自适应的未来网络体系架构

林 闯[1)] 贾子骁[1)] 孟 坤[1),2)]
[1)](清华大学计算机科学与技术系 北京 100084)
[2)](北京科技大学计算机与通信工程学院 北京 100083)

摘 要 随着计算技术和互联网业务的蓬勃发展,用户对网络应用提出了越来越高的要求,多样化的需求使得现有Internet架构难以适用,成为了网络业务进一步发展的瓶颈.文中在分析当前Internet网络存在的问题、总结本源性因素的基础上,指出了自适应是未来网络的发展方向,可控、可管、可扩展和可信是实现自适应特性应满足的基本指标.在介绍和分析现有自适应未来网络关键技术和体系架构的同时,深入讨论了相关技术和体系结构的优势和兼容性,并在此基础上提出了自适应的未来网络体系架构,为未来网络的研究提供了参考.

关键词 未来网络;架构;自适应;可控;可管;可扩展;可信;下一代互联网
中图法分类号 TP393 **DOI号**: 10.3724/SP.J.1016.2012.01077

Research on Adaptive Future Internet Architecture

LIN Chuang[1)] JIA Zi-Xiao[1)] MENG Kun[1),2)]
[1)](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)
[2)](*School of Computer & Communication Engineering, University of Science & Technology Beijing, Beijing* 100083)

Abstract With the flourishing of Internet application and the growth of computing techniques, customers require Internet with higher and higher performance. Nevertheless, diversified requirement of customers and lacking of elasticity of Internet architecture lead to wasting much Internet resource. The Internet became the bottleneck for further development of Internet service. Based on analysis of the present Internet, we list the fundamental factors that affect its elasticity, and point out that adaptive architecture is the potential development direction for the future Internet and discuss the adaption from the following aspects: the Controllability, the Manageability, the Scalability and the Trustworthy. Moreover, we survey the work about key technologies and architectures of the Adaptive Future Internet in detail, and analyze their advantages and the compatibility. As a result, we present an Adaptive Future Internet Framework (AFIF) which gives a reference for study on Future Internet.

Keywords future Internet; architecture; adaptive; controllability; manageability; scalability; trustworthy; next generation Internet

1 引 言

以IP技术为核心的Internet网络将大量的网络服务都推给了传输层及其之上的各层来实现,留下了简洁而又高效的网络层和数据链路层协议.这种设计模式简化了网络设备的功能,保证了网络具有较好的可扩展性,使得计算机网络迅速从实验室

收稿日期:2012-03-06;最终修改稿收到日期:2012-04-17.本课题得到国家"九七三"重点基础研究发展规划项目基金(2010CB328105,2009CB320505)、国家自然科学基金重点项目(60932003)和国家自然科学基金面上项目(61070182,60973144,61173008,61070021)资助.
林 闯,男,1948年生,博士,教授,博士生导师,主要研究领域为计算机网络、系统性能评价、安全分析和随机Petri网.E-mail:chlin@tsinghua.edu.cn.贾子骁,男,1986年生,博士研究生,主要研究方向为性能评价和下一代互联网.孟 坤,男,1980年生,博士研究生,主要研究方向为性能评价和随机模型.

走向了世界，已成为了人们生活必不可缺的一部分.

随着互联网业务在近几年来蓬勃发展，以Google搜索业务、YouTube视频业务为代表的网络新技术和新业务不断涌现. 伴随着不断提升的软硬件水平，网络业务的发展经历了从简单单机程序、集中式客户端/服务器的请求服务模式(C/S)、分布式点对点(P2P)资源共享模式等，到大规模云计算服务模式的转换，由此对互联网的基础硬件设施及运行其上的网络控制体系提出了更高的要求：对运算节点资源和网络传输资源实现细粒度的调度和管理，以获得较高的用户体验质量(Quality of Experience，QoE)[1]. 然而，在现有的网络体系架构中，网络控制层和数据层紧耦合，但混合式的网络控制逻辑与网络数据层松耦合，使得应用服务提供商(Application Service Providers，ASP)无法根据用户服务的需求分布对网络资源进行按需调度，只能通过增加额外的计算资源和冗余的服务部署来满足服务需求；网络用户(Network Users，NUS)无法与应用服务提供商进行有效的交互，盲目地探寻服务资源；网络服务运营商(Internet Service Providers，ISP)依赖扩充网络设备规模应对网络服务的需求. 这些“补丁式”的措施导致现在的互联网已经成为一个规模臃肿、结构繁杂、不可靠的确定性系统[2]，进一步加剧了网络数据层和网络控制层的压力，使得网络控制层越来越复杂，难以适应目前网络业务的发展.

现有网络体系难以适应目前业务应用需求的突出矛盾表现在以下方面：(1)有限的IP资源与无限增长的服务资源需求间的矛盾，地址与服务资源难以实现一一绑定，阻碍了资源的优化调度；(2)业务模式革命性转变与网络架构局限性的矛盾，现有网络协议难以承担以大规模数据传输为重点的网络传输的任务；(3)数据来源多样性、突发性与网络管理机制滞后的矛盾，多样性数据给网络带来更多的威胁，管理的滞后助长了安全事件的蔓延；(4)服务质量要求提升与网络性能提升不成正比，计算模式与存储技术发展加速了对服务质量要求的提升，网络性能成为满足服务质量的瓶颈.

针对上述问题，我们认为未来的网络应具备主动发现、识别网络主体和网络应用的特性，能根据不同网络要求进行自主调节网络配置的能力，能够满足各种角度用户使用友好性的要求. 简单地，我们称之为自适应网络，并把相应的实现技术称为自适应网络技术. 下述方法为构建自适应网络提供了方向：将网络控制层与网络数据层解耦，建立控制逻辑与网络数据层之间的紧耦合关系；实现控制逻辑可以根据准确、完整的网络状态信息，直接作用于网络数据层，依照网络业务的需求从较高层次上配置网络或者修改网络决策层的相关算法优化网络运行的技术. 已有的自适应网络技术主要包括设备主动管理和网络控制技术(如OpenFlow、NOX)、服务资源识别和定制技术(如NDN、PSIRP)、网络体系架构(如4D、GENI)等，为实现网络控制权从路由器/交换机及网络协议中分离、网络的按需控制、新型网络业务与网络控制的自主匹配提供了可能.

本文在分析当前以IP技术为核心的网络体系架构存在的根本性问题的基础上，对自适应网络技术和体系结构进行了系统调研，全面对比分析了各种技术的侧重点和兼容性，并提出了自适应的未来网络体系架构(Adaptive Future Internet Framework，AFIF).

本文第2节分析当前Internet网络体系结构存在的问题；第3节阐述未来Internet网络的发展要求和设计原则；第4节至第6节分别对目前自适应网络技术和自适应网络体系框架的研究进展进行综合对比分析；第7节提出一种自适应的未来网络架构AFIF；第8节对全文进行总结.

2 互联网现状与存在的问题

大流量网络业务的流行与网络用户的急剧增加、用户个性化的服务质量需求使得现有以IP技术为核心的Internet难堪重负. 本节深入分析了当前Internet的现状和存在的问题，并总结出导致这些问题的本源性因素，为自适应的未来网络体系架构设计指明了方向.

2.1 Internet体系现状

2.1.1 小核心和大边缘

现在的互联网依然是以IP技术为核心，IP技术采用了基于无连接的分组交换结构、存储转发的路由机制和尽力而为的服务模式[3]，保证了异构网络之间的互连互通. Internet创始人之一David Clark将这种模式总结为“边缘论(End-to-end Argument)”：应用功能作为通信系统内在的性质是不可能的，只有被放置于系统的边缘才能被完全和正确地实现[4].

“边缘论”设计模式的采用，形成了简洁、高效的网络核心，仅实现了通用的数据路由转发功能；大量

高层网络应用服务被放置在网络边缘，推给传输层及其之上的各层来实现. 这种核心简单、边缘复杂的设计模式便于异构网络的接入与新业务的部署，保证了网络良好的扩展性，但增加了边缘管理的复杂度.

2.1.2　业务需求多样化

随着软硬件水平的不断提升，网络业务的发展经历了从简单单机程序、集中式客户端/服务器的请求服务模式(C/S)、分布式点对点(P2P)资源共享模式等，到大规模云计算服务模式的转换. 为应对网络服务计算密集性的需求，实现硬件资源的高效利用，虚拟化技术被广泛应用，代表性的如 Google 数据搜索和 YouTube 视频业务. 这些业务都采用了以大规模数据中心为支撑的云计算架构，数据中心和云计算技术推动虚拟化技术发展到了一个新的阶段.

虚拟化技术从单机虚拟化发展到现在的以云计算为代表的服务虚拟化，虚拟化程度得到了提高，同时加速了网络资源一体化进展. 服务虚拟化技术需要调度的资源除了众多运算节点所拥有的硬件资源之外，还包括节点之间的网络传输资源，其调度的重要性不亚于运算节点资源. 节点之间网络传输资源的虚拟化成为了目前领域研究的重点.

2.1.3　网络社会性凸现

随着社交网络、电子商务和电子政务的不断发展，Internet 的社会性正逐步凸现.

首先，以 iPhone、iPad 为代表的智能终端的出现和 3G 网络的广泛应用，极大丰富了网络的接入方式，计算机网络的使用变得更为廉价和便捷，互联网已经融入到了人们的生活当中，它所承载的社会功能越来越多. 其次，互联网中的虚拟关系正与真实的社会人际关系相互融合，信息在网络中的传播和反馈呈现出社会性特点，网络行为折射了用户的价值取向. 同时，互联网中的隐私与安全问题成为各方关注的重点，CSDN 和人人网账户信息的泄漏为互联网安全敲响了警钟. 如何利用社会科学的理论成果引导和管理互联网成为了网络领域重要的研究课题.

2.1.4　混合式网络管理

互联网“边缘论”和无连接分组交换的互联网设计使得借助分布式路由协议间接控制网络核心区域成为必需.

