

# 基于 SRv6 的确定性网络服务共享保护方案

李硕朋<sup>1</sup>, 方娟<sup>1</sup>, 陈肯<sup>2</sup>

(1. 北京工业大学信息学部, 北京 100124; 2. 法国索邦巴黎北大学伽利略理工学院, 维尔塔纳斯 93430)

**摘 要:** 针对现有方法难以实现确定性网络的高效部署和服务保护的问题, 提出基于 SRv6 的确定性网络服务保护架构, 以实现确定性网络的高效管控与转发。在此架构下, 设计了面向服务的确定性网络服务保护方案, 对基于资源共享的服务保护策略进行了建模; 设计了基于最短路径的启发式算法, 通过共享备份路径带宽, 优化了网络资源的利用率和时延。实验结果表明, 相比于非共享算法, 共享保护算法具有明显优势。

**关键词:** 确定性网络; 分段路由; 服务保护; 故障恢复; 软件定义网络

**中图分类号:** TP393

**文献标识码:** A

**DOI:** 10.11959/j.issn.1000-436x.2021203

## DetNet service share protection scheme based on SRv6

LI Shuopeng<sup>1</sup>, FANG Juan<sup>1</sup>, CHEN Ken<sup>2</sup>

1. Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

2. Institute Galilee, University Sorbonne Paris Nord, Villetaneuse 93430, France

**Abstract:** To solve the problem that existing methods are difficult to achieve efficient deployment and service protection in deterministic network (DetNet), a DetNet service protection architecture based on SRv6 was proposed. By leveraging this architecture, a service-oriented DetNet protection scheme was designed and the share protection policy was formulated. With the aid of backup bandwidth share, the proposed heuristic based on shortest path optimized network resource utilization and delay. The simulation results show that the share protection algorithm achieves better performance than non-share algorithm.

**Keywords:** deterministic network, segment routing, service protection, failure recovery, software defined network

## 1 引言

近年来, 5G、云计算、物联网、自动驾驶等行业的快速发展给未来网络提出了新的挑战。行业应用的新需求催生了诸多网络新技术, 也推动了未来网络的发展。其中, 天地一体化网络、智能网络、区块链和确定性网络等关键技术代表着未来网络的发展方向<sup>[1]</sup>。这些关键技术可以在高带宽、高可靠性低时延、高安全性、万物互联等方面赋能未来

网络。

高可靠性低时延<sup>[2]</sup>作为 5G 的三大目标之一, 在工业互联网、自动驾驶等领域有着极其迫切的需求。确定性网络 (DetNet, deterministic network)<sup>[3]</sup>作为实现高可靠性低时延的手段之一, 旨在解决传统网络上, 交换和路由过程中欠缺服务质量保障的问题。不同于传统的基于尽力而为的网络, 确定性网络需要保障服务的端到端时延和抖动以及数据的完整性, 保证网络不会因故障导致数据分组丢

收稿日期: 2021-07-25; 修回日期: 2021-10-11

通信作者: 方娟, fangjuan@bjut.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2020YFF0305400); 北京市自然科学基金资助项目 (No.4192007); 北京工业大学国际科研合作种子基金资助项目 (No.2021B02, No.2021C02)

**Foundation Items:** The National Key Research and Development Program of China (No.2020YFF0305400), The Natural Science Foundation of Beijing (No.4192007), The International Research Cooperation Seed Fund of Beijing University of Technology (No.2021B02, No.2021C02)

失、乱序等问题发生。

确定性网络需要在二层和三层上实现。二层的确定性网络主要由时延敏感网络 (TSN, time sensitive network)<sup>[4]</sup>实现。TSN 利用循环队列和转发 (CQF, cyclic queuing and forwarding)<sup>[5]</sup>协议实现全局时间同步、确定性转发和帧保护。

三层确定性网络<sup>[6]</sup>采用典型的软件定义网络 (SDN, software defined network) 架构, 将控制平面与转发平面分离, 通过对三层网络设备的集中管理与配置, 实现确定性转发<sup>[7]</sup>。

确定性网络可以部署在 IP (Internet protocol)、MPLS (multi-protocol label switching) 等网络上。目前, 基于 MPLS 的确定性网络标准和草案较多。但是, MPLS 网络协议较复杂, 特别是流量工程、资源预留等确定性网络需求较多的功能中, MPLS 的诸多协议增加了网络的复杂性。

近年来, 分段路由 (SR, segment routing)<sup>[8]</sup>作为实现 SDN 的新手段, 受到越来越多的关注。分段路由作为一种源路由技术, 简化了协议, 在源路由器对数据报文进行“编码”, 在报头中插入有序的列表, 用于指示报文的转发路径。分段路由由相比传统的资源预留和分布式协议降低了控制的冗余性, 操作简单, 扩展性好, 具备强大的可编程能力, 被视为实现 SDN2.0 的关键技术。

SRv6 (segment routing over IPv6) 综合了分段路由和 IPv6 的优势, 能够大大减轻网络复杂度, 为确定性网络的部署实现带来便利性, 在提供服务保护等确定性网络关键功能上具有前景。

服务保护是确定性网络的重要功能。服务保护旨在自主地处理网络故障。网络故障包括节点故障和链接故障。服务保护通过配置备份路径, 为网络流提供抵御网络故障的能力, 保障端到端传输的完整性。

本文关注基于分段路由的确定性网络实现模式, 在 SRv6 确定性网络的条件下, 重点讨论服务保护机制的策略与算法实现。本文贡献有以下 3 个方面: 1) 提出了基于 SRv6 的面向服务的确定性网络服务保护框架; 2) 提出了基于带宽资源共享的确定性网络保护系统模型; 3) 提出了启发式的共享保护路径选择算法, 优化了网络资源的利用率。

## 2 相关工作

IEEE 802.1 TSN 工作组致力于为二层确定性服

务制定标准 (RFC, request for comment)。IETF (Internet engineering task force) 确定性网络工作组同 TSN 工作组协作作为三层确定性服务制定标准。确定性网络工作组已完成若干标准, 并提出了诸多草案。这些标准和草案定义了确定性网络的架构、流模型、部署方式和网络互联等。

确定性网络架构<sup>[6]</sup>由应用平面、控制平面和数据平面构成。应用平面通常是一个带有特定服务或应用请求的用户, 并通过北向接口和控制平面沟通应用请求。控制平面接收应用平面的请求, 利用自身的控制功能, 例如路径计算单元 (PCE, path computation element), 完成路径计算、网络管理, 并通过南向接口将指令下发给数据平面。数据平面由网络转发设备构成, 根据控制平面的指令执行转发操作, 并将网络状态通过南向接口传递给控制平面。

