对互联网体系结构创新的认识与思考

罗洪斌[1,2,3,4],张 珊[1,2,3,4],王志远[1,4*],孟晴开[1]
(1. 北京航空航天大学计算机学院,北京 100191;2. 北京航空航天大学软件开发环境国家重点实验室,北京 100191;
3. 数学、信息与行为学教育部重点实验室,北京 100191;4. 未来区块链与隐私计算北京高精尖创新中心,北京 100191)

摘 要: 互联网是促进现代社会经济发展和科技创新的重要信息基础设施;然而,支撑并规范互联网正常运行的关键核心技术——互联网的TCP/IP(Transport Control Protocol/Internet Protocol)体系结构——几十年来几乎保持不变. 本文首先从技术自身弊端、社会发展需求、技术转移周期、科技革命规律四个方面论述了开展互联网体系结构创新的必要性. 其次,运用系统科学原理阐明了TCP/IP体系结构弊端的根源. 再次,运用系统观念揭示了信息网络的功能本质和网络间的互联本质,发现了信息传递的四个自然属性(对象属性、身份属性、位置属性、手段属性). 在此基础上,简要介绍了基于两个本质和四个自然属性开展创新互联网体系结构创新的实例——共生网络. 最后,结合共生网络架构展望了部署新型互联网体系结构的总体路径.

关键词: 互联网体系结构;异构网络;网间互联;跨域通信
基金项目: 国家自然科学基金(No.62225201,No.62202021,No.62271019)
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112(2024)04-1411-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20231008

Understanding and Thinking About the Innovation on Internet Architecture

LUO Hong-bin[1,2,3,4], ZHANG Shan[1,2,3,4], WANG Zhi-yuan[1,4*], MENG Qing-kai[1]
(1. *School of Computer Science and Engineering, Beihang University, Beijing* 100191, *China*;
2. *National Key Laboratory for Software Development Environment, Beihang University, Beijing* 100191, *China*;
3. *Key Laboratory of Mathematics, Information and Behavioral Semantics, Ministry of Education, Beijing* 100191, *China*;
4. *Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Beijing* 100191, *China*)

Abstract: Internet is a crucial information infrastructure that promotes economic development and technology innovation. However, TCP/IP (Transport Control Protocol/Internet Protocol) architecture, i.e., the core technology that supports and regulates the operation of Internet, has remained almost unchanged for decades. This paper introduces the necessity of innovating Internet architecture from four aspects: the drawbacks of technology itself, the development of social economy, the transformation cycle of technology, and the revolution law of science and technology. From the perspective of the systems thinking, this paper elaborates the underlying causes of the disadvantages in TCP/IP architecture. Moreover, this paper leverages the systems thinking and reveals the nature of network functionality and the nature of network interconnectivity, and then clarifies the four properties of delivering information (i.e., object property, identity property, location property, and means property). Then this paper briefly introduces how CoLoR (Coupling service Location and inter-domain Routing) leverages the two natures and four properties to innovate the Internet architecture. Finally, this paper takes CoLoR as the example, and presents the basic idea of deploying novel Internet architectures.

Key words: Internet architecture; heterogeneous networks; internetworking; inter-domain communication
Foundation Item(s): National Natural Science Foundation of China (No.62225201, No.62202021, No.62271019)

收稿日期:2023-10-27;修回日期:2024-03-07;责任编辑:覃怀银
*通讯作者:王志远

1 引言

现代互联网源于1969年投入使用的阿帕网(Advanced Research Projects Agency Network,ARPANET)[1].经过五十多年发展,互联网已成为由10万多个自治系统(Autonomous System,AS)互联而成的复杂网络空间,是促进现代社会经济发展和科技创新最重要的信息基础设施,为生产力和生产关系、世界政治经济格局、国家主权和国家安全都带来了前所未有的影响[2].

互联网体系结构是规范并支撑互联网正常运行的关键核心技术.50多年来,以TCP/IP(Transport Control Protocol/Internet Protocol)为核心技术的互联网体系结构在报文格式、地址空间、转发逻辑等方面几乎保持不变.这虽然促进了互联网从一个仅有4个节点的实验网络快速发展成为规模庞大的网络空间,但也严重制约了互联网的迭代升级和演进发展,使其向更大范围、更宽领域、更深层次渗透时面临重重挑战,进而阻碍数字经济发展和数字中国建设[3].因此,亟需进行互联网体系结构创新.

2 创新互联网体系结构的必要性

从技术自身弊端、社会发展需求、技术转移周期、科技革命规律等四个方面论述创新互联网体系结构的必要性.

2.1 技术自身弊端

在互联网的发展历程中,其TCP/IP网络体系结构逐步暴露出诸多弊端,如安全保障能力弱、可扩展能力不足、移动性支持差等.

(1)安全保障能力弱:互联网先驱们当初设计TCP/IP体系结构时,假定互联网是一个相对封闭、可信的网络环境.相应的,TCP/IP体系结构采用"推"的通信模式:给定任意目的IP地址,网络会尽力而为地将去往该目的IP地址的分组发送给使用该目的IP地址的主机,而不管该主机是否需要该分组.这种通信模式,使得网络中任意节点可以在任意时刻向任意目的节点发送任意数量的数据包,为实施网络攻击提供了天然便利.随着互联网发展成为网络空间并与人类社会深度融合,各种实体(国家、组织、个人等)纷纷利用互联网实现不同的利益诉求,使得可信网络环境不复存在,导致分布式拒绝服务(Distributed Denial-of-Service,DDoS)攻击泛滥、隐私数据泄漏频发.例如,提供域名解析服务的美国Dyn公司在2016年遭到了3波DDoS攻击,严重影响了用户访问星巴克、Twitter、金融时报等网站[4];俄乌冲突期间,DDoS攻击峰值达到了1.5 Tbps(Terabits per Second)[5];2023年,韩国三星公司引入ChatGPT不到20天,就发生了3起数据泄密事故,半导体机密数据被曝外泄[6].

