是基础研究逐步得到重视, 各发达国家的科学基金和高技术研究计划纷纷资助互联网和新一代互联网基础理论的研究课题, 但是事实证明重新设计新一代互联网体系结构举步艰难. 目前正处于新一代互联网体系结构研究重要的历史机遇. 其中, 解决重大技术挑战的国际互联网 IETF 标准是体系结构的技术竞争制高点.

其次, 我们研究分析了各国新一代互联网的重大需求, 包括 IETF, GENI, FIND 和 FIRE. 分析结果表明, 这些研究计划的研究结果与我们的分析大体一致, 如表 1 所示. 这表明人们对新一代互联网需求的研究结果基本吻合, 认识基本一致.

表 1 国内外新一代互联网研究计划重大需求列表

IETF	GENI	FIND	FIRE	我们的分析
大规模路由扩展性			可扩展	扩展性
网络安全与可信	安全; 高可靠	安全可信; 普适感知、计算、内容、数据挖掘中的隐私保护	安全	安全性
IPv6 协议应用及过渡问题	高可用; 对无线通讯等新技术的支持	对未来新技术的适应性	对多跳自组网的适应性; 移动性和透明性	移动性
复杂网络环境下的管理	易配置、易管理、易错误定位	可管理、易使用		可管理
实时性流量的控制和管理		对应用的支持		高性能; 实时性
	经济增长持续性	经济增长持续性		

基于共同的研究需求, 各个国家在选择新一代互联网体系结构研究路线上却各有不同. 目前, 国内外对新一代互联网的研究有两种基本思路, 一种思路是基于现有的互联网体系结构来解决面临的重大技术挑战, 采用 IPv6 协议的大规模试验网, 攻克和实验相关的关键技术; 另一种思路是重新设计一种全新的互联网体系结构来解决面临的重大技术挑战. 人们必须承认, 互联网的技术精髓和成功经验(例如: 分层分布式体系结构、无连接分组交换、可扩展的

路由寻址、简单实用技术等)是几十年来互联网迅速发展壮大的根源, 是在互联网长期大规模技术实验的基础上逐步形成的体系结构的重要内容. 实践表明, 互联网体系结构本身具有很好的多维扩展特性. 因此, 在新一代互联网研究中, 要尽可能继承和发扬目前互联网体系结构的技术精髓, 坚持扩展和演进, 吸取创新, 将体系结构研究作为下一代互联网基础研究的重点, 使其继续在下一代互联网研究中发挥核心作用. IPv6 协议及相关技术是向新一代互联网演进技术的重要组成部分.

2 新一代互联网的主要特征及其面临的主要矛盾

2.1 新一代互联网及其基本特征

10 年来, 许多发达国家持续投入大量的人力和财力进行新一代互联网研究, 并且开展了广泛的国际交流活动. 在研究和交流过程中, 关于“什么是新一代互联网? 它和目前互联网的主要区别是什么?”, 始终没有形成统一、确切的定义. 但是, 人们面对目前互联网存在的主要技术挑战, 对新一代互联网的需求和基本特征还是有了比较一致的看法, 即: 新一代互联网应该比目前互联网“更大、更快、更及时、更方便、更安全、更易管理和更有效益”, 也可以说解决目前互联网在“扩展性、高性能、实时性、移动性、安全性、易管理和经济性”等方面存在的重大技术问题.

“扩展性”是指, 新一代互联网应该从目前互联网主要连接计算机系统扩展到连接所有可以连接的电子设备. 接入终端设备的种类和数量更多, 网络的规模更大, 应用更广泛.

“高性能”是指, 新一代互联网应该提供更高的传输速度, 特别是端到端的传输速度应该达到 10~100 Mbps, 用以支持更高性能的新一代互联网应用.

“安全性”是指, 新一代互联网应该在开放、简单和共享为宗旨的技术优势基础上, 建立完备的安全保障体系, 从网络体系结构上保证网络信息的真实和可追溯, 进而提供安全可信的网络服务.

“实时性”是指, 新一代互联网应该改变目前互联网“尽力而为”的网络服务质量控制策略, 提供可控制和有保障的网络服务质量控制, 支持组播、大规模视频和实时交互等新一代互联网应用.

“移动性”是指, 下一代互联网应该采用先进的无线移动通信技术, 实现一个“无处不在, 无时不在”的移动互联网, 真正成为人们随时可用、随处可用的生活、工作和学习环境.

“易管理”是指, 新一代互联网应该克服目前互联网难以精细管理的特点, 从网络体系结构上提供精细的网络管理元素和手段, 实现可靠的网络、业务和用户综合管理能力.

“经济性”是指, 新一代互联网应该克服目前互联网基础网络运营商投入巨资建设网络但是亏损, 网络信息内容提供商基于网络提供服务却高额盈利的不合理经济模式, 创立合理、公平、和谐的多方盈利模式, 保持它的良性和可持续的发展.

实现新一代互联网的上述基本特征, 是新一代互联网研究的主要目标. 10 年来, 各国的新一代互联网研究主要围绕实现这些基本特征展开.

2.2 新一代互联网络发展面临的主要矛盾

根据新一代互联网的基本特征, 我们分析总结了新一代互联网研究面临的 4 个基本矛盾.

2.2.1 网络体系结构的单一可扩展性和网络功能的复杂多样性之间的矛盾

虽然人们认为, 采用“边缘论”作为指导思想的基于尽力而为的互联网是体系结构可扩展性最好的网络, 但是这种体系结构的可扩展性也仅仅局限在网络互联互通的角度. 在支持新的服务方面则表现出越来越多的局限性. 例如, 很难对组播进行支持, 也很难支持大量主机都处于不断移动状态的情形. 这些问题出现的主要原因都是由于尽力而为的服务模型只考虑了互联互通的扩展性目标而没有考虑互联网络在服务等其他方面的可扩展性问题. 目前的网络体系结构在地址空间、寻址和路由方式、服务类型等方面都很难进一步扩展.

2.2.2 未知的网络行为与确定的传输控制目标之间的矛盾

基于分组交换的互联网络的流量模型和行为模型还没有得到很好的研究, 目前虽然在大规模网络的流量分析中得到了一些基于自相似和长相关的理论成果, 但是这些成果背后的科学指导作用还有待进一步发掘. 由于流量模型和行为模型的缺乏, 导致人们对大规模网络的控制和管理缺乏理论指导, 还停留在直观和经验的基础上, 这也远远不能满足要求网络提供更好的服务质量的需求.

2.2.3 网络的脆弱性和安全可信需求之间的矛盾

互联网络作为一个巨大的系统工程, 它有其固有的脆弱性. 网络上聚集了大量的硬件系统和无数的应用软件, 每一种硬件或者软件的缺陷都有可能被利用来对网络进行攻击或者恶意破坏. 那么, 如何从理论上分析网络的脆弱性并对其进行保护是还没有解决的难题. 网络在保证自身安全的基础上, 还必须为应用提供所需要的安全功能. 如何在应用规模不断增长, 性能要求不断提高的前提下保证其安全是一个困难的问题.

2.2.4 网络体系结构的相对稳定性和网络服务需求的复杂多变之间的矛盾

新一代互联网络的复杂性(规模更大、结构更复杂、异构性更强)以及用户和服务提供者对服务需求的复杂性和多样性(服务的互操作性、提供速度、可用性、可扩展性、可管理性和服务质量、服务的智能化和个性化等)使得人们急需对如何构建大规模互联网络服务的理论指导. 如何根据新一代互联网络的体系结构建立相应的服务模型, 如何快速灵活地为用户提供具有高可用性、良好互操作性和高性能的服务, 如何对现有的服务进行协调为端用户提供可重用的服务, 如何对服务进行管理, 都是困难而极有价值的理论问题.

3 主要研究内容

互联网体系结构说明了互联网的各部分功能组成及其相互关系, 是互联网基本形态的描述. 互联网体系结构基础研究是互联网基础研究的重要组成部分. 人们在研究新一代互联网的过程中, 始终认为应该首先研究新一代互联网体系结构的基本问题. 国家“973”计划项目“新

一代互联网体系结构理论研究”在探索新一代互联网体系结构所面临的基础问题上, 取得了初步的研究结果.

3.1 新一代互联网发展面临的关键科学问题及其内在联系

首先, 根据上述的互联网发展面临的基本矛盾, 分析得出了要解决的 4 个关键科学问题. 研究和解决这些关键科学问题, 可以为新一代互联网络体系结构研究奠定理论基础.

3.1.1 互联网体系结构的多维可扩展性问题

对该问题的研究有助于解决现有网络体系结构的单一可扩展性和网络功能的复杂多样性之间的矛盾.