应用平面的用户请求被抽象为确定性网络的流和服务模型。RFC 9016<sup>[9]</sup>定义了确定性网络服务的三层模型参数: 服务参数、流参数和流-应用参数。一个确定性网络服务可以包含一个或多个确定性网络流, 一个确定性网络流可以包含一个或多个确定性网络流-应用。服务参数包含服务的类型、特征、连接性、状态等。流参数除了包含服务的基本信息外, 还定义了流的部署方式 (IP、MPLS)、流量特征 (周期、周期内包数量和负载)、流优先级、流带宽时延需求等。流-应用参数与流参数类似。

确定性网络控制平面<sup>[10]</sup>统一了网络的控制层和管理层。控制层支持动态创建、修改和删除确定性网络流, 支持流的聚合和反聚合, 支持通过应用接口进行流的实例化, 支持基于时间同步的队列控制, 具备发布节点和链接资源的能力, 能够处理确定性网络域中的大规模确定性网络流。管理平面监测确定性网络流的性能, 支持流的完整性和连接性检测, 保证确定性网络性能达到要求。

确定性网络数据平面<sup>[11]</sup>由服务层和转发层构成。服务层提供包的复制、去重和排序功能 (PREOF, packet replication, elimination and ordering function)。转发层提供转发保证, 包括显性路径、流量工程和拥塞控制。

确定性网络数据平面可以部署在多种环境中。RFC 8939<sup>[12]</sup>定义了使用 IP 层和高层协议的头信息实现确定性网络流的标记和服务传递。RFC 8964<sup>[13]</sup>定义了利用伪线 (PW, pseudowire) 封装和 MPLS

流量工程 (MPLS-TE) 在 MPLS 网络上实现确定性网络。

基于 MPLS 的确定性网络数据平面包含 d-CW (DetNet control word)、S-Label 和 L-Label。d-CW 表示包的序号, S-Label 用于确定性网络服务身份识别, F-Label 用于提供显性路由。

确定性网络数据平面的多种部署方式都可以承载在 TSN 上。MPLS-TSN 草案<sup>[14]</sup>提出 MPLS 和 TSN 需要协同提供服务保护、资源分配和显性路由, 但并未提供具体的网络互联方法。

SRv6-TSN 草案<sup>[15]</sup>讨论了通过 SRv6 网络连接 TSN 的基础架构。分段路由是一种源路由方法, 可以在 IP 或 MPLS 上实现。源节点利用分段列表 (SL, segment list) 表示完整的转发路径。分段路由在流量工程中有着重要的应用<sup>[16-19]</sup>。

SRv6 利用 IPv6 地址 128 bit 的可编程能力, 丰富了 SRv6 指令表达的范畴, 使其不仅可以表达转发路径, 也可以在其他场景 (例如网络功能虚拟化<sup>[20]</sup>) 中实现网络的可编程性。但是, 现有的 SRv6-TSN 草案并未针对 SRv6 确定性网络数据平面的服务层、转发层和路由保护等提出具体方案。尽管如此, 我们依旧可以看到, SRv6 可以作为确定性网络的数据平面, 在确定性网络的场景中发挥不可或缺的重要作用。

确定性网络的服务保护机制是实现网络确定性的重中之重。保护机制包含网络故障的监测和路由保护。DetNet-OAM 草案<sup>[21]</sup>提出了利用 ACH 实现确定性网络流异常探测和性能测试。

现有的时延敏感网络/确定性网络的路由保护机制都是基于简单的帧/流的复制。例如, TSN 在 IEEE 802.1CB 中定义了保护机制 FRER (frame replication and elimination for redundancy)。PREOF 在确定性网络数据平面实现类似 FRER 的功能。基于复制的路由保护需要双倍的网络带宽的需求, 网络中有大量重复无效的包传输, 导致网络带宽利用率低。因此, 确定性网络需要更加灵活、高效的服务保护机制。本文认为路由保护策略是实现服务保护机制的重要方法。

路由保护策略<sup>[22]</sup>根据是否预留资源分为被动和主动保护策略。被动保护不预留资源, 当监测到网络故障时, 重新计算和配置可用路由; 主动保护预先计算并预留网络资源, 当监测到网络故障时, 直接使用备份路由。

根据备份路由的选择<sup>[23]</sup>, 路由保护策略又分为链接保护 (本地保护) 和路径保护 (全局保护)。链接保护针对网络中每一个链接选择一条备份路径; 路径保护针对一条端到端的路径, 提供一条不相交的备份路径。

### 3 基于 SRv6 的确定性网络服务保护架构

本节提出了基于 SRv6 的确定性网络服务保护架构。

#### 3.1 基于 SRv6 的确定性网络架构

基于 SRv6 的确定性网络架构如图 1 所示。SRv6 确定性网络控制平面为一个 SDN 控制器, 负责收集网络状态, 计算路径, 并下发指令。

数据平面二层 (L2) 采用 TSN, 三层 (L3) 采用 SRv6。分段路由头 (SRH, segment routing header) 用于实现确定性网络数据平面的服务层和转发层。本文将 SRH 中的分段表 (SL, segment list) 分为服务层分段表 (S-SL) 和转发层分段表 (F-SL)。S-SL 定义了服务层必需的 PREOF 功能。F-SL 通过每个 SL 提供基于源路由的显性路径转发。

数据平面设备由终端设备 (CE, customer equipment)、运营商边缘设备 (PE, provider edge) 和中继设备 (R, relay node) 构成。二层终端设备作为 TSN 的 Talker 和 Listener, 发送和接收 TSN 流。三层包含接入设备和中继设备。在图 1 中, 接入设备 1 根据发送端 TSN 流的需求特征和 SDN 控制器的路径结果, 将整个路径通过 SRv6 封装到 F-SL 中。中继设备根据 F-SL 执行转发。接入设备 2 解除 SRv6 封装并将 TSN 流转发给终端设备。

接入设备和中继设备需要在三层提供服务保护, 以便在网络节点或链接发生故障时, 保障网络的不中断和网络流的低时延。

#### 3.2 服务区分

本文将确定性网络服务分成三类, 严格确定性服务、一般确定性服务和尽力而为服务。针对不同的服务, 基于 SRv6 的确定性网络将提供不同的服务保护策略。

严格确定性服务是针对具有严格的低时延、高可靠性需求的服务, 在确定性网络层提供基于流复制的服务保护机制, 利用源点复制和终点重排序函数, 在网络中传递两份同样的网络流。