(2)可扩展能力不足:TCP/IP是一种以主机为中心的网络体系结构:为主机的接口分配IP地址,并基于主机IP地址(或IP前缀)建立路由表以维护IP地址(前缀)的全局可达性信息.相应地,路由表规模和路由动态性均随用户数量的增长而增长;研究表明,互联网路由表的规模与用户数量的平方根成正比[7].为了实现快速查找,路由表通常存放在路由器的TCAM(Ternary Content Addressable Memory)中.但TCAM价格昂贵且容量极小,难以应对路由表的飞速增长.例如,2014年8月12日,人类历史上曾经历了著名的"512K day",因路由表的规模(即512K)超过了部分路由器的TCAM容量上限,导致互联网断网[8].当前,互联网路由表的规模目前已达96万,人类将很快迎来"1024K day"[9].

(3)移动性支持差:TCP/IP体系结构采用层次化的策略分配IP地址:将拥有相同前缀的IP地址块分配给网络,网络再将该地址块中的某个IP地址分配给接入该网络的某台主机.虽然这种设计便于提升网络的规模可扩展能力,但主要适用于相对"固定、有线"的网络环境.一方面,当一台主机从一个网络A移动到另一个网络B时,需要从网络B获得新的IP地址.另一方面,TCP用IP地址表示节点在通信时的身份;当节点的IP地址改变时,TCP链接会中断,进而导致通信中断.正因如此,人们在用手机上网的过程中从蜂窝网络切换到Wi-Fi时,经常遇到断网.总之,由于IP地址既表征节点在网络中的位置信息,又表征节点在通信时的身份信息,使得TCP/IP网络体系结构的移动性支持能力不足.即使聚焦于单个网络,节点移动也会导致IP路由表频繁更新.美国DARPA在2013年指出:当网络规模超过50个节点后,TCP/IP网络体系结构在自组网场景中的性能会急剧恶化[10].

2.2 社会发展需求

近年来,随着社会经济的快速发展和信息技术的飞速进步,网络空间与物理空间正在加速融合,互联网逐渐向空、天、海洋等环境延伸,向实体经济渗透,催生了低轨卫星互联网、无人机集群网络、海洋信息网络、蜂窝车联网、工业互联网等具有独特拓扑和业务需求的新型网络.

与陆地互联网的网络拓扑相对固定不同,低轨卫星互联网具有周期性运动、拓扑规律性变化、链路间歇性连通等特征[11].一方面,轨道高度低导致轨道周期短,星地链路频繁切换.一颗550公里轨道高度的卫星,对地面固定节点的覆盖时间仅为2~3 min[12].另一方面,相邻卫星之间的链路受限于天线对准技术等瓶颈,在进入或离开极地区域时出现周期性的链路状态变化.若基于以主机为中心的TCP/IP体系结构开展大规模卫星网络组网与互联,频繁的链路状态变化会引起频繁的路由更新,进而导致路由不稳定,从而制约天

地一体化网络的传输性能. 此外,卫星网络运行于信道开放的非可信环境中,以主机为中心的TCP/IP体系结构缺少安全管控能力,导致卫星网络面临严重的网络安全隐患.

无人机集群网络需要在编队飞行、编队变化中实现协同控制和数据共享. 因此,无人机集群拓扑虽然在编队飞行时相对稳定,但在编队变化甚至对抗环境下呈现无规律的强动态性. 将TCP/IP体系结构应用于无人机集群时,将因拓扑强时变导致路由难收敛等问题,从而难以在各类编队状态下提供高质量的网络传输服务. 另外,无人机集群需要在复杂环境中承担通信、救援、监控等任务,缺少内生安全机制的TCP/IP体系结构致使无人机集群网络无法防御来自陆地网络或者其他空中恶意节点的网络流量攻击,从而使得原本就资源受限的无人机节点面临极大的负担.

蜂窝车联网不仅需要保障各类终端设备在车内局域网的联通,还需要提供车际网络连接以及广域化的车载移动互联网服务[13]. 因车辆具有强移动性,车载通信过程中需要频繁切换无线网络的接入点,导致网络拓扑频繁变化. 因此,将TCP/IP体系结构应用于蜂窝车联网时,也面临路由频繁更新、信息传输效率低等问题. 另外,联网车辆之间存在一定程度相似的内容需求(例如交通信息),而TCP/IP体系结构无法感知所传递的信息,只关注端到端连接,导致蜂窝车联网内存在大量冗余数据传输,链路带宽利用率低.

工业互联网需要为智能化生产流程提供实时安全可靠的数据传递,并在复杂的商业关系下实现公开数据的共享以及隐私数据的保障. 但如前所述,TCP/IP体系结构存在严重的安全缺陷,致使DoS/DDoS等网络攻击频繁、数据泄漏难以防御. 因此,基于TCP/IP构建的工业互联网系统难以保障关键数据的流通和隐私数据的防护,最终将制约工业互联网的演进和数字经济的发展. 同时,TCP/IP尽力而为的服务模式,也难以满足工业互联网对实时性的需求.

因此,从社会发展需求来看,TCP/IP体系结构难以适配低轨卫星互联网、无人机集群网络、蜂窝车联网、工业互联网等新型网络的功能需求.

2.3　技术扩散周期

人类科技发展史表明,科学技术的扩散转移周期约为60年. 科学技术的扩散转移周期是指:从一个新兴技术出现到被广泛应用和普及所需要的时间通常为20~30年;此后,这项技术开始进入成熟期并得到大规模应用;随着时间的推移,技术本身变得过时,难以适应新需求,亟需更新换代;再经过20~30年直至下一项颠覆性技术涌现并开始取代原有技术. 例如,从工业革命以来的历史经验看,蒸汽动力、电力、信息技术的扩散转移周期均大约为60年. 在扩散转移过程中,新技术的应用逐渐得到普及,原有行业结构和生产方式会发生深刻变化,带来新的机遇和挑战.