网络的控制逻辑与数据转发通道以分布式路由协议(BGP、OSPF 等)的方式在网络节点上进行了捆绑实现，这些路由协议同时兼顾了数据转发和网络控制的功能：一方面学习网络拓扑，根据网络的实时状态转发数据；另一方面执行网管配置的协议规则实现网络控制，如 BGP 域间路由策略等，网络控制与数据层构成了紧耦合关系.

网管人员直接参与节点级的网络协议，实现对数据层的控制，网络节点执行流量工程等人为配置规则和最短路径规则的混合体，在处理数据包时根据链路负载均衡、流量控制等机制自主调控，使得网络控制呈现出混合式的特征.

2.2　互联网存在的问题

当前互联网所处的网络环境和运行的网络业务都发生了日新月异的变化，传统 Internet 网络体系不再适应未来网络的发展，存在的突出问题可以归纳成以下几个方面.

2.2.1　信息不透明和资源浪费严重

在云计算业务模式里，网络中节点的硬件资源和节点之间的网络传输资源分别由应用服务提供商和网络服务提供商进行管理. 以 Google 为例，Google 在全球多个国家部署运行着 40 个数据中心[①]，这些数据中心通过本地的网络运营商接入到互联网. 这一现状为实现云计算的细粒度化管理和可靠性任务调度造成了不可逾越的鸿沟.

一方面应用服务提供商为了弥补该性能上的，耗费了大量的节点计算资源，雅虎公司中央数据库的拓扑结构发现功能通常要花费 30％以上的 CPU 处理周期来进行重复的计算，尽管网络拓扑的变化没有那么频繁[②].

另一方面云计算架构承载了越来越多的复杂业务流量，使网络基础设施不堪重负. 但网络运营商对网络所承载的应用层业务缺乏感知，这种盲目性使得 ISP 只能单纯依靠购买网络设备、扩充网络节点规模来应对不断增加的业务流量. 网络设备和虚拟化节点数目成倍增加，造成了网络设备利用率低、网络资源浪费，网络数据传输性能并没有得到相应提高.

以 IP 为核心的网络体系结构中，数据层对应用程序开发者不透明和硬接入的实现方式，无论从流量规模上，还是从功能接口上，都不能满足当今网络业务的需求. 网络体系结构束缚了网络业务的发展. 渐进式的改良方法对网络进行局部改进，只能暂时

① http：//www. vaughns-1-pagers. com/internet/google-data-centers. htm，2011

② http：//www. networkworld. com/community/blog/open-networking-summit-day-2-cisco-says-we-se，2011

缓解这一矛盾，并不能从问题的根源处解决.

2.2.2 信息交互差与控制日益复杂

互联网在设计之初只需要简单、高效的数据传输逻辑，如 IP 网和以太网的分布式计算路径逻辑，网络控制功能相应的也只需维护包转发表这一简单的分布式路由协议. 但随着互联网业务的发展，尽力而为的数据传输服务已远远无法满足当今网络业务的需求[5]：不仅是简单的建立下一跳路由，还需要实现隧道、访问控制、网络地址翻译、QoS 队列、流量工程等越来越多的控制功能. 这些功能需要大量的低层次配置命令去各个网络节点上单独配置. 这些配置命令和控制功能之间的相关性，使网络控制越来越复杂.

一方面，目前网络拓扑呈现规模大、复杂度高、不稳定的特点. 网管人员部署控制逻辑时无法准确获知网络运行状况，为了能适应网络实时状态的改变，不得不部署大量的路由器检测代码. 这种适应通过“揣摩”网络的行为来实现，不但没有实现网络控制逻辑与数据层的无缝融合，还增加了网络控制逻辑的复杂性. 过于分散的网络状态信息分析和决策容易导致控制逻辑与控制操作的不一致.

另一方面，网络管理需要借助分布式网络协议间接实现. 当今业务对网络不断提高的控制功能需求，受到了网络设备交互协议可扩展性的制约. 控制逻辑的分布式实现难以协调，增加了引入漏洞和脆弱性的几率，导致网络故障的发生，如网络自治系统的 BGP 域间策略冲突导致网络抖动和慢收敛现象[6]，使网络复杂度不断增加.

网络控制与数据层的紧耦合关系，再加上混合式的网络控制模式，加剧了新业务需求与网络控制层可扩展性之间的矛盾，导致网络的控制和管理越来越臃肿.

2.2.3 信息多元化和可信保障困难

随着网络技术的飞速发展和网络新应用的不断涌现，当前的互联网面临着严峻的安全挑战. 在传统的 Internet 网络体系中，假设用户是友好信任的，所以网络只需要负责数据的传输，而不需要其它控制功能. 这一假设不再适用于当今网络所生存的环境. 目前网络所面临的可信问题日益突出：难以识别异常的网络行为，对网络的破坏活动难以遏制；网络可信与安全攻击如拒绝服务 DDoS 攻击、间谍软件、僵尸网络、网络钓鱼等手段层出不穷，这些问题严重威胁了社会和经济的发展.

虽然目前人们已经认识到安全问题的严重性，试图通过安全补丁的手段加以解决，如增强网络层安全性的 IPSec、防御 Dos 攻击的互联网业务主动过滤机制(AITF)[7]等协议，但目前网络安全控制机制存在明显的局限性：大多采用了单一的防御手段、信息安全和打补丁附加的机制[8]，功能上的分散化和单一化难以进行有效的整合；这些手段附着在互联网体系结构上，不能解决可信网络的本原问题.

互联网在设计之初对安全问题考虑不足. 简单的核心对业务过于透明，控制手段相对薄弱，难以监测到业务层面存在的问题. 无法区分新业务和网络攻击行为[9]. 缺乏可信与体系架构的融合设计，其中僵化和脆弱的体系结构是导致网络众多脆弱性的一个重要因素. 未来互联网需要充分的可控能力来解决传统互联网所面临的安全问题，增强系统的鲁棒性并提供系统的安全服务，实现网络的高度可信.

综上所述，我们有必要对未来网络所应具备的基本属性进行重新审视和总结，以此勾勒出未来网络的发展需求和未来网络技术的研究方向.

3 未来网络的设计要求

3.1 未来网络发展需求

未来网络的参与者从提供服务的视角来看，分为应用服务提供商(ASP)、网络用户(NUS)以及网络服务运营商(ISP). 其中应用提供商开发、调试应用程序运行于网络；网络运营商负责维护网络、保障服务；网络用户享受服务. 这种角色分工模式与现在的网络是一致的，但各个角色的要求则日趋多样化：应用提供商希望网络平台能够自适应于网络应用；网络运营商希望能对网络业务充分、便捷的监管；网络用户则希望能够更加灵活地定制自己的业务. 由此可见，未来网络应具备自适应多种网络主体、多种网络应用的特性，满足不同使用角度用户的友好要求，如图 1 所示.

应用提供商希望能够拥有自己的网络操作视图. 通过这个视图能够便捷、实时、准确地获取网络运行状况数据，在此基础上实现对网络服务资源的细粒度化管理和任务的可靠性调度，同时也能够对网络服务所依托的网络环境参数进行灵活调整、针对性定制和优化.

网络运营商希望通过自己的网络操作视图，能够充分、实时地获取整体网络的运行状况，并对网络业务进行充分感知，如链路负载率、路由协议收敛性等网络参数和网络业务运行数据，在此基础上有针

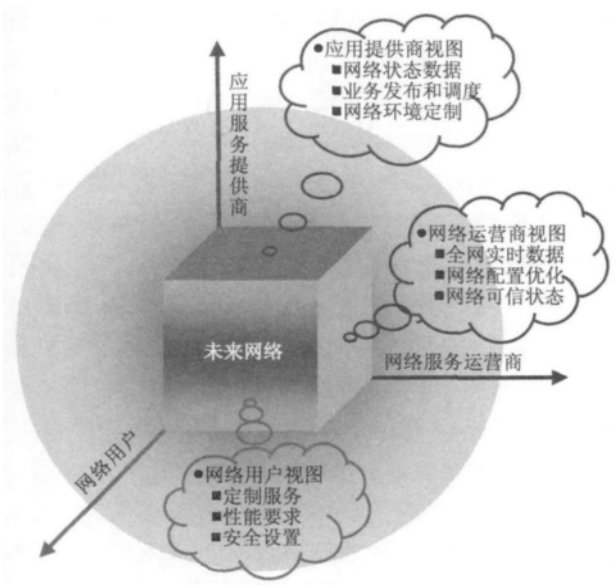

图 1　未来网络的不同视角

对性地对网络业务流进行调节和引导，以充分发挥网络基础设施和网络资源的使用效率，保证网络业务开展的良好性能；能够从高层次的网络管理逻辑入手，对网络进行便捷的配置和管理；具有一套自动处理逻辑，保证包括应用提供商和网络用户在内的网络参与者的行为始终处于可控、可管和可信的状态，网络活动参与者的任何操作都不影响其它业务的正常运转.

网络用户希望通过自己的网络操作视图，能够方便地为自己定制一套个性化的产品服务，包括业务名称、用户访问时间、上传/下载带宽、数据包路径要求、数据加密等级和备份规格等一系列在直观上就能够体验到的指标参数，以使个性化这一真正的客户价值属性得到充分满足.

为了适应上述各个视角对操作自适应的要求，未来网络的体系架构应提供方便感知、操作和控制的接口，并要求这些接口具有灵敏性、准确性和稳定性的自适应特点，保证网络信息能为各个网络主体及时准确获取. 一方面支持单方或多方联动调整网络的运行状态；另一方面要求保证网络能在网络遭受恶意行为的情况下具有较高的自愈特性.

3.2　未来网络实现指标

针对未来网络的设计，我们认为保证网络的可控、可管、可扩展和可信构成了未来网络自适应特性的必要条件，接下来我们从定义和内涵上对上述 4 个属性进行理论上的讨论.

定义 1.　可控(Controllability)[10]. 对于目标系统，若存在手段使得系统始终运行在允许状态，称该系统为可控系统.

形式化定义：假设目标系统 T 的状态空间为 S，允许状态空间为 S_a，如果存在控制 f 满足 $f: S \to S_a$，那么 f 为控制，目标系统 T 为可控的.