一般确定性服务适用于有低时延、高可靠性需求, 但服务等级低或不愿付出双倍带宽成本的用

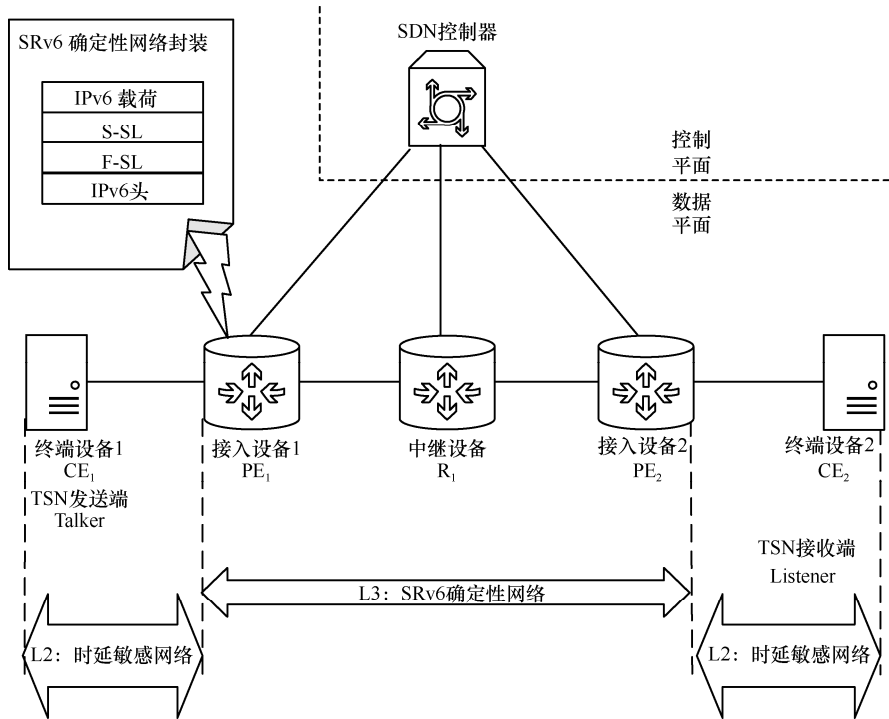


图 1 基于 SRv6 的确定性网络架构

户。对此，本文采用主动保护策略，预先计算备份路径并预留带宽，但只在主路径中传输流，不在备份路径中传输流。当主路径发生故障时，切换到备份路径，保障服务不中断和低时延。

尽力而为服务不提供备份路径，可利用链路的闲置带宽（包括备份路径的预留带宽）传输流。在高等级服务到来或备份路径预留带宽需要被启用时，尽力而为服务将被缓存或丢弃，所占用的资源将被释放。

图 2 解释了三类服务在链接上的带宽分布。在此链接中，严格确定性服务 a 的主路由和 c 的备份路由分别占据一部分的带宽；一般确定性服务 b 的主路由占据一部分的带宽；一般确定性服务 d 的备份路由和尽力而为服务共享一部分带宽。

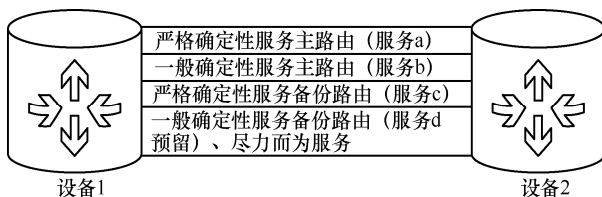


图 2 三类服务在链接上的带宽分布

### 3.3 SR Policy 实现服务保护

本文利用 SR Policy 实现针对不同服务的路由保护。SR Policy 定义了三元组 (headend, color,

endpoint)，其中 headend 为头节点，endpoint 为流的终点，color 可以用来定义优先级不同的服务。每种 color 可以携带多个带有优先级的候选路径。

为了实现确定性网络的保护机制，本文将严格确定性服务、一般确定性服务和尽力而为服务定义为 3 种 color。对于一般确定性服务，每个 color 携带一个主路径和一个备份路径。当主路径发生故障时，借助 SR Policy 实现备份路径的切换。

### 3.4 路径保护策略

根据备份路由选择策略，本文发现，链接保护的缺点是容易产生重复路径，导致路径变长。路径保护通过选择不相交路径，可以保证路径长度，具有较低的端到端时延。不相交路径保护也可同时实现点的保护。

在确定性网络中，需要保证路径尽可能短，以满足服务的时延需求。长路径会使时延变大，抖动变大。因此，在确定性网络中，本文采用不相交路径保护。

图 3 给出了路径保护的示例。假设确定性网络域由 5 个支持 SRv6 的路由器组成，网络中有 2 个确定性网络流  $D_1=(CE_1 \rightarrow CE_2)$  和  $D_2=(CE_3 \rightarrow CE_2)$ 。 $D_1$  的主路径为  $P_1=(CE_1 \rightarrow PE_1 \rightarrow R_2 \rightarrow PE_2 \rightarrow CE_2)$ ，备份路径为  $B_1=(CE_1 \rightarrow PE_1 \rightarrow R_1 \rightarrow PE_2 \rightarrow CE_2)$ ； $D_2$  的主路径为  $P_2=(CE_3 \rightarrow PE_3 \rightarrow PE_2 \rightarrow CE_2)$ ，备份路径为

$B_2=(CE_3 \rightarrow PE_3 \rightarrow R_1 \rightarrow PE_2 \rightarrow CE_2)$ 。  $B_1$  和  $B_2$  用于保护  $P_1$  和  $P_2$  上的链接, 也可以保护节点的故障。例如, 若中继设备  $R_2$  出现故障,  $B_1$  可确保网络流不受影响。

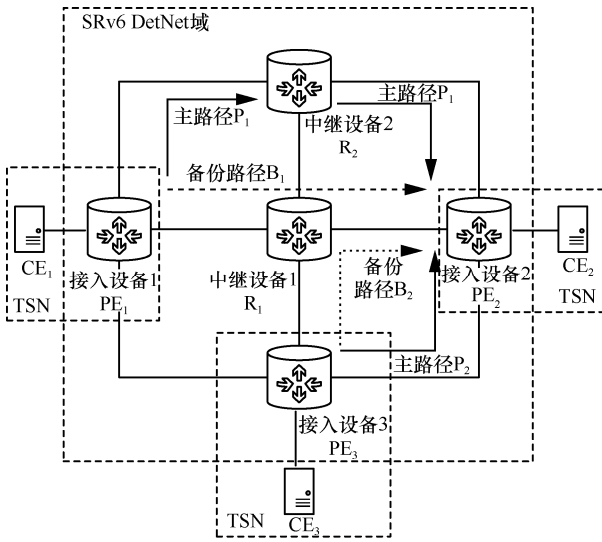


图 3 不相交路径保护策略

### 3.5 带宽资源共享

由于严格确定性网络和尽力而为服务的保护机制比较明确, 而一般确定性网络的保护配置更灵活, 因此本文在这里深入讨论一般确定性网络的保护策略。

针对一般确定性服务, 链接上仅预留备份带宽资源。由于网络中很少同时发生多个故障, 单链接故障是网络中最普遍的故障。注意到, 在单链接故障的情况下, 在同一条链接上的、用于保护不同主路径的备份路径上的带宽可以被共享。这种资源共享可以最大限度地减少备份带宽的占用率, 进而提升整个网络的效率。

