专题：新型网络技术

异构网络融合共生的需求、挑战与架构

罗洪斌[1,2,3,4]，张珊[1,2,3,4]，王志远[1,4]

（1. 北京航空航天大学计算机学院，北京 100191；
2. 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：随着通信网络技术的飞速发展与应用渗透，具有不同拓扑特征与业务需求的网络形态（如陆地互联网、卫星网络、工业互联网、无人机集群网络、车联网等）不断涌现，形成了众多差异化网络体制并存的局面。为此，阐述了异构网络融合共生的核心需求与面临的关键技术挑战，并介绍了共生网络——一种异构网络安全高效跨域互联的新型网络架构。共生网络从差异化网络体制一致的功能本质（信息传递）出发，引入多维名字空间用于普适化表征；并通过解耦域内路由和域间路由，保障异构网络的可演进性；在此基础上，构建了高效的跨域通信模式和安全保障机制。

关键词：异构网络；网络互联；网络结构；安全；高效

中图分类号：TP393

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2022132

Interconnection and coexistence of heterogeneous network: requirements, challenges, and architecture

LUO Hongbin[1,2,3,4], ZHANG Shan[1,2,3,4], WANG Zhiyuan[1,4]

1. School of Computer Science and Engineering, Beihang University, Beijing 100191, China
2. National Key Laboratory for Software Development Environment, Beijing 100191, China
3. Key Laboratory of Mathematics, Information and Behavioral Semantics, MoE, Beijing 100191, China
4. Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Beijing 100191, China

Abstract: With the rapid development of the network technology and applications, many networks with different types of topologies and services have been emerging, such as Internet, satellite Internet, industrial Internet, unmanned aerial vehicle swarm network, and vehicle Internet, forming a situation in which many differentiated network systems coexist, to this end, the requirements and challenges were elaborated for heterogeneous networks to be integrated and coexist. Then CoLoR, an architecture for securely and efficiently interconnect heterogeneous networks was introduced. Based on the consistent function (i.e., information transmission) among heterogeneous network systems,

收稿日期：2022−04−01；**修回日期：**2022−06−01

通信作者：王志远, zhiyuanwang@buaa.edu.cn

基金项目：国家重点研发计划项目（No.2019YFB1802803）；国家自然科学基金资助项目（No.61801011）

Foundation Items: The National Key Research and Development Program of China (No.2019YFB1802803), The National Natural Science Foundation of China (No.61801011)

CoLoR introduces multi-dimensional namespace for the universal representation. Moreover, CoLoR decouples the intra-domain routing and the inter-domain routing to ensure the evolution ability. Finally, CoLoR also constructs an efficient cross-domain communication mode and a security guarantee mechanism.

Key words: heterogeneous network, internetworking, network architecture, security, efficiency

0　引言

随着信息通信技术的飞速发展，具有不同特征的网络形态不断涌现，形成了异构网络并存的局面。一方面，网络空间与物理空间加速融合，传统的陆地互联网逐步向空天环境和海洋环境延伸，形成了卫星网络、无人机集群网络、海洋信息网络等具有各自拓扑特征和业务需求的网络形态；另一方面，网络空间与垂直行业相互渗透，蜂窝车联网、工业互联网等与人类生产活动息息相关的网络形态不断涌现，带来了车辆、机器等全新网络应用需求。以下结合卫星网络、无人机集群网络、海洋信息网络、蜂窝车联网、工业互联网，阐述几种典型网络形态的拓扑特征和业务需求。

（1）卫星网络

卫星网络具有为陆地偏远地区（如沙漠、森林等）提供全球覆盖的潜力，是空天地一体化信息系统的重要组成部分。其中，空间段由通信卫星组成，包含低地球轨道卫星、中地球轨道卫星、地球静止轨道卫星；地面段包括关口站等网络实体[1]。卫星网络在业务特征、拓扑特征等方面与传统的陆地互联网有较大的差异。在业务机制方面，低轨卫星具有星地链路损耗小、传输时延低等优势；通过大规模低轨卫星星座组网可实现全球覆盖，为用户提供低时延的远距离传输服务。因此，卫星网络不仅涉及平面化的星间组网，同时承担星地立体化传输服务。在网络拓扑方面，卫星网络具有拓扑规律性变化、节点间歇性连通、链路时延大尺度变化等特征[2]。特别是在极地区域，相邻轨道之间的卫星天线对准困难，导致卫星在进入或离开极地区域时出现周期性的链路断开或重新建立，为信息的可靠传输带来了新挑战。

（2）无人机集群网络

近年来，无人机在不同领域的应用需求逐渐凸显，如环境检测、应急通信、空中中继、空中侦察等[3]。随着无人机作业的任务复杂度升级，无人机往往难以单机完成复杂的作业任务，大规模无人机集群组网逐步成为一项关键技术。考虑无人机集群的协同作业任务和编队飞行需求，无人机集群网络具有其鲜明的拓扑特征。一方面，无人机集群执行协同作业任务时，各个节点的相对位置频繁发生变化，使无人机集群网络具有节点分割与重组、拓扑强时变等特征，为集群节点间的信息交互与共享带来了挑战。另一方面，长距离编队飞行过程中，无人机集群内各个节点的整体运动规律相似，无人机集群网络拓扑具有阶段化的稳定性。而在实际应用中，无人机集群经常需要在编队飞行中协同完成作业任务，因此无人机集群的动态网络拓扑往往蕴含相对稳定的连接关系。无人机集群网络的上述特征不仅显著区别于以“固定、有线”为特色的陆地互联网，也与其他移动自组织网络存在明显差异。

（3）海洋信息网络

海洋信息网络尝试将陆地互联网服务延展到占地球 71% 的海洋地区，是实现空天地海一体化信息系统的重要环节，也是发展海洋经济和海上国防的网络支撑[4]。海洋信息网络的建设与传统陆地互联网有天然的差异。在业务特征方面，海洋信息网络为海上运输、海上作业提供广域化的实时数据通信服务，水下传感器需要借助海洋信息网络实现环境监测。在传输技术方面，海洋信息网络受限于水声信道、海面水雾等干扰，信息传输效率往往较低。一方面，水声通信技术传