随着网络单元技术的不断发展和新的网络应用的不断出现, 研究人员不断地给互联网络增加新的功能. 但是随着功能的不断增加, 原有的基于“边缘论”的互联网络体系结构的局限性也暴露的越来越明显, 集中体现在网络的多维可扩展性方面. 我们知道, 互联网络在最初设计时是以互联互通为第一目标, 因此才确定了“边缘论”的设计思想, 网络提供尽量简单的服务模式, 采用基于尽力发送的分组交换模式. 保证数据可靠传输和其他的应用功能都由用户主机在网络边缘实现. 这种网络体系结构在网络规模可扩展角度的确具有良好的效果.

但是在应用要求网络能够提供多种多样不同目标和要求服务的今天, 这种单一模式的基于层次结构的网络体系结构已经力不从心. 例如, 为了使网络能够对不同的应用提供服务质量保证, 研究人员投入了大量的精力, 但是仍然难以使其投入实用. 这一方面是由于网络的控制和管理方面还没有取得重大的理论突破, 另一方面也是受现有网络体系结构的限制, 因为在现有网络体系结构下, 网络核心能够提供的功能非常有限. 因此, 新一代互联网络体系结构要解决的第一个基本科学问题就是现有网络体系结构的单一可扩展性和网络功能的复杂多样性之间的矛盾问题, 重点研究新一代互联网络的多维可扩展性问题.

网络体系结构的多维可扩展性问题主要体现在下面几个方面:

- 体系结构对于网络规模的可扩展性, 也就是说体系结构必须能够适应网络规模的不断增长, 包括网络层次结构、路由模型、地址结构等等;
- 体系结构对于网络支持的服务种类的可扩展性, 包括对单播、组播、任意播、服务质量保证和移动应用等多种服务的支持;
- 体系结构对于网络采用的不同传输技术的可扩展性, 包括对光传输技术、无线传输技术等新的技术的支持.

在研究新一代互联网体系结构的时候, 需要首先解决新一代互联网体系结构模型问题, 对现有网络分层体系结构进行深入研究, 新一代互联网体系结构首先要解决分层体系结构由于层次功能固定而难以进行扩展的问题, 同时将吸收主动性网络和应用层网络的优点, 设计出可扩展的、可管理的、高性能的、安全可靠的网络体系结构模型, 为实现新一代互联网络的发展目标提供保证.

协议是网络体系结构的关键组成部分, 需要研究面向新一代互联网络的协议验证和测试

理论.

IPv6 将是新一代互联网的主要网络层协议, 但是它只是部分解决了新一代互联网中的地址空间缺乏问题. 需要在新一代互联网体系结构框架内, 研究并设计鲁棒的基于 IPv6 协议的互联机制.

3.1.2 网络动态行为及其可控性问题

对该问题的研究有助于解决未知的网络行为与确定的传输控制目标之间的矛盾.

互联网络发展至今, 已成为一个庞大的非线性复杂巨系统. 具体表现为: 系统的规模和用户数量巨大且仍在不断增长, 异质异构的网络融合发展; 网络协议体系庞杂, 垂直方向上呈现出多样化的层次结构, 而水平方向上又以地域和功能为标准进一步形成分布且多级的架构; 在业务性质上表现为多种业务的集成与综合, 业务量突发性日渐明显, 且不同业务要求不同的服务质量保证; 网络节点间、节点与数据分组间由于协议而产生的非线性作用以及用户之间的合作与竞争, 使网络行为呈现出相当的复杂性并且难以预测. 如何建立系统、科学和刻画用户及其流量动态特性以及网络自身行为特征的模型是深刻认识和把握当前乃至新一代互联网网络行为的关键所在. 它必将对网络行为状态的描述与预测、新协议的设计、开发与应用、新一代互联网络的规划、管理与控制, 以及构建安全、可信赖的网络基础设施起到至关重要的指导作用.

就网络传输控制而言, 模型化工作中的突破, 即便是很小的进展, 往往会给该领域其他相关方向的研究带来意想不到的启发和促进. 理解业务流的基本属性是合理实施管理与控制的基础. 现在互联网无记忆性的基本假设和由此而演绎出的理论与方法面临严峻挑战. 突发自相似流量的重拖尾分布给队列分析制造了不小的障碍, 进而无法找到理想的资源预留策略和有效的连接接纳控制方法, 同时, 实时应用又进一步提出了对网络高阶性能指标进行分析与评价的要求. 构造独立业务源数学描述模型本身就困难重重, 而非线性协议的耦合作用又进一步增加了定量描述聚合流的困难. 前者固然重要, 但它们同控制策略与机制一起组成的子系统模型才是针对特定目标进行优化控制的基础, 当然如果能进一步构造出多个子系统复合而成的较复杂系统的描述模型, 则定会有益于诸如流量工程等从整体上优化网络传输性能的研究工作. 数学模型对于传输控制之所以重要, 是因为只有基于一定的模型, 才能够通过一定的观测变量较为准确地综合出网络的当前状态, 甚至有可能预测其变化趋势, 这样采取的控制策略才会有的放矢. 凭借局部经验和启发式算法, 对运动规律和行为状态浑然不知的复杂系统进行控制的结果是可以想象的, 某些典型网络流量控制算法的局部有限性便是最好的例证. 当然, 建立精确的网络流量模型决非易事, 甚至完全不可能, 但已有的研究表明: 粗线条的近似模型对于某些传输控制问题往往是足够充分, 模型应该是未知的网络行为与确定的传输控制目标之间建立联系的纽带.

此外, 以模型化为基础的网络行为学研究也将为网络实时监控提供一种新的解决方案. 从统计角度分析网络正常行为特征, 进而建立相应的网络流量正常行为基准模型; 从时间序列模型和网络流量的历史数据资料, 建立网络行为的预测模型, 然后基于这些模型来监测网络异常行为, 进而过滤和定位可能的攻击.

如何有效地管理和控制这个已经具备相当规模, 并不断发展的大尺度复杂巨系统? 在理论上和技术上至今依旧没有找到理想的解决方案. 目前有关网络管理与控制的多数研究, 在方法上沿袭了体系结构设计中的思路, 过分依赖于经验和直觉, 没有充分强调理论分析的重要性, 缺乏具有普适性结论和定律的归纳与描述. 固然, 互联网自身的复杂性使问题变得异常困难, 但是, 借助一定的成熟理论, 或者发现新的方法, 去透彻地认识和理解这个人工非线性复杂系统的动力学行为, 并基于所得结论和适当的模型对具体的管理控制机制、协议和算法逐渐加以完善和优化, 使互联网向更及时、更高效、更健壮、更可管理的方向演进, 应该是研究充分管理与控制当前乃至新一代互联网的指导思想.

在既定的网络体系结构下, 如何保障所构建的网络稳定而高效地依照预期运行, 取决于是否能找到行之有效的流量管理措施和控制方法. 因为模型的不完备和有效理论分析方法的欠缺, 目前大多数研究采用不依赖模型的启发式算法设计, 配合典型仿真实验加以验证的方法, 取得了一些局部性的研究成果. 但随着网络规模和复杂性的日益扩大, 此方法将会越来越力不从心, 其所得结果的局限性也将越发明显. 为寻找可能的、较为彻底的解决方案, 需要从体系结构、协议机制和算法实现等各个层次上强调模型和理论分析的重要性, 抓住业务流量的突发性, 网络状态的时变性和控制作用的滞后性等网络传输控制中的鲜明特征, 提出合理的、可实践的服务质量(QoS)架构, 并依赖成熟且可行的理论方法设计能够保证 QoS 实现的具体机制与算法, 并使它们具有良好的动态自适应特性, 从而克服目前多数启发式静态和准动态算法适应性差的缺陷. 在算法性能的评价和验证方面, 仅仅依赖典型、有限、局部的仿真试验往往无法得出系统、科学、可信的判断, 理论分析与证明的过程不可缺少, 需要在网络传输控制的研究中给予充分重视, 从而避免目前一些仅依赖仿真验证的典型算法在应用环境发生变化时再一次通过试验确定参数的尴尬局面.

3.1.3 脆弱复杂巨系统的可信性问题

对该问题的研究有助于解决网络的脆弱性和安全可信需求之间的矛盾.

虽然计算机网络已经成为社会重要的基础设施, 但是现在的计算机互联网中普遍存在的脆弱性导致互联网是不可信任的. 例如: 路由系统无法验证数据包的来源是可信的; 用户担心敏感信息或个人隐私泄露、关键应用的开发者和所有者担心互联网受攻击影响应用系统的可用性、出了问题之后无法追查肇事者等.

互联网的脆弱性(vulnerability)表现在设计、实现、运行管理的各个环节. 首先, 互联网设计阶段的脆弱性, 尽力而为的设计思想使得网络中间节点对传输数据包的来源难以验证和审计, 导致地址假冒、垃圾信息泛滥, 大量的入侵和攻击行为无法跟踪. 其次, 无论新一代互联网的体系结构设计如何完美, 计算机软件和硬件系统在实现过程中的脆弱性仍然是难以避免的, 而且在网络运行和管理阶段各种安全漏洞或者安全机制与管理政策之间的不一致性是普遍存在的. 另外, 即便对于国家机要部门, 也难免不使用国外厂商的软硬件系统构造网络基础设施, 担心这些系统内部存在后门, 也是导致互联网不可信任的因素之一.