例如, 在图 3 中,  $(R_1 \rightarrow PE_2)$  用于同时保护  $D_1$  和  $D_2$ 。在  $P_1$  和  $P_2$  不同时发生故障的情况下,  $(R_1 \rightarrow PE_2)$  上的备份带宽资源可以被共享。

## 4 共享保护系统模型

本节给出了基于 SRv6 的确定性网络服务共享保护机制的数学模型。

### 4.1 网络模型

设确定性网络拓扑结构有向图  $G=(V,E)$ , 其中  $V$  代表点的集合,  $E$  代表链接的集合。每个链接上总的可用带宽为  $BW_{ij}$ 。确定性网络流由七元组  $d=(id, source, destination, bandwidth, time, duration, delay)$

表示, 其中  $id$  为确定性网络流标识符,  $source$  为源点,  $destination$  为终点,  $bandwidth$  为带宽需求,  $time$  为流的到达时间,  $duration$  为持续时间,  $delay$  为最大时延。

确定性网络流请求随机到达网络, 共享保护模型的目标是根据网络现有流的主路由和备份路由的情况, 给出当前请求的主路由和备份路由的方案, 在满足网络资源、请求时延限制条件的前提下, 减少链接带宽的占用率, 提升资源利用率, 进而提升确定性网络流的整体接收率。

### 4.2 优化问题模型

共享保护系统模型的实质是一个优化问题, 对此建立如下模型。

#### 4.2.1 路径限制条件

设二元变量  $x_{ij}^d$  表示确定性网络流  $d$  在链接  $ij \in E$  上的主路由,  $x_{ij}^d=1$  表示  $d$  的主路由通过  $ij$ ,  $x_{ij}^d=0$  表示  $d$  的主路由不通过  $ij$ 。因此, 主路由的限制条件为

$$\sum_{i \in V} (x_{ij}^d - x_{ji}^d) = \begin{cases} -1, j = source \\ 1, j = destination \\ 0, 其他 \end{cases} \quad (1)$$

$$\forall j \in V, \exists ij \in E$$

同理, 设二元变量  $y_{ij}^d$  表示  $d$  在链接  $ij \in E$  上的备份流量。备份路径限制条件为

$$\sum_{i \in V} (y_{ij}^d - y_{ji}^d) = \begin{cases} -1, j = source \\ 1, j = destination \\ 0, 其他 \end{cases} \quad (2)$$

$$\forall j \in V, \exists ij \in E$$

根据路径保护理论, 主路径和备份路径不相交

$$x_{ij}^d + x_{ji}^d + y_{ij}^d + y_{ji}^d \leq 1, \forall ij \in E \quad (3)$$

式(3)保证了在一条链接上, 有且仅有主路由或备份路由。式(1)~式(3)共同保证确定性网络流  $d$  具有 2 条不相交的路径, 分别作为主路径和备份路径。

#### 4.2.2 共享保护带宽限制条件

设二元变量  $y_{mn}^d(ij)$  表示对于网络流  $d$ , 链接  $mn$  用于保护包含链接  $ij$  的路径。换言之, 若主路径经过  $ij$  且备份路径经过  $mn$ , 则  $y_{mn}^d(ij)=1$ , 否则  $y_{mn}^d(ij)=0$ 。因此, 有以下关系

$$y_{mn}^d(ij) = y_{mn}^d x_{ij}^d, \forall mn \in E, \forall ij \in E \quad (4)$$

图 4 给出了链接  $ij$  上的共享保护带宽示意。其中,  $F^d$  表示确定性网络流  $d$  的带宽需求,  $PB_{ij}$  表示在该链接上已使用的主路径带宽 ( $PB$ , primary bandwidth) 之和,  $BB_{ij}$  表示最大备份路径带宽 ( $BB$ , backup bandwidth),  $BB_{ij}(mn)$  表示主路径在  $mn$  上、备份路径在  $ij$  上的所有网络流的带宽之和。

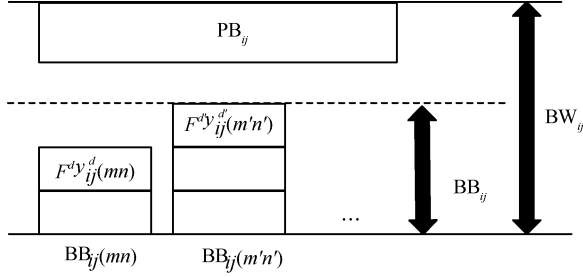


图 4 链接  $ij$  上的共享保护带宽示意

在图 4 中,  $mn$  和  $m'n'$  的备份路径同时经过  $ij$ , 两者的备份带宽资源在  $ij$  上被共享,  $ij$  上只需预留两者的最大值, 即可满足备份带宽资源的要求。当有新的网络流  $d$  到达时,  $F^d y_{ij}^d(mn)$  将被添加到  $BB_{ij}(mn)$  上, 同时更新  $BB_{ij}$ 。因此链路上的备份带宽需满足

$$BB_{ij} = \max_{mn \in E} [BB_{ij}(mn) + F^d y_{ij}^d(mn)], \forall ij \in E \quad (5)$$

由图 4 也可以看出, 任意链路上的主路由带宽和备份路由带宽之和需小于链路总带宽, 即满足限制条件

$$BB_{ij} + PB_{ij} + F^d x_{ij}^d \leq BW_{ij}, \forall ij \in E \quad (6)$$

式(4)~式(6)实现了确定性网络共享保护模型的核心思想, 通过对网络中带宽资源的共享, 提升了资源利用率。

#### 4.2.3 确定性网络时延限制条件

TSN 的循环队列转发机制(CQF, cyclic queuing and forwarding) [24]定义了保证 TSN 确定性传输的模型。在确定性网络共享保护模型中, 本文采用基于 CQF 的时延限制条件, 即 CQF 模型的最大时延需小于确定性网络的时延条件。因此, 主路由和备份路由都需满足

$$\left( \sum_{ij \in E} (x_{ij}^d + x_{ji}^d) + 1 \right) CT \leq \text{delay}^d \quad (7)$$

$$\left( \sum_{ij \in E} (y_{ij}^d + y_{ji}^d) + 1 \right) CT \leq \text{delay}^d \quad (8)$$

