# 共生网络——异构网络安全高效互联的体系结构与机理

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. 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**：介绍了共生网络——一种异构体制网络安全高效互联的体系结构与机理。首先，分析了异构网络互联面临的挑战，凝练出了异构网络互联亟须解决的科学问题。然后，分析和研究了异构网络互联而成网络空间的普适表征机理、体系结构模型、基本工作机理、跨域安全保障机理等。实验结果表明，共生网络已经形成了部分能力，如防范跨域攻击和数据泄露等。最后，介绍了待进一步解决的问题。

**关键词**：异构网络；网络互联；网络体系结构；安全；高效

**中图分类号**：TP393

**文献标志码**：A

**DOI:** 10.11959/j.issn.1000−436x.2022079

# Architecture and mechanisms for secure and efficient internetworking of heterogeneous network

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, 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:** An architecture named CoLoR (coupling service location and inter-domain routing) was introduced to securely and efficiently interconnect networks with different architectures (called heterogeneous networks below). First, the fundamental challenges and scientific problems that have to be addressed by CoLoR were raised. Then, the core aspects of CoLoR were described, including how to characterize and represent the cyberphysical system comprised by heterogeneous networks, the network architecture, the basic communication model and how secure internetworking was achieved. After that, results from prototype implementation were presented to demonstrate the feasibility and capability of CoLoR, including defending against attacks and preventing data leakage. Finally, some open issues were outlined for future studies.

**Keywords:** heterogeneous network, internetworking, network architecture, security, efficiency

## 0 引言

随着通信网络技术的飞速发展，已形成多种网络体制并存的自然趋势。一方面，不同特征的网络形态持续涌现，迫切需要不同的网络体制。具体而言，当前互联网向陆海空天延展、向实体经济渗透，相继形成了车联网、海洋信息网络、无人机集群网络、卫星互联网、工业互联网等各种网络形态。这些网络形态的特征不仅各不相同，而且显著区别于传统以“固定、有线”为主的陆地互联网。例如，海洋信息网络具备水声信道、海面水雾干扰导致的误码率高等特征；无人机集群网络具备节点分割与

**收稿日期**：2022−01−05；**修回日期**：2022−03−22

**通信作者**：张珊, zhangshan18@buaa.edu.cn

**基金项目**：国家重点研发计划基金资助项目（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)

重组、拓扑（强）时变等特征；卫星互联网具备拓扑规律性变化、节点间间歇性连通、链路时延大尺度变化等特征。由于这些特征的存在，将传统陆地互联网中广泛应用的 IP 应用于这些新兴网络形态时，面临性能恶化甚至不可用的问题。事实上，美国 DARPA（Defense Advanced Research Projects Agency）早在 2013 年就指出，若将 IP 应用于移动自组织网络，当节点数量超过 50 个时，网络性能急剧下降，导致网络不可用。为此，DARPA 急于寻求基于非 IP 的移动自组织网络组网方式。

另一方面，随着互联网规模和应用范围持续扩大，其 TCP/IP 网络体制逐步暴露出安全性差、演进难等诸多原始设计缺陷。为了从体系上克服这些缺陷，学术界对新型网络体制的探索从未停止。事实上，斯坦福大学 Cheriton[1]早在 1989 年就提出了 Sirpent；1990 年，麻省理工学院 Clark 和 Tennenhouse[2] 提出了 ALF（application layer framing）。后来，主动网络[3]、Triad[4]、DONA（data-oriented network architecture）[5]、NDN（named data networking）[6-7]、MobilityFirst[8]、XIA（expresive Internet architecture）[9]、FII（future Internet for innovation）[10]、SCION（scalability, control, and isolation）[11]、Trotsky[12]、标识网络[13]等各种网络体制相继涌现；NDN 和 SCION 等已有小规模应用。这些网络体制的提出为多体制网络并存奠定了技术基础。

同时，从互联网长期演进的角度看，采用不同网络体制的异构网络必然长期共存。首先，当前已然形成 IPv4、IPv6、NDN、SCION、标识网络等共存的局面。其次，网络体制的演进，必然意味着从一个已有网络体制演进到一个新网络体制，而网络体制的演进是一个长期过程；事实上，IPv4 向 IPv6 演进已历时 20 余年，但据 Google 统计，全球 IPv6 流量仅占所有流量的 35.53%（截至 2021 年 12 月 6 日）。最后，随着各种网络形态日趋异构化，没有一个网络体制能适应所有网络形态；相反，只有根据每种网络形态的特点为其设计合适的网络体制，才能充分发挥该网络形态的优势[14]。

随着数据成为生产要素，不同体制的异构网络只有通过安全高效互联、打通数据流动通道，才能释放数据价值。然而，目前仍缺乏异构体制网络之间安全高效互联的体系和机理。虽然可以通过协议转换的方式实现异构体制网络之间的互联互通，但是协议转换不仅效率低下，而且难以保障安全[15]。类似地，尽管 FII、Trotsky、ALF 等能够支持异构体制网络的互联互通，但是难以保障安全。

为此，本文介绍共生网络——异构网络安全高效互联的体系结构与机理。首先，分析异构体制网络安全高效互联面临的挑战与科学问题。然后，分析和研究异构体制网络互联而成网络空间的普适表征机理、体系结构模型、基本工作机理、跨域安全保障机理等。在此基础上，介绍共生网络的部分系统实验结果和共生网络已经形成的部分能力，如防范跨域攻击和数据泄露等。最后，介绍共生网络中还需进一步解决的问题。

## 1　挑战与科学问题

本节分析异构体制网络安全高效互联面临的主要挑战和亟须解决的本质科学问题。

### 1.1　主要挑战

建立异构体制网络安全高效互联的体系与机理，面临以下主要挑战。

1) 体制异构性挑战。由于不同网络体制在名字空间、路由机制、寻址方式、分组格式等方面存在巨大差异，一种网络体制的分组无法直接在采用另一种体制的网络里转发。目前的通用做法是在边界网关处进行协议转换，但存在至少三大缺点。第一，协议转换效率低、跨域安全性难以保障。第二，负责协议转换的网关同时连接 2 个（甚至多个）异构体制的网络，使协议转换出现错误甚至恶意转换时难以追责。第三，当一种网络体制的原始分组通过协议转换成另一种网络体制的新分组时，新分组通常不能完整准确地反映原始分组的语义，导致语义损失，尤其是当分组跨越多个异构体制的网络时，多次协议转换会导致严重的语义损失，甚至影响正常通信。

2) 安全保障挑战。随着互联网向实体经济渗透，网络和数据安全日益重要。采用不同体制的异构网络需要在互联的同时，既能防范来自其他网络的攻击，又能有效防止网络内部的数据被泄露。例如，对于一个工厂的网络，其既希望与其他网络互联从而提高生产效率，又不希望遭受来自外网的网络攻击，同时也需要保障数据安全，防止数据被非法泄露到外网，影响企业安全与发展。

3) 信息高效分发挑战。众多异构体制网络互联

的根本目的在于高效实时共享/分发数据，促进数据流通，释放数据价值，但如何充分利用各种数据传输通道、减少重复传输、提高数据传输效率面临挑战。

4) 可扩展性挑战。一方面，众多异构网络互联之后，每个网络原有的规模可扩展性应不受影响；同时，互联体系要能够支持数十万、数百万甚至数千万异构的固定和移动网络安全高效互联。

5) 普适性挑战。互联体系既要能够互联已有的异构体制网络，又要能够互联未来采用新体制的网络；同时，互联体系要允许现在采用某种体制的网络未来升级成另一种新体制。此外，互联体系既要能够支持固定网络间的互联，又要能够支持固定网络和移动网络间的互联，还要能够支持移动网络间的互联。