根据允许状态的不同，可控可以分为状态可控、输出可控和操作可控. 若允许空间与输入状态无关，称该系统为状态可控；若允许空间与输入状态有关，该系统为输出可控；若允许空间不仅与输入状态有关，而且还与其他参数变量(这里称为操作)有关，称该系统为操作可控.

为评价可控能力，可以选择相应的指标，如状态平均转换时间、控制耗费成本等.

可控网络的可控是指网管人员具有对网络参与者行为、网络运行和网络资源 3 个方面进行有效控制的能力：对网络参与者行为的可控保证对参与者行为的有效监测，及时发现和控制异常行为；对网络运行的可控是指能够对网络参数进行按需配置，及时提取、分析和诊断网络运行状态，对网络异常做出针对性的处理；对网络资源的可控是指对网络物理资源和服务资源进行有效调度，最大化满足用户服务质量需求.

定义 2.　可管(Manageability). 对于正常运行的系统，若存在手段管理和调度系统资源，使得系统具有不同的运行性能，称该系统为可管系统.

形式化定义：假设 $F=\{f_i\}$ 为使目标系统 T 正常运行的控制策略集合，$P(f_i)$ 表示策略 f_i 下的系统性能，若存在函数 $M: F \to F$，若存在 $M(f_1)=f_2$，使得 $P(f_1) \neq P(f_2)$，那么 M 为管理，目标系统 T 为可管的.

可管常被应用于商业和社会科学领域，常见的有商业管理、人事管理等；在计算机网络领域，文献[11]从实施的角度较为详细地讨论了网络管理与可管理网络的关系. 根据定义，对于给定的考察指标(如机密性、吞吐率等)，系统关于该指标的可管性可用下列方法评价：

(1) 极差法：$\left|\max_{f\in F}\{P(f)\}-\min_{f\in F}\{P(f)\}\right|$.

(2) 比值法：$\left|\dfrac{\max\limits_{f\in F}\{P(f)\}}{\min\limits_{f\in F}\{P(f)\}}\right|$.

对于系统的可管性，可以用下列方法评价：

(1) 支持类别：$|I_a|$，其中 I 为指标集合，I_a 为支持的指标集合，且 $I_a \in I$.

(2) 加权平均：$\dfrac{1}{|I_a|}\sum\limits_{J\in I_a}\left(w_J\left|\dfrac{\max\limits_{f\in F}\{P_J(f)\}}{\min\limits_{f\in F}\{P_J(f)\}}\right|\right)$,

其中 I_a 为支持的指标集合，$P_J(f)$ 为指标 J 下的性能.

网络的可管理是指提供方便、灵活的管理手段，可以对网络运行的各个方面实施全面、高效的管理[3]. 可管性要对网络运行期间的各种状态进行及时、充分的感知，在网络环境和资源受到内外因素干扰的情况下，对网络运行参数和网络活动参与者的行为进行持续性的监测、分析和决策，对网络设备和网络协议的控制参数进行自适应优化配置，保证为用户提供能够达到预期服务质量约定(Service-Level Agreement，SLA)的网络服务.

定义 3. 可扩展(Scalability)[12]. 对于目标系统，如果无论设施和业务规模如何变化，服务质量和系统开销始终保持一定关系，那么称该系统为可扩展的.

形式化定义：对于目标系统 T，ΔT 表示系统的变化量，$Q(*)$ 表示系统 $*$ 的服务质量，$C(*)$ 表示系统 $*$ 的系统开销，$R(Q(*),C(*))$ 表示服务质量与系统开销的关系函数，令 B 表示关系界限，若对于任意的 ΔT 都有 $R(T+\Delta T)\geq B$，那么称系统 T 为可扩展的，相应的 $R(T+\Delta T)$ 可以表示系统的可扩展性.

特殊地，可以取 $R(Q(*),\ C(*))=\dfrac{Q(*)}{C(*)}$，用 $\max\limits_{\Delta T}\{R(T+\Delta T)\}$ 来衡量目标系统 T 的可扩展性. 关于服务质量和系统开销的度量可以参阅文献[13].

定义 4. 可信(Trustworthy). 对于目标系统 T，其输出总能达到期望的目标状态，且独立于输入，称该系统 T 为可信的.

形式化定义：系统可以用函数 D：$In\rightarrow Out$ 来表示，对于输入 $i\in In$，$A(i)$ 为状态 i 对应的期望状态，若对于任意的输入 i，都有 $D(i)\in A(i)$，那么系统 T 为可信的.

可信的定义具有较强的扩展性，例如针对安全领域可被规定为可信任[14]，对传统的安全概念在内涵和外延上进行较好的拓展；针对用户行为，该定义又可被特殊化为行为可信[15]等. 但是，上述可信的定义依赖于系统期望状态，往往需要大量的测试和分析，增加了对系统可信性评价的难度，成为了该领域研究的重点，相应的模型和评价方法可以参考文献[14-18].

对于计算机网络而言，可信具有更为具体的定义，常被称为可信网络，指的是网络和用户的行为及其结果总是可预期与可管理的计算机网络[8]. 重点强调了两层含义：信任是可预期的前提；可预期是基于信任的.

通过对上述定义分析，我们不难发现可控保证了网络的可操作性，是实现自适应网络的基础；可管为网络资源的动态管理提供可能，是实现自适应网络的条件；可扩展强调了系统的可发展，保证了系统能在保证服务质量的情况下实现系统开销最小；可信通过设置可信根和可信链的方法给出了实现自适应网络的手段. 总之，设计自适应的未来网络，可控、可管、可扩展和可信已成为了必须考虑的指标.

3.3 未来网络设计方法论

针对未来网络发展的需求和实现的指标要求，用 $T_1,T_2,\cdots,T_n$ 表示网络设计所需实现的目标，并用 OPT：T_x 表示目标 T_x 的最优值；用 f_{ij} 表示第 i 种主体的第 j 种需求，其中 $i\in\{ISP,NUS,ASP\}$，j 为整数，那么网络设计等价于求解如下的规划问题：

$$\text{OPT：}\ T_x,\ x=1,2,\cdots,n,$$
$$\text{s.t.}\ \ f_{ij}.$$

针对上述问题，一个可行的方法是转化多目标规划为多个单目标规划并的问题，采用分而治之的方法实现，本文将从目标函数的可分离与约束条件可分离角度来探讨未来网络的可行架构.

接下来，本文首先分析现有自适应网络的相关技术，从硬件设备支撑和体系架构等方面阐述它们在未来网络中的应用，并在此基础上给出自适应的未来网络体系结构框架(AFIF)和实现方式.

4 已有自适应网络的实现技术

4.1 主动控制技术

通过对网络设备增加管理接口，方便使用者根据需要对网络设备进行管理，是一种较为直观的主动管理技术，其中 OpenFlow① 是较为典型的代表.

OpenFlow 由 Nicira 公司的首席技术官 Martin Casado 在 2007 年提出，其初衷是通过对交换机或路由器定义一套软件操作 API，建立可编程的、开放式的虚拟化设备平台. 可以方便地将路由协议、安全模型、寻址方案等策略应用于网络，实现网络优化目标. OpenFlow 体系结构如图 2 所示，由支持 OpenFlow 协议 API 的交换机、路由器和中心控制器(Controller)组成. 操作对象被定义为网络中的“流”，即根据过滤

① http://www.openflow.org/

规则筛选出的一组定义的数据帧或者数据包(如源/目的端口号和 IP 地址等),以及与流对应的一组规范化操作(如转发数据包、打包传送给控制器、丢弃数据包等). OpenFlow 的中央控制器与交换机之间通过建立一对一或者多对一的安全信息传输通道,将网络配置信息发送给交换机或路由器节点;节点通过配置一组规则用来定义一个"流"及其附属的某些操作序列,并根据自己的类型执行这些规则.

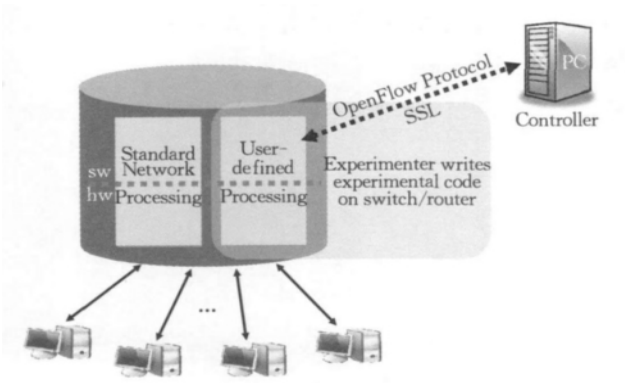

图 2　OpenFlow 体系结构[19]

OpenFlow 处理网络数据包有两种方式:第一种通过配置网络交换节点,将流经交换节点的所有数据包实时路由给中央控制器或网络处理器处理①;第二种是中央控制器在全网节点上预先配置业务流逻辑,通过修改各个节点的流规则定义流操作序列,节点通过依次匹配 Flow Tables 和 Group Tables 流规则,对流量数据包进行"管道"(pipeline)式的操作②,实现对数据包的序列化处理. 相比较而言,前者节点不需要额外注入流过滤规则,易于进行部署和调试,适用于新协议的功能正确性验证;后者更易实现节点一致性的预先部署,适用于大范围的网络业务部署.

OpenFlow 将网络控制权与网络物理底层硬件的数据交换分离独立实现,改变了传统网络中交换机和路由器控制数据包转发的模式;控制层软件通过与网络设备标准接口对网络流量进行探针式抽取,建立网络实时状态和历史状态信息的中央视图;将用户管理界面与网络设备细节分离,方便了用户的精细化管理.

目前,随着由谷歌、微软、Verizon、雅虎发起建立的 Open Networking Foundation(ONF)机构的推动,包括 Broadcom、Cisco、Ericsson、Juniper 等在内的几乎所有主流网络设备都支持 Openflow 规范. 但是 OpenFlow 同样面临着巨大挑战③:一方面,目前的协议规范仅实现了简单的、低级别的底层网络接口,对操作接口的更高层次包装和抽象仍具有较大难度;另一方面,OpenFlow 未经过大规模的网络部署测试,其可扩展性和安全容错性都受到质疑.