互联网的可信任性(trustworthiness)比安全的概念更加广泛, 目标是给用户提供一个可信赖的计算环境. 一个可信任的互联网络应该具有如下特性: 1) 传统意义上的安全性, 即系统和

信息的保密性(confidentiality)、完整性(integrity)、可用性(availability); 2) 真实性(authenticity), 即用户身份、信息来源、信息内容的真实性; 3) 可审计性(accountability), 即网络实体发起的任何行为都可追踪到实体本身; 4) 私密性(privacy), 即用户的隐私是受到保护的, 某些应用是可匿名的; 5) 抗毁性(survivability), 在系统故障、恶意攻击的环境中, 能够提供有效的服务; 6) 可控性(controllability), 指对违反网络安全政策(security policy)的行为具有控制能力.

可信任性是新一代互联网的目标, 但是从根本上消除脆弱性、企图设计并实现一个绝对安全的互联网络是不切实际的. 新一代互联网络可能在安全体系结构设计上减少一定的脆弱性, 但是在实现、运行管理等方面的脆弱性仍将长期存在. 因此, 可信任性不得不建立在脆弱的网络基础上. 多层木桶原理(即在纵深防御系统保护下, 系统的安全保护的强度等于最强的安全措施的保护强度)给我们一些启示, 在一个脆弱性的网络上建立可信任性是可能的. 事实上, 互联网最初的设计思想中也体现了基于脆弱性之上的可靠性, 比如分组交换和动态路由技术.

建立在脆弱性之上的可信任性的理论基础是系统模型的宏观监测、预测与模型干预理论. 首先需要从运行安全的角度对互联网建立一个数学模型, 其中包括量化的脆弱性、可信任性相关的参数. 利用一些基本的数理统计方法, 比如 Bayes 预测动态模型、Markov 链、数字滤波、小波分析等方法, 评估网络系统状态的脆弱性与可信任性. 该数学模型中应该加入管理者的经验, 能够预测大规模突发事件, 并且可以模拟管理者控制措施的效果.

3.1.4 稳定网络体系结构的服务多样性问题

对该问题的研究有助于解决网络体系结构的相对稳定性和网络服务需求的复杂多变之间的矛盾.

快速灵活地为用户提供具有高可用性、可伸缩性、互操作性、高性能的服务是互联网发展的主要目标. 由于网络体系结构的相对稳定性导致网络结构演进缓慢, 网络技术的继承性增强. 因此, 随着新一代互联网规模的扩大, 网络环境将更复杂, 网络设备和终端的异构性更强, 用户和服务提供者对服务的互操作性、提供速度、可用性、可扩展性、可管理性和服务性能等提出了更高的要求. 如果随着网络规模、环境和技术, 以及用户和服务提供者需求的改变, 独立开发不同的服务, 将重复大量的工作, 耗费巨量的资源, 从而极大地限制了网络服务在深度和广度上向前发展.

因此, 必须在理论上深入剖析独立于具体网络环境和用户需求的互联网服务的共有和特有的本质行为特征, 根据服务共有的行为特征抽象出服务框架, 在服务框架的基础上, 依据服务所特有的本质行为特征来描述复杂多变的互联网服务, 并构建服务的运行环境. 这样, 才能快速地构建满足需求的互联网服务, 才能灵活地对服务的特征进行伸缩剪裁. 此外, 必须研究服务本质行为特征之间的关系, 检测和解决服务特征冲突, 提高服务的可用性. 还需要研究服务的动态发现和装配方法, 使得互联网服务能够更方便快捷地提供给用户.

服务的可管理性是新一代互联网服务的核心问题之一. 可以预见互联网上的服务将与时俱增, 如果没有科学的方法对服务进行管理, 互联网的服务将不可控. 如何对服务的属性、故障、性能进行描述, 如何对服务的性能进行管理, 如何在服务出现故障时及时地进行故障检测和诊断, 如何在不同的服务功能组件之间进行协调, 如何确立服务计费的指导性原则和计费

模型, 这些是服务管理必须解决的理论问题.

以上4个关键科学问题的内在联系如图1所示. 互联网体系结构是从功能的角度来研究网络的. 描述互联网应该提供的功能、功能划分以及各功能模块之间的关系, 是对互联网静态的描述. 多维可扩展的互联网体系结构需要解决多个维度的可扩展性问题, 包括如何在服务、安全、控制等维度都能提供扩展性良好的框架. 这个问题的解决将为后续几个科学问题的解决奠定良好的研究基础.

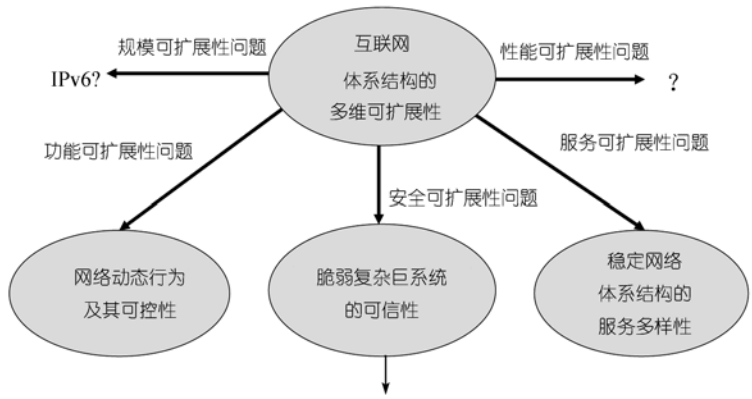

图 1 新一代互联网体系结构的关键科学问题和内在联系

互联网发展到今天, 规模越来越大, 协议越来越复杂, 传输的信息越来越多, 互联网行为与当初的设计思想已经有很大偏差. 因此还需要观察分析互联网的动态行为特性, 即从互联网行为学的角度研究互联网. 而互联网的动态性和不确定性使得对互联网的控制越来越难, 在新一代互联网基础研究中要重点解决网络的可控性问题, 主要体现在传输控制和安全控制. 传输控制和安全控制基础理论的建立将有助于我们认识新一代互联网络的本质特征, 更好地掌握其在动态发展变化中的本质规律, 从而可以更充分地发挥互联网络对信息社会的巨大推动作用.

互联网发展的历史表明, 相对于网络本身, 网络应用的发展和变化是非常快的. 为了适应不断变化的应用需求和相对稳定的基础网络, 需要提供一种可扩展的, 可管理的服务框架来解决这一矛盾. 这一问题的解决将弥补相对稳定的网络体系结构和不断变化的服务需求之间的矛盾, 使新一代互联网络可以提供更快, 更好、更方便、更令人满意的服务.

“973”计划项目“新一代互联网体系结构理论研究”围绕上述 4 个关键科学问题, 主要从 6 个方面展开研究: 1) 新一代互联网体系结构基础理论; 2) 新一代互联网路由交换理论; 3) 网络动态行为和传输控制理论; 4) 可信任的互联网安全体系结构和安全监控理论; 5) 新一代互联网服务模型和服务管理理论; 6) 互联网综合实验和验证理论. 下面概要介绍这6个方面的主要研究进展和初步成果.

3.2 新一代互联网体系结构基础理论

该研究的主要进展包括: 定义了新一代互联网的多维可扩展性, 初步提出了一种多维可

扩展的新一代互联网体系结构(图 2)并定义了其 5 项基本要素.

3.2.1 多维可扩展的新一代互联网体系结构

从互联网存在的四大基本矛盾的分析中, 不难发现, 新一代互联网要解决的第一个基本问题就是现有互联网体系结构的单一可扩展性和互联网功能的复杂多样性之间的矛盾.