### 1.2 本质科学问题

为了克服上述主要挑战，必须解决以下2个相互关联的本质科学问题。

**科学问题 1** 异构网络互联而成的网络空间的普适表征问题。对事物进行科学表征是正确认识事物的重要手段（甚至是基础与前提）。对异构体制网络互联而成的网络空间而言，不同网络体制在名字空间及其基础上的路由机制、寻址方式等方面存在巨大差异。例如，IPv4网络采用32 bit的IPv4地址，IPv6网络采用128 bit的IPv6地址，NDN采用内容名字。当众多异构体制网络互联时，应该用哪些名字空间对互联而成的网络空间进行普适化表征？显然，由于网络体制的差异性，不可能用单一名字空间表征互联而成的网络空间，而必须采用多维名字空间。其难点在于，究竟应该采用哪些维度的名字空间。如果名字空间的维度太多，不同维度名字空间之间的映射可能会变得十分复杂而使效率低下；反之，又难以满足安全高效互联的需求。对每一个维度的名字空间该如何命名与表征，才能既实现高效互联，又能保障网络的安全和规模可扩展性？

**科学问题 2** 多维名字空间的协同与耦合问题。虽然每个网络可以用其路由、寻址和转发等方式，完成数据在该网络内部的传递，但当2个网络采用的体制不同时，如何充分利用各种网络的分组投递功能，同时克服不同网络内部的潜在安全缺陷，实现数据的跨域传递并保障跨域互联安全？这又包含如何发现跨域资源、如何确定数据的跨域投递路径、如何实现分组高效跨域转发、如何认证节点合法性、如何防范跨域攻击和数据泄露、如何快速精准溯源等诸多问题。显然，解决上述诸多问题需要多维名字空间之间进行分工、协作甚至耦合，才能克服前述主要挑战，实现异构体制网络的安全高效互联。其难点在于，解决上述每个问题各自需要哪些名字空间（即如何分工和协作），这些名字空间能否复用，如何复用（即协同与耦合）？

## 2 共生网络

本节介绍共生网络——一种实现异构体制网络安全高效互联的体系结构与机理。针对科学问题1，提出共生网络对异构体制网络互联而成网络空间的普适表征机理。针对科学问题2，基于前述普适表征机理，给出共生网络的体系结构模型，建立共生网络的基本工作机理和共生网络的跨域安全保障机理。

### 2.1 普适表征机理

如前所述，必须采用多维名字空间对异构网络互联而成的网络空间进行普适化表征。然而，随着互联网发展成为网络空间，互联网涉及经济、社会等众多维度，为普适化表征带来巨大挑战。因此，必须抓住互联网最本质的特征。虽然社会上广泛认为互联网最本质的特征是提供“连接”，但近年来学术界逐步认识到，互联网最本质的特征是传递信息，而提供连接仅仅是手段。相应地，产业界提出了众多以信息为中心的网络体系架构[6-8]。

本文团队通过长期深入研究发现，传递信息是互联网（或者网络空间）的功能本质，涉及以下5个相互独立的自然属性：① 传什么（即内容属性），② 传给谁（即身份属性），③传到哪（即位置属性），④怎么传（即手段属性），⑤何时传（即时间属性）。由于网络空间的信息传递绝大多数情况下是即时的，且已有对时间的普适表征方法（即年、月、日、时、分、秒），后文不再单独考虑时间属性，而是在共生网络的工作机理、安全保障机理中利用时间属性。

根据上述自然属性，共生网络利用以下4个名字空间对异构网络互联而成的网络空间进行普适化表征：内容名字，即SID（service identifier），用于表征传什么；节点标识（NID, node identifier），用于表征传给谁；各类地址（address），用于表征

传到哪；路径标识（PID, path identifier），用于表征怎么传。

#### 2.1.1 内容名字

内容名字由两部分构成。当一个节点要跨网提供一个内容时，该内容的名字 SID 为 NID+*N*，其中，NID 为该节点的节点标识；*N* 为该节点为该内容生成的唯一标识，对静态内容而言，*N* 为内容的哈希，对动态内容或者服务而言，*N* 由节点 NID 指定。采用这种层次化的内容名字，便于网络间通告内容名字时进行内容名字的聚合（类似 IP 前缀聚合），从而保障网络的规模可扩展性。

#### 2.1.2 节点标识

尽管每个网络可以用各自的方式描述节点身份，共生网络采用层次化、具备自证明特征的节点标识，既便于聚合保障网络的规模可扩展性，又便于进行安全认证。具体而言，对每一个需要进行跨域通信的节点，其节点标识由两部分构成：网络部分和自证明部分。网络部分代表节点在哪个网络，由 IANA（Internet assigned numbers authority）分配，网络部分的长度为 32 bit，便于与现有互联网兼容。自证明部分由一个公钥/私钥对生成，是公钥的 128 bit 哈希值，私钥则由该节点保管而不向外通告，一个节点的自证明部分由该节点自身生成，并通过所在网络保证唯一性，出现冲突时则重新生成。

#### 2.1.3 各类地址

每种网络体制可以有自己的地址，如 IPv4、IPv6、地理坐标等，便于根据网络特点在网内进行分组转发，从而充分发挥该网络的优势。这样，共生网络可以兼容现有的 IPv4、IPv6 等网络体制，从而实现各种不同网络的共生融合。

#### 2.1.4 路径标识

共生网络的核心目的是利用各种异构体制网络，完成网络之间的信息传递。由于这些网络有的采用分组交换，有的采用电路交换，因而共生网络采用分组交换的方式跨域传递信息。与 IPv6 试图替代 IPv4 不同，共生网络旨在利用已有的各种网络进行分组转发。分组在跨越某种体制的网络时，可以在相应入口路由器处封装上该网络体制的报头，然后用该报头将分组转发到相应的出口路由器，最后由出口路由器将相应报头解封，并转发给下一个网络（类似 IP 分组跨越数据链路层异构的网络）。因此，共生网络重点关注异构网络之间的分组转发。

异构网络之间的互联方式繁多，2 个网络既有可能利用光纤直连，也有可能利用 IP 隧道连接，或者通过交换中心，如 IXP（Internet exchange point）连接，还有可能通过无线连接。同时，2 个网络之间的连接通道也可能不是一条，而是多条；即使只有一条通道，该通道中 2 个网络的端点也可能随着时间变化（如通过无线连接时，节点移动会导致通道的端点变化）。因此，共生网络不关注某种具体的连接方式，而是对这些连接方式进行统一抽象。

本质上，随着互联网发展成为网络空间，网络间的互联关系逐渐演变成人类社会关系在网络空间的投射，即网络间根据社会（商业）关系建立域间路径，而连接方式是实现这种社会关系的具体手段。相应地，给定 2 个网络间的连接关系，其连接方式可以多种多样。因此，共生网络对网络间的域间路径（代表社会关系）进行命名。具体而言，共生网络为每条域间路径分配一个域间路径标识前缀 PX。假定域间路径标识的长度为 $L$ bit，路径标识前缀 PX 的长度为 $l$ bit，则 PX 代表 $2^{L-l}$ 个连续的域间路径标识，其中第一个域间路径标识能够被 $2^{L-l}$ 整除。例如，设 $L=32$，$l=24$，则路径标识前缀 192.168.10.0/24 代表了 192.168.10.0, 192.168.10.1, …, 192.168.10.255 共 256 个连续的域间路径标识。

由于域间路径的数量众多，共生网络按照“正交复用”的原则为域间路径分配域间路径标识前缀。给定 2 个网络 A 和 B，以及 A 和 B 间的一条域间路径 $P_0$，此外分别有 $M$ 和 $N$ 条域间路径。记 A、B 与所有相邻网络的域间路径集合分别为

$$P(\mathrm{A})=\{P_0,P_1(\mathrm{A}),P_2(\mathrm{A}),\cdots,P_M(\mathrm{A})\} \tag{1}$$

$$P(\mathrm{B})=\{P_0,P_1(\mathrm{B}),P_2(\mathrm{B}),\cdots,P_N(\mathrm{B})\} \tag{2}$$

记 $\mathrm{PX}_j(Y)$为域间路径 $P_j(Y)$的域间路径标识前缀，其中 $Y$ 代表 A 或 B，$j$=1,2,…,max($M$, $N$)，路径标识前缀的分配如图 1 所示。正交分配是指任意给定 $j\neq 0$，$\mathrm{PX}_j(Y)$与 $\mathrm{PX}_0$ 没有交集，即没有相同的域间路径标识。然而，在满足正交分配的原则下，$\mathrm{PX}_0$ 可以被网络中的多条域间路径复用，从而避免集中分配域间路径标识，既降低分配域间路径标识的复杂性，又防止垄断。例如，$\mathrm{PX}_0$ 可以同时分配给图 1 中虚线示意的两条域间路径。