其中,  $CT$  表示时隙长度。

#### 4.2.4 优化目标

为了保证网络时延并提高资源利用率, 优化目标同时考虑了主路径、备份路径和链路带宽。优化目标为

$$\min \left( \sum_{ij \in E} x_{ij} + \lambda_1 \sum_{ij \in E} y_{ij} + \lambda_2 \sum_{ij \in E} BB_{ij} \right) \quad (9)$$

其中,  $\lambda_1$  表示路径优化权重, 其值决定主路径和备份路径的时延;  $\lambda_2$  表示备份带宽优化权重, 由于备份路径共享特征的存在, 较长的路径也有可能提升路径共享效率, 进而降低整体带宽占用消耗。

因此, 优化主路径和备份路径是保证网络低时延的关键。同时, 优化备份带宽对于提升网络资源的利用率也具有重要意义。

### 5 路径选择算法

上述优化问题为典型的整数线性规划问题, 属于 NP 完全问题。为解决上述优化问题, 本文提出基于最短路径的启发式算法, 伪代码如算法 1 所示。

#### 算法 1 共享资源路径选择算法

输入 确定性网络流  $d$ , 链接上带宽状态

输出 主路由路径  $x_{ij}^d$ , 备份路由路径  $y_{ij}^d$

- 1) 设置链接权重  $\text{cost} = 1 / (BW_{ij} - BB_{ij} - PB_{ij})$ ;
- 2) 在拓扑图上, 删除不满足带宽条件式(6)的链接;
- 3) 预计算主路径, 并满足确定性网络时延限制条件式(7);
- 4) if 主路径存在:
- 5) 在拓扑图上, 删除主路径;
- 6) 在拓扑图上, 删除不满足备份带宽条件式(5)和式(6)的链接;
- 7) 设置链接权重为  $\text{cost} = 1 / \gamma_{ij}$ ;
- 8) 预计算备份路径, 并满足确定性网络时延限制条件式(8);
- 9) if 备份路径存在:
- 10) 保存主路径和备份路径;
- 11) 更新  $BB_{ij}(mn)$ 、 $BB_{ij}$ 、 $PB_{ij}$ ;
- 12) 确定性网络流部署成功;
- 13) else
- 14) 部署失败;
- 15) end if
- 16) else
- 17) 部署失败;

18) end if

算法的输入为确定性网络流和网络带宽的状态, 输出为该流的主路径和备份路径。

算法 1)~3)行用于计算主路由。为了优化链路带宽利用率, 将链路权重设为剩余带宽, 此权重用于计算主路由。第 2)行根据确定性网络流带宽需求, 删除不满足带宽限制条件的链接。第 3)行利用 Dijkstra 最短路径算法预计算主路径。

算法 4)~8)行用于计算备份路由。如果主路径存在, 为了计算不相交备份路径, 在第 5)行删除主路径。第 6)行根据网络备份带宽状态, 删除不满足备份带宽限制条件的链接。第 7)行设置链路权重为  $1/\gamma_{ij}$ , 其中  $\gamma_{ij}$  为备份带宽参数, 计算方法为

$$\gamma_{ij} = E_{mn \in \text{path}} [BB_{ij} - BB_{ij}(mn)] + \varepsilon \quad (10)$$

其中, path 为已计算的主路径;  $\varepsilon$  是一个较小的数, 防止结果为 0。式(10)对于主路径 path 上的所有链接  $mn$ , 计算备份路径的剩余带宽均值。事实上, 这个值反映了带宽资源共享的程度。例如, 在  $BB_{ij}(mn) + F^d y_{ij}^d(mn) \leq BB_{ij}$  的情况下, 结合式(5)可以得出,  $F^d$  部署后不会增加备份带宽  $BB_{ij}$  的值, 即带宽共享被最大化利用。随后, 第 8)行利用 Dijkstra 最短路径算法预计算备份路径。

如果备份路径存在, 则在第 9)和第 10)行保存主路径和备份路径, 并更新带宽参数, 确定性网络流部署成功。若主路径或备份路径不存在, 都会导致确定性网络流部署失败。

算法 1 复杂度由第 11)行“更新  $BB_{ij}(mn)$ ”决定, 故算法复杂度为  $O(E^2)$ 。

## 6 实验评估

### 6.1 环境配置

本文设计了一个离散模拟器用于评估确定性网络共享保护模型的性能。模拟器使用 python 开发。网络拓扑结构采用真实的欧洲网络 Cost239 和中国网络 China55<sup>[25]</sup>。Cost239 包含 11 个节点和 26 个链接。China55 包含 55 个节点和 104 个链接。每个链接的带宽为 100 Mbit/s, 时隙长度为 1 ms。Cost239 和 China55 的拓扑结构如图 5 和图 6 所示。此外, 在评估网络节点数影响的实验中, 采用随机生成拓扑结构。

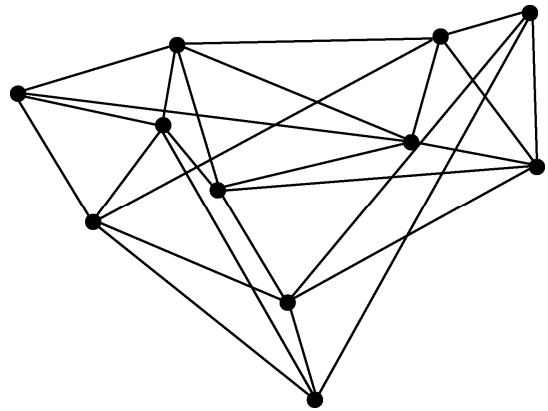


图 5 欧洲网络 Cost239 拓扑

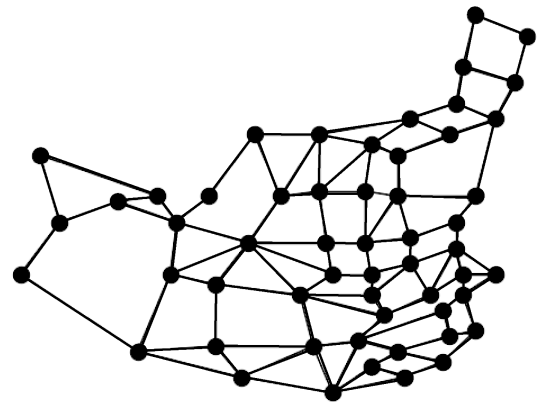


图 6 中国网络 China55 拓扑

确定性网络流随机产生, 到达间隔符合参数为  $\beta$  的指数分布。每个确定性网络流参数为七元组(id, source, destination, bandwidth, time, duration, delay)。确定性网络流源点和目标点在节点中随机选择, 流带宽需求为  $[20,40]$ Mbit/s, 到达时间间隔服从参数为  $\beta$  的指数分布, 持续时间服从  $\beta' = 200$  的指数分布, 时延需求为 10 ms, 模拟总时间为 1 000 时间单位。