TCP/IP体系结构诞生至今已经近60年,虽然未来仍会长期存在,但技术红利已濒临耗竭. 一方面,全球主要国家互联网渗透率已经接近饱和,2021年全球互联网渗透率已经达到65.6%,中国渗透率达到65.2%,美国渗透率达到90%;互联网行业已经逐渐进入获取“增量”困难、只能依靠“存量”拼杀的红海时代. 另一方面,如前所述,TCP/IP体系结构难以实现低轨卫星网络、无人机集群网络、工业互联网等新兴网络的大规模组网和互联. 因此,亟需创新互联网体系结构,推动互联网科技和产业演进发展,在网络空间确立技术领先地位.

2.4　科技革命规律

互联网与其他信息通信技术带来的科技革命,正在促进物理空间与网络空间加速融合,逐步形成以数据为生产要素的基础体系. 当前,我国不断推动针对数据要素的相关研究,把发挥数据要素价值提升至重要战略高度. 2019年,党的十九届四中全会发布的《中共中央关于坚持和完善中国特色社会主义制度推进国家治理体系和治理能力现代化若干重大问题的决定》,首次将数据与劳动、资本、土地并列作为重要的生产要素. 2022年12月,中共中央国务院发布了《关于构建数据基础制度更好发挥数据要素作用的意见》,以促进海量数据和应用需求融合,进一步释放数据要素的潜能,形成经济发展新动能.

数据要素的管理关乎国家发展大局. 首先,随着信息技术的发展和普及,越来越多的业务被数字化,参与到了企业生产和管理等方面. 其次,数据规模在互联网发展过程中呈爆炸式增长,数据背后往往蕴含巨大商业价值和社会价值. 最后,互联网的发展使得数据变得更加容易共享和交流,不同行业、领域之间的数据迫切需要进行整合与利用. 因此,在互联网时代,数据逐渐成为了促进社会经济增长的全新生产要素,也是推动当前科技革命的核心力量之一. 然而,TCP/IP体系结构以主机为中心忽略了对数据要素的表征,使得网络仅通过IP地址进行无状态转发,既无法感知所传递的数据本身,也无法对数据传递进行有效管控,导致海量网络孤岛和数据孤岛,难以实现数据的高效共享. 因此,亟需构建以数据为中心的新型互联网体系结构,促进关键数据的安全、高效流通,从而赋能数字经济发展.

3　导致互联网各种弊端的原始根源

如前所述,互联网在发展过程中逐步暴露出安全保障能力弱、可扩展性差、移动性支持不足等弊端. 几

十年来，业界做了各种尝试，以解决这些弊端. 例如，为解决IPv4地址空间不足的问题，业界提出了无类别地址(Classless Inter-Domain Routing，CIDR)，但互联路由表的规模依然快速增长，目前已近100万；为提升互联网的安全保障能力，业界提出了RPKI(Resource Public Key Infrastructure)[14]、ROV(Route Origin Validation)[15]、BGPSec[16]等，但是网络安全问题依然层出不穷. 因此，我们不禁要问，为什么这些尝试收效甚微？为了回答这个问题，必须弄清楚导致这些弊端的根源. 本文运用系统科学原理，结合图1从功能、结构的角度阐明导致互联网各种严重弊端的原始根源. 互联网经过几十年的发展，已经成为一个开放复杂巨型系统，应该遵循系统科学的基本原理——功能选择结构、结构决定功能.

从功能选择结构来看，TCP/IP体系结构是根据特定的功能需求设计的. 互联网先驱、麻省理工学院教授David Clark先生曾总结TCP/IP互联网架构的七个功能需求[17]：(1)故障时的通信能力；(2)多类通信服务支持；(3)不同类型网络接入；(4)资源分布式管理；(5)成本效益；(6)主机低代价接入；(7)网络资源计费. 为满足以上功能需求，互联网先驱们设计了以细腰模型为典型特征的TCP/IP体系结构，如图1所示.

系统科学原理指出：结构决定功能，即结构一经确定，其功能也就确定. 对TCP/IP体系结构而言，由于在设计时并未考虑安全性、可扩展性、平滑演进、移动性支持等功能需求[18-20]，因而只对该体系结构进行修补，必然难以高效地支持安全性、可扩展性、平滑演进、移动性等功能需求. 同时，在TCP/IP体系结构中，虽然网络层以上和网络层以下均为开放系统，支持多种协议，但是网络层只能采用IP协议，因此网络层是一个封闭系统. 在互联网发展初期，这种细腰模型具有较好的灵活性和互操作性，便于互联网大规模推广应用. 然而，热力学第二定律指出，封闭系统一定是熵增系统. 因此，封闭的IP层难以同时兼顾未来互联网的各种功能需求，最终导致互联网系统日趋复杂，难以演进. 因此，只有运用系统科学原理，根据互联互通、安全性、移动性、可演进、可扩展、可管理等功能需求，创新互联网体系结构，才能从根本上克服互联网的各种弊端，支撑数字经济快速发展，赋能网络强国和数字中国建设.