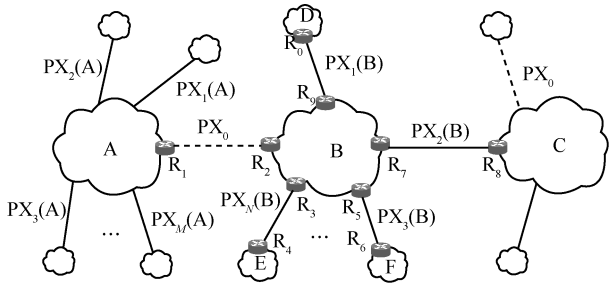



图 1　路径标识前缀的分配

## 2.2　共生网络的体系结构模型

TCP/IP 网络体系结构模型和共生网络体系结构模型如图 2 所示。如前所述，共生网络旨在通过各种体制异构网络的跨域安全互联，实现信息的跨域传递。因此，共生网络的物理层、数据链路层与已有网络体制类似。在网络层，共生网络在充分利用 IPv4、IPv6 等各种网络体制的同时，引入域间 PID 进行跨域分组转发。在网络层之上，共生网络抓住网络传递信息的功能本质，引入内容路由层，通过内容名字 SID 进行跨域互联，从而屏蔽各种网络体制的差异。需要指出的是，根据部分网络的特点，内容路由层可以直接运行在数据链路层之上，而不是必须运行在网络层之上。最上层是应用层，与内容名字（而非 IP 地址）绑定。


（a）TCP/IP网络体系结构模型　　（b）共生网络体系结构模型

图 2　TCP/IP 网络体系结构模型和共生网络体系结构模型

与 TCP/IP 网络体系结构模型相比，共生网络体系结构模型没有显式的传输层。然而，这并不代表共生网络不需要传输协议；相反，本文认为应该有各种传输协议组成的协议库，供各种应用根据需要调用，从而鼓励各种传输协议的创新与应用。当然，某些应用也可以不调用协议库中的传输协议，而是将拥塞控制等功能内嵌到应用中，类似 Chrome 内嵌 QUIC（quick UDP Internet connection）。

## 2.3　共生网络的基本工作机理

共生网络的基本工作机理包含三方面：域内域间解耦的路由组织模式、内容名字驱动的跨域互联模式、“以拉促推、推拉结合”的跨域通信模式，分别介绍如下。

### 2.3.1　域内域间解耦的路由组织模式

由于不同体制网络采用的名字空间、分组格式、分组转发方式等存在差异，共生网络严格区分域内和域间路由。域内路由根据每个网络采用的网络体制确定；相应地，每个网络内部的分组转发方式也由其采用的网络体制确定。

相反，共生网络用域间路径标识进行跨域分组转发。为此，每个网络的边界路由器需要维护一个域间路由表，其中的一个路由表项对应一个域间路径标识前缀。该表项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。例如，图 1 中边界路由器 $R_2$ 的域间路由表如表 1 所示；其中设网络 B 采用 IPv4，且网络 A 的边界路由器 $R_1$ 和网络 B 的边界路由器 $R_2$ 之间使用多协议标签交换（MPLS, multi-protocol label switching）。表 1 中的第一行对应域间路径标识前缀 $PX_0$ 的表项，记录了该前缀对应的域间路径（即 $R_1$～$R_2$）连接的是网络 A，去往 A 的下一跳节点是 $R_1$，且通过封装 MPLS 报头可将分组从边界路由器 $R_2$ 发给 $R_1$。类似地，表 1 中的第二行对应域间路径标识前缀 $PX_1$(B)的表项，记录了该前缀对应的域间路径（即 $R_0$～$R_9$）连接的是网络 D，去往 D 的下一跳节点是边界路由器 $R_9$，且通过封装 IPv4 报头可将分组从边界路由器 $R_2$ 发给 $R_9$。

**表 1　　路由器 $R_2$ 的域间路由表**

| PID 前缀 | 邻域 | 下一跳节点 | 通信方式 |
|---|---|---|---|
| $PX_0$ | A | $R_1$ | MPLS |
| $PX_1$(B) | D | $R_9$ | IPv4 |
| $PX_2$(B) | C | $R_7$ | IPv4 |
| $PX_3$(B) | F | $R_5$ | IPv4 |
| ⋮ | ⋮ | ⋮ | ⋮ |
| $PX_N$(B) | E | $R_3$ | IPv4 |

当边界路由器收到（携带域间路径标识）的分组时，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。例如，当图 1 中的边界路由器 $R_2$ 收到一个携带域间路径标识 PID（属于 $PX_0$）的分组时，$R_2$ 通过查找其域间路由表可知，应该将该分组发送给网络 A 的边界路由器 $R_1$；类似地，当 $R_2$ 收到一个携带域间路径标识 PID（属于 $PX_1$(B)）的分组时，$R_2$ 通过查找其域间路由表，可知应该将该分组发送给网络 B 的边界路由器 $R_9$。这里需要说明以下几点。

1) 2.1 节所述域间路径标识的正交分配原则，保证了每个域间路径标识在某个给定边界路由器最多只能匹配一个路由表项，使边界路由器可以利用精确匹配（而不是最长前缀匹配）进行路由表的查找，从而提高查表效率。

2) 由于每个网络的邻域数量较少，边界路由器所维护域间路由表的规模较小，从而保障了共生网络跨域互联的规模可扩展性。事实上，截至 2021 年 12 月 14 日，互联网中一个自治系统（AS, autonomous system）的邻域数量最多为 9 259 个。即使 2 个邻域之间有 4 条域间路径，共生网络中域间路由表的规模也不到 4 万条。与此对比，现有互联网核心网路由表中的路由条目已超过 93 万条，是共生网络域间路由表规模的 23 倍。由于存储小规模路由表所需的三态内容寻址存储器（TCAM, ternary content addressable memory）更小，且 TCAM 能耗极高，因此共生网络边界路由器的能耗将低于 IP 路由器。

3) 由于 2 个网络之间的域间路径数量由它们之间的社会关系确定，这使 2 个网络之间的连接关系相对稳定，因而共生网络中的边界路由器不会频繁更新域间路由表，具有更好的路由稳定性。相反，IPv4 核心网路由器的路由表频繁更新，例如 2021 年 12 月 2 日 BGP（border gateway protocol）的峰值更新速率高达 7 899 前缀/秒，均值也高达 18.19 前缀/秒。

4) 为每条域间路径分配一个域间路径标识前缀（而不是一个固定的域间路径标识），使共生网络可以利用内容名字、节点标识等信息，耦合生成域间路径标识，从而实现安全的跨域互联。

从上面的描述可以看出，通过将域内域间路由解耦，并用域间路径标识转发跨域分组，共生网络能够支持各种异构网络的融合共生。同时，一个网络所用网络体制的更新换代，不会影响其他网络，也不需要其他网络的协同。因此，共生网络不仅具备很好的普适性，而且可以鼓励网络体制的创新与应用。

### 2.3.2　内容名字驱动的跨域互联模式

如前所述，尽管不同网络体制采用的名字空间、分组格式等不同，但它们的功能本质相同，即传递信息。因此，共生网络为网络中的信息（或内容）命名，并在网络间通告内容名字的可达性，屏蔽网络异构性的同时实现跨域互联。

由于网络体制不同，且不希望改变每个网络体制的既有工作方式，使共生网络不能像 IP 或者 NDN 那样，在每个路由器通告内容名字的可达性（虽然新网络可以尝试这样做）。因此，共生网络在每个网络部署一个逻辑上集中但可分布式实现的资源管理器（RM, resource manager），以层叠的方式在该网络运行。每个资源管理器维护一个内容路由表，记录内容名字的可达性。内容路由表中的每个路由条目对应一个内容名字（前缀），记录去往相应内容提供者的下一跳节点，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等信息如表 2 所示。