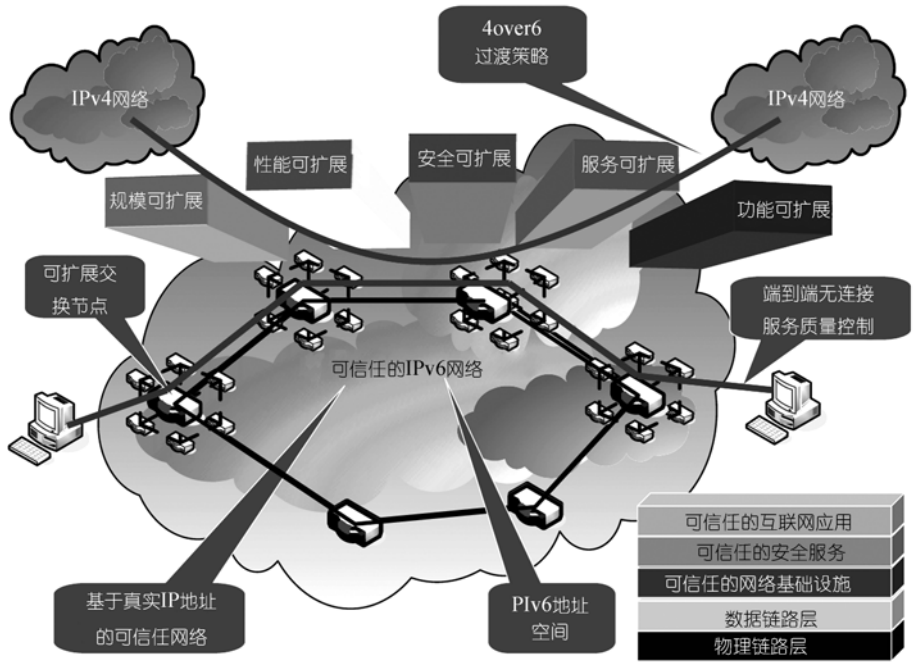

图 2 多维可扩展的新一代互联网体系结构

新一代互联网体系结构的多维可扩展性可以定义为:

1) 规模可扩展. 规模可扩展指的是随着网络节点和链路数量的增长, 网络的性能(如带宽利用率、网络核心设备资源利用率)和端到端性能能够继续得到相应增长的性质. 对于针对该问题的具体实例, 可以通过求解在相应约束条件下的网络效用函数最大化问题来评价.

2) 性能可扩展. 性能可扩展指的是在网络资源(如: 链路、节点等)能力增长以后, 网络的性能和端到端性能是否能够继续得到相应增长的性质. 对于针对该问题的具体实例, 可以通过求解在相应约束条件下的网络效用函数最大化问题来评价.

3) 服务可扩展. 服务可扩展性指的是网络中服务的可部署性是否能够随着总体服务规模的增长得到相应增长的性质. 对于针对该问题的具体实例, 可以根据服务总量和各类服务所占比重建立约束条件下的网络效用函数, 并通过求解最大值来评价.

4) 安全可扩展. 安全可扩展指的是网络中安全机制的性能和效用是否能够随着该机制部署规模的扩大而得到相应增长的性质. 对于针对该问题的具体实例子, 可以根据在不同体系结构下针对安全机制效用函数的比较来进行评价.

5) 功能可扩展. 功能可扩展指的是网络中的各种功能可以在一个统一的体系结构框架

下进行扩展的性质. 例如: 网络的单播、组播、隧道等.

新一代互联网体系结构的多维可扩展性也可以提供更高层次的概括: 网络体系结构的可扩展性指的是网络的特性(如性能、部署代价等)随着网络相关约束条件(如发送速率、规模、服务类型)的变化能够继续得到相应改善的性质.

也就是说, 可扩展性指的是总体效用 K 与网络特性(如: 源速率 x_s, 网络规模 $|V|+|E|$)的变化关系. 可以表示为: $K=\alpha U+(1-\alpha)Q$. 其中, $U=\sum_{s\in V_u}k_{1s}\sum_{w\in W}k_{1w}U(x_s,w)$, 代表具有不用权重的网络中用户的效用之和, 而 $Q=\sum_{l\in E}Q_1(\mu_l)+\sum_{s\in V_c}Q_2(\eta_s)=\sum_{l\in E}k_{2l}$ $\sum_{w\in W}k_{2w}Q_1'(\mu_l,w)+\sum_{s\in V_c}k_{3s}\sum_{w\in W}k_{3w}U_c(\eta_s,w)$ 代表网络中与链路利用率相关的链路效用和以及与系统资源相关的网络中间设备的总体效用之和. 在上式中 α 为平滑参数, 用来调节该效用函数中网络效用与用户效用所占的比例.

3.2.2 多维可扩展的新一代互联网体系结构中的 5 个基本要素

在定义可扩展性的基础上, 我们进一步提出了多维可扩展的新一代互联网体系结构必须包含的 5 项基本要素.

1) IPv6 协议. IPv6 已经成为新一代互联网网络层的事实标准, IPv6 可以解决 IPv4 地址空间不足的问题, 并有助于解决安全可扩展和性能可扩展问题.

2) 真实地址访问. 现有互联网存在的大量安全问题均是由于互联网对用户的源地址不加验证而带来的. 我们认为, 在新一代互联网中必须解决用户真实地址访问的问题, 这将有助于解决安全可扩展和服务可扩展问题 [4].

3) 可扩展的网络节点能力. 随着用户需求的不断增长, 新一代互联网的核心交换节点必须具备可扩展的处理能力, 这将有助于解决规模可扩展和性能可扩展问题 [5, 6].

4) 无连接的网络服务质量控制. 互联网的服务质量控制能力一直是研究人员关注的热点问题. 我们认为, 如何在保持现有互联网逐跳路由的无连接特性的基础上实现服务质量控制是新一代互联网的研究目标之一, 这将有助于解决性能可扩展和服务可扩展问题 [7].

5) IPv4 over IPv6 的网络过渡策略. 新一代互联网必须能够和现有的互联网协调工作并为用户提供服务, 而目前的网络过渡策略均只能用于小规模的IPv6 网络, 不适应新一代互联网的发展要求. 因此, 需要进一步研究现有IPv4 网络过渡到未来以IPv6 为核心的新一代网络的过渡策略, 这将有助于解决规模可扩展和服务可扩展问题 [8, 9].

以上 5 个要素可以支撑新一代互联网的在规模、功能、性能、安全和服务方面的可扩展性.

3.3 新一代互联网路由交换理论

“网络单元”是互联网的基本组成部分, 互联网科学问题的解决方案最终要落实到网络单元中. 通过对新一代互联网路由和交换理论的研究, 着重从网络单元的角度解决网络的多维可扩展性问题, 特别是性能和规模的扩展问题.

该研究主要成果体现在两方面: 一方面是提出了可扩展的新一代互联网路由器体系结构,

另一方面是提出了一套互联网域间路由拓扑和参数配置以及出口选择的优化理论, 对新一代互联网域间路由的设计具有指导意义. 具体如下:

3.3.1 基于 ForCES 的开放路由器体系结构

当前路由器体系结构尤其是路由器控制体系结构在控制的开放性、功能的可扩展性、规模的可伸缩性、系统的可用性和应用的感知性等方面存在不足, 难以适应新型网络应用需求. 从规模、性能、控制、服务和应用感知等多维开放可扩展的理念出发, 我们提出了一个结构灵活、开放可扩展的通用路由器体系结构——OpenRouter 模型(图 3), 并以该模型为基础展开研究.

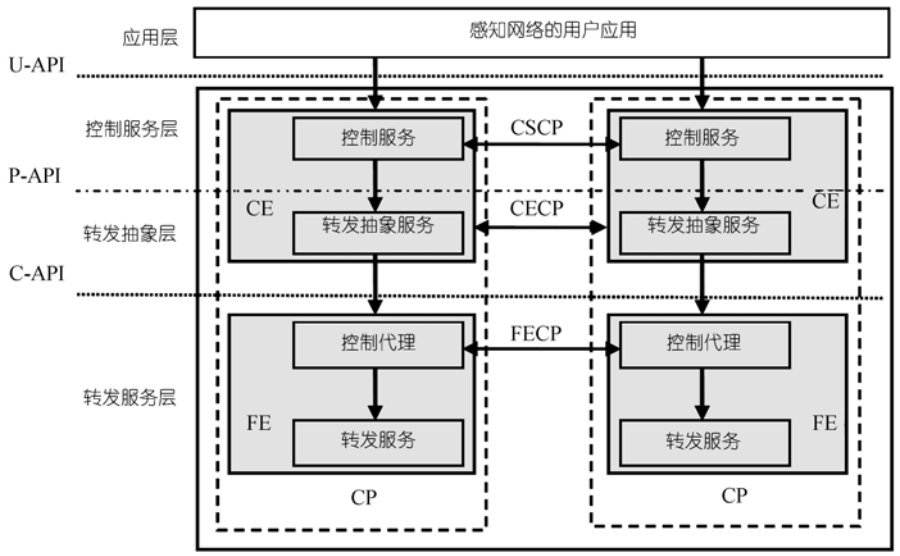

图 3 OpenRouter 体系结构模型

OpenRouter 将网络节点分为转发单元 FE 和控制单元 CE. 随着网络处理器的发展, 以及嵌入式处理器性价比的提高, 使得在 FE 中实现部分简单的控制协议功能成为可能, FE 可以对某些处理简单的控制报文不重定向到控制平面, 而在 FE 中处理, 提高控制平面的效率. 尤其对于大接口密度的路由器, 因为路由邻居众多, 邻接关系维护的工作量较大, 对控制协议整体效率影响较大, 而一旦卸载到 FE 中, 控制协议随邻居数目增加, 性能可以得到明显改善.