输速率低、传输时延长且通信能耗大。另一方面，水下激光通信技术虽然具有较高的传输速率和传输时延，但是极易受到水下障碍物遮挡而受限于传输距离。因此，海洋信息网络作为关系国家海洋经济和海上攻防体系的重要通信网络，在业务需求、传输技术等方面与传统陆地互联网存在巨大的差异性。

（4）蜂窝车联网

蜂窝车联网是物联网技术在智能交通领域的一个典型网络形态，在 6G 无线通信网络中发挥着重要作用。蜂窝车联网实际涵盖了小范围的车内网络、局域化的车际网络连接、广域化的车载移动互联网[5]。在这种网络形态下，联网车辆不仅仅是移动通信设备，也是移动用户服务（如车载缓存服务）请求的承载设备[6]。因此，蜂窝车联网面临的业务环境往往非常复杂。首先，联网车辆自身移动性强，导致车际网络拓扑变化快，车载通信过程需要频繁切换无线网络的接入点。其次，联网车辆与车外移动用户之间的相对位置变化频繁，导致移动用户通过联网车辆获取服务过程中接入、中断频繁。最后，联网车辆（如联网私家车、联网公交车等）存在商业关系层面的差异性，致使车际网络的协同问题更加复杂。以上论述表明，蜂窝车联网的业务形式与传统陆地互联网有较大差异；同时，蜂窝车联网的网络拓扑动态规律与无人机集群网络也有较大区别。

（5）工业互联网

随着互联互通的需求逐渐从消费者向工业生产环节延伸，工业互联网时代已然成为数字经济的下半场[7]。智能制造的工艺流程对相应的网络形态提出了鲜明的要求。一方面，差异化的智能制造业涵盖了不同的生产环节，工业互联网需要针对具体的生产流程、生产工艺进行定制化的部署，以提供实时、高效的生产数据共享。另一方面，商业关系、隐私数据等因素对智能制造的安全保障提出了更高要求。为此，工业互联网亟须解决数据流通与数据保护的矛盾，保障生产数据的安全性和可信性[8]。显然，工业互联网不是网络通信技术在智能制造领域的简单投射，需要结合具体的生产环节，充分融合隐私数据保护技术。因此，工业互联网与传统的陆地互联网在网络形态和业务需求等方面存在明显的差异。

1 异构网络融合共生的需求

随着数据成为生产要素，如何在各类网络形态日趋差异化的背景下，实现异构网络的“融合与共生”是未来网络发展的关键科学问题。其中，“融合”是指打破异构网络之间的通信“壁垒”，保障不同形态网络的互联互通，支撑高效的跨网数据传输与信息共享，以释放数据价值。为此，亟须探索面向异构网络跨域互联的全新架构。另外，网络发展过程中的大量事实说明，没有一个放之四海皆准的网络体制能够适应所有不同形态的网络；相反，为了发挥不同形态网络的内在优势，必须基于其固有特征设计合适的网络体制。因此，异构网络不仅具有“融合”发展需求，也应该具备“共生”的能力。其中，“共生”即多体制并存，允许不同形态的网络使用与其网络特征与业务需求匹配的网络体制。

1.1 陆地互联网

随着陆地互联网的不断发展，TCP/IP 体制暴露出诸多弊端，例如演进性弱、资源浪费、安全性差等问题。因此，学术界和工业界一直在探索面向陆地互联网的新型网络体制。

（1）演进性弱

TCP/IP 体制以主机为中心并为所有联网主机分配 IP 地址。随着 32 位 IPv4 地址的耗尽，从 IPv4 地址向 128 位 IPv6 地址的演进已经历时二十余年，然而全球 IPv6 流量依然仅占所有流量的 36.92%（截至 2022 年 4 月 1 日）[9]。

（2）资源浪费

TCP/IP 体制为陆地互联网用户提供的是传输

通道，而不关心传输的内容，复杂、重复的内容传输，消耗了带宽资源。为此，学者们提出了信息中心网络（information-centric network，ICN）体制，例如 CCN（content-centric network）[10]和 NDN（named data network）[11]。

（3）安全性差

TCP/IP 网络体制在设计之初默认主机的安全性，即 IP 网络接受任何主机发送的内容，这种情况导致任意（恶意）信息均能被发送到接收者，这是 IP 网络容易被攻击的根源。因此，近年来学术界围绕安全性问题探索并设计了新型网络体制，例如 SCION（scalability, control, and isolation on next-generation networks）[12]。

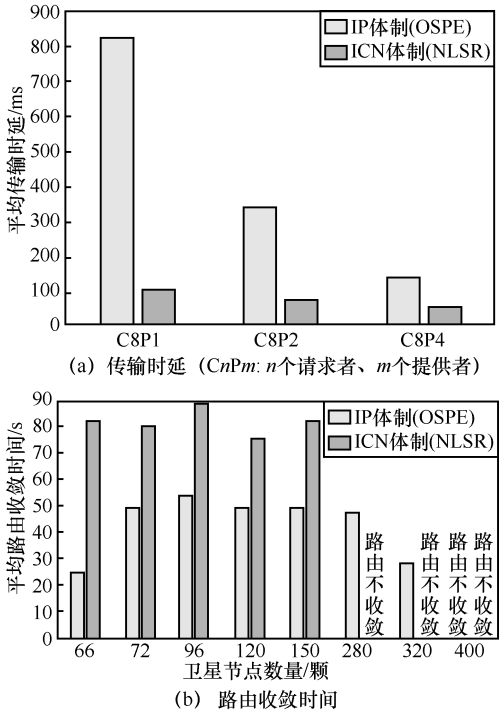
总体来说，单一的 TCP/IP 体制目前依然无法满足陆地互联网的业务需求；同时，陆地互联网中已经形成了 IPv4、IPv6、NDN、SCION 等网络体制共存的局面，且这些体制的网络必然会长期共存。