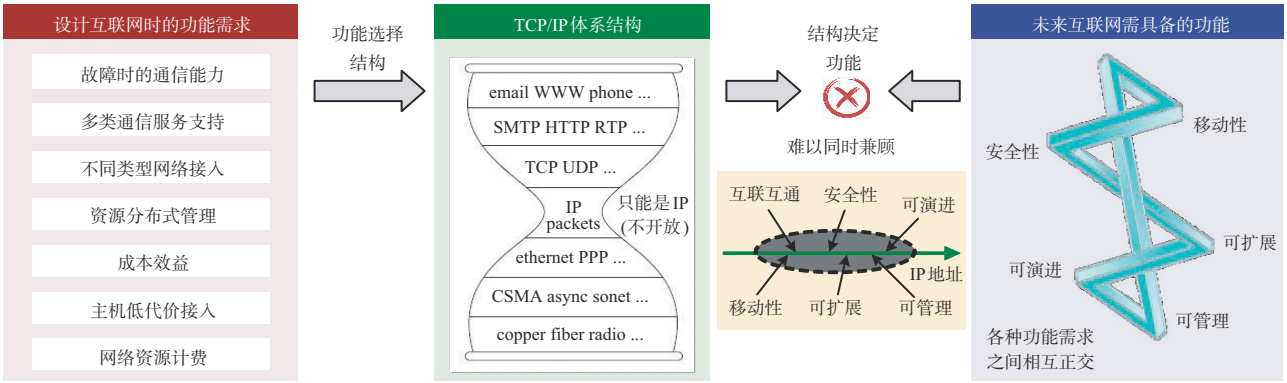

图1 从系统观念看互联网体系结构

4 互联网的功能本质和网络间互联本质

如前所述，互联网已发展成为一个开放复杂巨系统. 因此，创新互联网的体系结构，必须要以系统观念为指引. 系统观念是马克思主义基本原理与中国实际相结合的必然结果，是中国共产党领导革命、建设和改革的重要思想方法和工作方法，是推动党和国家事业不断从胜利走向胜利的重要认识论和方法论.《中共中央关于制定国民经济和社会发展第十四个五年规划和二零三五年远景目标的建议》，将“坚持系统观念”作为“十四五”时期国家经济社会发展必须遵循的五大原则之一；党的二十大报告将“必须坚持系统观念”作为“六个坚持”之一.

系统观念要求我们运用系统思维的原则和方法，从系统观点出发去把握事物本质及其发展规律，运用系统观点洞察问题、分析问题和解决问题. 相应的，要创新互联网的体系结构，必须弄清楚互联网的功能本质和网络间的互联本质.

4.1 互联网的功能本质

尽管互联网已经发展成为人类社会最重要的信息基础设施，但业界对互联网功能本质的认识，存在很多说法. 例如，马化腾认为：“互联网的本质就是促进信息沟通，使得信息交流和获取的效率更高、成本更低”；张朝阳认为，互联网的本质是“信息的加工聚合，最终实现公众对于事件无限接近真实的了解”；马云认为，“互联网的本质是‘分享’”.

一种更广泛的认识是，互联网的本质是连接. 例如，邬贺铨院士2016年接受中央纪委监察部网站访谈时认为，

“互联网的本质是连接,连接人与人,连接人与物,连接人与整个社会”,“正因为这种连接,使得我们可以足不出户就知道外面的世界”;“互联网之父”Robert Elliot Kahn在2015年第二届世界互联网大会上接受央广网采访时认为:“互联网提供了全球连接的能力,每个人都可以通过计算机进行世界范围内的交流,人们连接互联网后,可在任何地点与任何人进行交流并获取信息”.

那么,互联网的功能本质究竟是什么? 我们认为,互联网的功能本质是传递数据(或信息);相反,提供连接的目的是传递信息,而连接本身仅仅是一种手段. 这不仅可以从Robert Elliot Kahn接受采访时的话语得到证实,而且可以从近年来学界对信息中心网络的研究窥见端倪. 不同于TCP/IP体系结构,信息中心网络为数据(而非以主机或者接口)命名[21]. 特别的,每个数据内容都具有唯一的内容名字;用户通过携带内容名字的报文来拉取数据,而不必知道数据存储于哪个节点. 这样不仅可以保证数据可寻址性,同时也可以进行网内缓存和重复使用. 命名数据网络(Named-Data Network,NDN)是信息中心网络的典型案例[22]. 总之,随着数据逐渐成为生产要素,互联网作为传递数据的载体,其功能本质必然也只能是传递数据.

与物理世界中传递物品类似,传递信息必然涉及以下五个自然属性:

(1)对象属性:既然互联网的功能本质是传递信息,那就应该提供适当的标准来表征所需传递的信息或内容,从而回答“传什么”问题.

(2)身份属性:在表征信息的基础上,还需要明确哪个用户或者节点需要获取该内容,因此需对身份属性进行表征,从而回答“传给谁”问题.

(3)位置属性:寻址和路由是网络的必备功能,保障信息能被正确地传递到身份属性对应的位置. 位置属性是身份属性在网络空间的投影,用来回答“传到哪”问题.

(4)手段属性:对于给定位置属性的传输任务,需要找到相应的域间路径从而将信息传递到相应节点. 因此,手段属性也是体系结构设计的必要环节,对应“如何传”问题.

(5)时间属性:在上述四个自然属性的前提下,还需要知道什么时间来执行既定的传输任务,即时间属性对应“何时传”问题.

除了上述自然属性外,安全性和隐私性也是网络的重要属性,但与上述自然属性并不独立,例如,第3.3节将结合共生网络架构介绍如何通过动态耦合上述自然属性来保障跨网安全,实现了攻击数据难入网、隐私数据难出网. 因此,本文未将安全和隐私属性作为基本的自然属性. 另外,由于实际中的信息传递通常是按需且即时的,所以不再单独考虑时间属性. 针对相互独立的自然属性,需要分别对它们进行标识和表征,从而形成由内容名字、节点标识、各类地址、路径标识组成的多维名字空间. 图2具体展示了基于网络功能本质得到四个基本自然属性及其相应标识的逻辑:

(1)内容名字:从网络的功能本质出发,为了表征网络的对象属性,需要对网络中所传递的内容进行命名.

(2)节点标识:每个网络可用各自的方式标识网络内节点的身份,并为每个节点分配节点标识,从而表征身份属性. 节点标识既需要便于聚合,又便于进行节点的安全认证.

(3)各类地址:每个网络都可以有各自的编址方式,例如32位IPv4地址、128位的IPv6地址、地理坐标等. 通过各类地址表征网内位置属性,便于根据网络特点进行网内分组转发.

(4)路径标识:从网间互联的本质出发,表征网络的手段属性,需要对网间路径进行命名,从而便于进行跨域信息传递的管控.

