

# 互联网域内路由可用性综述

耿海军<sup>1</sup> 张爽<sup>1</sup> 尹霞<sup>2</sup>

(山西大学软件学院 太原 030006)<sup>1</sup> (清华大学计算机科学与技术系 北京 100048)<sup>2</sup>

**摘要** 路由可用性是指用户能够得到所请求服务的概率。随着互联网的发展,大量实时业务涌现,对网络实时性的要求也越来越高,对互联网的“自我修复能力”也提出了很高的要求。网络故障频繁发生,在修复网络故障的过程中可能会发生路由环路和收敛时间过长等问题,而且修复故障的时间一般在几秒到几十秒之间,已经无法满足实时应用对目前互联网的可用性需求。因此,提高路由可用性已经成为目前亟需解决的问题。文中总结和分析了目前已有的提高路由可用性的方案,并将这些方案主要分为被动恢复方案和路由保护方案两大类;详细介绍了目前国内外的科研成果,对比了各方案的优缺点,总结分析了这些方案的主要贡献及不足,并探讨了进一步的研究方向。

**关键词** 路由可用性,网络故障,路由环路,路由保护方案

中图分类号 TP309.7 文献标识码 A DOI 10.11896/j.issn.1002-137X.2019.07.001

## Overview of Routing Availability in Intra-domain Routing Networks

GENG Hai-jun<sup>1</sup> ZHANG Shuang<sup>1</sup> YIN Xia<sup>2</sup>

(School of Software Engineering, Shanxi University, Taiyuan 030006, China)<sup>1</sup>

(Department of Computer Science & Technology, Tsinghua University, Beijing 100048, China)<sup>2</sup>

**Abstract** Route availability refers to the probability that a user can get the requested service. With the development of the Internet, a large number of real-time services have emerged, and the requirements for the timeliness of the network is becoming higher and higher, and high demands have been placed on the “self-repairing ability” of the Internet. However, network faults occur frequently, and routing loops and long convergence times may occur during the process of repairing network failures. The repair time is usually between several seconds and tens of seconds, which cannot meet the real-time requirements of the Internet. Therefore, improving routing availability has become an urgent problem to be solved. This paper summarized and analyzed the existing schemes to improve routing availability, and divided these schemes into two major categories, namely passive protection scheme and route protection scheme. The research results at home and abroad were introduced in detail, the advantages and disadvantages of each program were compared, the main contributions and shortcomings of these programs were summarized and analyzed, and the research directions were proposed for further research.

**Keywords** Routing availability, Network failure, Routing loop, Routing protection scheme

## 1 引言

互联网起源于 20 世纪六七十年代的美国军用网络阿帕网<sup>[1]</sup>。由最初的军用网络发展到如今全球性的网络平台,仅仅用了几十年的时间<sup>[2-3]</sup>,并且其应用范围已经涉及到人们生活的方方面面。毋庸置疑,互联网已经成为我们生活中不可分割的一部分。

随着信息化程度的不断加深,以及大量实时业务<sup>[4-6]</sup>的涌现,互联网的应用范围也发生了翻天覆地的变化,由原先简单的非实时应用,如传输文件和电子邮件等,发展到了如今的在线股票交易、远程手术、视频流媒体和即时通信等实时应用。路由可用性<sup>[7-13]</sup>已经成为衡量网络性能的重要指标之一。

在目前的互联网中,网络故障不可避免地频繁发生<sup>[14-17]</sup>。在这种情况下,如果互联网依然要保证正常的通信,则需要有很强的“自我恢复能力”,即在故障发生时,互联网需要及时发现并且保证数据包及时、准确地发送到目的地。互联网通常采用路由协议<sup>[18-19]</sup>来修复网络中的故障。现在广泛使用的域内路由协议有 OSPF 和 IS-IS 等,但是这两个协议在修复故障的过程中,网络中可能会出现路由环路和路由黑洞等问题,并且收敛时间较长<sup>[20-23]</sup>。研究发现,如果采用路由协议修复故障,所需要的修复时间一般在几秒到几十秒之间,在这段时间内将会有大量的报文可能被丢弃。因此,如何提高互联网的域内路由可用性<sup>[24-32]</sup>已经成为科研工作者们研究的重要科学问题。

到稿日期: 2018-09-05 返修日期: 2018-11-29 本文受国家自然科学基金资助项目(61702315)资助。

耿海军 男,博士,讲师,主要研究方向为网络体系结构和路由算法等, E-mail: ghj123025449@163.com(通信作者);尹霞 女,博士,教授,主要研究方向为网络体系结构、路由算法、SDN、协议测试;张爽 女,主要研究方向为路由算法。