1.2　低轨卫星网络

低轨卫星网络具有周期性的拓扑动态性，尤其当卫星网络规模较大时，链路状态变化更加频繁；哪种类型的网络体制更适用于低轨卫星网络是学术界和工业界一直在探索的问题。

TCP/IP 体制虽然技术成熟度高、协议支持好，但是该体制的拓扑动态性支持能力差，部署于卫星网络会导致传输效率低和可扩展性差等弊端。IP 体制与 ICN 体制在卫星网络中的性能比较如图 1 所示，图 1（a）给出了铱星星座中，基于 IP 和基于 ICN 体制的服务获取时延性能表现，包含 3 种测试场景（其中，C*n*P*m* 表示 *n* 个请求者和 *m* 个提供者）。结果表明，ICN 体制比 IP 体制的服务获取时延低，其内在原因在于 ICN 体制对内容命名带来的内容缓存能力，便于服务内容就近获取。而基于TCP/IP体制的卫星网络可能大量重复传输相同的内容，严重浪费了有限的星上带宽资源，导致网络拥塞和信息分发效率低。

实际上，传统的基于 TCP/IP 和基于 ICN 的网络体制均无法为卫星网络提供大规模星座组网支持。在星座规模较大的情境下，链路状态时变性更强，导致路由更新频繁甚至无法收敛。如图 1（b）所示，ICN 体制的路由收敛时间比 IP 体制更长；当卫星节点数量达 280 颗时，基于 ICN 的路由协议无法完成路由收敛。另外，当卫星节点数量达 400 颗时，基于 IP 和基于 ICN 的路由协议均无法在下一次拓扑变化前收敛。



(a) 传输时延（C*n*P*m*: *n*个请求者、*m*个提供者）

(b) 路由收敛时间

图 1　IP 体制与 ICN 体制在卫星网络中的性能比较

上述讨论说明，如果直接将现有的 IP 体制和 ICN 体制的路由方法应用到卫星网络，往往难以适应大规模星座的动态性。为了解决该问题，必须针对卫星网络的特征进行有针对性的组网设计。例如，学术界提出通过星间区域划分屏蔽卫星网络拓扑高动态性[13]，即缩小路由通告区域、降低路由协议开销、增强路由稳定性和提高路由可扩展性。

1.3　无人机集群网络

无人机集群网络是一种具有拓扑高动态、强

时变特征的移动自组织网络，直接将现有的 IP 体制或 ICN 体制的路由组织模式用于无人机集群，往往难以实现高效的组网。

（1）IP 体制在无人机集群网络的缺陷

IP 地址既代表节点在网络中的位置又代表节点的身份，导致网络的移动性支持能力不足。首先，为新节点分配 IP 地址和接入认证的时延较大，不利于实现节点的快速接入。其次，无人机节点间链路经常中断，而 TCP 难以保障中断后的自我恢复。最后，网络拓扑高动态、强时变，给 IP 路由协议的收敛时间和可扩展性带来困难。美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）早在 2013 年指出：基于 IP 的自组织网络技术，当网络节点超过 50 个时，网络性能会急剧恶化；为此，DARPA 启动了新项目，探索不依赖于 IP 的全新组网方式[14]。

（2）ICN 体制在无人机集群网络的缺陷

ICN 体制为网络中的内容分配标识，采用内容驱动的通信模式，不再依赖于建立节点之间的路径，具有较强的移动性支持能力。但其路由方式完全依赖内容标识，网络需要维护规模庞大的内容路由表，面临路由可扩展性问题，制约着无人机集群的规模。同时，ICN 体制还忽略历史路径信息，在无人机集群拓扑稳定时仍重复进行路径探测，造成带宽资源浪费等问题。

上述两方面说明，必须针对无人机集群的拓扑动态特征制定合适的组网方法。本文发现基于节点和内容的混合路由机制，相较于将 TCP/IP 或者 ICN 路由方法直接应用于无人机集群网络，有明显优势。如图 2（a）所示，在 8 个请求者向 2 个提供者请求内容的移动（速度：20 m/s）场景中，所提方法的网络规模相较于 IP 和 ICN 方法提高 265%和 155%。如图 2（b）所示，在 8 个请求者对 2 个提供者的固定规模（64 节点）场景下，所提方法的请求成功率相较于 IP 方法提高 38.9%～61.0%，相较于 ICN 方法提高 26.2%～33.9%。

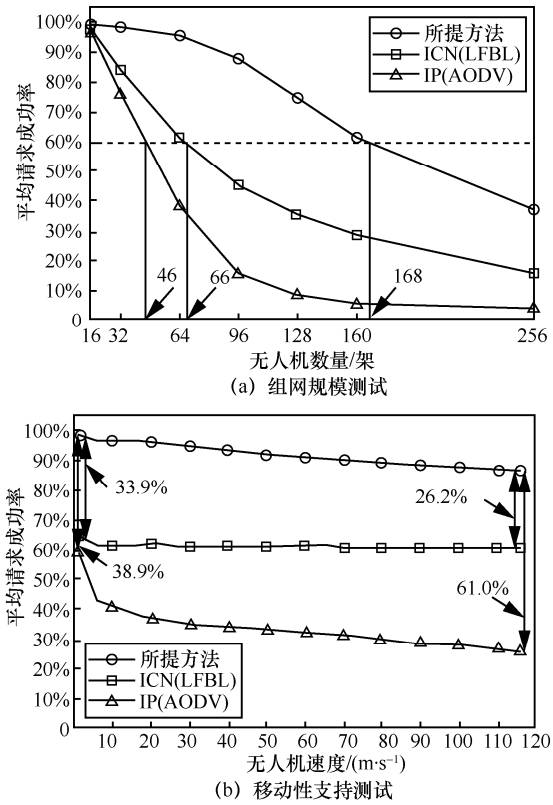


图 2 不同网络体制在无人机集群网络中的性能对比

综上所述，只有针对无人机集群的拓扑特征，开展有针对性的网络体制定制化设计，才能实现高效的无人机集群组网。这样一来，无人机集群定制化的网络体制便面临与其他网络体制共生的需求。