本文使用确定性网络流接收率、网络带宽占用率和网络流时延 3 个评价指标考察算法性能。确定性网络流接收率为已接收网络流与网络流总数的比值, 网络带宽占用率为各链接上已使用带宽的平均值, 单个网络流的时延用跳数表示, 网络流时延为所有已接收网络流时延的平均值。

在下面的实验中, 本文对比共享保护方案和非共享保护方案的性能, 非共享保护方法的备份路由带宽在备份路径上直接叠加, 分别观察上述 3 个评价指标随网络流到达时间间隔、系统运行时间以及网络节点数的变化。所有实验结果为 20 次实验的平均值。

### 6.2 确定性网络流到达时间间隔

到达时间间隔参数  $\beta$  反映了网络的负载情况。 $\beta$  越小，网络流到达越密集，网络中共存的请求数越多，网络负载越大。本文设置到达时间间隔参数  $\beta \in [5, 20]$ 。图 7~图 9 分别展示了 Cost239 中网络流接收率、带宽占用率和网络流时延随到达时间间隔变化的结果。针对 Cost239，本文定义  $\beta \in [5, 10]$  为网络高负载区， $\beta \in [10, 15]$  为网络中负载区， $\beta \in [15, 20]$  为网络低负载区。值得注意的是，上述负载区的定义不仅与  $\beta$  相关，也与网络拓扑结构相关。

由图 7 可知，随着网络请求到达间隔的增加，由于网络平均负载减少，确定性网络流的接收率在逐步上升。通过比较共享保护算法和非共享保护算法的曲线可以看到，共享保护算法在确定性网络流接收率方面比非共享保护算法普遍高 10~20 个百分点。共享保护算法在提升确定性网络流接收率方面作用明显。

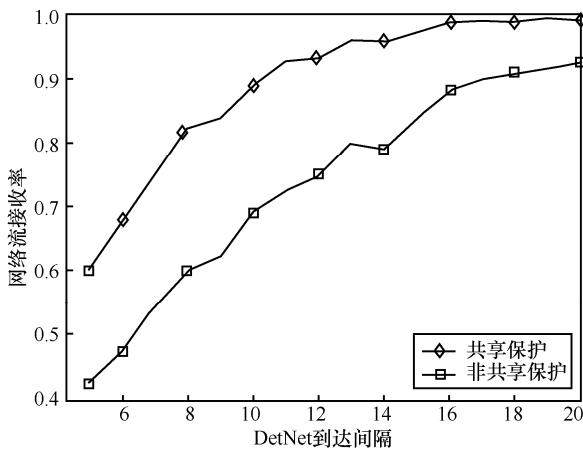


图 7 Cost239 接收率随到达间隔的变化

图 8 中，在高负载区，共享保护方法的带宽占用率比非共享保护方法高，共享保护方法利用较高的带宽占用率实现了较高的请求接收率，因此资源利用率更高。在中负载区，共享保护方法和非共享保护方法的带宽占用率相似。在低负载区，请求接收率在 90% 以上，共享保护方法的带宽占用率低于非共享保护方法，共享保护仍有富余的带宽用于接受更多请求，因此资源利用率较高。综上所述，共享保护算法可以提升网络带宽的利用率。

图 9 中，在高负载区，非共享保护主路由的平均时延明显小于共享保护主路由。这个现象产生的原因是共享保护方法接收了更多较长的网络流请

求，使平均时延升高；而非共享保护方法由于资源不足，拒绝了较长的网络流请求，使平均时延降低。随着网络负载变小，接收率升高，上述差异减小，2 种方法的主路由趋于相等。在低负载区，共享保护方法对主路由时延几乎没有影响。

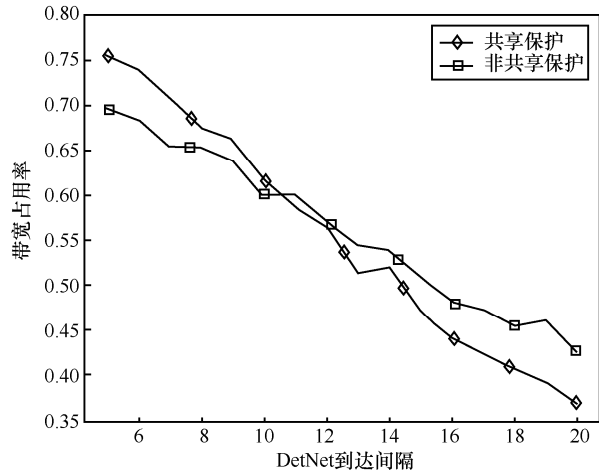


图 8 Cost239 带宽占用率随到达间隔的变化

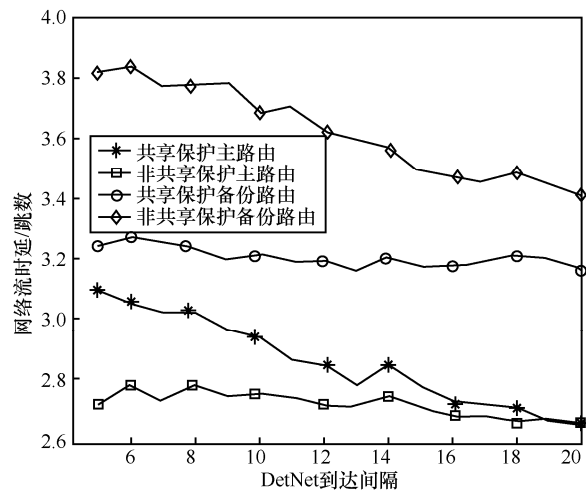


图 9 Cost239 时延随到达间隔的变化

与此同时，可以观察到，共享保护备份路由时延始终小于非共享保护备份路由时延，这说明共享保护方法对于缩短备份路由的时延效果显著。

### 6.3 系统运行时间

本节固定  $\beta=14$ ，选取 China55 网络，比较 3 个评价指标随运行时间的变化。此实验反映了网络从启动到逐渐稳定的过程。

图 10 展示了网络流接收率随时间的变化。从图 10 可以看到，在 0~200 时间单位，确定性网络流在网络中处于建立阶段，共享模型和非共享模型的请求接收率差别较小。随着时间的推移，网络中