**表 2　资源管理器 $RM_b$ 维护的内容路由表**

| SID(前缀) | 下一跳节点 | 下一跳网络 | PID 前缀 |
|---|---|---|---|
| $SID_1$ | $R_7$ | C | $PX_2(B)$ |
| $SID_2$ | $R_7$ | C | $PX_2(B)$ |
| $SID_3$ | $R_9$ | D | $PX_1(B)$ |
| ⋮ | ⋮ | ⋮ | ⋮ |

当一个内容提供者要将某个内容向其他网络提供时，该内容提供者首先向其本地资源管理器通告相应内容名字。内容名字（前缀）通告如图 3 所示，当内容提供者 $S_2$ 有名为 $SID_1$ 和 $SID_2$ 的内容要向外提供时，其先将 $SID_1$ 和 $SID_2$ 通告给本地资源管理器 $RM_c$。本地资源管理器收到该内容名字通告后，首先检查其内容路由表中是否记录有相应内容名字的表项。如果有，则检查内容提供者与表项中记录的内容提供者是否相同；如果相同，则更新相应条目的 TTL（time to live）值。如果内容路由表中没有记录相应的内容名字，或者记录的下一跳节点与通告消息中的内容提供者不同，则为该内容名字增加一个表项，表项中的下一跳节点为发送该内容名字通告的节点，下一跳网络和 PID 前缀为空。之后，本地资源管理器根据策略将该内容名字通告消息发送给邻域；如图 3 所示，$RM_c$ 将通告消息发送给 $RM_b$。

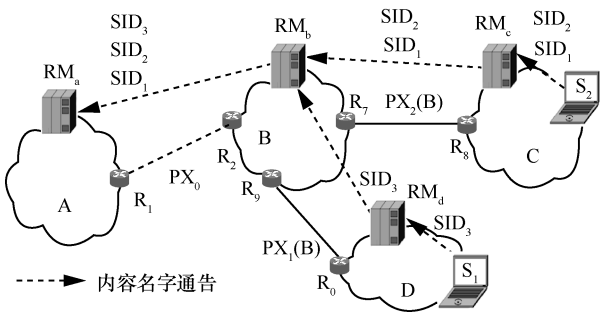



图 3　内容名字（前缀）通告

需要注意的是，资源管理器在将内容名字通告消息发送给邻域之前，需将资源管理器所在网络和邻域之间的域间路径标识前缀添加到内容名字通告消息中。这样，资源管理器所在网络的边界路由器可以根据该域间路径标识前缀将该通告消息发送给邻域；同时，邻域的资源管理器收到该内容名字通告消息后，也可以知道该内容名字通告消息来自哪个网络。

当资源管理器收到从邻域发来的内容名字通告消息时，检查其内容路由表中是否记录有相同内容名字的表项。如果有，则检查表项中的下一跳网络是否与内容名字通告消息中携带域间路径标识前缀对应的邻域相同；如果相同，则更新相应条目的 TTL 值。如果内容路由表中没有记录相应的内容名字，或者记录的下一跳网络与内容名字通告消息中对应的网络不同，则为该内容名字增加一个表项，表项中的域间路径标识前缀通告消息中携带域间路径标识前缀，下一跳网络为该域间路径标识前缀对应的邻域。例如图 3 中，当资源管理器 $RM_b$ 接收到从邻域 C 发来的内容名字通告消息时，则将内容名字 $SID_1$ 和 $SID_2$ 加入其内容路由表，如表 2 中第一行和第二行所示。此后，资源管理器根据策略，将该通告消息发送给邻域。

需要指出的是，由于内容名字的层次化设计，资源管理器可以对邻域通告的内容名字进行聚合。例如表 2 中，当 $SID_1$ 和 $SID_2$ 中的 NID 部分相同时，$RM_b$ 可以将这 2 个表项聚合成一个只包含 NID 的表项。通过聚合，可以减少内容路由表的条目数量和内容名字通告数量，保障网络的规模可扩展性。

### 2.3.3 “以拉促推、推拉结合”的跨域通信模式

IP 采用“推”的通信模式，网络中一个节点可以向任意节点主动推送任意数量的分组，可能会导致网络攻击泛滥[16]。NDN 颠覆了 IP 推的通信模式，采取“拉”的通信模式[7]；但是 NDN 中的每个请求只能返回一个数据分组，导致请求分组数量太多。因此，共生网络采用“以拉促推、推拉结合”的跨域通信模式。共生网络的通信模式如图 4 所示，当一个用户 U 需要获取某个内容时，向其本地资源管理器（图 4 中 $RM_a$）发送一个请求消息；该请求消息包含所需内容的内容名字（如 $SID_1$）、请求者 U 的节点标识等信息。当本地资源管理器 $RM_a$ 收到该请求消息时，查询其内容路由表，得知应该将该请求消息发送给邻域 B，且去往邻域 B 的下一跳为边界路由器 $R_1$，$R_1$ 与邻域 B 间的域间路径标识前缀为 $PX_0$。此时，资源管理器 $RM_a$ 用式(3)为该请求消息计算一个域间路径标识 $PID_1$（属于路径标识前缀 $PX_0$），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 $R_2$。

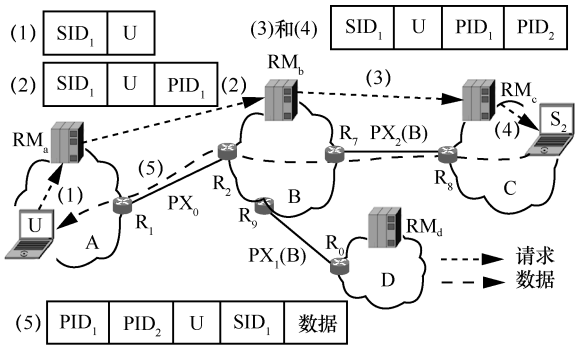



图 4 共生网络的通信模式

当边界路由器 $R_2$ 收到该请求消息后，将该请求消息转发给其本地资源管理器 $RM_b$。资源管理器 $RM_b$ 收到请求消息后，查找其内容路由表，得知应该将该请求消息发送给邻域 C，且去往邻域 C 的下一跳为边界路由器 $R_7$，$R_7$ 与邻域 C 间的域间路径标识前缀为 $PX_2(B)$。类似地，资源管理器 $RM_b$ 为该请求消息计算一个域间路径标识 $PID_2$（属于路径标识前缀 $PX_2(B)$），然后将 $PID_2$ 添加在请求消息的尾部，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邻域 C 的边界路由器 $R_8$。

当边界路由器 $R_8$ 收到该请求消息后，将该请求消息转发给其本地资源管理器 $RM_c$。资源管理器 $RM_c$ 收到请求消息后，查找其内容路由表，得知应该将该请求消息发送给内容提供者 $S_2$。内容提供者 $S_2$ 收到 $RM_c$ 发来的请求消息时，通过请求消息中的 $SID_1$，得知用户 U 需要的内容；通过请求消息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。此时，内容提供者 $S_2$ 将 $SID_1$ 对应内容以分组的形式推送给用户 U，其中每个分组都应携带域间路径标识 $PID_2$ 和 $PID_1$，用户 U 的节点标识以及 $SID_1$。

事实上，内容提供者 $S_2$ 根据域间路径标识 $PID_2$，可知应该将分组发送给边界路由器 $R_8$；而 $R_8$ 根据域间路径标识 $PID_2$，可知应该将分组发送给边界路由器 $R_7$。边界路由器 $R_7$ 收到分组后，首先

用式(3)校验 $PID_2$ 的合法性，若 $PID_2$ 非法，边界路由器 $R_7$ 直接丢弃该分组，否则边界路由器 $R_7$ 根据域间路径标识 $PID_1$，可知应该将分组发送给边界路由器 $R_2$；而 $R_2$ 根据域间路径标识 $PID_1$，可知应该将分组发送给边界路由器 $R_1$。若 $PID_1$ 合法，边界路由器 $R_1$ 则将分组发送给用户 U。

需要指出三点。首先，请求消息在从用户 U 转发到内容提供者的过程中，会收集沿途各个网络的最大传输单元（MTU, maximum transmission unit），从而便于内容提供者封装合适大小的分组。其次，内容提供者在向用户 U 推送分组的过程中，涉及拥塞控制等。最后，内容提供者可以对用户分组进行加密传输。