2 异构网络融合共生的挑战

异构网络日益增强的融合共生需求，亟须全新的网络体系架构支撑。然而，设计相应的网络架构面临诸多挑战。

2.1 体制异构性挑战

体制异构性是异构网络融合共生的根本瓶颈。允许不同形态的网络采取适合其自身特征的网络体制，需要解决异构网络体制互联互通的问题。然而，不同网络体制在标识空间、寻址方式、路由组织、报文格式等方面存在巨大的差异，一种网络体制下的报文无法直接在另一种网络体制下转发。目前的解决方案是通过协议转换实现异

构体制网络的互联[15]。但是，协议转换往往存在语义缺失、效率低下、安全性差等弊端，特别是当报文需要跨过多个体制各异的自治系统时，多次协议转化会进一步放大上述弊端。因此，如何将体制异构性的网络有效互联，是异构网络融合共生的首要挑战。

2.2　内容传输挑战

在差异化网络体制下实现高效的内容传输，是异构网络融合共生需要解决的核心挑战。具体来说，异构网络融合共生的根本目标是通过高效的内容传输，促进数据流通从而释放数据价值。但是，在多种网络体制并存的复杂网络环境，如何运用内容标识、如何从多个自治系统中快速地发现目标内容、如何实现跨自治系统的高效内容传输，均面临诸多挑战。

（1）内容标识

在以信息为中心的网络体制（如 CCN/NDN）下，内容标识虽然有利于通过缓存提高内容分发效率，但是，当该体制与以主机为中心的 TCP/IP 体制并存时，如何在跨自治系统的内容请求/传输过程中合理地运用内容标识依然需要进一步探索。

（2）内容发现

异构网络融合共生需要针对用户的内容请求，快速地确定目标内容由哪个自治系统提供，从而将请求报文向该自治系统转发。当多种网络体制并存时，部分自治系统先天缺失针对内容的标识，在这种情况下，如何快速地发现目标内容需要进一步探索。

（3）内容传输

当多种网络体制并存时，高效地传输不仅取决于自治系统内部的路由组织形式，也与自治系统之间的跨域互联方式密切相关。二者相互耦合，导致异构网络的内容跨域传输机制更加复杂。

2.3　可扩展性挑战

异构网络融合共生架构需要良好的可扩展性，包括单自治系统内的可扩展性和自治系统间的可扩展性。

（1）自治系统内的可扩展性

不同网络体制的自治系统互联之后，单个自治系统规模的可扩展性不仅与自治系统内部的路由组织方式有关，也受限于自治系统之间的路由方式。因此，单个自治系统规模的可扩展性与差异化网络体制互联存在耦合关系。

（2）自治系统间的可扩展性

随着网络的发展，具有各自特征的网络自治系统不断涌现。一方面，异构网络融合共生架构需要为大规模的自治系统提供高效的跨域路由转发；另一方面，异构网络融合共生架构必须能够兼容未来涌现的全新网络体制。

2.4　安全保障挑战

随着网络空间与经济生产环节的融合，采用不同体制的网络自治系统在支持互联互通的同时，更需要保障安全，具体表现在两个层面。

- 异构网络融合共生架构，需要防止自治系统内的隐私数据被非法转发至其他自治系统。当前，数据已被列为新的生产要素，其商业和社会价值日益凸显，数据使用主权和隐私性需通过网络安全得以保障。例如，某企业的工业互联网需要支持涉及商业秘密的隐私数据传输，如果与其他自治系统互联互通会导致其隐私数据被非法泄露，那么该企业必将拒绝与其他体制网络融合共生，而选择继续维持网络“孤岛”的现状。
- 异构网络融合共生架构，需要防止自治系统内的节点受到来自其他自治系统的网络攻击。随着网络空间与社会空间的深度融合，各种设备可能随遇接入网络，网络安全性也将影响社会安全。例如，接入网络的车辆若遭受其他网络的攻击，可能导致车辆失控而造成严重交通事故，必须通过安全可靠的网络跨域机制，防止车辆受到来自传统互联网等其他网络的流量攻击。

3 异构网络融合共生架构

针对异构网络融合共生的需求与挑战，本节将介绍一种具有潜力的新型网络架构——共生网络[16-17]。共生网络从异构网络体制相同的功能本质（传递信息）出发，引入多维度名字空间用于普适化表征；并通过域内域间解耦的路由组织方法，保障异构网络的可演进性；在此基础上，构建了“以拉促推、推拉结合”的跨域传输模式以及入域出域安全保障机制。

3.1 多维度网络名字空间表征

网络技术发展过程中，虽然差异化的网络体制不断涌现，但是任何一种网络体制的设计与构建，都离不开网络的功能本质——传递信息。只有从该功能本质出发，才能克服体制异构性挑战。为此，共生网络首先将信息传递的功能本质映射到 4 个基本维度：内容属性（传什么）、身份属性（传给谁）、位置属性（传到哪）、方式属性（怎么传）。并在此基础构建相应的名字空间，以对体制异构的网络空间进行普适化表征：内容名字（service identifier，SID）表征内容属性、节点标识（node identifier，NID）表征身份属性、各类地址（address）表征位置属性、域间路径标识（path identifier，PID）表征方式属性。

（1）SID

针对内容属性，共生网络架构为内容命名并基于内容名字进行内容查找，便于充分利用缓存资源[18]，这不仅可以大幅降低内容获取的平均时延，又能够降低网络传输负载[19]。同时，共生网络为内容构建了支持自校验功能的内容名字。当某个节点标识为 NID 的节点需要跨网提供内容时，相应的内容名字 SID 定义为：归属部分（160 bit）+ 标识部分。其中归属部分为该节点的节点标识 NID；标识部分为该节点为该内容生成的唯一标识，可以通过内容的哈希表征静态内容的标识部分，动态内容的标识部分可由节点指定。