在 OpenRouter 模型中, 允许将若干异构的转发实体通过转发协同协议构建为一个转发集群. 根据转发集群 FE 规模范围和 FE 执行控制协议能力的不同, 提出一种分布路径构造策略 DPCA. FE 具备执行寻径协议能力, FE 分布运行类似网络路由协议一样的内部寻径协议, 适用于 FE 互连规模和部署范围相对较大且 FE 执行控制协议能力较强的情况. DPCA 算法基本思想是所有 FE 自动发现与相邻 FE 的局部邻接关系, 并协商接口类型, 然后 FE 邻居间相互通告自身的外部接口情况, 按照路径向量路由算法计算通往相应外部接口的路径转发信息.

3.3.2 可扩展的交换设备模型

随着 IPv6 协议的部署以及互联网规模的不断扩大, 现有路由器分布转发、集中交换的体

系结构已暴露出许多难以克服的问题, 如性能问题、复杂性问题、规模扩展问题和节能问题等.

从体系结构创新入手, 通过对分组转发交换流程进行重新划分和映射, 提出一个与现有路由器分布转发、集中控制体系结构完全不同的新型体系结构——MPFS(massive parallel forwarding and switching)[10]. 该结构不但硬件实现简单, 性能和规模可以像MPP计算机一样通过部件的堆叠扩展, 而且支持在体系结构层次实现灵活的功率管理. 与现有路由器不同, MPFS不包含独立报文转发和交换模块, 所有转发交换功能分布在多个低速的、硬件同构的FSN实现. 报文交换路径上的每个FSN既包含控制转发的网络处理器, 又包含基本的交换单元. 其基本思想是将报文转发操作融入到交换网络中分布执行, 采用边转发边交换的方式, 实现FIB表的分布式存储及报文转发操作的流水执行. 而现有路由器采用的是FBS(forwarding before switching)机制, 即报文在进入交换网络交换之前必须完成精确转发以确定其输出端口.

3.3.3 域间路由优化理论与技术

在域间出口选择优化方面, 针对当前域间出口选择机制存在的若干不足, 提出了基于流量平衡的BGP出口选择优化框架BGP-RCS[11]. 其离线优化计算RCS通过与所有的eBGP路由器建立iBGP连接, 获取所有边界路由器的BGP可达信息. RCS计算动态阶段所需控制规则, 并将控制规则通告给每一个BGP路由器. RCS同时负责网络事件的检测, 并将发生的事件通告给每个BGP路由器, 这样可以避免BGP优化选择的实现依赖于IGP(如OSPF)的实现.

为提高 BGP 出口选择优化的时间性能, 改进 BGP 出口选择优化的路由稳定性和流量平衡性, 针对典型的 BGP 出口选择动态阶段算法存在参数计算复杂性、相关因素考虑的片面性等缺点, 提出了随负载变化的可调自适应域间出口选择算法 ATIE、短暂故障鲁棒的域间出口选择算法 RTF_TIE、基于链路状态的域间出口选择算法 BGP-RO-ES 等算法. 模拟实验表明这些算法在路由稳定性、流量平衡性、控制的灵活性和计算复杂性上更优.

在 IBGP 拓扑优化方面, 在综合考虑路由系统和数据平面及管理平面之间的关系、以及路由系统内的域内路由协议和域间路由协议的相互影响的基础上, 提出了度量 IBGP 拓扑健壮性的一个新测度(流量损移率)以及相关的 IBGP 拓扑规划方法. 基于该测度定义了路由反射器可冗余及会话约束的 IBGP 拓扑设计问题, 讨论了路由反射器冗余度和流量损移率的关系, 给出该问题的优化下界. 对每一个簇内都有一个冗余路由反射器的拓扑设计问题给出可解条件, 讨论了问题的复杂性. 模拟实验表明, 基于该测度进行 IBGP 拓扑规划, 可以有效降低故障对网络流量的影响.

3.4 网络动态行为和传输控制理论

该研究的关键科学问题是“网络动态行为及其可控性”, 以解决未知的网络行为与确定的传输控制目标之间的矛盾. 我们认为, 研究网络行为就是对网络中表现的各种现象进行合理的解释, 并能够预测出行为未来的发展趋势. 网络的动态行为通过基于不同数学模型的各种行为测度体现, 是设计网络体系结构和各种网络协议的理论依据, 因此本研究方向的目标是以测度为基础, 研究网络行为的描述理论; 以抽样为手段, 研究新的网络测量实验科学方法; 以突发数据流为典型, 研究刻画互联网行为的多维理论模型.

该方向围绕科学问题主要进行两个方面的研究工作:

3.4.1 高性能传输系统研究

1) 归纳分析高速网络拥塞控制中的相关研究成果. 对已有的高速网络拥塞控制算法、经典的拥塞控制分析模型以及拥塞控制算法的性能评价指标进行了归纳分析, 指出了高速网络拥塞控制研究中的主要问题, 为研究的开展指明了方向.

2) 经典高速传输协议的建模和分析. 针对传统的 TCP 协议以及最早研究高速网络中 TCP 低效问题的经典高速传输协议, 建立了一个通用的流体流模型来描述传输控制系统的动态行为, 应用小信号线性化方法得到了系统的线性化模型, 然后在此基础上推导出了系统的稳定性判据, 并借助控制理论中稳定裕度的概念研究了网络参数对于系统稳定性的影响.

3) 基于种群演化模型的高速传输协议设计. 运用类比的方法, 在种群生态学所研究的对象和网络拥塞控制所研究的对象之间建立了直观而合理的映射关系, 并成功地将一些经典的种群演化模型扩展到高速网络拥塞控制研究之中. 以此为基础, 设计出了 3 种新的高速传输协议EVLF-TCP[12], CLTCP[13]和PE-TCP[14]. 在整个设计过程中以模型为主导, 有的放矢地选择拥塞控制策略, 提出了路由器显式虚拟负载因子反馈和路由器显式带宽预分配两种拥塞控制方案, 并通过理论分析确定了算法中的具体控制参数, 而且通过仿真试验验证了这两种算法的良好性能.

4) 定量的拥塞控制算法性能评价指标和分析方法. 对所提出的高速拥塞控制算法进行了包括效率、公平、稳定和收敛特性在内的多角度理论分析, 系统地分析了高性能传输系统的综合性能 [15]. 这些基于理论分析得出的结论能够对高速拥塞控制算法的关键指标给出定量而非定性的描述, 从而避免目前一些仅依赖仿真验证的典型算法在网络环境发生变化时再一次通过实验确定参数的尴尬局面.

3.4.2 网络行为研究

1) 高速网络测量技术研究. 重点探索了高速信道的流测量问题, 主要研究资源可控制的自适应高速网络流量和流数测量技术和方案, 在网络流量测量方面提出了新的资源可控制的网络流测量方法, 实现在系统资源可控制条件下, 提高网络流的估计精度, 减少系统测量资源的消耗, 测量通过链路的网络流信息. 在流数测量实现方法提出了一些方法, 在改善资源使用效率方面取得较好的结果. 例如, 提出了一个基于 Bloom Filter 的超点检测方法(图 4), 它能够直接实时检测出超点信息, 节省测量资源的消耗并提高超点流数的检测精度.

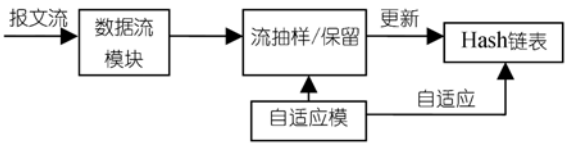

图 4 自适应抽样超点检测算法

2) 网络测度体系研究 对现有测度进行系统性分析归纳的基础上, 重点开展一些能够反映网络协议交互特性和揭示用户行为特征的新型测度的研究, 这些测度由于不能通过传统的基于 SNMP 的网络管理系统获得, 因此还很少被探讨过. 这些测度的探索对于构建完整的网络行为测度体系是十分有益的. 这里主要研究 SLA 网络服务承载测度和 P2P 主机离散度两种类型测度.

SLA 网络服务承载测度研究主要分析下一代互联网 NGI 的网络承载服务 SLA(NSLA)的应用需求, 针对 NSLA 可能的应用场合及 IPv6 特点定义了适用于 NSLA 的 QoS 测度参数: IP 分组传送延迟(IPTD)、IP 分组延迟变化(IPDV)、IP 分组传送失败率(IPFR)和 IP 分组吞吐能力(IPTC), 其中 IPTC 能有效刻画公用 IP 网段集维持业务流量模式的能力.

鉴于网络中的 P2P 应用给目前的网络管理所带来的困扰, 提出了一个新的称为"主机离散度"的网络空间测度, 适用于标识和发现多方通信活动的行为. 通过对应用协议和用户流量的分析, 发现单用户主机的 BT 类 P2P 应用流量与传统应用和其他 P2P 应用(如 Skype)流量最大区别体现在通信对端主机的分布特征上. 据此提出一种基于通信对端主机离散度(RHD)识别 BT 类流量的方法. 该方法是一种基于流量特征的应用识别方法, 比常用的基于端口、应用特征等内容特征的应用识别方法更适于识别多变的 BT 类 P2P 应用.