### 2.4　共生网络的跨域安全保障机理

随着互联网与实体经济深度融合，众多网络在互联互通的同时，迫切需要保障跨域互联安全，包含 2 个主要方面：攻击数据进不来，隐私数据出不去。攻击数据进不来，意味着凡是未经某个网络允许进入该网络的数据，都不能进入该网络；隐私数据出不去，意味着凡是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，共生网络基于前述基本工作机理，通过将多维名字空间的耦合与协同，建立了跨域安全保障机理。

#### 2.4.1　基于路径标识耦合生成的跨域攻击防范机理

如前所述，每个网络的资源管理器在通过某条域间路径（对应域间路径标识前缀 PX）向邻域转发跨域请求消息时，会为该请求消息生成一个域间路径标识 PID[17]。假设一个请求消息携带的内容名字为 SID，请求者的节点标识为 NID，该请求消息携带的域间路径标识为 $PID_0$（若未携带，则 $PID_0$=0）。该资源管理器所在网络周期性生成一个私密的随机数（SN, secret number），并按照式(3)生成域间路径标识 PID。

$$\text{PID} = \text{PX}\ (l\ \text{bit}) \,||\, \text{HMAC}\ (L-l\ \text{bit}) \tag{3}$$

其中，||为连接运算符，将 $l$ bit 的 PX 与 $L-l$ bit 的 HMAC 连接成 $L$ bit 的域间路径标识 PID；HMAC 按照式(4)耦合生成。

$$\text{HMAC} = f(\text{NID}, \text{SID}, \text{SN}, \text{PX}, \text{PID}_0) \tag{4}$$

在实际实现时，$f$ (•)为单向散列函数，既便于资源管理器高效计算，又难以被其他节点伪造（因为不知道 SN）[18]。当该资源管理器的边界路由器收到一个分组时，根据上述域间路径标识的生成机理，校验分组中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。同时，边界路由器还可以维护一个计数器，记录从邻域发来的携带非法域间路径标识的分组数量。如果没有攻击行为发生，则域间路径标识不会出错。这是因为虽然信道有误码率，但考虑到数据链路层纠错，则域间路径标识不会出错。相反，即使有攻击行为，也可以被快速检测，且攻击数据分组在边界路由器处被丢弃而不能进入网络。

同样，这里需要指出两点。首先，由于域间路径标识的空间有限，攻击者可以低速率猜测某个网络用于计算域间路径标识的 SN；因此，每个网络应该周期性改变 SN。但是，当 SN 改变后，上一周期生成的域间路径标识不能用当前周期的 SN 进行校验。为此，边界路由器需要用 2 个周期的 SN 分别校验域间路径标识；只要其中一个可以得到合法的域间路径标识，即可放行分组。其次，式(4)中计算 HMAC 时，使用了上一跳域间路径标识 $PID_0$，从而将请求消息和分组经过的所有域间路径“链接”起来，使攻击者更难伪造合法的域间路径标识。

#### 2.4.2　基于多维名字逐分组过滤的数据泄露防范机理

为了实现隐私数据出不去，内容提供者所在网络的资源管理器和边界路由器基于多维名字空间，对出网数据分组进行逐分组过滤。为此，边界路由器维护一个请求列表；该列表中的每一个条目对应一个内容名字，记录了以下信息。

1) 发送该请求的用户（图 4 中 U），保证数据仅能发送给对应的用户。

2) 该请求经过的域间路径标识序列（图 4 中的 $PID_1$ 和 $PID_2$），保证数据仅能根据指定路径发送给对应的用户。

3) 内容提供者的节点标识（图 4 中的 $S_2$），防止网络内的其他节点通过侦听获取 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。

共生网络中基于多维名字逐分组过滤的数据泄露防范机理如图 5 所示。当边界路由器收到请求消息后，将该请求消息转发给其本地资源管理器，如图 5 中(1)所示。资源管理器查询其内容路由表，如果未能找到请求消息中携带内容名字对应的条目，则将该请求消息作为异常信息甚至请求分组攻击告警；如果找到对应的条目，则向边界路由器发送通告，将内容提供者的节点标识发送给边界路由器，

如图 5 中(2)所示。同时，资源管理器向内容提供者转发该请求消息，如图 5 中(3)所示。边界路由器收到该通告后，在请求列表中为请求的内容名字增加一个条目。当内容提供者收到请求消息后，将相应内容以分组形式经边界路由器发送给内容请求者，如图 5 中(4)所示。边界路由器收到分组后，查询其请求列表，并将分组中携带信息与表中记录的信息进行比对。只有比对成功，才向外网转发该分组。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，从而减少请求表的规模，如图 5 中(5)所示。

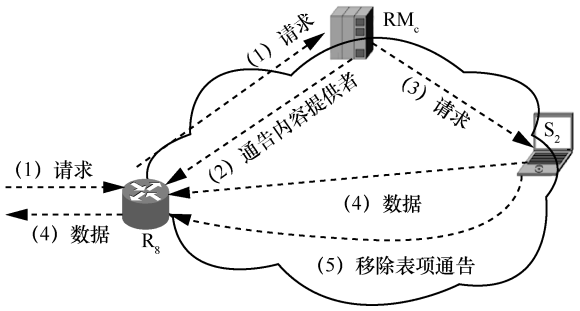



图 5 数据泄露防范机理

需要指出的是，上述数据泄露防范机理仅从网络的角度进行考虑，若上层应用被敌手控制并利用共生网络的合法通信流程，将数据编码在合法数据中传给网外，则是共生网络解决不了的。因此，保障应用本身的安全，在共生网络中依然十分重要。不过，只要将边界路由器的请求表作为日志进行记录，即可追踪数据在何时、从哪个节点、沿什么路径、被泄露到了哪里，从而便于威慑和发现数据泄露者。

## 3 系统验证与能力生成

本文开展了大规模仿真，研发了协议软件，研制了原型设备，构建了原型系统，对共生网络的上述工作机制和机理的可行性与正确性进行了验证。下面介绍原型系统的部分实验结果和目前已经生成的部分能力。

### 3.1 原型系统的实验结果

本文从大规模仿真和小规模原型系统实验 2 个方面，对共生网络的基本工作机制和跨域安全保障机理等进行了验证。首先，基于 OMNet++仿真软件，构建了包含 3 万个网络(含 IPv4 网络、IPv6 网络、NDN、基于路径标识和内容名字进行转发的网络[19-20])、20 万个节点的大规模仿真环境，验证了共生网络基本工作机制和跨域安全保障机理的可行性与正确性[21]。其次，研发了协议软件，研制了原型设备，构建了如图 6 所示的原型系统，开发了文件传输、视频传输、Web 浏览等典型应用，验证了共生网络的实用性，并成功验证了共生网络的跨域攻击防范和数据泄露防范能力[22]。限于篇幅，本文仅给出边界路由器和资源管理器等共生网络核心设备的性能测试结果。

#### 3.1.1 边界路由器的性能测试结果

边界路由器性能测试采用两台 Dell PowerEdge R740 服务器，服务器 CPU 型号为 Intel(R) Xeon(R)