（2）NID

针对身份属性，共生网络架构为任意节点构建了具有自证明特性的节点标识，从而便于进行接入安全认证。具体来说，节点标识长度为 160 bit，由两部分构成：网络部分（32 bit）+自证明部分（128 bit）。NID 网络部分表征该节点处于哪个网络自治系统。NID 的自证明部分基于一组公钥/私钥生成，即自证明部分是公钥的 128 bit 哈希值，私钥则由该节点保管而不向外通告。

（3）address

针对位置属性，共生网络架构支持各个自治系统采取最适合其网络特征的体制，例如，IPv4 网络可以继续使用 32 bit 的 IPv4 地址；IPv6 网络继续使用 128 bit 的 IPv6 地址；有的网络可以使用地理坐标作为地址等。

（4）PID

共生网络架构在允许各个自治系统采用原始地址的前提下，聚焦于跨域信息传递，并引入 L bit 的 PID 进行跨域分组转发。具体而言，PID 随节点的内容请求而动态生成，包括两部分：前缀部分 PX（l bit）+ 耦合生成部分（($L-l$) bit）。其中，PX 由该域间路径联接的两个自治系统协商决定，按照“正交复用”的原则为域间路径分配域间路径标识前缀。这样一来，PX 实际代表 2^{L-l} 个连续的域间路径标识。另外，耦合生成部分是单向哈希函数的返回结果，该函数的输入信息包括 NID、SID、PID_0（请求报文的上一跳）、随机数等。上述耦合生成机制便于共生网络构建可靠跨域安全保障。

基于上述多维度名字空间，共生网络进一步构建了域内域间解耦的路由组织形式和内容名字驱动的跨域互联模式。

3.2 域内域间解耦的路由组织形式

为了保障异构网络体制融合的可演进性，必须在不改变各个网络体制既定运作方式的前提下，实现异构互联。为此，共生网络通过解耦域

内路由与域间路由，构建了具有良好演进性的路由组织形式。

（1）域内路由

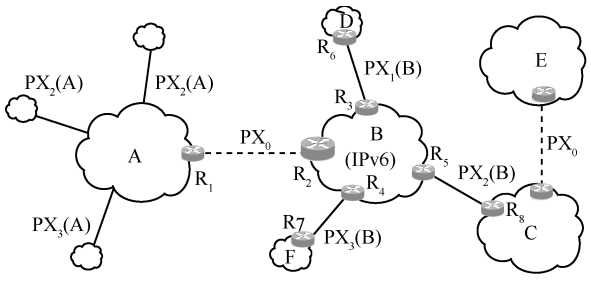
在共生网络架构下，每个网络的域内路由可以根据该网络所采用的网络体制确定。相应地，每个网络内部的报文转发方式由其采用的网络体制确定。

（2）域间路由

通过多年研究发现，网络间的互联本质——根据一定的社会（或商业）关系建立域间路径，并基于该域间路径传递信息。为此，共生网络对网络之间的域间路径进行抽象，并用域间路径标识表示域间路径，进而屏蔽域间互联的具体方式。边界路由器域间路由表示意图如图 3 所示，网络 A 和网络 B 之间的域间路径用多协议标签交换（multi-protocol label switching，MPLS）转发分组，而网络 B 和网络 C 之间的域间路径使用 IPv4 转发分组；但共生网络不关心这些细节，而是为这些域间路径分配域间路径标识前缀。在此基础上，各个网络的边界路由器维护一个域间路由表，通过域间路径标识进行跨域分组转发。域间路由表的每个表项对应一个 PX，记录该域间路径标识对应的域间路径连接的网络、去往该网络的下一跳节点、去往下一跳节点的通信方式等。当边界路由器收到分组时，通过查找域间路由表，可知应该将该分组发往哪个下一跳节点。图 3 展示了一个简单的异构网络，以及边界路由器 R_2 的域间路由表。假定网络 B 采用 IPv6，且网络 A 和网络 B 之间使用 MPLS。边界路由器 R_2 的域间路由表的第一行对应 PX_0，该域间路径连接的是网络 A，去往网络 A 的下一跳节点是边界路由器 R_1，通过封装 MPLS 报头可将分组从边界路由器 R_2 发给 R_1。第二行对应 $PX_1(B)$，该域间路径连连网络 D，去往网络 D 的下一跳节点是边界路由器 R_3，通过封装 IPv6 报头可将分组从边界路由器 R_2 发给 R_3。

3.3　内容名字驱动的跨域互联模式

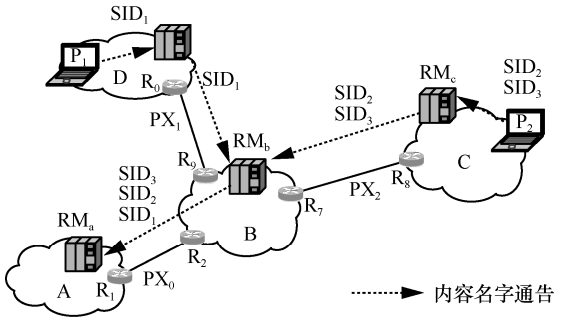
虽然不同网络体制的名字空间不同，但其传递信息的功能本质相同。为此，共生网络从这一功能本质出发，为异构网络提供的信息/内容命名，并在网络间通告内容名字的可达性，以克服体制异构性挑战。具体来看，共生网络在各个网络自治系统中部署一个资源管理器（resource manager，RM），以层叠的方式运行在该网络。根据实际需求，RM 可以是逻辑上集中、分布式部署的。每个资源管理器维护一个内容路由表，每个路由条目对应一个内容名字（或一组内容名字的前缀），记录以下信息：去往相应内容提供者的下一跳域内节点，去往内容提供者的下一跳网络、该资源管理器所在网络与下一跳网络之间的域间路径标识前缀。基于上述路由表项，RM 可以将对某个内容的请求报文，转发至相应的边界路由器，从而完成请求报文在本域的路由工作。资源管理器的内容路由表示意图如图 4 所示，展示了一个异构网络拓扑，以及资源管理器 RM_b 的内容路由表。假定网络 D 的内容提供者 P_1 能提供名为 SID_1 的内容，并向网络 B 和网络 A 通告该内容名字。假定网络 C 的内容提供者 P_2 能提供名为 SID_2 和 SID_3 的内容，并向网络 B 和网络 A 通告这两个