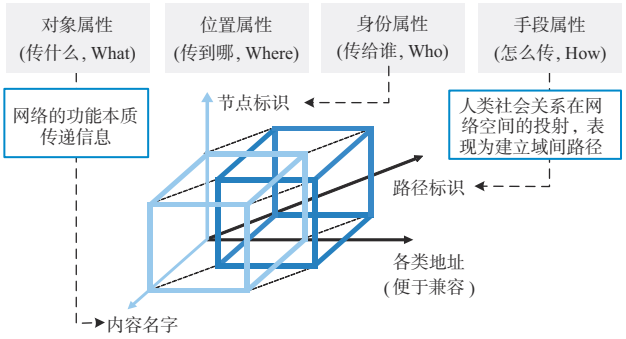

图2　多维名字空间

4.2　网络间的互联本质

众所周知,互联网是网络的网络“Network of Networks”,通过将众多网络自治域连接起来,完成相互通信和数据共享. 然而,互联网中有数万自治系统,且这些自治系统之间不是两两直接互联形成一个全连接的网络拓扑,而是形成一个层次化的网络拓扑:最核心部分由数量极少的Tier-1自治域组成,Tier-2自治域与部分Tier-1和Tier-2自治域连接,而Tier-3自治域与部分Tier-2和Tier-3自治域连接. 例如,据网站bgp.tools统计,截至2023年7月18日,中国电信的AS 4809仅与美国NTT的AS 2914等313个自治系统直接相连.

一个很自然的问题是:为什么中国电信AS4809仅与这313个自治系统直接相连,而不与其他自治系统直接互联? 这就涉及到网络间的互联本质. 我们认为,网络间的互联本质是,特定政治、经济、地理、文化等约束下,人类社会关系在网络空间的投射. 对两个自治系统而言,它们之间要直接相连,首先需要签署商业协议,

明确相互之间的权利和义务，如谁为谁付费、怎么计费、何时付费、两个网络间建立多少连接、在哪里建立连接等．在此基础上，两个自治系统才建立互联关系，具体表现为建立域间路径．至于具体的连接方式，则是差异化的，可以通过光纤直连，采用IP隧道相连，也可以通过IXP(Internet Exchange Point)交换中心连接，或者采用无线通信技术进行连接．

然而，TCP/IP体系结构忽略了网络间的互联本质，未定义网络间接口．互联网先驱David Clark先生指出[23]："The third interface that is relevant to the IP layer is the interface between ISPs. This interface was not specified in the original design of the Internet. In the original Internet, the designers downplayed the importance of this interface (sometimes called the network-network interface, or NNT). That decision was perhaps shortsighted"．正因如此，TCP/IP体系结构下，所有自治系统内部和自治系统之间，都用同一IP地址空间组网，严重制约了互联网的可演进性、可管理性、可扩展性甚至可用性．

4.3 基于两个本质和四个自然属性的互联网体系结构创新

互联网的发展历程说明，忽略上述两个本质和四个自然属性而创建的互联网体系结构，难以适应未来互联网的发展需求．以TCP/IP体系结构为例，它既没有利用网络的功能本质，也忽略了网间互联本质，仅用IP地址表征位置属性，并基于IP地址完成路由、寻址和分组转发等功能．但如前所述，随着互联网规模扩大，TCP/IP体系结构暴露出安全保障能力弱、可演进性差等诸多弊端．例如，虽然IPv6早在1995年就已标准化且被认为可以解决地址空间不足的问题，但网络体制难演进的缺陷使得部署和应用IPv6长期陷入困境．根据Google的统计，截至2023年4月全球IPv6流量仅占所有流量的43.24%[24]．再如，近年来提出的新型互联网体系结构NDN[22]，因抓住网络的功能本质，引入内容名字为数据命名，并基于内容名字完成路由、寻址和分组转发，得到美国国家自然科学基金委长达10年的持续资助，受到业界广泛关注．然而，NDN试图抛弃IP地址而不再利用位置属性，不仅难以兼容IPv4和IPv6导致增量部署困难，而且在大规模应用时面临规模可扩展性问题．同时，NDN忽略了网间互联本质，缺少对域间路径的表征与利用，使其可演进能力匮乏．近年来，国际上还提出了ALF[25]、MobilityFirst[26]、XIA[27]、SCION[28]、Trotsky[29]、SDN/NVF等诸多新型互联网体系结构，但都未能抓住网络的功能本质和网络间的互联本质，也未同时利用信息传递的四个自然属性，至今未见有大规模部署．因此，只有抓住两个本质并充分利用四个自然属性，创建的新型互联网体系结构，才有可能从根本上同时解决互联网面临的各种问题．

作为一种探索和颠覆性创新，共生网络[30,31]是基于两个本质和四个自然属性创建的一种互联网体系结构．特别的，共生网络基于两个本质与四个自然属性构建了四维名字空间，从而完成了对网络空间的统一表征．在此基础上，将一维空间解决不了的瓶颈问题，升维到多维空间解决．图3展示了由一维名字空间向多维名字空间转变为网络性能保障带来的转变．例如，通过路径标识与各类地址的分工协同，实现了域内域间解耦的路由组织模式[32]，使得各个网络可以"因地制宜"，采取最适合其自身特征的协议体系以释放网络潜能[33]；其次，通过抓住网络的功能本质，在网络间按需可控通告内容名字，不仅完成了异构体制网络的互联，而且有利于防止数据泄露；再次，利用"以拉促推"的通信模式，并基于多维名字空间耦合生成路径标识，便于进行跨域安全防护．共生网络既有利于解决体制异构网络的互联挑战，保障高效的跨网传输[34]，又能够支持各网络独立演进、增量部署．在安全保障方面，共生网络已具备数据泄露防范[35,36]、跨域攻击防范[37,38]、精准实时溯源[39]等能力．