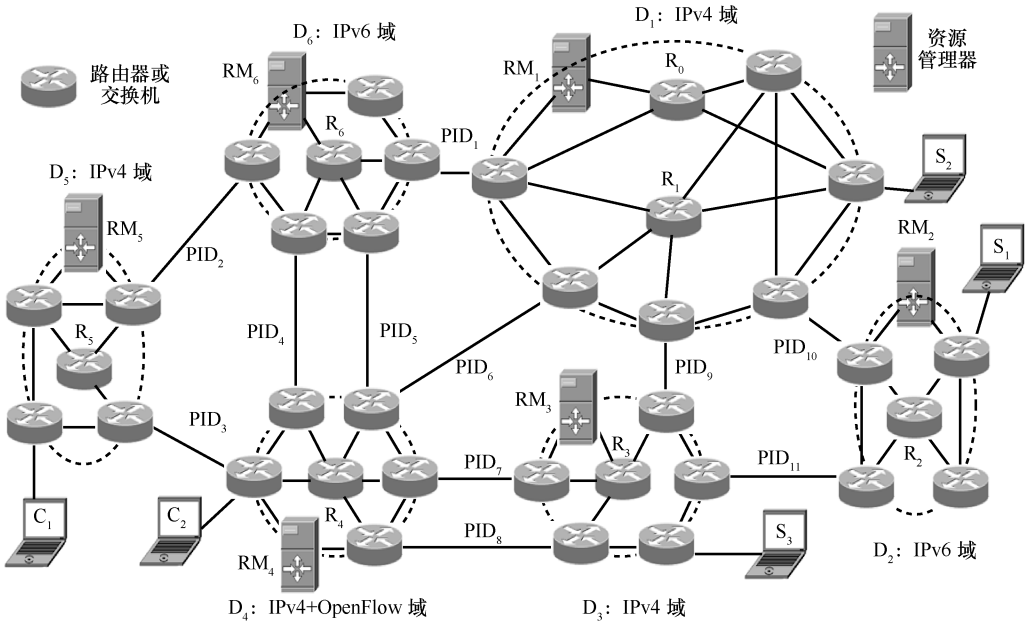



图 6 原型系统

Gold 5218，操作系统为 Ubuntu 16.04，DPDK 版本为 17.11.10，网卡型号为 Intel(R) Ethernet Converged Network Adapter XL710-Q2，具有 2 个 40 Gbit/s 端口。在一台服务器上运行边界路由器程序，另一台服务器上运行发包软件，两台服务器的 2 个网口分别通过两根光纤直连，由发包软件向边界路由器发送数据分组并统计边界路由器的转发速率。

当数据分组总长度为 1 108 B、边界路由器维护的域间路由表表项数量为 100 时，边界路由器转发数据分组的性能测试结果如图 7 所示。

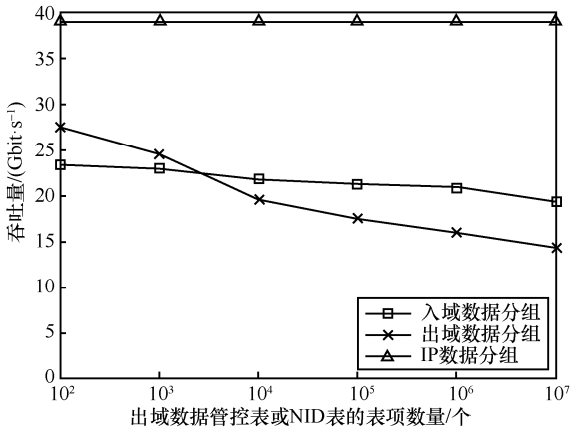



图 7 边界路由器转发数据分组的性能测试结果

从图 7 可以看出，边界路由器目前每秒可以处理 19.4～23.4 Gbit/s 的入网流量，对应 219 万～264 万分组。需要指出的是，随着表项数量的增加，路由器能够处理的入域数据分组流量仅略有降低。这主要是因为路由表查找采用精确匹配，且式(3)用的哈希算法跟路由表大小无关[23]。边界路由器目前每秒可以处理 14.5～27.3 Gbit/s 的出网流量，对应 164 万～308 万分组。同时，随着出网数据对应内容名字的增加，路由器处理的出网数据流量逐步下降。这主要是因为，为了防止数据泄露并对数据的流向进行精细粒度管控，数据源所在网络的边界路由器在转发出网分组时，不仅需要查找分组中携带的 SID 是否在出域数据管控表中，而且要将该分组中携带的域间路径标识序列与表中记录的序列进行比对。IP 流量可以充分利用 40 Gbit/s 的带宽，这主要是因为 IP 仅做尽力而为的分组转发，而不做哈希校验等安全操作。

#### 3.1.2 资源管理器的性能测试结果

资源管理器的性能测试环境与上述边界路由器相同。表 3 给出了资源管理器在不同情形下转发请求包的性能测试结果[24-25]。结果显示，当资源管理器不为请求包耦合计算域间路径标识时（第一行和第三行），目前每秒能够转发超过 300 万个请求；而耦合计算域间路径标识时（第二行和第四行），资源管理器目前每秒只能转发 100 万个左右的请求。需要说明的是，上述结果是单核处理场景；若采用多核处理，可以提升转发性能。同时，当用户需求太大时，可以采用分布式处理。

**表 3　资源管理器在不同情形下转发请求包的性能测试结果**

| 情形 | 测试结果/(万个·秒$^{-1}$) |
|---|---|
| 请求分组来自域内，发往域内 | 352.6 |
| 请求分组来自域内，发往域外 | 121.9 |
| 请求分组来自域外，发往域内 | 321.1 |
| 请求分组来自域外，发往域外 | 96.6 |

### 3.2 已经生成的能力

目前，共生网络已经形成了跨域攻击防范、数据泄露防范、精准实时溯源、精准实时态势感知、精细粒度管控等一系列能力，简要介绍如下。

#### 3.2.1 跨域攻击防范能力

如前所述，共生网络的域间路径标识耦合生成机理，用节点标识、内容名字等信息耦合生成域间路径标识，使攻击者难以伪造域间路径标识。结合共生网络以“拉促推、推拉结合”的跨域通信模式，使一个节点只有收到请求者发送的请求并从中获得合法域间路径标识（序列），该节点才能将数据分组发送到请求者；否则，数据分组会因为携带的域间路径标识非法而被边界路由器丢弃，而不能到达请求者。正因如此，共生网络能够从根本上防范 IP 网络中广泛存在的反射攻击。

然而，共生网络中的内容提供者要将内容名字通告给外网，且要接收外网发来的请求消息。因此，共生网络中的内容提供者有可能遭受请求分组攻击，即攻击者通过发送大量请求消息来实施攻击。幸运的是，共生网络很容易检测与防范请求分组攻击[26]。若攻击者发送大量合法请求（即请求的内容名字确实存在），则将会有数据分组返回给攻击者。由于一个请求消息对应的内容通常需要多个数据分组进行发送，且数据分组的大小通常远大于请求消息的大小，攻击者发送大量合法请求时，易形成针对攻击者自身的反射攻击。因此，攻击者通常不会通过发送合法请求实施攻击。若攻击者通过发送

非法请求进行攻击，则由于请求的内容名字不存在，这样的请求很容易被检测。此时，请求消息中携带的域间路径标识（序列），可以被用于对攻击者的精准溯源，从而阻止攻击[26]。

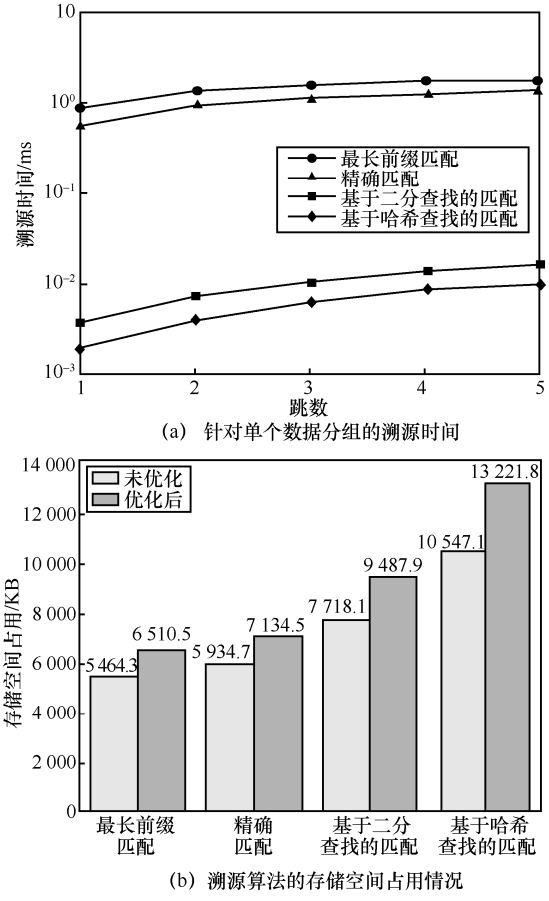
### 3.2.2　数据泄露防范能力

共生网络基于多维名字逐分组过滤的数据泄露防范机理，能够有效阻止数据在未经授权的情况下被泄露到外网。一个数据要被合法发送到外网，数据提供者必须要将该数据的内容名字通告给外网。为了防止内容名字通告过程中出现数据泄露，共生网络采取了两点措施。首先，通告消息必须经其本地资源管理器转发；其次，共生网络设计了不同的分组类型，严格区分通告消息、请求消息和数据分组，而通告消息和请求消息的格式固定且不能承载数据[27]。