3) 网络行为分析研究. 重点探讨网络新型测度的应用, 主要包括: 基于最大属性熵的报文分类、TCP 宏观平衡性测度、IP 流的统计分布行为、BitTorrent 流行为分析等 4 个方面.

基于最大属性熵的 GIDS 报文分类算法, 研究了适用于 GIDS 的经典分类算法 HiCuts 和针对它的修改升级算法 P-HiCuts, 针对 P-HiCuts 没有考虑报文域的特征对于分类树的影响的缺点提出了基于最大属性熵的分类树本地优化策略和新的分类树生成算法 MaxFeatureEntropy. 最大属性熵策略从理论上保证减小决策树高度.

基于 TCP 宏观平衡性的研究, 提出自然着色过程利用有部分重叠的短比特串映射, 使两个 Hash 函数间带有相同的颜色, 为判定两个 Hash 串是否同源提供了重要依据. 自然着色过程大大扩展了 TCP 宏观平衡性的应用领域, 为网络安全检测、监测和安全事件分布评估提供了有力的支持.

在 IP 流的统计分布行为模型方面, 提出了大规模网络状况下 IP 流流长分布经验模型. 该模型在表达大规模网络 IP 流流长分布上, 其精度高于原有 Pareto 模型, 其复杂度低于原有双 Pareto 模型.

在流量类型识别方面, 深入研究了 BitTorrent 应用的流长、流持续时间、流速以及结点传输的流量、连接数等测度的分布情况, 指出其流长、持续时间均服从 Weibull 分布, 流速较一般 TCP 流速慢, 并且 BitTorrent 网络呈现很强的不平衡性, 同时分析了各分布中的异常情况.

3.5 可信任的互联网安全体系结构和安全监控理论

该研究的关键科学问题是"脆弱复杂巨系统的可信性问题". 主要从真实源地址的网络体系结构、可信任模型、网络安全监控与恶意代码分析等方面开展了研究, 提出了基于真实源地址认证的可信任互联网安全体系结构 [4], 从身份认证、访问控制、信任和信誉系统模型等研究了可信任和信任模型 [16], 从网络流量分析、异常检测和恶意代码分析等方面研究了网络安全监控理论和网络的可生存性 [17].

主要研究成果包括:

3.5.1 真实 IPv6 源地址寻址体系结构研究

提出了一个基于真实IPv6 源地址认证的寻址结构 [4](图 5), 以确保互联网上传输的分组来

自于源地址授权的用户. 可信任下一代互联网体系结构是一个分层模型, 从基础设施、安全服务、可信应用 3 个层面解决互联网的可信任问题. 在这一寻址体系结构下, 开展了以下研究: 在自治系统间, 提出了基于自治系统互联关系的真实IPv6 源地址认证方法和基于签名的真实IPv6源地址认证方法; 在自治系统内, 合理的部署入口地址过滤(ingress filtering); 在接入子网内, 提出基于IPv6 地址认证绑定的真实IPv6 源地址认证方法. 该体系结构的实现和部署将大大提高互联网的可信任性.

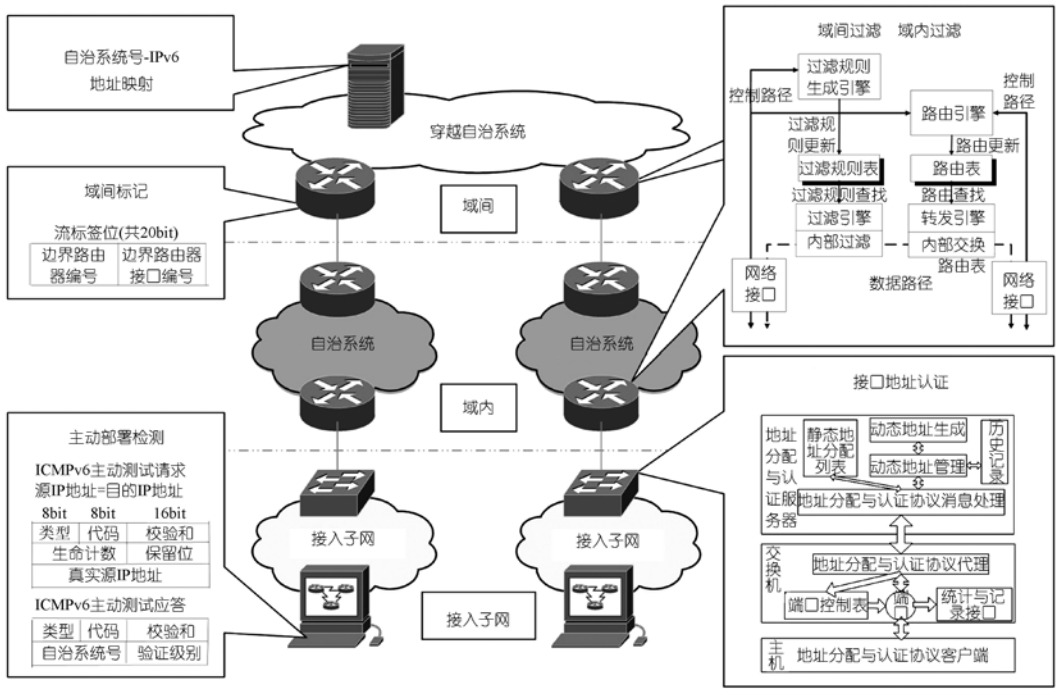

图 5　真实 IPv6 源地址认证的寻址体系结构

3.5.2　可信任和信任模型

1) 研究了网络环境中用户之间的动态信任关系, 提出了支持噪音过滤的动态信任数学模型. 针对传统访问控制机制表达能力差、可扩展性差、缺乏传递性的缺点, 研究了网络计算环境中实体的信任属性的定义、信任的发展变化、信任的传递过程; 在不同跨域的环境中, 实体的信任策略和信任管理机制, 包括信任关系的建立、变化和撤销过程. 在此基础上提出了支持噪音过滤的动态信任数学模型.

2) 提出基于信任的角色访问控制模型. 现有访问控制模型在实现角色的自动分配以及角色行为管理方面存在不足. 针对上述问题, 提出一种基于用户可信度的角色访问控制模型T-RBAC, 将用户行为的可信度评价作为分配用户角色的一种度量, 可以在为管理员提供一定程度的辅助决策支持, 同时在用户的访问过程中进行实时地监控与控制, 进一步加强了系统的安全性, 避免恶意用户的破坏性行为.

3) 设计并实现了分布式信任机制仿真系统. 信任机制的目的是在网络用户之间建立起一种类似人类社会的信任关系, 主要是通过对用户的历史行为进行评价来决定该用户在后继交互中是否可信. 设计并实现了一个分布式信任机制仿真系统, 该系统模拟了分布式交互环境中 5 类用户行为, 能够从交互成功率、平均信任值以及评价偏差等 3 个方面对现有多种信任机制进行评价与对比, 通过分析模拟结果可以指导我们进行新的信任机制的设计.

3.5.3 流量分析、安全监控与恶意代码分析

流量分析和安全监控研究的主要目的是保证对网络流量中的恶意行为能够及时发现. 而对于网络流量的分析与监测可以在协议、流量、语义, 以及仿真多个维度上进行.

1) 基于网络协议的多态蠕虫特征生成研究. 研究内容包括建立一个基于字段长度的多层流模型, 设计特征生成算法, 对算法性能(特征的虚警率和漏报率)下限的理论证明, 以及利用实际网络数据对算法性能进行实验验证.

2) 基于网络内容的多态蠕虫特征码生成研究. 研究的内容包括, 建立一个可以和早期预警系统联动的特征码提取原型系统, 正常流量白名单的生成算法, 频繁模式挖掘算法, 恶意流的聚类算法, 以及利用大规模网络数据进行算法验证.

3) 恶意网络行为的提取与分析. 研究内容主要包括: 网络恶意行为的定义与建模, 网络数据流归并技术, 基于数据流的网络行为分析以及网络事件的定义与构建.

4) 多态攻击的行为分析与检测. 研究内容包括: 实现建立多态攻击分析和检测的形式化框架模型, 设计检测算法, 实现一个可执行代码的动态模拟与分析环境, 以及利用实际数据对方法的性能进行试验验证.

3.5.4 基于源地址认证的组播安全认证

在组播准入控制机制研究中, 由于缺乏用户的身份认证信息, 给组播成员的准入控制判别带来了困难. 基于源地址认证的组播安全认证, 为 IP 组播提供了一种安全有效的认证和授权方法, 每个主机地址的真实用户身份都可以得到确认, 极大地方便了组播成员的管理, 也为一直难以解决的组播成员的身份认证和授权认证问题找到了一条新的解决途径. 基于源地址认证的组播安全认证是基于真实 IPv6 源地址认证寻址体系的一个重要应用, 对可信任互联网的进一步推广具有重要意义.