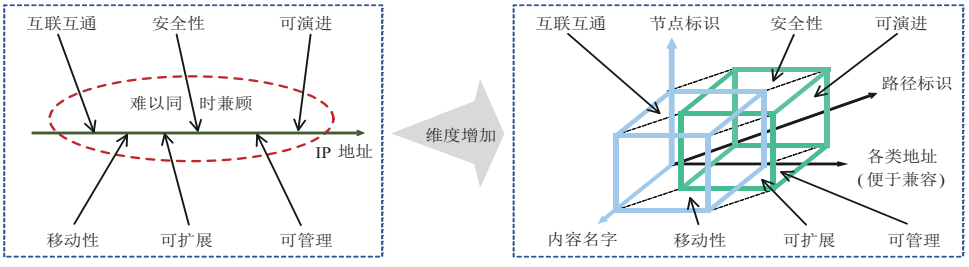

图3 名字空间增维

类似社会分工提升生产效率，共生网络通过多维名字空间的合理分工与协同，不仅具备上述能力，而且整体效率比IP还高．例如，IP路由表的规模已近100万，且采用最长前缀匹配，无法实现$O(1)$时间的精确查

表. 相反,共生网络域间路由表的规模仅数万,且采用精确匹配,查表的时间复杂度为$O(1)$.

5　新型互联网体系结构的部署路径

部署新型互联网体系结构,使我国从互联网大国成为互联网强国,并非一朝一夕能够完成. 前文提到的技术转移周期表明,一个新兴技术从出现到被广泛应用和普及所需要的时间周期通常为20~30年. 另外,根据IPv6、NDN、SICON等体系结构的发展经验来看,部署新型互联网体系结构面临重重阻碍. 因此,本文认为部署新型互联网体系结构的总体战略路径应该分为两个阶段:立足国内市场,解决内需;扩大创新成效,走向世界. 具体而言,在第一阶段中,应基于国内行业的特别需求开展相应的体系结构应用与测试. 以下结合网络孤岛互联和工业互联网两个典型案例,阐述新型互联网体系结构部署的战略路线.

5.1　从网络孤岛互联看新型互联网体系结构部署

在国内的互联网发展历程中,我国各行各业均建设了海量网络孤岛. 这些孤岛网络往往体制异构且数量众多,制约着数据要素流通. 孤岛网络出现的原因可归纳为两方面:

(1)安全关键,不敢互联:由于TCP/IP体系结构存在天然的安全弊端,各类具有高安全等级的网络自治域通常选择物理隔离,不敢与其他网络互联,更不敢通过民用互联网进行数据交互. 如此一来,各个安全关键的孤岛网络只能依靠人工搬运、光盘拷贝等传统方式进行数据传递,信息交互效率低,严重制约着数字经济发展.

(2)体制异构,不能互联:已有的网络孤岛往往是由各个单位或部门独立搭建,所采取的网络体制往往是该单位或部门独立决定. 因此,各个孤岛网络的网络体制经常各不相同. 强行通过TCP/IP体系结构互联存在技术瓶颈,协议转换易出错且效率较低.

在过去几十年中,由于技术和政治等方面的原因,海量网络孤岛已然形成. 然而,数字经济发展和联合全域作战都迫切需要破除网络壁垒,打通数据流动通道,实现数据的可控流动. 因此,部署新型互联网体系结构可以考虑从孤岛互联需求中寻求突破. 以下根据前文提到的共生网络架构,介绍如何部署新型互联网体系结构,破除网络孤岛:

(1)增量部署,平滑演进:部署新型互联网体系结构的最大难点在于,难以实现增量式的部署和平滑的网络演进. 因此,早期互联网体系结构往往缺乏大规模应用. 例如,NDN体系结构尝试抛弃TCP/IP体系,导致大规模部署会带来巨大经济开销和维护难度. 共生网络架构从网间互联本质出发,通过域间路径标识实现域内域间解耦的路由组织模式. 通过这种路由组织模式,避免了重新分配IP地址的过程,同时孤岛网络中已有的设备及其应用均可保持不变,便于实现增量部署. 另外,通过共生网络架构实现互联的孤岛网络,可以独立更新其域内网络体系、自主升级其网络设备,实现平滑演进.

(2)因地制宜,释放潜能:部署新型互联网体系结构的另一个难点在于,互联后的孤岛网络缺少一个统一且合适的网络体制. 具体来说,由于各个孤岛网络承载的业务不同、拓扑特征不同,因此,最适宜其自身需求的网络体系和路由组织模式往往也各不相同. 例如,NDN、SICON等新型架构尝试以统一的体系结构来适配各类网络,因此难以被大规模应用. 相反地,只有根据每种网络形态的特点来选择相应的网络体系结构,才能充分发挥该网络形态的优势. 不同于上述体系结构,共生网络架构支持多体制并存,允许不同形态的网络使用与其网络特征和业务需求匹配的体系. 因此,便于孤岛网络因地制宜地发展,在互联互通的同时释放各自潜能.

(3)精细管控,安全保障:部署新型互联网体系结构的第三个难点在于,互联后的孤岛网络如何保障安全. 互联安全主要包含两方面:域外攻击数据进不来、域内隐私数据出不去. 共生网络架构根据信息传递的四个自然属性,耦合生成域间路径标识,易校验且难伪造,便于对入域、出域的分组进行合法性校验. 因此,共生网络能够消除TCP/IP网络中广泛存在的DDoS攻击和数据泄漏问题,实现精细力度的管控,保障互联后的网络安全.

基于共生网络体系结构,可以首先在国内实现海量网络孤岛之间、孤岛与民用互联网之间的安全高效互联. 这样不仅有利于打通数据流通管道,赋能数字经济发展,又能服务于联合全域作战需求和网络强国重大战略.

孤岛网络的安全高效互联不仅是国内的需求,也是世界各国面临的网络技术瓶颈. 在国内推行的新型互联网体系结构部署成果,可进一步促进异构网络安全高效互联技术走出国门. 在世界范围内解决孤岛互联难题,促进人类经济社会信息流通,从而为构建人类命运共同体贡献中国力量,为国际互联网行业输出中国智慧.