路由器 R_2 域间路由表

域间路径标识前缀	邻域	下一跳节点	通信方式
PX_0	AR	R_1	MPLS
$PX_1(B)$	DR	R_3	IPv6
$PX_2(B)$	CR	R_5	IPv6
$PX_3(B)$	FR	R_4	IPv6

图 3　边界路由器域间路由表示意图



资源管理器 RM_b 内容路由表

内容名字	下一跳网络	下一跳节点	域间路径标识前缀
SID_1	DR	R_9	PX_1
SID_2	CR	R_7	PX_2
SID_3	CR	R_7	PX_3
—	—	—	—

图 4　资源管理器的内容路由表示意图

内容名字。网络 B 的资源管理器 RM_b 维护的内容路由表中，第一行表项对应内容名字 SID_1，记录请求该内容的下一跳网络为网络 D，下一跳节点为 R_9，对应的域间路径标识为 PX_1；第二行与第三行表项分别对应内容名字 SID_2 和 SID_3，请求这两个内容的下一跳网络为网络 C，下一跳节点均为边界路由器 R_7，域间路径标识均为 PX_2。

3.4　“以拉促推、推拉结合”的跨域通信机制

本节将基于上述名字空间、路由组织形式和跨域互联模式，介绍共生网络的跨域通信机制。

TCP/IP 体制基于主机 IP 地址进行数据报文传输，因此当某个节点知晓其他节点的 IP 地址时，便可以向其“推”送任意数量的报文，一定程度上助长了网络攻击。NDN 体制则为内容命名，不再包含主机 IP 地址，并基于内容名字“拉”取相应内容。内容提供者只有收到请求报文，才回传相应的数据报文，一定程度上使请求包数量大，消耗了网络资源。为了克服这两种通信模式的弊端，共生网络采取“以拉促推、推拉结合”的跨域通信模式。共生网络通信机制流程如图 5 所示。

图 5 展示了 4 个网络自治系统，记为{A,B,C,D}，4 个自治系统依据其拓扑特征和业务需求，可以采用不同的网络体制。各个网络自治系统，包含一个资源管理器，记为{RM_a, RM_b, RM_c, RM_d}。考虑自治系统 C 内的内容提供者 P 可以提供内容名字为 SID_1 的内容，同时自治系统 A 内的用户 U 希望获取该内容。在本示例中，“以拉促推、推拉结合”的跨域通信模式主要包含请求步骤 1～步骤 4 和数据传输步骤 5。

步骤 1　用户 U 向其本地资源管理器 RM_a

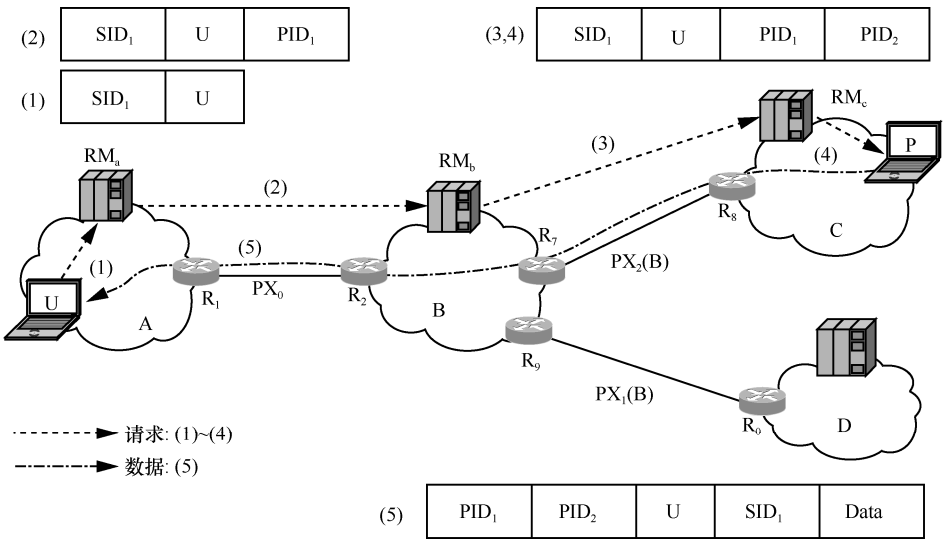


图 5　共生网络通信机制流程

发送一个请求报文，该请求报文包含用户 U 所需内容的内容名字 SID_1、请求者 U 的节点标识（记为 U）等信息。

步骤 2　当本地资源管理器 RM_a 收到该请求报文时，查询其内容路由表得知应将该请求报文转发给自治系统 B、去往自治系统 B 的下一跳为边界路由器 R_1、边界路由器 R_1 与自治系统 B 之间的域间路径标识前缀为 PX_0。进而，资源管理器 RM_a 为该请求报文计算生成域间路径标识 PID_1（具体计算方法见第 4.4.1 节），然后将该域间路径标识添加在请求消息的尾部，并将该请求发送给边界路由器 R_1。边界路由器 R_1 收到该请求后，通过 PID_1 得知应该将该请求消息转发给邻域 B 的边界路由器 R_2。边界路由器 R_2 收到该请求报文后，将该请求报文转发给其本地资源管理器 RM_b。

步骤 3　资源管理器 RM_b 收到请求报文后，查找其内容路由表得知应将该请求报文发送给自治系统 C、去往自治系统 C 的下一跳为边界路由器 R_7、边界路由器 R_7 与自治系统 C 之间的域间路径标识前缀为 PX_2。类似地，资源管理器 RM_b 为该请求报文计算生成域间路径标识 PID_2，然后将 PID_2 添加在请求报文的尾部，并将该请求发送给边界路由器 R_7。边界路由器 R_7 收到该请求后，通过 PID_2 得知应该将该请求转发给自治系统 C 的边界路由器 R_8。边界路由器 R_8 收到该请求报文后，转发给其本地资源管理器 RM_c。