3.6 新一代互联网服务模型和服务管理理论

该研究的关键科学问题是“稳定网络体系结构的服务多样性问题”, 对该问题的研究将解决网络体系结构的相对稳定性和网络服务需求的复杂多变之间的矛盾. 如果随着网络规模、环境以及用户和服务提供者需求的改变, 独立开发不同的服务, 将重复大量的工作, 耗费巨量的资源, 从而极大地限制了网络服务在深度和广度上向前发展. 基于以上认识, 本方向重点研究如何根据用户的需求快速地生成、部署和管理服务. 在这一领域, 面向服务计算技术和网络中间件为该问题的解决提供了很好的研究思路.

取得的主要研究成果如下:

3.6.1 基于范例推理的服务组合框架

将专家知识和经验封装成服务范例透明地提供给用户, 通过设计适当的检索、调整、重用和存储机制以获取能够满足用户需求的组合服务逻辑集. 提高了对已有的成功服务组合的可重用性和服务组合准确率, 减少了服务组合的代价.

3.6.2 分布式环境中的服务组合的迭代选择算法

组合服务提供商面临的一个难题是如何跨越多个不同的自治网络或商业域选择一组服务实例来实现组合服务, 并且向用户提供端到端的QoS保障. 该算法[18]用于QoS驱动的服务组合, 运行于一个P2P的服务执行环境(图 6). 该算法可以在组合服务执行之前或者组合服务运行时执行, 不需要作任何更改. 该算法还可以提供极好的选择结果并且具有很好的性能.

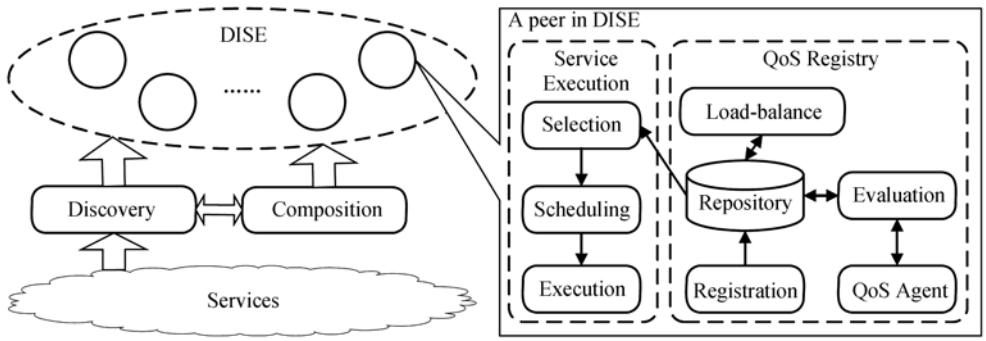

图 6 分布式智能服务执行环境

3.6.3 基于遗传算法的面向全局 QoS 限制的服务选择算法

围绕具有全局 QoS 限制的服务组合问题, 对遗传算法的实现机制进行了研究, 提出了一个服务组合框架, 并给出了满足全局 QoS 限制的服务组合与选择流程, 框架核心为遗传算法中间件, 它通过遗传算法选择最优组合的功能, 并且具有用户需求分析及重计划功能. 目的在于根据用户提出的功能需求及非功能需求, 找出最优组合方案.

3.6.4 基于时态描述逻辑的语义服务行为描述和匹配方法

基于时态描述逻辑的服务行为描述模型反映了服务行为中的行为时序约束特征, 能够在服务发现过程中保证服务行为时序的准确性和服务行为语义描述的正确性. 通过时态描述逻辑, 对基于时序约束的服务行为进行语义描述, 使服务发现过程中可以融入服务行为的特点和因素.

3.6.5 服务双边协商模型

通过双边协商, 一个服务提供者和一个服务请求者逐渐对服务提供的细节尤其是服务的非功能属性达成一致意见, 形成一个服务合约. 在该模型中, 利用模糊命题表示协商参与者对服务的约束, 这些约束是非数值化的; 使用效用函数表示对数值化的服务非功能属性的偏好, 采用二者相结合的方法建模对服务非功能属性的偏好选择.

3.6.6 基于集合论的服务故障诊断方法

在故障监测阶段能够发现故障, 但是较少的探针结果并不足以诊断故障根源, 需要启动故障诊断模块来定位故障. 分析故障检测阶段的探针结果, 进一步发送探针检测可能故障. 由于探针可能存在较大冗余度, 采用基于集合论的算法来选取发送的探针. 仿真结果证明, 在存在大量接入网的情况下, 结合故障监测方法, 该方法能够利用较小的探针开销, 获得较高的故障检测率和较低的误判率.

3.7 新一代互联网综合实验和验证理论

基于运行网络利用测量分析方法进行的实验验证面临诸多难以克服的挑战, 如网络行为的时空差异性、网络行为的不可重现性以及网络过程的不可控性等, 都是影响实验的重要因素. 该研究目标是, 通过全面研究新一代互联网实验验证研究所面临的挑战性问题, 探讨复杂网络行为的纯化、简化方法, 以及加速、延缓和再现网络现象的实验技术, 构造共享科学实验环境的服务模式, 并设计互联网科学实验的标准过程, 在理论上, 探索互联网科学实验理论; 在实践上, 完成实验平台建设, 提供具体的实验方法、实验工具和实验环境来满足项目的科学实验和验证需求, 支撑新一代互联网重要研究理论成果的展示.

其主要研究成果包括:

3.7.1 DRAGON-Lab 网络数据共享平台的设计与实现

在探索研究互联网综合实验验证的基本理论框架的基础上, 初步建成新一代网络远程实验室DRAGON-Lab(distributed research & academic gigabits open network lab)[19]. DRAGON-Lab能够随时摄录和重放IPv4/IPv6 运行网络流量, 可支持真实网络环境的实验; 能够从运行网络引入OSPF, ISIS和BGP路由信息, 因此通过 DRAGON-Lab可进行大时间和空间跨度的真实网络行为研究和运行网络实验; 通过DRAGON-Lab专用实验配置系统, 能够可视化定义所需的实验环境、自动生成实验环境定义脚本、远程提交实验环境定义脚本, 并申请实验时间; 实验操作通过互联网远程进行, 无需专程来到实验室. DRAGON-Lab管理平台结构如图 7 所示.

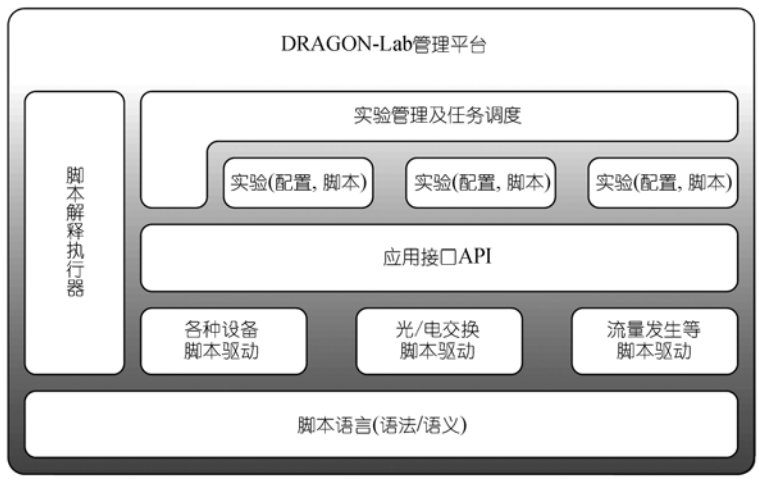

图 7 DRAGON-Lab 管理平台

该系统最大的好处在于: 一方面, 系统不对数据的格式进行要求, 数据的格式完全由数据源来确定, 并有数据源在数据的发布时提供相应的说明文件, 这样使得系统具有最大的扩展能力, 无论数据是 netflow 记录、Apache 日志、Pcap 格式的流量记录, 都能够在这一架构中; 另一方面, 研究者通过数据访问网关来得到一个指定的数据访问服务器, 便于大量研究者的同时研究, 而且, 研究者不必将庞大的网络数据下载到本地, 避免了大量下载所造成的时间浪费和庞大的带宽要求.

目前, DRAGON-Lab 能够提供的服务包括: 网络实验服务、系统实验服务、真实网络流量和路由信息、流量研究中心、路由研究联邦 BGP-Grid、全球分布式性能测量联邦 GPERF 等.