5.2　从工业互联网看新型互联网体系结构部署

随着人工智能、物联网技术在智能制造行业的发展,网络间互联互通的需求逐渐在向工业生产环节延伸,工业互联网已然成为数字经济发展的下半场. 不同于传统网络自治域,工业互联网需要考虑智能制造的工艺流程和生产数据,因此对网络互联提出了更高的

要求. 首先,工业互联网需要针对具体生产流程和生产工艺进行定制化网络部署. 其次,工业互联网需解决生产数据流通与工艺数据保护上的内在矛盾,保障隐私数据的安全. 虽然工业互联网是数字经济发展的关键环节,但是由于异构网络安全互联机理缺失,工业互联网也长期处于不能连、不敢联的低速发展状态:

(1)网络形态体制异构,导致不能连:由于工业互联网需要根据其生产工艺和生产流程,定制化部署各自的网络,导致各个网络自治域的业务特征与需求各异,所采取的网络体制难以统一,最终导致工业互联网自治域不能相互连通.

(2)生产工艺数据敏感,导致不敢连:工业互联网的生产数据具有极高的商业价值,一旦泄漏可能会导致核心技术泄密,甚至会影响企业正常经营. 因此,大部分工业互联网企业宁可承担不连通导致的低生产效率现状,也不愿冒险开展联网生产.

综上所述,工业互联网是另一个可以考虑开展新型互联网体系结构试点部署的行业. 借助共生网络体系结构帮助工业互联网实现安全高效互联,不仅有利于促进数据流动从而提高生产效率,也有利于展现共生网络在跨域安全防护方面的先天优势. 最终,新型互联网体系结构的部署成果将进一步促进该技术实现由国内到国际的全产业推广.

6 总结

以TCP/IP技术为根基的互联网体系结构已经诞生了50余年,但是从技术自身弊端、社会发展需求、技术转移周期、科技革命规律等方面来看,TCP/IP体系结构制约着互联网向更大范围、更宽领域、更深层次渗透,严重阻碍了数字经济发展和数字中国建设. 因此,开展互联网体系结构创新迫在眉睫. 考虑到互联网是一个复杂巨型系统,本文从系统观念的角度剖析了互联网的弊端根源;并在系统观念的指导下揭示了网络的功能本质是传递信息,具有四个自然属性(对象属性、身份属性、位置属性、手段属性);网间的互联本质是人类社会关系在网络空间的投射,表现为建立域间路径. 在此基础上,以共生网络为例阐述了如何基于两个本质和四个自然属性创新互联网体系结构,并展望了分两阶段部署新型互联网体系结构,促进我国从互联网大国成为互联网强国.

参考文献

[1] ROBERTS L. The Arpanet and computer networks[C]// Proceedings of the ACM Conference on The history of personal workstations. New York: ACM, 1986: 51-58.

[2] 习近平. 在全国网络安全和信息化工作会议上的讲话[EB/OL]. (2018-04-20)[2023-07-24]. https://www.theorychina.org.cn/c/2021-02-08/1341742.shtml.

[3] 邬江兴, 兰巨龙, 程东年, 等. 新型网络体系结构[M]. 北京: 人民邮电出版社, 2014.
WU J X, LAN J L, CHENG D N, et al. Novel Network Architecture[M]. Beijing: Posts & Telecom Press, 2014. (in Chinese)

[4] KELLI Y. Cyber Case Study: The Mirai DDoS attack on Dyn[EB/OL]. (2022-01-10)[2023-07-24]. https://coverlink.com/case-study/mirai-ddos-attack-on-dyn.

[5] ALEX S. Ukraine war drives DDoS attack volumes ever higher [EB/OL]. (2022-08-18) [2023-07-24]. https://www.computerweekly.com/news/252523959/Ukraine-war-drives-DDoS-attack-volumes-ever-higher.

[6] WHOOPS CECILY M. Samsung workers accidentally leaked trade secrets via ChatGPT[EB/OL]. (2023-04-06) [2023-07-24]. https://mashable.com/article/samsung-chatgpt-leak-details.

[7] BU T, GAO L X, TOWSLEY D. On characterizing BGP routing table growth[C]//Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE. Piscataway: IEEE, 2002: 2185-2189.

[8] WIKIPEDIA. 512k day[EB/OL]. (2022-07-05) [2023-07-24]. https://en.wikipedia.org/wiki/Talk%3A512k_day.

[9] DANNY P. What will happen when the routing table hits 1024k[EB/OL]. (2021-03-01)[2023-07-24]. https://blog.apnic.net/2021/03/03/what-will-happen-when-the-routing-table-hits-1024k/.

[10] DARPA Seeks Clean-Slate Ideas for Mobile Ad Hoc Networks (MANETs) [EB/OL]. (2013-04-30) [2023-07-24]. https://www.darpa.mil/news-events/2013-04-30.

[11] GIULIARI G, KLENZE T, LEGNER M, et al. Internet backbones in space[J]. ACM SIGCOMM Computer Communication Review, 2020, 50(1): 25-37.

[12] BHATTACHERJEE D, SINGLA A. Network topology design at 27,000 km/hour[C]//Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies. New York: ACM, 2019: 341-354.

[13] CONTRERAS-CASTILLO J, ZEADALLY S, GUERRERO-IBANEZ J A. Internet of vehicles: Architecture, protocols, and security[J]. IEEE Internet of Things Journal, 2018, 5(5): 3701-3709.

[14] BUSH R, AUSTEIN R. The Resource Public Key Infrastructure (RPKI) to Router Protocol: RFC6810[S/OL]. (2013-01-01) [2024-03-10]. https://datatracker. ietf. org/

doc/rfc6810/.

[15] HAAG W, MONTGOMERY D, Tan A, et al. Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation[R]. Gaithersburg: National Institute of Standards and Technology, 2019.

[16] LEPINSKI M, SRIRAM. K. BGPsec Protocol Specification: RFC8205[S/OL]. (2017-09-01)[2024-03-10]. https://datatracker.ietf.org/doc/rfc8205/.