步骤 4　资源管理器 RM_c 收到请求报文后，查找其内容路由表，得知应该将该请求报文转发给内容提供者 P。内容提供者 P 收到 RM_c 发来的请求报文后，一方面，通过该请求报文中的 SID_1 得知用户 U 需要的内容；另一方面，通过该请求中携带的域间路径标识 PID_2 和 PID_1，得知去往用户 U 的域间路径。

步骤 5　在内容回传阶段，内容提供者 P 将 SID_1 对应内容以分组的形式推送给用户 U，每个分组均携带域间路径标识 PID_2 和 PID_1、用户 U 的节点标识、内容名字 SID_1。具体而言，内容提供者 P 根据域间路径标识 PID_2 可以得到域间路径标识前缀 PX_2，从而得知应该将分组发送给边界路由器 R_8。为了防范数据泄露，边界路由器 R_8 需要根据其维护的请求表进行出域数据的校验，如果合法才进一步转发给边界路由器 R_7。依据上述过程，最终边界路由器 R_1 则将分组发送给用户 U。

3.5　跨域安全保障机制

随着不同体制的网络空间与实体经济相互渗透，保障跨域互联的安全性越发迫切。共生网络架构从两个方面为异构网络融合提供跨域安全保障：攻击数据进不来、隐私数据出不去。具体而言，攻击数据进不来是指未经某个网络允许进入该网的数据，都不能进入该网；隐私数据出不去是指未经某个网络允许发送到网外的数据，都不能被转发到该网络之外。为了实现上述目标，共生网络通过对多维名字空间进行耦合协同，并结合“以拉促推、推拉结合”的跨域通信模式，建立了可靠的跨域安全保障机理，包括基于 PID 耦合生成的跨域攻击防范机制，以及基于多维名字逐包过滤的数据泄露防范机制。

3.5.1　基于 PID 耦合生成的跨域攻击防范机制

共生网络通过基于 PID 耦合生成的跨域攻击防范机制，保障攻击数据进不来。该机制主要涉及两个步骤，分别由资源管理器与边界路由器执行。

首先，在请求报文转发过程中，RM 需要为请求消息生成一个域间路径标识 PID，用于跨域转发。如果某个请求报文携带请求者 NID、SID、PID_0（全 0 表示未携带），资源管理器根据式（1）生成域间路径标识 PID：

$$\mathrm{PID} = \mathrm{PX} + f(\mathrm{NID}, \mathrm{SID}, \mathrm{SN}, \mathrm{PX}, \mathrm{PID}_0) \quad (1)$$

其中，SN 表示该资源管理器 RM 周期性生成的一个私密的随机数 （secret number，SN），函数 $f(\bullet)$ 为单向哈希函数，便于资源管理器 RM 高效地计算。不难发现，式（1）定义的域间路径标识生成方式，将请求的内容、内容请求者、跨域路径对

应的多维名字空间耦合，并通过私密随机数进一步强化了 PID 的难伪造性。

其次，当边界路由器收到分组时，会根据上述域间路径标识的生成机理，校验分组携带域间路径标识的合法性。只有当域间路径标识合法时，才继续转发该分组；否则，丢弃该分组。这样一来，攻击数据因无法伪造 PID 序列被边界路由器丢弃。不难发现，PID 的难伪造性，决定着上述安全机制的效果。实际上，共生网络能够通过动态 PID 机制进一步强化跨域安全保障（详细内容请参见文献[20-22]）。

3.5.2 基于多维名字逐包过滤的数据泄露防范机制

共生网络通过基于多维名字逐包过滤的数据泄露防范机制，保障隐私数据不泄露。该机制中，边界路由器需要维护一个内容请求列表，列表中的每个条目对应一个 SID，负责记录了以下信息。

- 发送该请求的节点 NID：保证该节点请求的内容仅能发送给对应的节点。
- 该请求经过的域间路径标识序列：保证请求的内容仅能根据指定路径发送给对应的节点。
- 内容提供者的节点标识：防止网络内的其他节点通过侦听获取到 U、域间路径标识序列、SID 等信息后，利用这些信息将隐私数据发送到网外。

当边界路由器收到出域数据报文时，需要与上述请求列表对比，对比成功说明该数据报文是针对合法内容请求的响应，才继续向外网转发数据报文。同时，当内容提供者发送完毕相应数据后，向边界路由器发送一个通告消息，让其从请求列表中将相应内容名字对应的条目删除，从而减少请求列表的规模。

3.6 共生网络的系统验证与能力生成

为了验证共生网络的工作机理的正确性和可行性，本文开展了大规模仿真实验，并开发了小规模原型系统。在仿真实验部分，基于 OMNet++ 仿真平台搭建了包含 3 万个网络、20 万个节点的大规模仿真环境，验证了共生网络的路由组织形式、跨域通信机制以及跨域安全保障机理的可行性与正确性。在原型系统方面，针对共生网络的基本工作机制研发了协议软件，并面向共生网络的资源管理器和边界路由器研制了原型设备，构建了支持文件传输、视频传输、Web 浏览等典型应用的原型系统。限于篇幅，共生网络核心设备的性能测试结果可参见文献[16]。下面简要介绍共生网络已经生成的能力。