### 3.2.3　精准实时溯源能力

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）。一个内容提供者只需维护域间网络拓扑（网络、域间路径及域间路径标识），通过将域间路径标识与网络拓扑进行匹配，即可准确知道请求分组的来源网络。相应地，内容提供者也可以准确知道数据分组的去向网络。类似地，内容请求者只需通过将数据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，即可知道数据分组的来源网络。边界路由器也可以利用同样的方法，准确知晓数据分组的来源网络和去向网络。因此，共生网络能够提供针对单个数据分组的精准溯源能力[26]。

在溯源实时性方面，将单个域间路径标识与网络拓扑进行匹配的最优时间复杂度为 $O(1)$；假设数据分组/请求消息中携带的域间路径标识数量为 $M$，则对单个数据分组/请求消息进行溯源的最优时间复杂度为 $O(M)$[26]。本文在自治域规模为 60 000 的网络中，评估了针对单个数据分组的溯源开销如图 8 所提方法（基于哈希查找的匹配）针对单个数据分组的溯源时间及存储空间占用情况，并将其与 3 种经典的方法进行了对比，包括最长前缀匹配、精确匹配、基于二分查找的匹配，结果如图 8 所示。从图 8(a)中可以看出，在数据分组/请求分组中携带 5 个域间路径标识的情况下，针对单个数据分组的溯源时间低至 10 μs。从图 8(b)中可以看出，结合拓扑分解与匹配优化，所提方法实现实时溯源所需的存储空间不到 14 MB。



(a)　针对单个数据分组的溯源时间

(b)　溯源算法的存储空间占用情况

图 8　共生网络中针对单个数据分组的溯源开销

### 3.2.4　精准实时态势感知能力

共生网络体系下，内容提供者、内容请求者、边界路由器等能够精准实时感知网络的跨域流量等态势[26]。如上所述，内容提供者可以对收到的每个请求分组进行精准溯源；相应地，内容提供者可以清楚知晓该请求分组的来源网络和从来源网络到请求者经过的所有网络。因此，给定域间网络拓扑，内容提供者可以精准实时统计源自每个网络的请求分组数量、每个网络转发给该内容提供者的请求分组数量。类似地，内容请求者可以精准实时统计源自每个网络的数据分组、每个网络转发给该请求者的数据分组数量。边界路由器也可以精准实时统计源自每个网络的数据分组数量、去往每个网络的数据分组数量等，进而形成跨域流量态势。

### 3.2.5　精细粒度管控能力

共生网络能够赋予用户对每个内容的精细粒度管控能力[22]。一方面，前述基于多维名字逐分组过滤的数据泄露防范机理，能够对每个内容的出网（甚至去向）进行管控。另一方面，给定域间网络拓扑，内容提供者可以为每个内容名字指定通告路

径，使内容名字（而不是内容）只能沿着指定路径通告给指定网络的指定节点。当内容提供者收到请求消息时，根据请求消息中携带的域间路径标识序列，很容易判断针对该内容名字的通告是否超出通告范围，以及哪个网络进行了超范围通告。若内容提供者发现某个内容名字被超范围通告，则可告警且不将相应的数据发送给请求者。此外，从域间流量工程的角度而言，共生网络可以赋予网络对域间流量的精细管控能力[28-29]。

#### 3.2.6　路由解耦释放网络潜能的能力

共生网络通过域内域间路由解耦，使每个网络可以根据自身特点采用合适的网络体制，在充分利用该网络优势的同时，赋予了每个网络独立演进的能力。事实上，项目组结合节点标识和内容名字设计的移动自组网路由机制[30]，性能较采用 AODV（ad hoc on-demand distance vector）路由协议的 IP 网络和采用 LFBL（lister first broadcast later）的 NON 有大幅度提升。设网络中有 8 个请求者、2 个内容提供者，运动模型为随机游走，节点运动速度为 20 m/s，运动场地为方形，面积随节点数量增多而增大，但保持节点平均密度为 $1\times10^{-2}$ 架/平方千米，IP、NDN 和所提方法的分组投递成功率如图 9 所示。从图 9 中可以看出，当给定节点规模时，所提方法的分组投递成功率显著高于 IP 和 NDN。当给定分组投递成功率时，所提方法能够支撑更大的网络，如当分组投递成功率为 50%时，IP 仅能支撑 50 余个节点的移动自组网，NDN 能够支撑约 120 个节点的移动自组网，而所提方法能够支撑超过 256 个节点的自组网。上述结果说明，根据不同的网络特点设计有针对性的组网机制，比所有网络都采用相同的机制（如 IP）更好。因此，共生网络通过路由解耦，能够充分释放网络潜力。

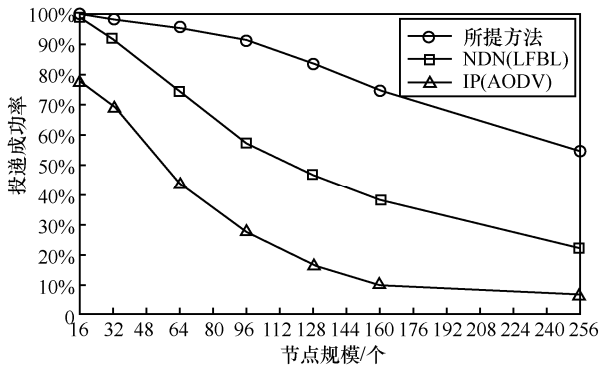



图 9 移动自组织网络中不同机制的分组投递成功率

#### 3.2.7　网络空间权益保障能力

如前所述，共生网络中每个网络维护一个逻辑上集中但可分布式实现的资源管理器，管理内容名字的可达性；同时，请求消息也发送给资源管理器，由资源管理器进行解析。相应地，一个网络内部节点间的内容交换，不用依靠外部就可以独立运行，不受外部影响和控制。类似地，共生网络中，网络间根据策略等考虑，平等进行域间互联，并相互通告内容名字的可达性，避免了类似 DNS（domain name system）集中式设计带来的“断网停服”问题。因此从长远看，共生网络具备保障网络空间权益的能力。

#### 3.2.8　高效性能力

由于其独特设计，共生网络还具备内容高效分发能力，并增强网络的可管能力。首先，共生网络为内容命名并基于内容名字进行内容查找，便于网络缓存内容并进行利用[31]。例如，车联网环境下，通告对内容进行缓存，不仅可以大幅降低节点获取内容的平均时延，且能够降低网络的传输负载。其次，共生网络中，每个跨域分组都携带了域间路径标识，因此，入口边界路由器根据域间路径标识进行分组转发时，可以得知分组的出口边界路由器。这样，入口边界路由器就可以很方便地统计从该入口边界路由器到网络中其他边界路由器的流量，从而形成实时准确的流量矩阵[32]，进而为域内路由选择、路径规划甚至流量异常检测等提供便利。

## 4　待进一步解决的问题

虽然共生网络的基本工作机制和安全保障机理等已经得到了成功验证，但仍有部分问题有待进一步解决。

### 4.1　广域开放环境下域间路径标识前缀的分配问题

前文介绍了共生网络中域间路径标识前缀的“正交复用”分配的原则。当域间网络拓扑是静态的且已知的情况下，域间路径标识前缀可以集中分配。但是，在广域开放互联环境下，各个网络为了保护隐私，通常不会对外公布与其他网络之间的互联关系；同时，域间互联关系也会动态变化。因此，2 个网络之间需要根据“正交复用”分配原则，在不考虑其他网络的情况下为它们之间的每条域间路径分配域间路径标识前缀。因此，从全网的角度看，这种分配是分布式实现的。相应地，如何实现域间路径标识前缀的分布式分配，使全网使用的域