[17] CLARK D. The design philosophy of the DARPA Internet protocols[C]//Symposium Proceedings on Communications Architectures and Protocols. New York: ACM, 1988: 106-114.

[18] 吴建平, 林嵩, 徐恪, 等. 可演进的新一代互联网体系结构研究进展[J]. 计算机学报, 2012, 35(6): 1094-1108.
WU J P, LIN S, XU K, et al. Advances in evolvable new generation Internet architecture[J]. Chinese Journal of Computers, 2012, 35(6): 1094-1108. (in Chinese)

[19] 谢高岗, 张玉军, 李振宇, 等. 未来互联网体系结构研究综述[J]. 计算机学报, 2012, 35(6): 1109-1119.
XIE G G, ZHANG Y J, LI Z Y, et al. A survey on future Internet architecture[J]. Chinese Journal of Computers, 2012, 35(6): 1109-1119. (in Chinese)

[20] 黄韬, 刘江, 霍如, 等. 未来网络体系架构研究综述[J]. 通信学报, 2014, 35(8): 184-197.
HUANG T, LIU J, HUO R, et al. Survey of research on future network architectures[J]. Journal on Communications, 2014, 35(8): 184-197. (in Chinese)

[21] AHLGREN B, DANNEWITZ C, IMBRENDA C, et al. A survey of information-centric networking[J]. IEEE Communications Magazine, 2012, 50(7): 26-36.

[22] ZHANG L X, AFANASYEV A, BURKE J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[23] CLARK D D. Designing an Internet[M]. Cambridge: MIT Press, 2018.

[24] GOOGLE INC. IPv6 Statistics[EB/OL]. (2023-06-15)[2023-07-24]. https://www.google.com/intl/en/ipv6/statistics.html.

[25] CLARK D D, TENNENHOUSE D L. Architectural considerations for a new generation of protocols[J]. ACM SIGCOMM Computer Communication Review, 1990, 20 (4): 200-208.

[26] RAYCHAUDHURI D, NAGARAJA K, VENKATARAMANI A. MobilityFirst[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2012, 16(3): 2-13.

[27] NAYLOR D, MUKERJEE M K, AGYAPONG P, et al. XIA[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 50-57.

[28] PERRIG A, SZALACHOWSKI P, REISCHUK R M, et al. SCION: A Secure Internet Architecture[M]. Cham: Springer International Publishing, 2017.

[29] MCCAULEY J, HARCHOL Y, PANDA A, et al. Enabling a permanent revolution in Internet architecture[C]// Proceedings of the ACM Special Interest Group on Data Communication. New York: ACM, 2019: 1-14.

[30] 罗洪斌, 张珊, 王志远. 共生网络: 异构网络安全高效互联的体系结构与机理[J]. 通信学报, 2022, 43(4): 36-49.
LUO H B, ZHANG S, WANG Z Y. Architecture and mechanisms for secure and efficient internetworking of heterogeneous network[J]. Journal on Communications, 2022, 43(4): 36-49. (in Chinese)

[31] 罗洪斌, 张珊, 王志远. 异构网络融合共生的需求、挑战与架构[J]. 电信科学, 2022, 38(6): 18-30.
LUO H B, ZHANG S, WANG Z Y. Interconnection and coexistence of heterogeneous network: Requirements, challenges, and architecture[J]. Telecommunications Science, 2022, 38(6): 18-30. (in Chinese)

[32] LUO H B, CHEN Z, CUI J B, et al. CoLoR: An information-centric Internet architecture for innovations[J]. IEEE Network, 2014, 28(3): 4-10.

[33] LUO H B, CHEN Z, CUI J B, et al. An approach for efficient, accurate, and timely estimation of traffic matrices [C]//2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE, 2014: 67-72.

[34] ZHANG S, LI J J, LUO H B, et al. Low-latency and fresh content provision in information-centric vehicular networks[J]. IEEE Transactions on Mobile Computing, 2022, 21(5): 1723-1738.

[35] CHEN Z, LUO H B, ZHANG M, et al. Improving network security by dynamically changing path identifiers in future Internet[C]//2015 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE, 2015: 1-7.

[36] LUO H B, CHEN Z, LI J W, et al. On the benefits of keeping path identifiers secret in future Internet: A DDoS perspective[J]. IEEE Transactions on Network and Service Management, 2018, 15(2): 650-664.

[37] LUO H B, CHEN Z, LI J W, et al. Preventing distributed denial-of-service flooding attacks with dynamic path identifiers[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1801-1815.

[38] LUO H B, LIU Z B, ZHANG S. Preventing DDoS flood-

ing attacks with cryptographic path identifiers in future Internet[J]. IEEE Transactions on Network and Service Management, 2022, 19(2): 1690-1704.

[39] 刘洲彪. 共生网络中的DDoS攻击检测及溯源机制研究与验证[D]. 北京: 北京航空航天大学, 2020.

作者简介

罗洪斌 男, 1977年出生于重庆. 博士,北京航空航天大学教授、博士生导师. 主要研究方向为互联网体系结构、异构网络跨域互联机理等.
E-mail: luohb@buaa.edu.cn

张 珊 女, 1989年出生于河南焦作. 博士,北京航空航天大学副教授、博士生导师. 主要研究方向为异构网络资源管理、边缘网络缓存与智能等.
E-mail: zhangshan18@buaa.edu.cn

王志远 男, 1993年出生于山东淄博. 博士,北京航空航天大学副教授. 主要研究方向为网络体系结构、卫星互联网、边缘计算、算法博弈论等.
E-mail: zhiyuanwang@buaa.edu.cn

孟晴开 男, 1995年出生于湖南岳阳. 博士,北京航空航天大学博士后. 主要研究方向为网络体系结构、数据中心网络、网络传输协议等. 中国电子学会会员编号:E190156533M.
E-mail: mengqingkai@buaa.edu.cn