- 防范跨域攻击能力：在跨域通信机制中，共生网络基于多维名字耦合生成了难以伪造的域间路径标识。只有携带合法域间路径标识的报文才能被边界路由器转发入域，携带非法域间路径标识的数据报文将被边界路由器丢弃，共生网络从而具备了防范跨域攻击的能力。
- 防范数据泄露能力：共生网络架构下，边界路由器负责维护内容请求表，以实现基于多维名字逐包过滤的数据泄露防范机制，能够有效阻止隐私数据在未经授权的情况被泄露到外网。
- 精准实时溯源能力：在共生网络中，请求消息和数据分组均携带域间路径标识序列，使共生网络具备针对单个数据包的精准溯源能力。内容提供者通过将域间路径标识（序列）与域间网络拓扑进行匹配，知晓请求包的来源网络；内容请求者通过将分组中携带的域间路径标识（序列）与域间网络拓扑进行匹配，获得分组的来源网络。基于 20 000 个网络的大规模仿真结果表明，在域间互联关系及其域间路径标识不向全网通告的前提下，基于单个数据包的溯源准确度高达 95%，且所有错误都在最有一跳（域间）；同时，单包溯源的实时性达毫秒级。

- 实时态势感知能力：基于上述精准溯源能力，内容提供者、内容请求者均能够清楚地知晓源自每个网络的数据包数量、去往每个网络的数据包数量等信息，进而获悉了实时的跨域流量态势。
- 精细粒度管控能力：共生网络具有针对内容的精细粒度管控能力。内容提供者可以为每个内容名字指定通告路径，管控该内容对哪些网络可见。另外，基于多维名字逐包过滤的数据泄露防范机制，则管控着哪些内容可以出网。

4　结束语

本文从差异化网络体制并存的现状出发，着重阐述了异构网络融合共生的需求与关键挑战，并介绍了共生网络这种新型网络架构。系统性地对共生网络的多维名字空间、域内域间解耦的路由组织形式、跨域通信模式和跨域安全保障机理进行了详细介绍。异构网络融合共生的架构研究是一项符合国家重大战略需求的基础性研究内容，目前仍面临很多开放问题。未来仍需要结合共生网络架构，进一步探索机动网络和固定网络融合、广域环境域间路径标识前缀分配、动态网络拓扑推断等关键问题。

参考文献：

[1] 朱立东, 张勇, 贾高一. 卫星互联网路由技术现状及展望[J]. 通信学报, 2021, 42(8): 33-42.
ZHU L D, ZHANG Y, JIA G Y. Current status and future prospects of routing technologies for satellite Internet[J]. Journal on Communications, 2021, 42(8): 33-42.

[2] 张更新, 王运峰, 丁晓进, 等. 卫星网络若干关键技术研究[J]. 通信学报, 2021, 42(8): 1-14.
ZHANG G X, WANG Y F, DIGN X J, et al. Research on several key technologies of satellite Internet[J]. Journal on Communications, 2021, 42(8): 1-14.

[3] 卓琨, 张衡阳, 郑博, 等. 无人机自组网研究进展综述[J]. 电信科学, 2015, 31(4): 134-144.
ZHUO K, ZHANG H Y, ZHENG B, et al. Progress of UAV ad hoc network: a survey[J]. Telecommunications Science, 2015, 31(4): 134-144.

[4] 姜胜明. 海洋互联网的战略战术与挑战[J]. 电信科学, 2018, 34(6): 2-8.
JIANG S M. Marine Internet: strategies, tactics and challenges[J]. Telecommunications Science, 2018, 34(6): 2-8.

[5] 王良民, 刘晓龙, 李春晓, 等. 5G 车联网展望[J]. 网络与信息安全学报, 2016, 2(6): 1-12.
WANG L M, LIU X L, LI C X, et al. Overview of Internet of vehicles for 5G[J]. Chinese Journal of Network and Information Security, 2016, 2(6): 1-12.

[6] 王君, 纪晓东, 张欣然, 等. 5G 蜂窝车联网组网性能研究[J]. 电信科学, 2020, 36(1): 49-57.
WANG J, JI X D, ZHANG X R, et al. Performance evaluation of 5G cellular vehicle networks[J]. Telecommunications Science, 2020, 36(1): 49-57.

[7] 蒋林涛. 数据网的现状及发展方向[J]. 电信科学, 2019, 35(8): 2-15.
JIANG L T. Current situation and development trend of data network[J]. Telecommunications Science, 2019, 35(8): 2-15.

[8] 任语铮, 谢人超, 曾诗钦, 等. 工业互联网标识解析体系综述[J]. 通信学报, 2019, 40(11): 138-155.
REN Y Z, XIE R C, ZENG S Q, et al. Survey of identity resolution system in industrial Internet of Things[J]. Journal on Communications, 2019, 40(11): 138-155.

[9] Statistics [EB]. 2022.

[10] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking named content[C]//Proceedings of the 5th international conference on Emerging networking experiments and technologies-CoNEXT '09. New York: ACM Press, 2009: 1-12.

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

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

[13] ZHANG X, YANG Y, XU M W, et al. ASER: scalable distributed routing protocol for LEO satellite networks[C]//Proceedings of 2021 IEEE 46th Conference on Local Computer Networks. Piscataway: IEEE Press, 2021: 65-72.

[14] DARPA Seeks Clean-Slate Ideas for Mobile Ad Hoc Networks (MANETs) [EB]. 2013.

[15] NARAYAN S, ISHRAR S, KUMAR A, et al. Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols[C]//Proceedings of 2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN). Piscataway: IEEE Press, 2016: 1-7.

[16] 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.

[17] 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.

[18] ZHANG M, LUO H B, ZHANG H K. A survey of caching mechanisms in information-centric networking[J]. IEEE Communications Surveys & Tutorials, 2015, 17(3): 1473-1499.

[19] 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.

[20] 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.

[21] 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.

[22] LUO H B, LIU Z B, ZHANG S. Preventing DDoS flooding attacks with cryptographic path identifiers in future Internet[J]. IEEE Transactions on Network and Service Management, PP(99): 1.

[作者简介]

罗洪斌（1977− ），男，博士，北京航空航天大学计算机学院教授、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。

张珊（1989− ），女，博士，北京航空航天大学计算机学院副教授、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、存算传一体化融合架构等。

王志远（1993− ），男，博士，北京航空航天大学计算机学院副教授、硕士生导师，主要研究方向为云网边端资源协同、边缘/云计算、算法博弈论等。