4.2　主动管理技术

通过对网络设备管理接口进行高层次封装,方便使用者根据需要对网络整体进行统一管理,其中 NOX[20] 是一个具有代表性的开源 OpenFlow 管理器.

NOX 实现了一个提供集中式开发环境的网络操作中间件,该开发环境提供了针对全网的通用标准开发接口,这个接口具有集中式的编程模式和高层次网络抽象两个特性:

(1)集中式编程模式是指在综合处理收集到网络的状态信息之后再进行功能实现,在开发者看来整个网络就像一台具有统一资源管理和接口的计算机;

(2)高层次网络抽象是指在以 OpenFlow 作为底层网络接口的基础上对网络操作进行了高层次的抽象和封装,为应用程序的开发提供高层次接口.

NOX 系统组成如图 3 所示,包括若干支持 OpenFlow 的交换机和软件控制系统. 软件控制系统包括若干分布在不同服务器上的控制器进程和一个存储在数据库中的唯一网络视图,网络视图为网络应用程序和网络控制程序提供了包括交换机级网络拓扑、网络用户位置、网络终端位置在内的网络物理资源的高层次视图,以及对网络设备名称和地址的映射绑定. NOX 编程接口采用了网络事件驱动的

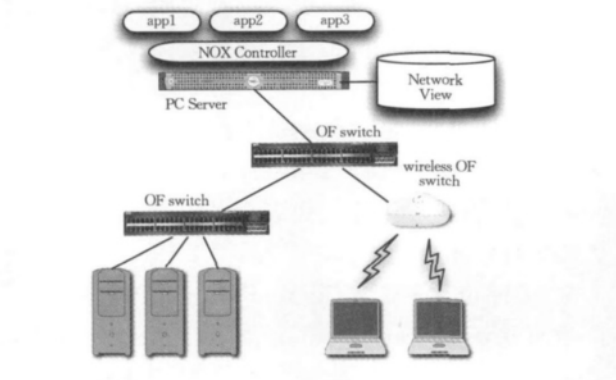

图 3　NOX 系统组成[20]

① NetFPGA: Programmable Networking Hardware. http://netfpga.org

② Openflow-Spec-v0.8.9: OpenFlow Switch Specification, Version 1.1.0. http://www.openflow.org/documents/openflow-spec-v0.8.9.pdf, 2011

③ Openflow is the answer. http://networkheresy.wordpress.com/2011/06/15/openflow-is-the-answer-now-what-was-the-question-again/

方式，除了包括交换机加入和退出、数据包接收、交换机状态更改等底层网络事件之外，NOX 应用还包括一些如用户权限审核、网络服务发现、重建交换机级拓扑等较高层次的应用事件提供给上层程序使用. NOX 还提供了网络开发中的高层次服务库模块，包括路由模块、快速包分类、标准网络服务以及基于策略的网络过滤模块等.

采用 NOX 接口实现的网络应用系统可以大大降低工作量和加快开发进度，如全网访问控制系统 Ethane[21] 使用 C++实现需要 45 000 多行代码，而采用 NOX 实现只需几千行代码. 但 NOX 目前的应用仅限于实验室网络，在体系架构方面并未考虑实际网络中应用程序大规模并发的情形，在任务处理方面能否支持大规模的实际网络还有待验证，一个运行在普通计算机上的 NOX 控制进程大约能够支持每秒 100 000 个流的初始化[20].

与 NOX 项目类似，SANE[22] 在网络控制层上定义了一个保护层，用以管理大型互联网的所有连接，对访问服务的所有路由和访问控制策略进行集中式的统一监管，提高网络管理的鲁棒性和安全性；Maestro[23] 将网络管理功能通用模块化，实现了并行处理的 OpenFlow 控制器，其目标是将网络中的功能抽象为便于定制和组装的单一模块，具有易维护、高可靠性的优势，在多核处理器系统上实现近似线性的任务处理复杂度；Onix[24] 是由 Nicira 公司维护的，面向产品的分布式 NOX 实现，它完成了一套互联网级的 OpenFlow 部署方案；DIFANE[25] 通过对 OpenFlow 的底层设备接口进行高层次的功能封装，为交换机提供了丰富的策略配置集，从而提高了网络控制器的性能，降低了任务处理复杂度.

4.3 服务定制技术

通过重新设计 IP 网络体系结构，实现对网络服务的可定制和可管理. 其中 NDN(Named Data Networking)[26] 是一种具有代表性的开放式网络存储资源管理技术.

NDN 也称 CCN(Content-Centric Networks)，该项目来源于 Future Internet Architecture(FIA) program，其独特的以数据为中心的思想改变了当今互联网所广泛采用的数据传输模式. IP 地址同时包含标识和位置信息的双重属性是导致目前互联网路由可扩展性、移动性差的根本原因. IP 网络采用基于网络地址的数据传输方式，用户请求数据时首先要获知拥有数据主机的网络地址，然后再与该网络地址进行数据的请求和传输. NDN 设计人员认为网络本来的属性是为了数据分发而不是为了节点间的通信，因此致力于使互联网不考虑内容存储所在的物理位置，直接提供面向内容的功能.

NDN 对网络信息进行了命名，结构可以是层次化的可聚合形式，也可以是扁平化的方式. NDN 的层次结构如图 4 所示，NDN 数据传输对象是大小固定的数据分片(chunk)，由此取代了传统网络结构中 IP 的细腰. 与数据分片层相邻的分别是负责 NDN 策略缓存策略、数据请求策略、数据转发策略的策略层和保证数据完整性、可靠性的安全层.

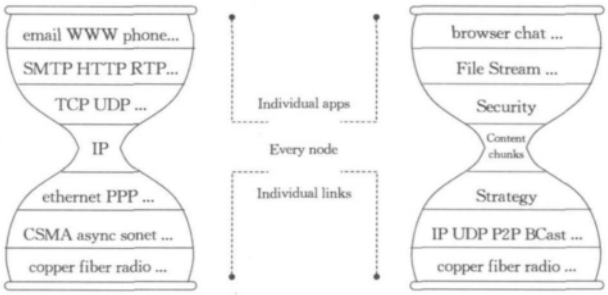

图 4 NDN/CCN 层次结构[27]

NDN 网络中有两种基本的包格式：数据请求包(Interest package)和数据返回包(Data package). 客户请求数据只需要在数据请求包中注明数据的名称，而不需要声明去哪里获取. 路由器节点上需要维护 3 个表结构：

(1) Content Store(CS)用来缓存数据以及更新缓存策略；

(2) Forwarding Information Base(FIB)用来存储下一跳转发接口和内容名字的映射表，由基于名称的路由协议来生成；

(3) Pending Interest Table(PIT)用来记录数据的请求接口记录，从而建立数据返回包的传输路径，同时聚合邻居节点对相同内容的请求.

路由节点在收到数据请求包后，首先在 CS 表中进行查找，如果命中就返回数据，若没有命中就查询 PIB 表，PIB 表中没有该数据的请求接口记录则加入 PIB 表，然后再根据 FIB 表和策略层配置选择一个或多个接口转发该数据请求. 当数据返回包在由 PIB 表建立的反向路径传输时，各个路由节点会根据一定的策略对数据进行缓存，然后再依照 PIB 表中的请求端口记录，将数据复制多份转发给各个请求接口.

NDN 这种独特的根据命名的路由和转发方式具有很多天然优势：首先数据请求与源/目的网络地

址解耦，有效地支持网络终端的移动性，在 PIB 表聚合请求以及多个 FIB 接口转发的机制支持多路径路由，从而天然支持数据分组的广播和组播；其次客户在请求数据服务时不限定提供资源的服务器，NDN 节点上的策略层可以针对不同数据业务的不同服务质量要求分配不同的服务器资源，策略层缓存选取策略灵活多变[28]，再加上内容的分布式存储[29]，就可以方便地实现网络业务的灵活定制和网络资源的灵活配置；再次 NDN 所采用无连接的数据传输方式，改变了传统数据传输中只保障数据容器（网络链路、服务器）安全，而不是数据本身安全的方式，对数据本身进行数字签名和加密来保证信息的完整性和可靠性；最后 NDN 网络技术与现有网络体系结构具有较好的兼容性，支持渐进式部署.

与 NDN 类似采用以信息为中心的网络（ICN）技术还有 PSIRP（Publish-Subscribe Internet Routing Paradigm）①[30] 技术，它采用汇聚点（Rendezvous）对内容进行统一管理，数据源在汇聚点发布信元（Information object），数据接收者在汇聚点通过层次化的 DHT 方法查询已发布的信元，获得可以被解析和路由的信元标识符来标示数据源与接收者之间的通信信道，接收者以此向数据源进行消息的订阅和注册；4WARD-NetInf② 为了保证命名空间的持久性和内容的独立性使用了平面命名空间，其数据的请求和路由方法采用了基于内容名称的 DHT 解析和 IP 路由协议；TRIAD[31] 使用了与 IP 体系兼容的层次化内容命名空间，采用了与 NDN 一致的洪泛查找路由策略；DONA（Data-Oriented Networking Architecture）[32] 的内容名称解析采用了层次化的体系架构，数据发布者通过 Register 消息发布和注册数据，数据请求者通过 Find 消息层层查询离自己最近的数据，在返回数据时数据源既可以与请求者建立基于 IP 的连接，也可以使用基于数据的路由方法，依照内容名称解析出的路径逐跳转发.

5　已有自适应网络的体系结构

5.1　控制优先的层次化网络体系

4D（Decision，Dissemination，Discovery，Data）[33-34] 由美国卡内基梅隆大学的研究课题组提出，该体系遵循 3 个设计原则：第一个是满足网络级的控制目标，将网络如性能、可靠性、策略等方面的配置目标与具体的网络元素相分离，实现对网络的可靠配置，避免使用网络节点级命令分别配置各个节点，网络级配置目标转成特定协议或机制目标时容易产生的语义错误；第二个是提供一个准确、完整的网络数据层视图，这个网络视图包括各个网络组件的物理属性快照以及拓扑、流量信息、网络事件等实时信息；第三个设计原则是指网络的控制逻辑具备对网络数据层直接控制的能力，网络控制逻辑不再与运行在网络节点的分布式协议紧耦合，两者相互之间的关联性仅存在于控制逻辑的输出接口.