3.7.2 地址随机化算法研究

隐私处理的主要环节是 IP 地址的随机化处理. 地址随机化算法的一个理想的特征就是, 它应当是一致的, 只要参数确定, 那么 IP 地址的映射方案就应当是一定的, 不受 IP 地址出现顺序等因素的影响. DRAGON-Lab 对于地址随机化算法的需求在于: 一方面, 作为一个联邦, 各方对于所采用的地址随机化算法常常有不同的需求, 一些数据源所发布的数据安全级别较低, 因此可以采用一些保留信息较多的地址随机化算法, 而另外一些数据源所发布的数据有可能十分敏感, 因此往往会采取一些更为严格的地址随机化方案, 因此希望地址随机化系统能够兼容各种安全强度的地址随机化算法, 而以往的研究则大多侧重于保持地址前缀随机化算法方面; 另一方面, 联邦中的一些数据源不仅能够为研究者所使用, 也能够为自己所使用以节省存储和管理资源, 为此, 希望能够针对不同的实验人员, 所采用的随机化算法可以根据其相应的安全权限而设置, 而当自己使用时, 则可以通过预先设置的密码等来得到原来的 IP 地址. 针对数据源去隐私化、地址随机化问题的研究, 设计了具有多访问权限的地址随机化算法的设计, 并针对地址随机化算法, 研究了其面临的攻击和相应的抗攻击水平.

3.8 小结

综上所述, 经过近 5 年的研究, 本项目在探索新一代互联网体系结构所面临的基础理论问题上, 取得了一些研究成果, 包括: 新一代互联网多维可扩展体系结构、新一代互联网多维可扩展体系结构及其必须涵盖的 5 项基本要素、可信任安全体系结构、可扩展集群路由器结构、高性能网络传输控制系统的优化方案和新一代互联网体系结构实验验证平台, 并且进行了实验验证, 推广应用和产业化, 其中两项重要成果推动国际互联网标准组织 IETF 成立了专门的工作组 SAVI 和 SOFTWIRE, 研究制定系列国际互联网核心标准. 目前我们提交了近 10 项 IETF 标准草案, 已经有两项获 IETF 批准, 分别是: RFC4925, RFC5210. 使中国参与 IETF 国际标准方面实现了新的突破. 其中 RFC4925 是基于项目研究成果“4over6 过渡技术”, 在国际上首次提出“IPv4overIPv6 网状体系结构过渡技术”, 该技术的提出推动 IETF 成立了专门工作组 SOFTWIRE. RFC5210 基于项目的研究成果“基于真实 IPv6 源地址认证寻址体系结构”, 这是我国第一个非信息类(informational)的 RFC, 并且 IETF 以此为基础成立了专门工作组 SAVI.

项目研究成果“真实 IPv6 源地址认证结构”和“4over6 过渡技术”通过“863”课题进行了关键技术开发, 并应用于中国下一代互联网示范工程 CNGI 示范网络核心网 CNGI-CERNET2 主干

网和国产核心 IPv6 路由器的开发和产业化. 并且, CNGI-CERNET2 和 IPv6 核心路由器项目分别获得国家科技进步二等奖. 实践证明, 解决新一代互联网体系结构的主要技术挑战, 需要体系结构方面的理论基础和科学依据支持.

4 总结与展望

经过十多年时间, 人们越来越深刻地认识到下一代互联网研究的重要性、复杂性、艰巨性和长期性, 发达国家纷纷把下一代互联网研究列入未来信息技术领域的重点发展方向. 近年来新一代互联网研究已得到我国政府的高度重视, 并且列入“国家中长期科技发展规划”. 面对目前互联网存在的重大技术挑战, 单靠一般的技术发明和工程实践, 很难找到理想的解决方案. 基础理论在新一代互联网研究中具有重要的指导作用.

2003 年立项的“973”计划项目“新一代互联网体系结构理论研究”, 围绕新一代互联网体系结构中的基本科学问题进行研究. 初步研究了新一代互联网络体系结构的理论和相关机理, 在新一代互联网多维可扩展体系结构及其包括的基本要素, 可扩展的路由和交换系统, 高效网络传输和服务质量控制机制, 可信网络安全体系结构, 网络服务管理和新一代互联网综合试验验证环境等方面取得初步的研究成果, 参与 IETF 国际标准的制定, 开始在国际新一代互联网科学研究领域有了一定的话语权, 为进一步深入研究新一代互联网体系结构和协议奠定了良好的基础.

面对近年来国际新一代互联网体系结构基础研究的新形势和互联网许多创新应用对体系结构的新需求, 在已有研究成果基础上, 我们突出重点, 有所为、有所不为, 提炼出了一些新的关键科学问题, 我们认为, 新一代互联网体系结构要解决下面 5 个关键科学问题: 1) 互联网体系结构的扩展性和演进性问题; 2) 大规模路由的可信和收敛问题; 3) 海量数据的高效网络传送问题; 4) 非连接网络的实时传送问题; 5) 用户跨域访问的复杂自治网络管理问题.

在技术路线上, 我们将走“坚持演进, 积极创新”的路线, 在 IPv4 向 IPv6 演进的基础上, 基于 IPv6 平台, 解决互联网面临的主要技术挑战. 从注重体系结构的理论探索, 到注重体系结构和协议的基础研究; 从紧紧研究体系结构最基本的问题, 到更加面向新一代互联网重大应用的需求; 重点研究新一代互联网络体系结构和协议的原理、机理和算法, 依托近年来已经建成的国家新一代互联网实验环境对上述研究成果进行较大规模的试验和验证, 积极参与新一代互联网国际标准制定工作, 努力使研究成果成为 IETF 国际标准, 力争使我们的研究进入国际新一代互联网前沿科学技术研究的先进行列, 部分成果达到或进入国际领先行列, 逐步形成新一代互联网体系结构和协议理论体系.

参考文献

1 Wu J P, Xu K. Next generation internet architecture. J Comput Sci Technol, 2006, 21(5): 726—734
2 Li X, Dawkins S, Ward D, et al. Softwire Problem Statement. RFC 4925. 2007
3 Wu J P, Bi J, Li X, et al. A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience. RFC 5210. 2008
4 Wu J P, Ren G, Li X. Source address validation: architecture and protocol design. In: Proc Int Conf Netw Protoc

ICNP. Washington: IEEE Computer Society, 2007. 276—283
5 Wu K, Wu J P, Xu K. A tree-based distributed model for BGP route processing. In: Gerndt M, Kranzlmüller D, eds. High Performance Computing and Communications. LNCS, Vol 4208. Heidelberg: Springer-Verlag, 2006. 119—128
6 Yue Z H, Wu J P, Zhao Y J. CR: scalable routers based on a new architecture. J Softw, 2007, 18(10): 2624—2634
7 Cui Y, Wu J P, Xu K. Precomputation for intra-domain QoS routing. Comput Netw, 2005, 47: 923—937 [DOI]
8 Wu J P, Cui Y, Li X, et al. The transition to IPv6, part Ⅰ: 4over6 for the China education and research network. IEEE Internet Comput, 2006, 10(3): 80—85
9 Cui Y, Wu J P, Li X, et al. The transition to IPv6, part II: the softwire mesh framework solution. IEEE Internet Comput, 2006, 10(5): 76—80
10 Dai Y, Sun Z G, Su J S. Analysis of an evolvable architecture of internet routers. In: Workshop on High Perf Switch Rout HPSR. Washington: IEEE Computer Society, 2007. 1—5
11 Liu Y P, He J F, Gong Z H. BGP-ESOM: BGP egress selection optimization model based on traffic demand. In: Proc Future Gener Commun Netw FGCN. Washington: IEEE Computer Society, 2007. 118—123
12 Huang X M, Lin C, Ren F Y. A novel high speed transport protocol based on explicit virtual load feedback. Comput Netw, 2007, 51(7): 1800—1814 [DOI]
13 Huang X M, Lin C, Ren F Y, et al. Ungsunan, improving the convergence and stability of congestion control algorithm. In: Proc Int Conf Netw Protoc ICNP. Washington: IEEE Computer Society, 2007. 206—215
14 Huang X M, Ren F Y, Yang G W, et al. End-to-end congestion control for high speed networks based on population ecology models. In: Proc Int Conf Distrib Comput Syst ICDCS. Washington: IEEE Computer Society, 2008. 355—364
15 Ren F Y, Lin C, Wei B. A nonlinear control theoretic analysis to TCP-RED system. Comput Netw, 2005, 49: 580—592 [DOI]
16 Xu Y, Chen Z F. Sentence digest algorithm and its application on anti-spam. J Comput Inf Syst, 2007, 3(3): 1081—1086
17 Lu X, Duan H X, Li X. Identification of P2P traffic based on the content redistribution characteristic. In: Int Symp Commun Inf Technol ISCIT. Washington: IEEE Computer Society, 2007. 110—116
18 Li F, Yang F C, Shuang K, et al. Q-Peer: A decentralized QoS registry architecture for web services. In: Gerhard G, Juris H, Jan L, eds. Service-Oriented Computing-ICSOC 2007. LNCS, Vol 4749. Heidelberg: Springer-Verlag, 2007. 145—156
19 Zhang Q L, Wang J L, Li X. On the design of fast prefix-preserving IP address anonymization scheme. In: Gerhard G, Juris H, Jan L, eds. Information and Communications Security. LNCS, Vol 4861. Heidelberg: Springer-Verlag, 2008. 177—188