的带宽资源趋于饱和，共享模型的接收率开始高于非共享模型，且这种差距逐渐拉大。在 800 时间单位之后，两者的接收率趋于稳定。

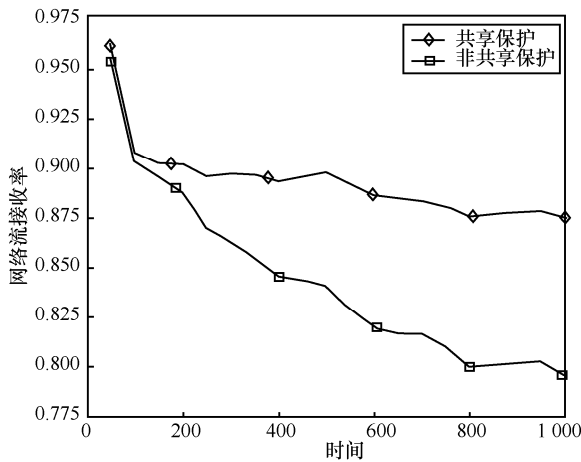


图 10 China55 接收率随系统运行时间的变化

图 11 为带宽占用率随系统运行时间的变化。从图 11 可以看到，由于网络中不断有新的网络流进入和旧的网络流离开，在 800 时间单位后，带宽占用率围绕 0.3 呈波动稳定状态。同时，由于网络处于中负载区，共享保护和非共享保护的带宽占用率始终相似，差距很小。

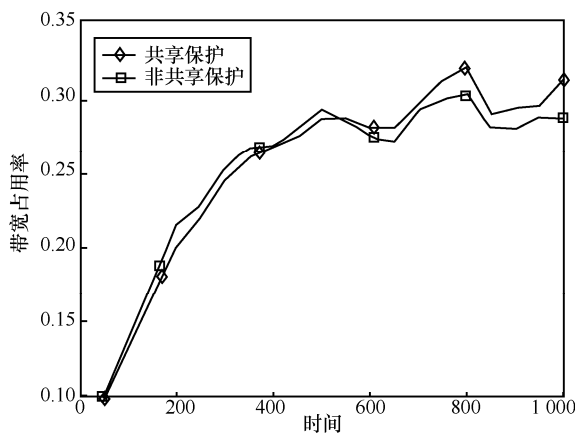


图 11 China55 带宽占用率随系统运行时间的变化

图 12 展示了网络流时延随时间的变化。同图 10 相似，随着时间的推移，4 个时延的值逐渐稳定。其中共享保护主路由时延大于非共享保护主路由时延，共享保护备份路由时延小于非共享保护备份路由时延。此现象与图 9 的中负载区现象一致。

综上所述，随着系统运行时间的变化，2 种方法的各评价指标在 China55 网络中逐渐稳定，且最终结果与 Cost239 一致。

### 6.4 网络节点数

在这个实验中，本文关心共享保护模型在随机生成的网络中的效果。本节固定  $\beta=16$ ，采用随机生成的拓扑结构，节点数量在 20~50 内变化。实验结果如图 13~图 15 所示。

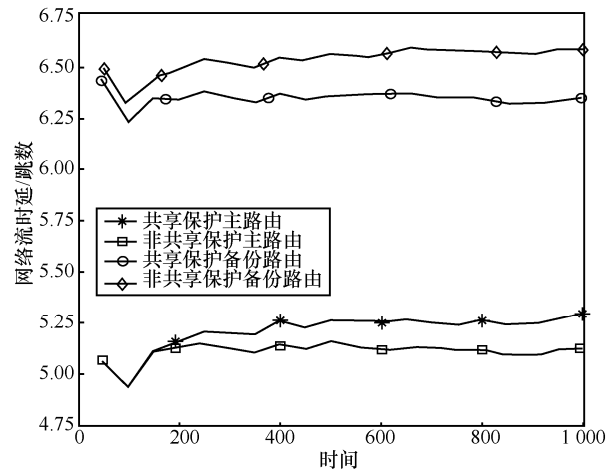


图 12 China55 时延随系统运行时间的变化

由图 13 可知，网络接收率普遍大于 90%，网络处于低负载区，且随着网络节点数的增加，网络负载降低，请求的接收率升高。在此种条件下，图 14 印证了前述结论，即共享保护带宽占用率低于非共享保护。

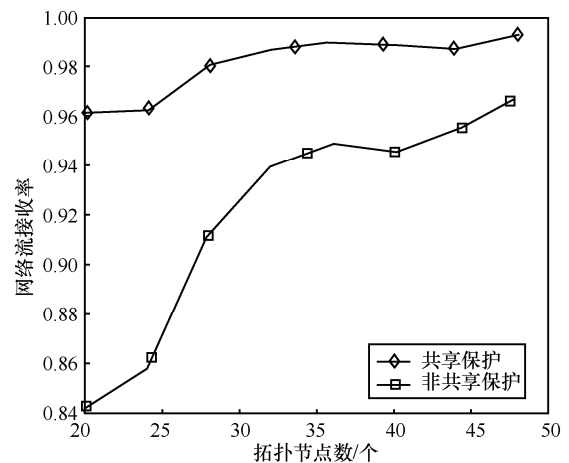


图 13 随机拓扑接收率随节点数的变化

从图 15 可以看出，当网络处于低负载区时，共享保护主路由和非共享保护主路由的时延几乎一致，即 2 种方法都能保证主路由的时延。因此，共享保护对主路由的影响很小。时延区别较大的是备份路由。共享保护方法的备份路由时延要明显低于非共享保护方法的备份路由时延。因此，共享保护策略在保证

备份路径的时延上优势明显。产生此现象的原因是非共享保护方法的资源较紧张，必须采用更长的备份路径，导致备份路径时延增大。从这个角度也可以看出，共享保护策略对网络资源的利用率较高。