如图 5 所示，4D 网络的体系机构由 4 个层面组成：

（1）位于最上层的是决策层（Decision），它是由许多决策单元组成，用来接收网络管理者发出的如网络可达矩阵、负载均衡目标等网络级的控制逻辑，通过算法运算将其直接转换成数据层可直接执行的如转发表条目、包过滤规则、队列参数等网络配置指令；

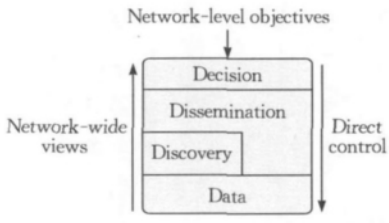

图 5　4D 网络体系结构[34]

（2）体系结构中枢是信令分发层（Dissemination），它为其它三层提供了高效、可靠的消息传输通道，这个通道与数据层面共享物理通道，但逻辑上与数据层面独立，在网络路由协议还未建立转发表或发生故障时，4D 系统的配置信令依然能够完整地通过信令分发层到达网络节点；

（3）信息发现层（Discovery）实时发现网络物理设备及其属性，包括网络设备属性（设备接口、FIB 容量）、邻居发现、网络链路属性（设备容量）等，登记网络物理设备进行统一命名管理，实时更新各个物理设备的状态标志位，这些信息提供给决策层生成准确、完整的网络数据层视图；

（4）位于体系结构最底层的是数据传输层（Data Transportation），这一层依照决策层输出的配置指令处理网络中的数据包，实现在网络控制逻辑下的数据转发功能，同时还收集网络中的环境信息提供给信息发现层.

① The PRISP project. http://www.psirp.org/publications
② The FP7 4WARD project. http://www.4ward-project.eu/

4D 网络将网络控制逻辑从网络分布式系统中彻底剥离出来，如网络路径计算功能不再由路由协议生成；支持网络级的配置目标，提升了网络管理的抽象程度，使得网管人员可以专心控制逻辑设计，不必顾及分布式网络协议细节，简化了网络控制，同时也保证了控制逻辑和网络运行状态的一致性，大大降低了由于配置错误造成性能、安全方面的风险.

4D 网络受到很大挑战：如今互联网节点呈现规模大，层次复杂的特征，网络状态不稳定、变化大，路由器需要处理成千上万的前缀信息，信息发现层难以生成稳定、准确的全网级网络视图供决策层使用；信令分发层需要建立独立的、不借助于现有网络协议的传输体系，虽然其数据流量较小，但要维护这些数据连接通道，又不影响实际网络的运行难度较大；4D 网络架构缺乏安全方面的考虑，采用集中式的控制方式，信令分发层和决策层受到攻击会对网络整体的控制权造成威胁.

5.2 管理优先的并行化网络体系

GENI 项目[35]全称为 Global Environment for Networking Innovation，即全球化网络创新环境计划，由美国自然科学基金在 2005 年发起，其目标在于构建一个全新、安全、普适于所有设备，支持多种新型网络体系结构进行大规模部署、实验和研究的基础网络设施，特别是对互联网进行革命式设计及体系结构的相关研究.

GENI 的体系架构如图 6 所示，从上到下依次被划分成 3 个层次：用户服务层、GENI 管理核心(GENI Management Core，GMC)以及物理层.

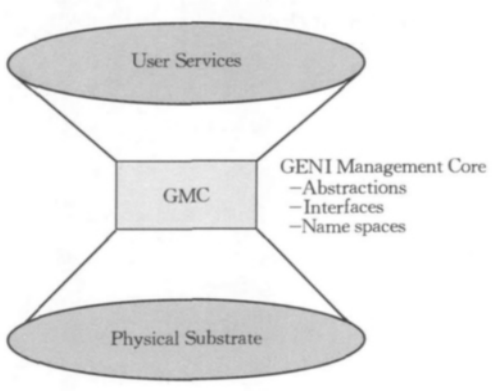

图 6 GENI 体系架构①

处于体系最底层的是物理层，物理层包括路由器、处理器、数据链路、无线设备等物理设施，其设计目标是为了确保物理资源、布局和网络拓扑能够充分支持 GENI 的研究目标.

用户服务层位于体系的最顶部，为 GENI 的各类用户提供一套丰富的支撑服务集. 通过这套服务集合，基础设施所有者可以对其拥有的底层设施资源进行分配或制定相应的分配策略；GENI 管理员可以对 GENI 物理层进行管理，包括部署新设备，淘汰老损设备，安装或更新系统软件，监测 GENI 网络的性能、功能和安全；为研究人员提供丰富的程序库和灵活的语言执行环境，使之可以借助于 GMC 接口方便地创建和发布实验成果，自定义资源分配或者调试软件；GENI 开发人员可以获得 GENI 的物理底层信息，部署高层次的监控、测量、审计和资源发现服务.

GENI 管理核心位于物理层和用户服务层之间，GMC 作为 GENI 系统核心目的在于定义一个稳定、前瞻、持久的系统框架，通过该管理服务和操作的框架，能够实现用户和高层服务对底层 GENI 资源的访问和控制. 该框架包括组件、切片和集合体 3 个概念：组件是指物理资源(CPU、存储、硬盘、带宽)、逻辑资源(文件描述、端口号)和综合性资源(包转发路径)的封装体，GMC 通过组件管理接口(CM)将组件资源分配给不同的用户任务. 组件具备 4 个特性：(1) 多路复用. 支持以虚拟化或资源分片的方式供多用户使用，虚拟接口(Virtual Interface)可以根据切片定制信息与网络资源动态绑定；(2) 可控. 组件的行为可控，可以限定组件/分片的数据发送速率、可访问的组件/分片等一系列安全保障机制，当发生异常时能迅速切断组件与网络之间的联系，并重置组件到安全状态；(3) 虚拟接口. 虚拟接口是指任务切片访问网络的接入方式，包括 Socket 接口、虚链路接口、虚拟无线/有线接口；(4) 层次化管理授权. 切片如图 7 所示是指横跨 GENI 组件集合由 GMC 创建和管理的一系列分片，研究人员在这些分片上配置、加载和执行代码来运行试验程序. 集合体是指由一些具有共同性质的 GENI 元素构成的集合，这些元素可以是组件或集合体，它们具有如在同一个物理位置的、共享相同物理链接、被同一机构管理、相同配置等共同性质，对集合体元素的操作通过集合体管理接口(AM)完成.

① GENI-SE-SY-RQ-01.9：GENI Systems Requirements，Prepared by GENI Project Office. BBNTechnologies，http://groups.geni.net/geni/attachment/wiki/SysReqDoc/GENI-SE-SY-RQ-02.0.pdf，2009

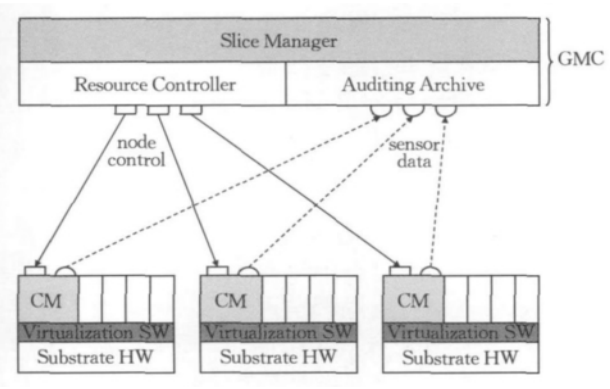

图 7　GMC 资源垂直分片管理①

GMC 安全性原则包括明确灵活的定义方式、最小权限原则(只给予系统组件能保证其履行工作的最小权限)、迅速反应原则(当系统密钥发生泄露或被篡改后,能够迅速地撤销或更换密钥,重置受影响的节点)、问题可审计性、安全自治性、安全框架的可扩展性和易用性、低安全开销等原则.

GENI 支持在管理框架下定义的操作接口,其可编程性为研究人员提供了必要的灵活性,开放式体系结构能够同时支持多组实验和多用户应用. 多种新型网络体系结构可以同时配置运行,实现了同一个物理网络承载多个不同逻辑网络的设计模式. GENI 安全可控的体系结构对实验进行约束,消除外在的、不受控的因素影响,避免实验本身影响到网络上的其它业务以及 GENI 系统本身的稳定性,确保整个 GENI 系统运行在一个安全和可控的状态.

5.3　侧重可信的综合化网络体系

文献[36]提出了基于信任维护与行为控制的可信网络,认为可信网络就是一个行为可以预期的网络,行为状态可监测、行为结果可评估和异常行为可控制作为组成可信系统的三要素,通过可信网络的信任维护与行为机制,实现了可信网络行为动态过程的闭环机制. 如图 8 所示,维护信任信息的过程采用了流水线式的处理方式:信任信息采集提供了具体的采集手段,按采集手段划分为集中式安全检测、分布式节点自检和第三方通告三种,这三种方式在部署成本、可行性、准确度方面相互补充;信任信息在经过存储、传播之后,到达信任分析与决策部分,通过行为可信性分析之后输出行为的信任等级和相应的处理策略,以此驱动和协调需要采取的行为控制;行为控制的手段根据处理的方式包括被动式预警处理、主动式免疫隔离两种:前者通过自适应的调整或限制全部或部分网络资源的访问权限,同时报告潜在的或已发生的破坏性行为,后者是指在攻击和破坏行为出现之前的一种主动式防御措施.