间路径标识前缀尽可能少，从而在域间路径标识长度固定的情况下尽量提升网络安全性，是需要进一步研究的问题。

### 4.2 机动网络和固定网络的融合问题

共生网络抓住网络间互联的本质，为网络之间的域间互联关系（体现为域间路径）命名，使其能够高效支持移动网络之间、移动网络和固定网络之间的互联互通。固定网络之间互联时，边界路由器通常固定不变，因而不用经常更新边界路由器的路由表。但机动网络和固定网络互联时，或者机动网络和机动网络互联时，节点移动会导致边界路由器经常发生变化。基于共生网络的基本工作机制，若 2 个网络之间的连接关系不变，则它们之间的域间路径标识前缀不变。当边界路由器发生改变时，只需更新该域间路径标识前缀对应域间路径的端点，并将相应更新通告给网络中的其他节点，便于其他节点更新域间路由表，从而将分组发送给新的边界路由器。但是，移动环境下如何发现新的边界路由器、如何实现新旧边界路由器之间的切换、如何将新的边界路由器通告给其他边界路由器等，是需要研究解决的问题。

### 4.3 路径标识快速匹配算法

如前所述，将数据分组（或请求消息）中携带的域间路径标识（序列）与已知域间网络拓扑进行匹配，可以对数据分组（或请求消息）进行精准溯源。目前的匹配算法对单个域间路径标识进行匹配时，时间复杂度为 $O(1)$；当序列中有 $M$ 个域间路径标识时，整个序列的匹配时间为 $O(M)$。因此，如何设计更高效的匹配算法，提高精准溯源和精准实时态势感知的实时性，是需要解决的另一个问题。

### 4.4 路由器设计

虽然本文给出了边界路由器的部分性能测试结果，但该边界路由器是基于软件实现的，分组转发过程中涉及的步骤只能串行执行，性能受限。因此，研制基于硬件实现的边界路由器，将分组转发过程中可以并行处理的步骤通过硬件进行并行处理从而提升分组转发性能，是下一步的重点工作。

## 5 结束语

本文针对不同体制异构网络之间的安全高效互联问题，提出了共生网络。在分析异构网络安全高效互联面临挑战与科学问题的基础上，基于网络传递信息的自然属性，提出了共生网络对异构体制网络互联而成网络空间的普适表征机理，即用内容名字、节点标识、地址和域间路径标识分别表征传什么、传给谁、传到哪、怎么传。在此基础上，重点介绍了共生网络的体系结构模型、基本工作机理（包含域内域间解耦的路由组织模式、内容名字驱动的跨域互联模式、“以拉促推、推拉结合”的跨域通信模式）。原型系统的部分实验结果表明，共生网络能够实现数据的安全高效跨域传递，并具备跨域攻击防范能力、数据泄露防范能力、精准实时溯源能力、精准实时态势感知能力、精细粒度管控能力、路由解耦释放网络潜能的能力、网络空间权益保障能力、高效性能力等。同时，本文指出了共生网络有待进一步解决的问题。

## 参考文献：


[1] CHERITON D R. Sirpent: a high-performance internetworking approach[J]. ACM SIGCOMM Computer Communication Review, 1989, 19(4): 158-169.

[2] 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.

[3] TENNENHOUSE D L, WETHERALL D J. Towards an active network architecture[J]. ACM SIGCOMM Computer Communication Review, 1996, 26(2): 5-17.

[4] CHERITON D. Triad[J]. ACM SIGOPS Operating Systems Review, 2000, 34(2): 34.

[5] KOPONEN T, CHAWLA M, CHUN B G, et al. A data-oriented (and beyond) network architecture[J]. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 181-192.

[6] 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. New York: ACM Press, 2009: 1-12.

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

[8] RAYCHAUDHURI D, NAGARAJA K, VENKATARAMANI A. MobilityFirst: a robust and trustworthy mobility-centric architecture for the future Internet [J]. ACM SIGMOBILE Mobile Computing and Communication Review, 2012, 16(3): 2-13.

[9] NAYLOR D, MUKERJEE M K, AGYAPONG P, et al. XIA: architecting a more trustworthy and evolvable Internet[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 50-57.

[10] KOPONEN T, SHENKER S, BALAKRISHNAN H, et al. Architecting for innovation[J]. ACM SIGCOMM Computer Communication Review, 2011, 41(3): 24-36.

[11] PERRIG A, SZALACHOWSKI P, REISCHUK R M, et al. SCION: a secure internet architecture[M]. Cham: Springer International Publishing, 2017.

[12] 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 Press, 2019: 1-14.

[13] 张宏科, 苏伟. 新网络体系基础研究: 一体化网络与普适服务[J]. 电子学报, 2007, 35(4): 593-598.
ZHANG H K, SU W. Fundamental research on the architecture of new network—universal network and pervasive services[J]. Acta Electronica Sinica, 2007, 35(4): 593-598.

[14] HEGLAND A M, HAUGE M, HOLTZER A. Federating tactical edge networks: ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks[J]. IEEE Communications Magazine, 2020, 58(2): 72-78.

[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] CLARK D D. Designing an Internet[M]. Massachusetts: The MIT Press, 2018.

[17] 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.

[18] 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.

[19] LUO H B, CUI J B, CHEN Z, et al. Efficient integration of software defined networking and information-centric networking with CoLoR[C]//Proceedings of 2014 IEEE Global Communications Conference. Piscataway: IEEE Press, 2014: 1962-1967.

[20] 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.

[21] 李红祎. 基于 OMNeT++的 CoLoR 分组转发机制仿真与分析[D]. 北京: 北京交通大学, 2019.
LI H Y. OMNeT++-based simulation for packet forwarding mechanisms in CoLoR[D]. Beijing: Beijing Jiaotong University, 2019.

[22] 张康宁. 共生网络中数据跨域传输管控机制的设计与实现[D]. 北京: 北京航空航天大学, 2021.
ZHANG K N. Design and implementation of a control mechanism for data cross-domain transmission in CoLoR network[D]. Beijing: Beihang University, 2021.

[23] 潘刚. 智慧协同网络中边界路由器的设计与开发[D]. 北京: 北京交通大学, 2018.
PAN G. Design and development of the border router in SINET[D]. Beijing: Beijing Jiaotong University, 2018.

[24] 温兴泵. 服务标识通告和查找机制的设计与实现[D]. 北京: 北京交通大学, 2018.
WEN X B. Design and implementation of announcement and lookup mechanisms for service identifiers[D]. Beijing: Beijing Jiaotong University, 2018.

[25] WEN X B, LUO H B, LIN Y. Interest forwarding in CoLoR: a baseline implementation and performance evaluation[C]//Proceedings of 2016 IEEE/CIC International Conference on Communications in China (ICCC). Piscataway: IEEE Press, 2016: 1-6.

[26] 刘洲彪. 共生网络中的 DDoS 攻击检测与溯源机制研究与验证[D]. 北京: 北京航空航天大学, 2020.
LIU. Z B. DDoS attack detection and traceback in CoLoR network: mechanism design and validation[D]. Beijing: Beihang University, 2020.

[27] 陈哲. 智慧协同网络基于路径标识的路由体系及安全性研究[D]. 北京: 北京交通大学, 2016.
CHEN Z. Research on path-identifier-based routing architecture and its security in smart identifier network[D]. Beijing: Beijing Jiaotong University, 2016.

[28] LI J W, LUO H B, ZHANG S, et al. Traffic engineering in information-centric networking: opportunities, solutions and challenges[J]. IEEE Communications Magazine, 2018, 56(11): 124-130.

[29] LI J W, LUO H B, ZHANG S, et al. Design and implementation of efficient control for incoming inter-domain traffic with information-centric networking[J]. Journal of Network and Computer Applications, 2019, 133: 109-125.

[30] 李隽杰. 基于共生网络的无人机集群路由机制设计与仿真[D]. 北京: 北京航空航天大学, 2020.
LI J J. CoLoR based routing mechanism for UAV swarm networking: design and simulation[D]. Beijing: Beihang University, 2020.

[31] 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.

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

[作者简介]

**罗洪斌**（1977− ），男，重庆人，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。

**张珊**（1989− ），女，河南焦作人，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。

**王志远**（1993− ），男，山东淄博人，博士，北京航空航天大学副教授，主要研究方向为边缘计算、网络资源协同、移动互联网机制设计等。