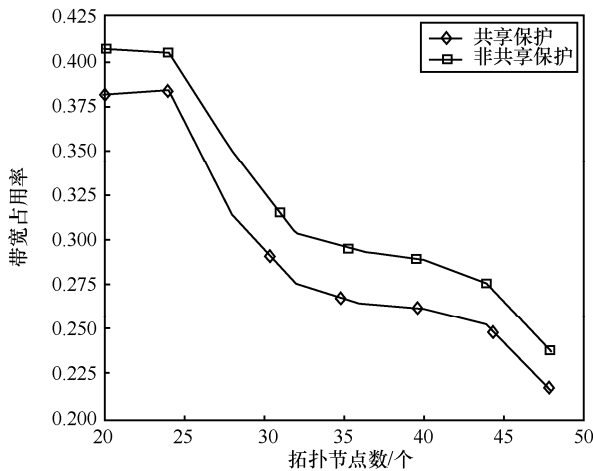


图 14 随机拓扑带宽占用率随节点数的变化

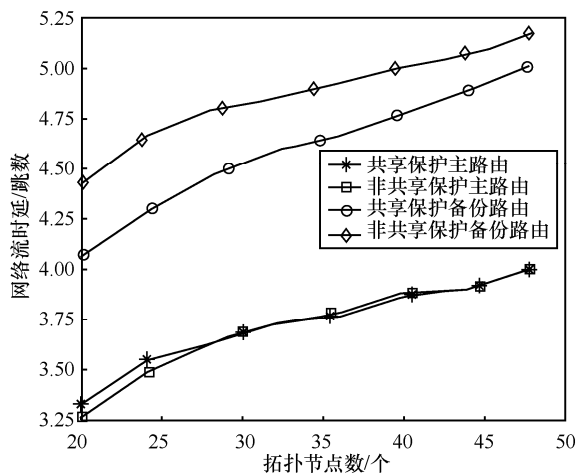


图 15 随机拓扑时延随节点数的变化

## 7 结束语

针对确定性网络的部署实现问题，本文提出了基于 SRv6 的确定性网络服务保护架构，利用 SRv6 的可编程性简化了确定性网络的部署实现。针对确定性网络服务保护问题，本文提出了面向服务的路由保护方案。通过服务区分，本文对不同的确定性网络服务采取不同的保护策略。基于该方案，对基于带宽资源共享的保护系统进行了建模，提出了启发式的共享保护路径选择算法，优化了网络带宽的利用率。实验表明，相比于非共享保护算法，共享保护算法在网络流接收率、带宽占用率和网络流时延上具有明显优势。

## 参考文献:

- [1] 黄韬, 刘江, 汪硕, 等. 未来网络技术与发展趋势综述[J]. 通信学报, 2021, 42(1): 130-150.  
HUANG T, LIU J, WANG S, et al. Survey of the future network technology and trend[J]. Journal on Communications, 2021, 42(1): 130-150.
- [2] NASRALLAH A, THYAGATURU A S, ALHARBI Z, et al. Ultra-low latency (ULL) networks: the IEEE TSN and IETF DetNet standards and related 5G ULL research[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 88-145.
- [3] 黄韬, 汪硕, 黄玉栋, 等. 确定性网络研究综述[J]. 通信学报, 2019, 40(6): 160-176.  
HUANG T, WANG S, HUANG Y D, et al. Survey of the deterministic network[J]. Journal on Communications, 2019, 40(6): 160-176.
- [4] NASRALLAH A, BALASUBRAMANIAN V, THYAGATURU A, et al. TSN algorithms for large scale networks: a survey and conceptual comparison[J]. arXiv Preprint, arXiv: 1905.08478, 2019.
- [5] STEINER W, CRACIUNAS S S, OLIVER R S. Traffic planning for time-sensitive communication[J]. IEEE Communications Standards Magazine, 2018, 2(2): 42-47.
- [6] FINN N, THUBERT P, VARGA B, et al. Deterministic networking architecture[R]. RFC Editor, 2019.
- [7] LI Y H, ZHANG P, ZHOU Y C, et al. A data forwarding mechanism based on deep reinforcement learning for deterministic networks[C]//Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2020: 285-290.
- [8] VENTRE P L, SALSANO S, POLVERINI M, et al. Segment routing: a comprehensive survey of research activities, standardization efforts, and implementation results[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 182-221.
- [9] VARGA B, FARKAS J, CUMMINGS R, et al. Flow and service information model for deterministic networking (DetNet)[R]. RFC Editor, 2021.
- [10] MALIS A, GENG X, CHEN M, et al. Deterministic networking (DetNet) controller plane framework[R]. RFC Editor, 2020.
- [11] FARKAS J, BERGER L, MALIS A, et al. Deterministic networking (DetNet) data plane framework[R]. RFC Editor, 2020.
- [12] FARKAS J, BERGER L, FEDYK D, et al. Deterministic networking (DetNet) data plane: IP[R]. RFC Editor, 2020.
- [13] FARKAS J, BERGER L, MALIS A, et al. Deterministic networking (DetNet) data plane: MPLS[R]. RFC Editor, 2021.
- [14] VARGA B, FARKAS J, MALIS A, et al. DetNet data plane: MPLS over IEEE 802.1 time-sensitive networking (TSN)[R]. RFC Editor, 2021.
- [15] WANG X, DAI J, LIU J, et al. DetNet data plane: IEEE 802.1 time sensitive networking over SRv6[R]. RFC Editor, 2020.
- [16] LI X Q, YEUNG K L. Traffic engineering in segment routing networks using MILP[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1941-1953.
- [17] PEREIRA V, ROCHA M, SOUSA P. Traffic engineering with three-segments routing[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1896-1909.
- [18] SCHÜLLER T, ASCHENBRUCK N, CHIMANI M, et al. Failure

resiliency with only a few tunnels - enabling segment routing for traffic engineering[J]. IEEE/ACM Transactions on Networking, 2020, 29(1): 262-274.

- [19] TIAN Y, WANG Z L, YIN X, et al. Traffic engineering in partially deployed segment routing over IPv6 network with deep reinforcement learning[J]. IEEE/ACM Transactions on Networking, 2020, 28(4): 1573-1586.
- [20] ABDELSALAM A, CLAD F, FILSFILS C, et al. Implementation of virtual network function chaining through segment routing in a linux-based NFV infrastructure[C]//Proceedings of 2017 IEEE Conference on Network Softwarization (NetSoft). Piscataway: IEEE Press, 2017: 1-5.
- [21] MIRSKY G, CHEN M. Operations, administration and maintenance (OAM) for deterministic networks (DetNet) with MPLS data plane[R]. RFC Editor, 2021.
- [22] SHEN G X, GUO H, BOSE S K. Survivable elastic optical networks: survey and perspective (invited)[J]. Photonic Network Communications, 2016, 31(1): 71-87.
- [23] YANG Z, YEUNG K L. SDN candidate selection in hybrid IP/SDN networks for single link failure protection[J]. IEEE/ACM Transactions on Networking, 2020, 28(1): 312-321.
- [24] YAN J L, QUAN W, JIANG X Y, et al. Injection time planning: making CQF practical in time-sensitive networking[C]//Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 616-625.
- [25] KNIGHT S, NGUYEN H X, FALKNER N, et al. The Internet topology zoo[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(9): 1765-1775.

### [作者简介]



李硕朋（1989- ），男，满族，辽宁抚顺人，博士，北京工业大学助理研究员，主要研究方向为软件定义网络、深度学习等。



方娟（1973- ），女，辽宁鞍山人，博士，北京工业大学教授、博士生导师，主要研究方向为高性能计算、异构智能计算、边缘计算等。



陈肯（1960- ），男，上海人，博士，法国索邦巴黎北大学教授、博士生导师，主要研究方向为无线传感器网络、软件定义网络等。