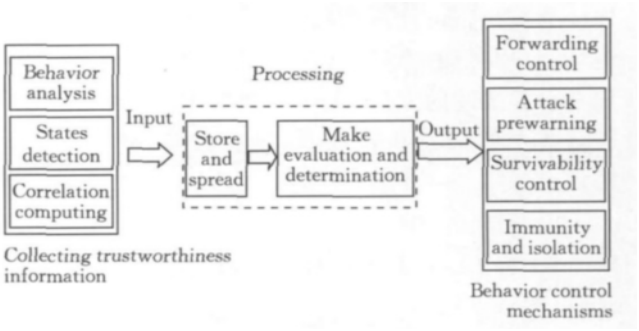

图 8　可信网络的信任维护与行为控制[36]

文献[37]提出了可信控制体系模型,该模型如图 9 所示将网络分为数据传输平面和可信控制平面,其中数据传输层面负责承载网络数据业务,同时保障网络协议的可信性;可信控制平面包括一组可信协议和控制信令,采用了水平分层的结构,包括身份管理、生存管理、行为管理等可信管理. 在该模型中数据平面和可信控制平面相互依存:可信控制平面监控数据平面的同时,也向其提供例如网络可信度的查询接口和业务运行模式的信任定制接口.

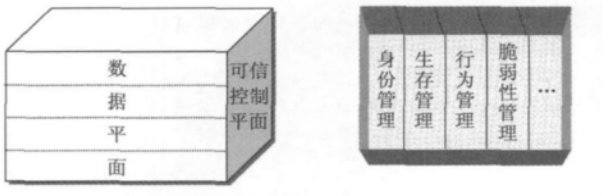

图 9 可信控制体系[37]

文献[38]提出了一体化可信网络的架构,如图 10 所示,提出了两层的网络体系结构:交换路由层的目标是在一个可信的网络平台上提供多元化的网络和终端接入,保证信息交互的可信性和移动性. 交换路由层采用了接入标识和交换路由标识分离的方法,接入层使用代表用户身份的接入标识转发数据,以此实现网络用户的接纳控制,通过网络的接纳控制对接入终端进行严格的鉴权,确保网络用户的身份合法性、隐私安全性以及行为可信任[15],保证

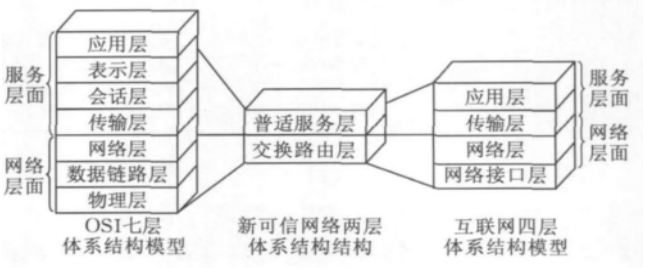

图 10　一体化可信网络[38]

了网络的可控性和可管性，在核心层使用代表终端地址的交换路由标识进行控制管理和路由交换，保证了用户身份的隐私性；普适服务层使用了服务标识和服务描述的方法，实现对网络中的资源和服务进行统一的描述和管理，同时支持多路径的传输协议.

6 已有技术和框架的对比分析

本文在前两节介绍了自适应网络关键技术和体系架构的研究进展，详细阐述和分析了各种技术的主要研究目标、研究思路以及具体的框架实现模型. 表 1 对现有的自适应网络关键技术和体系框架进行了综合对比分析.

在自适应网络的关键技术以及体系框架研究中，将网络的控制权从网络数据层抽取出来，实行统一化的网络管理体系，能够获得很好的控制交互性，但对网络统一化控制管理对于抗击网络鲁棒性、抗击网络恶意行为攻击方面具有天生的弱势，因此控制的安全性是必须考虑的一个重要方面；以网络控制权作为基础，对网络的控制业务进行合适粒度的服务封装可以大大提高网络维护、应用业务的开发和部署效率，减轻网络管理人员和应用程序开发人员的负担.

表 1 自适应网络关键技术和框架对比分析

分类	名称	技术目标	技术路线	研究内容	设计原则					
					网络业务友好性	系统可扩展性	控制交互性	控制安全性	服务封装	增量部署
关键技术	OpenFlow	实现以软件方式对网络进行灵活配置，促进和推动网络创新应用	将网络控制层软件与网络物硬件的数据交换分离，将用户管理界面与网络设备细节分离	网络控制接口通用规范、网络中央视图	√	√	√	×	×	√
	NOX	提供具有集中式编程模式和高层次网络抽象特性的通用标准开发接口	提供全网唯一的网络视图，对网络服务进行高层次的抽象和封装	网络资源高层次视图、高层次网络服务集	√	—	√	×	√	—
	NDN/CCN	以基于内容的路由技术取代目前以网络 IP 地址为核心的数据传输方式	根据内容的名称进行数据的请求和分发，在网络节点上缓存内容，直接对内容加密	内容命名体系、基于内容的路由算法、基于内容的安全、网络业务的策略模型	√	√	×	×	—	√
体系框架	4D	建立新的支持网络级配置目标的网络控制体系，提升网络管理抽象程度	网络控制逻辑与网络路由协议解耦，控制指令直接作用于网络数据层	统一的网络高层视图、网络级配置目标翻译、独立于网络路由的信令传输	√	—	√	×	√	—
	GENI	为未来互联网的研究、开发和部署提供完全可控、可配置的大规模通用实验平台	对网络资源虚拟化重组，定义清晰管理框架，为研究人员提供受安全约束的标准操作接口	可编程技术、资源虚拟化切片、安全可控实验	√	√	×	√	√	—
	可信控制体系	通过垂直的控制管理平面增强新一代互联网节点的控制能力	层间联合设计思想立体型协议模型	可信协议、控制信令设计、控制平面水平分层	√	√	—	—	—	√
	基于信任维护与行为控制的可信网络	通过保证行为状态可监测，行为结果可评估和异常行为可控制，实现网络的可信控制	建立可信网络的信任维护与行为机制的有机体，实现可信网络行为动态过程的闭环机制	体系结构设计、可控性及可生存性设计、建立网络用户行为可信模型	—	√	—	√	—	√
	一体化可信网络	具备安全性、可靠性、可控性、可管性等特性，支持普适服务的新网络体系架构	交换路由层将接入标识与交换路由标识分离，普适服务层引入服务标识和连接标识	接入控制管理技术、可信路由及服务质量、多流传输技术、网络监测管理技术	√	√	—	—	—	√

从表 1 中可以看出，目前对于自适应网络体系框架的研究对网络控制层的功能进行了层次上的重新设计和划分，对各种网络业务具有较好的灵活性，相比于目前的 IP 网络，大大降低了网络控制层的负担，但也存在两个突出问题：首先缺乏统一的框架体系，如何定义一个统一的、基于自适应网络关键技术

的体系框架，在这个框架中能够把现有的技术进行很好的融合是本文提出并解决的一个问题；其次如何对网络控制的安全性进行衡量和评估，在保证网络控制统一管理的优点下，确保网络控制权的合法性是迫切需要解决的另一个问题.

7　自适应的未来网络架构

通过以上的讨论，我们认为自适应的未来网络不仅应满足可控、可管、可扩展和可信任的要求，而且还应满足建设和管理成本最优的要求. 因此，在自适应未来网络体系架构设计中，应遵循以下几个原则：(1) 功能分层原则. 对整个框架的逻辑功能进行分层设计，能够降低整个逻辑功能框架的复杂度，通过各个功能层之间的标准接口进行逻辑上的重组；(2) 最小模块功能化原则. 在进行模块划分时，在保持模块功能逻辑的基础上，将不可分割的原子功能独立实现，加上统一的外部接口，以通用化的原则构建模块；(3) 模块独立化原则. 各个逻辑功能层里的具体实现要模块化，根据最小模块功能化原则进行模块化划分，对外定义通用的调用接口和标准调用参数，内部功能实现规范化、标准化，保证功能模块之间的独立性.

为了帮助未来网络的研究人员清晰地划分各功能组成的外延和内涵，集中精力实现各个功能，我们构建了一个自适应的未来网络体系结构框架(AFIF)，从应用服务提供商、网络用户和网络服务运营商对网络需求的角度出发，实现可信前提下网络的细粒度控制和管理(见图 11).

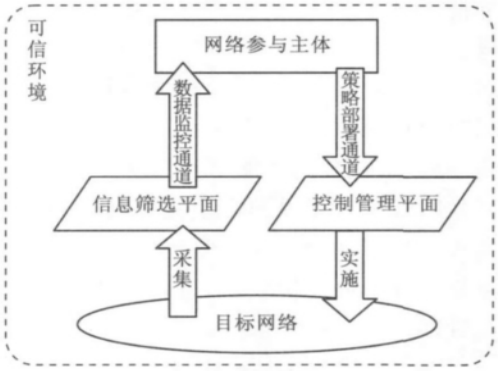

图 11　AFIF 设计框架

AFIF 体系结构框架如图 12 所示，由开发管理服务、分布式控制服务、贯穿其中的可信中枢层以及网络环境 4 个部分组成，其中点线框定义了完整的一套从网络控制逻辑作用到网络设备及其存储的操

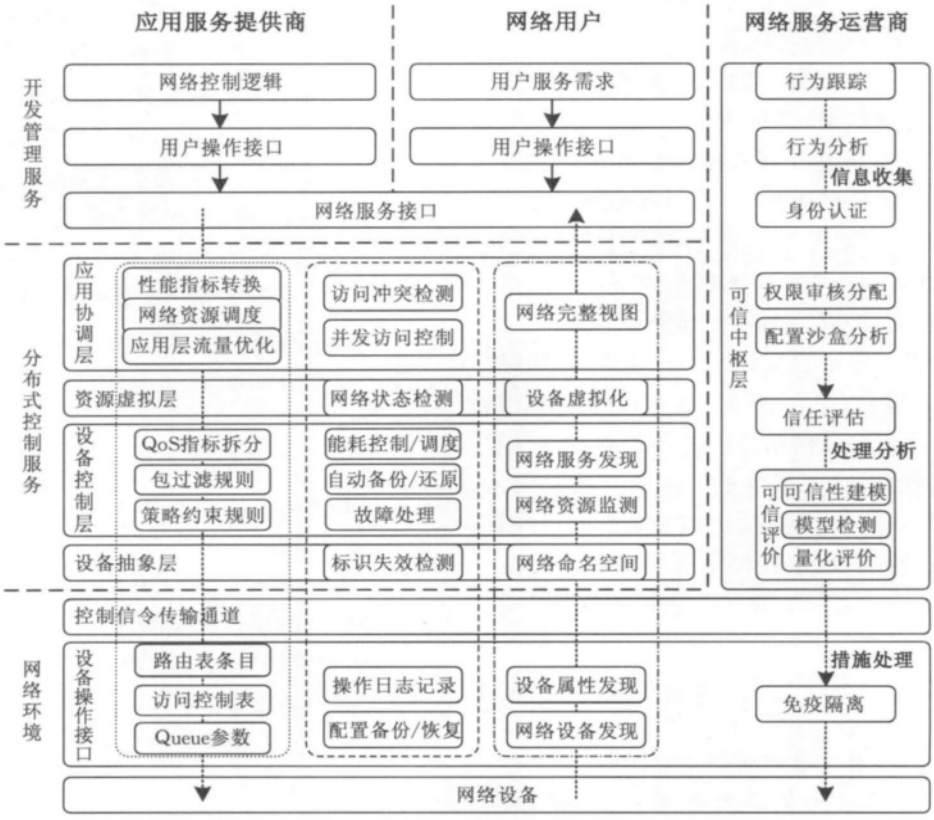

图 12　AFIF 体系框架

作框架，点划线框定义了从网络设备和网络存储中采集信息生成高层次的统一网络视图功能，虚线框定义了自适应系统中的自维护服务.

7.1 控制管理服务

开发管理服务由许多开发管理终端组成，这些开发管理终端自由分布在网络中，每个管理终端都需要从网络运营商处购买网络管理服务，并进行相应的注册，获得局限于所开发应用运行范围的网络参数管理授权. 每个开发管理终端包括一个用户操作接口，可以接收应用开发管理的高层次网络控制逻辑，如直观的网络可达矩阵、流量工程等控制逻辑以及用户服务需求. 网络服务接口为用户操作接口提供开发网络服务需要的高层次服务库模块，包括路由模块、快速包分类模块、标准网络服务模块以及基于策略的网络过滤模块等，方便网络应用程序的开发和管理工作.

分布式控制服务包括应用协调层、资源虚拟层、设备控制层和设备抽象层 4 个部分. 大量的分布式网络控制逻辑作用在同一个网络上，需要在多个网络控制逻辑之间对网络资源进行集中协调和调度，优化上层应用服务集的并发执行，因此在应用协调层对网络业务的应用层业务进行多目标优化①[39]. 访问冲突检测模块和并发访问控制模块用来检测和处理上层应用程序对相同网络资源并发操作时产生的语义冲突，最大化满足各个网络控制逻辑对网络资源的需求；资源虚拟层对网络服务进行拆分后，再根据规则进行重组，从而充分支持细粒度的多服务并发执行、实现任务的最优化融合，同时网络物理设备也在虚拟化拆分和重组后提供给多个应用服务；设备控制层通过对已有效融合的网络控制逻辑集进行层层拆分和编译，将其“汇编化”成可直接作用于网络节点、在网络节点上直接执行的控制指令，同时确保应用程序的运行时间、开销、可靠性等性能指标；设备抽象层用来抽象网络中的各种资源，通过提供高层次名称到低层次网络设备地址的双向映射、绑定和翻译服务，建立一个高层次的命名空间，为网络管理提供易用的接口，这样位于网络抽象层之上的程序就不需要耗费大量的时间和资源来处理繁杂的网络底层事件.

网络环境包括用来保障控制信令可靠传输的信令传输通道和部署在各个网络节点上的设备操作接口. 控制信令传输通道共享网络设备之间的链路，但在逻辑上独立于分布式网络路由协议，这样可以建立更可靠的监控机制，及时反映网络的行为状态，快捷高效地实施监控；设备操作接口是一个简单的、低层次的底层网络操作接口，通过该接口可以直接对网络设备进行配置，如添加/修改路由表条目、添加/修改路由器的访问控制表或者修改网络节点端口的队列缓存参数等.

以上 3 个部分中都嵌入了网络状态视图，如图 12 中点划线框所示数据的采集和传输流程，这个视图在低层次的网络环境中对网络物理设备及其设备属性进行自动发现；然后在设备抽象层对发现的网络物理设备及其属性建立统一的命名空间，对网络设备名称和地址进行绑定，提供命名空间到实际物理设备的翻译服务；并在设备控制层实时监测网络资源、发现网络服务；在资源虚拟层通过虚拟化网络设备为所有的开发管理终端提供一个统一的、完整的网络视图界面，避免在网络配置过程中出现网络状态信息分散、网络连接状态不一致的情况.

7.2 可信中枢层

AFIF 对网络安全的外延和内涵都提出了更大的挑战. 在传统网络中，网络软硬件的运行模式固定、单一，在这种环境下仅需要实现应用程序对用户的可信就能保证较高的安全性；而在 AFIF 网络中网络软硬件的运行呈现灵活和多元的特征，除了要保证应用程序对用户的可信，还要保证各层网络环境对运行其上的应用程序可信. 同时由于存在网络环境与应用程序之间的紧耦合可信关系，用户在使用应用程序时，除了担心软件是否完整没有被篡改、是否安全无恶意代码、是否正常运行之外，也会担心应用程序产生的数据在网络中是否经过了可靠的路由进行完整的传输，因此也存在各层网络环境与用户间的间接可信关系. 由此可见，可控、可管和可信性在 AFIF 网络中占据着至关重要的地位，因此有必要将该部分功能独立于其它模块实现，命名为可信中枢层.

可信中枢层保证了应用提供商、网络环境和网络用户三者之间的可信关系. 可信中枢层包括 3 个部分：信息收集、处理分析和措施处理.

行为跟踪和行为分析模块实现信息收集功能，通过多样化的手段来获取全面、合适粒度的用户证据，用于对网络应用开发者的信任度进行评估. 收集手段包括网络流量监测与分析、审计跟踪系统日志和用户日志以及专用的软硬件数据采集等.

① IETF ALTO Working Group. http://datatracker.ietf.org/wg/alto/charter/

处理分析包括信任评估和可信评价两部分. 信任评估是指对网络应用开发者的整体行为信任进行逐层分解，将综合、复杂的用户行为信任评估问题，通过层层细分，量化成可测量、可计算的行为证据的评估问题. 用户的行为信任属性包括安全信任属性，性能信任属性和可靠性信任属性 3 个组成部分[40]. 每个信任属性均包括若干证据指标，通过对这些证据指标进行定量的归一化和规范化处理，综合考虑信任评估的历史性累积效应和局部性效果，构建出信任评估模型，计算出用户行为的信任属性值.

可信评价是指获得和保证可信网络系统关键性质的检测理论和技术，避免由于网络对应用的自适应性和网络管理开放性所导致的软件错误，如应用软件的设计缺陷、开发缺陷或外部干扰导致系统的软硬件故障. 可信评价包括系统的形式化可信性建模、模型检测以及可信性量化评价 3 个阶段，其中可信性建模包括形式化建模技术和形式化检测技术等，模型方法有进程代数方法、模型检测方法、随机 Petri 网方法等. 对可信进行评价需要一套完整的可信评价指标体系，根据系统不可信问题的来源进行划分如图 13 所示：安全性用来描述系统在受到恶意攻击时安全指标发生的反应；可信赖性描述了系统内部故障等对系统性能指标的影响；系统的可生存性描述了网络系统在遭到攻击入侵、内部故障和操作事故等安全威胁或影响时，仍完成关键功能或恢复正常服务的能力[41-42]. 在评价时需要综合考虑各属性指标之间的关系，多方面多维度刻画系统的可信特征属性，然后给出包括瞬态定义和稳态定义在内的基于概率和随机模型的各可信性指标的量化定义，文献[43]从系统可信性指标计算的层面给出了多种安全属性计算方法的关系.

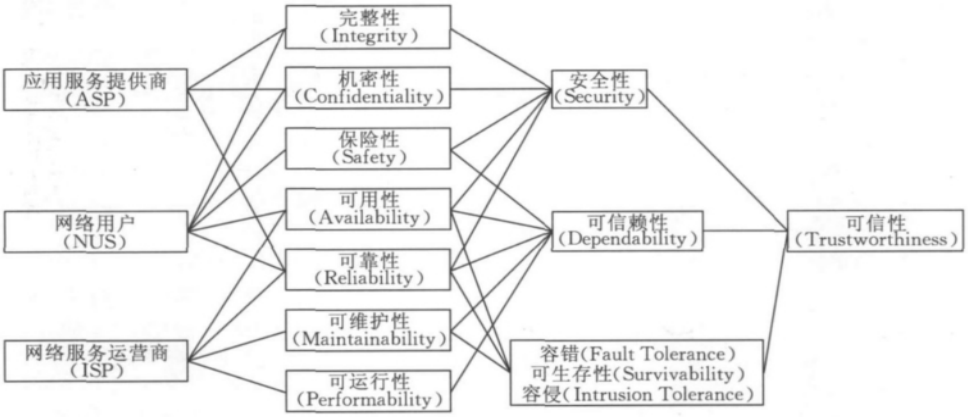

图 13　可信评价指标体系

通过免疫隔离实现措施处理功能，通过接收处理分析结果，对网络节点进行隔离操作或免疫操作：隔离操作通过对网络节点进行针对性的操作，将网络节点的配置信息回滚至正常状态；免疫操作是一种主动式的防护措施，根据历史信息进行相应的修改，使得网络节点获得针对特定误操作或恶意程序的免疫效果，避免网络故障的再次发生，如修改路由器访问控制规则或者读写权限. 通过措施处理功能消除和避免外在的、不受控的因素对网络业务以及网络系统本身稳定性的影响，确保其始终运行在一个安全和可控的状态.

8　总　结

本文在分析现有的 Internet 网络架构的基础上，对目前互联网存在的问题进行了深入剖析；从应用服务提供商、网络用户和网络服务运营商的需求角度，指出了未来网络应具备自适应于多种网络主体、多种网络应用和多种服务要求的特性，满足各种角度用户友好性的要求. 因此，提出了自适应未来网络的概念，通过讨论可控、可管、可扩展和可信等概念的内涵与外延，发现可控、可管、可扩展和可信较好地构成了自适应未来网络特性的指标体系. 在此基础上，我们对现有自适应网络关键技术和体系架构进行了详细的介绍和分析，总结了它们的优缺点和兼容性，并提出了一种自适应的未来网络体系架构(AFIF). 该架构将对未来网络的研究提供参考.

参　考　文　献

[1]　Lin Chuang, Hu Jie, Kong Xiang-Zhen. Survey on models

and evaluation of quality of experience. Chinese Journal of Computers, 2012, 35(1): 1-15(in Chinese)
(林闯, 胡杰, 孔祥震. 用户体验质量(QoE)的模型与评价方法综述. 计算机学报, 2012, 35(1): 1-15)

[2] Feldmann A. Internet clean-slate design: What and why? ACM SIGCOMM Computer Communication Review, 2007, 37(3): 59-64

[3] Lin Chuang, Ren Feng-Yuan. Controllable, trustworthy and scalable new generation Internet. Journal of Software, 2004, 15(12): 1815-1821(in Chinese)
(林闯, 任丰原. 可控可信可扩展的新一代互联网. 软件学报, 2004, 15(12): 1815-1821)

[4] Saltzer H, Reed D P, Clark D. End to end argument in system design. ACM Transactions on Computing System, 1984, 2(4): 277-288

[5] Leiner B M, Cerf V G et al. A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 2009, 39(5): 22-31

[6] Griffin T, Shepherd F, Wilfong G. The stable paths problem and interdomain routing. IEEE/ACM Transactions on Networking(TON), 2002, 10(2): 232-243

[7] Argyraki K, Cheriton D. Active Internet traffic filtering: Real-time response to Denial-of-service attacks. USENIX Annual Technical Conference, Anaheim, USA, 2005: 135-148

[8] Lin Chuang, Peng Xue-Hai. Research on trustworthy networks. Chinese Journal of Computers, 2005, 28(5): 751-758(in Chinese)
(林闯, 彭雪海. 可信网络研究. 计算机学报, 2005, 28(5): 751-758)

[9] Clark D, Partridge C, Ramming J, Wroclawski J. A knowledge plane for the Internet. ACM SIGCOMM Computer Communication Review, 2003, 33(4): 3-10

[10] Ogata K. Modern Control Engineering. 3rd Edition. Prentice Hall, Upper Saddle River, NJ, 1997

[11] He J, Rexford J, Chiang M. Design principles of manageable networks. Princeton University Computer Science, Technical Report TR-770-06, 2006

[12] Jogalekar P, Woodside C. A scalability metric for distributed computing applications in telecommunications//Proceedings of the International Teletraffic Congress. Washington, USA, 1997, 1: 101-110

[13] Lin Chuang, Shan Zhi-Guang, Ren Feng-Yuan. Quality of Service of Computer Networks. Beijing: Tsinghua University Press, 2004(in Chinese)
(林闯, 单志广, 任丰原. 计算机网络的服务质量(QoS). 北京: 清华大学出版社, 2004)

[14] Algridas A, Laprie J, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11-33

[15] Lin Chuang, Tian Li-Qin, Wang Yuan-Zhuo. Research on user behavior trust in trustworthy network. Journal of Computer Research and Development, 2008, 45(12): 2033-2043 (in Chinese)
(林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究. 计算机研究与发展, 2008, 45(12): 2033-2043)

[16] Ruohomaa S, Kutvonen L. Trust management survey//Proceedings of the ITRUST 2005. Lecture Notes in Computer Science 3477. Paris, France, 2005: 77-92

[17] Pal P, Webber F, Atighetchi M, Combs N. Trust assessment from observed behavior: Toward and essential service for trusted network computing//Proceedings of the International Symposium on Network Computing and Applications. Cambridge, USA, 2006: 285-292

[18] Luo An-An, Lin Chuang, Wang Yuan-Zhuo, Deng Fa-Chao, Chen Zhen. Security quantifying method and enhanced mechanisms of TNC. Chinese Journal of Computers, 2009, 32(5): 887-898(in Chinese)
(罗安安, 林闯, 王元卓, 邓法超, 陈震. 可信网络连接的安全量化分析与协议改进. 计算机学报, 2009, 32(5): 887-898)

[19] McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J. Openflow: Enabling innovation in college networks. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74

[20] Gude N, Koponen T, Pettit J, Pfaff B, Casado M, McKeown N et al. NOX: Towards an operating system for networks. ACM SIGCOMM Computer Communication Review, 2008, 38(3): 105-110

[21] Casado M, Freedman M, Pettit J, Luo J, Mc Keown N, Shenker S. Ethane: Taking control of the enterprise. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 1-12

[22] Casado M, Garfinkel T, Freedman M, Akella A, Boneh D, McKeown N, Shenker S. SANE: A protection architecture for enterprise networks//Proceedings of the USENIX Security Symposium. Vancouver, Canada, 2006: 137-151

[23] Cai Z, Cox Alan L, Eugene Ng T S. Maestro: A system for scalable OpenFlow control. Rice University Technical Report TR10-08, 2010

[24] Koponen T, Casado M, Gude N et al. Onix: A distributed control platform for large-scale production networks//Proceedings of the USENIX Conference on Operating Systems Design and Implementation. Berkeley, USA, 2010: 1-6

[25] Yu M, Rexford J, Freedman J, Wang J. Scalable flow-based networking with DIFANE. Princeton University Computer Science Technical Report TR-877-10, 2010

[26] Jacobson V, Smetters D, Thornton J, Plass M, Briggs N, Braynard R. Networking named content//Proceedings of the International Conference on Emerging Networking Experiments and Technologies. Rome, Italy, 2009: 1-12

[27] Zhang L X, Estrin D, Burke J et al. Named Data Networking (NDN) project. NSF Future Internet Architecture Project, 2010

[28] Van Jacobson, Smetters D, Thornton J et al. Networking named content. Communications of the ACM, 2012, 55(1): 117-124

[29] DiBenedetto S, Papadopoulos C, Massey D. Routing policies in named data networking//Proceedings of the ACM SIGCOMM Workshop on Information-Centric Networking (ICN). Toronto, Canada, 2011: 38-43

[30] Visala K et al. LANES: An inter-domain data-oriented routing architecture//Proceedings of the Re-Architecting the Internet (ReArch). Rome, Italy, 2009: 55-60

[31] Gritter M, Cheriton D. An architecture for content routing support in the Internet//Proceedings of the USENIX Symposium on Internet Technologies and Systems. San Francisco, USA, 2001: 37-48

[32] Koponen T, Chawla M, Chun B et al. A data-oriented (and beyond) network architecture. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 181-192

[33] Rexford J, Greenberg A, Hjalmtysson G, Maltz D, Myers A, Xie G, Zhan J, Zhang H. Network-wide decision making: Toward a wafer-thin control plane//Proceedings of the ACM SIGCOMM HotNets. San Diego, USA, 2004

[34] Greenberg A, Hjalmtysson G, Maltz D et al. A clean slate 4D approach to network control and management. ACM SIGCOMM Computer Communication Review, 2005, 35(5): 41-54

[35] Elliott C. GENI: Opening up new classes of experiments in global networking. IEEE Internet Computing, 2010, 14(1): 39-42

[36] Peng Xue-Hai, Lin Chuang. Architecture of trustworthy networks//Proceedings of the International Symposium on Dependable, Autonomic and Secure Computing. Indianapolis, USA, 2006: 269-276

[37] Lin Chuang, Lei Lei. Research on next generation Internet architecture. Chinese Journal of Computers, 2007, 30(5): 693-711(in Chinese)
(**林闯，雷蕾. 下一代互联网体系结构研究. 计算机学报**, 2007, 30(5): 693-711)

[38] Zhang Hong-Ke, Dong Ping, Yang Dong. Theory and key technologies of new generation Internet. ZTE Communications, 2008, 14(1): 17-20

[39] A Survey on Research on the Application-Layer Traffic Optimization (ALTO) Problem. RFC 6029

[40] Trustworthy Computing. US National Science Foundation (NSF) Guideline, FY 2011

[41] Ellison R, Fisher D, Linger R et al. Survivable network systems: An emerging discipline. Pittsburgh, Software Engineering Institute, Carnegie Mellon University, 1997

[42] Deavours D, Sanders W. An efficient disk-based tool for solving large Markov models. Performance Evaluation, 1998, 33(1): 67-84

[43] Lin Chuang, Wang Yang, Li Quan-Lin. Stochastic modeling and evaluation for network security. Chinese Journal of Computers, 2005, 28(12): 143-156(in Chinese)
(**林闯，汪洋，李泉林. 网络安全的随机模型方法与评价技术. 计算机学报**, 2005, 28(12): 143-156)

LIN Chuang, born in 1948, Ph. D., professor, Ph. D. supervisor. His research interests include computer networks, performance evaluation, network security analysis, and Petri net theory and its applications.

JIA Zi-Xiao, born in 1986, Ph. D. candidate. His research interests include performance evaluation and next generation internet.

MENG Kun, born in 1980, Ph. D. candidate. His research interests include performance evaluation and stochastic models.

Background

The Internet has been continuously developing to satisfy people's growing demand since its birth and greatly changed our lives. Nowadays the way of Internet architecture forward has become one of the hot research topics. This paper points out that adaptive architecture is the potential development direction for the future Internet and provides a complete overview of current technologies and architectures of the Adaptive Future Internet, and then proposes a future Internet Framework named AFIF.

This work is partly supported by the National Basic Research Program (973 Program) of China (Nos. 2010CB328105, 2009CB320505), National Natural Science Foundation of China (Nos. 60932003, 61070182, 60973144, 61173008, 61070021). These projects aim to provide better performance in computer networks and information systems. Our group has been working on the performance evaluation of the computer networks and computer systems using the stochastic theoretical models, and using optimization techniques to solve the network design problems. Many good papers have been published in respectable international conferences and transactions, such as INFOCOM, IEEE Journal on Selected Areas in Communication and IEEE Transactions on Parallel and Distributed Systems. This paper summarizes the key technologies and architectures of the Adaptive Future Internet.