## 2 域内路由可用性提高方案的分类

提高域内路由可用性的方案可以分为被动恢复方案和路由保护方案<sup>[33]</sup>两类,如图1所示。

(1)被动恢复方案:该方案主要通过改变路由协议的参数来调整路由协议的收敛时间。

(2)路由保护方案:该方案的主要策略是提前计算备份路径,若网络出现故障,则使用备份路径来完成数据的传输,以保证数据及时、准确送达。根据报文转发形式的不同,可以将路由保护方案进一步细化为逐跳转发方法和非逐跳转发方法<sup>[34]</sup>。其中,逐跳转发方法主要包括:ECMP、LFA、U-turn、DMPA、路由偏转、O2、MRC、FCP和FIR等;非逐跳转发方法主要包括:Not-Via、HLP、Tunnel、MPLS和段路由等。

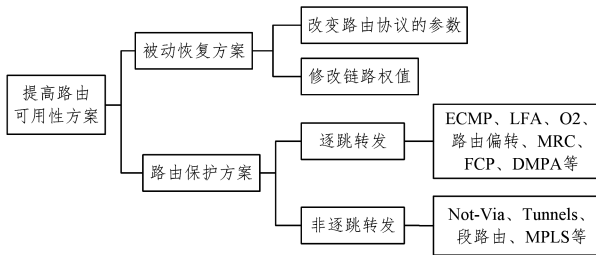


图1 路由可用性方案的分类

Fig.1 Classification of routing availability schemes

## 3 路由可用性方案的概述

### 3.1 被动恢复方案

#### 3.1.1 改变路由协议的参数

当网络中出现故障时,路由协议的收敛过程一般分为4个阶段:故障检测阶段、故障通知阶段、路由重计算阶段和转发信息阶段。路由收敛时间一般为从故障发生到完成收敛的总时间。下面将分别讲述前3个阶段的优化方法。

(1)故障检测阶段:在这个阶段期间,相邻路由器按照固定的时间间隔交换HELLO数据包,同时也有失效时间间隔。通过修改HELLO数据包的发送时间虽然可以调整故障检测的速度,但同时也会使得网络的维护成本发生变化,影响网络的稳定性。若减小发送HELLO报文的时间间隔,则可以缩短检测时间,但这也大大增加了通信开销。

(2)故障通知阶段:为了将故障信息告知全网,路由协议一般采用洪泛法来传递消息,但此过程可能由于局部路由有抖动而引起网络严重动荡。为了缩小故障的影响范围,防止出现网络动荡,文献[35]提出了两种方法,分别是BUA(Branch-Update Algorithm)和VMA(Vector-Metric Algorithm)。这两种算法不仅可以减小洪泛的范围,而且可以减少不必要的数据包丢失。

(3)路由重计算阶段:文献[36-37]利用增量最短路径算法(incremental Shortest Path First, iSPF)来加快计算路由的速度。当网络状态改变时,iSPF是在原来最短路径树的基础上做局部修改,而不是重新计算最短路径树,因此可以大大提高计算路由的效率,降低路由器的计算开销。

#### 3.1.2 修改链路权值

网络中选择的最优路径是所有路径权值之和最小的路径,因此链路的权值在路由方面起着重要的作用。因为链路的权值可以在网络管理员允许的范围之内随意选取,所以通过修改链路权值可以提高路由可用性并避免出现环路。

文献[38]提出了无环路收敛(Loop Free Convergence, LFC)方案,旨在解决网络收敛过程中可能出现环路的问题。文献[39]提出了动态改变部分链路权值的算法,此算法主要根据当前流量和链路带宽来对权值进行改变,流量越大,权值越大。文献[40]提出了静态链路权值分配方案,其避免了流量过于集中的问题,从而可以适应时间较短的链路故障。

### 3.2 路由保护方案

#### 3.2.1 逐跳转发方式

##### (1)等价多路径路由

等价多路径路由(Equal Cost Multiple Paths, ECMP)<sup>[41]</sup>是一种容易实现并且易于部署的多路径路由方法。如果节点对之间不存在多条代价相同的最短路径,则该节点对之间不存在备份路径;如果节点对之间存在多条代价相同的最短路径,则可以选择其中一条作为默认路径,其余为备份路径。

##### (2)无环备选项

无环备选项<sup>[42]</sup>(Loop Free Alternates, LFA)是目前最受欢迎的路由保护方案,该方案包括3个无环路规则,分别为LFC(Loop Free Condition),NPC(Node Protection Condition)和DC(Downstream Condition)。下面分别介绍这3个规则,其中 $dist(x, d)$ 表示节点 $x$ 到节点 $d$ 的最小代价。

1)LFC:如果目的节点是 $d$ ,计算节点为 $c$ ,则其邻居节点 $x$ 满足 $c$ 到目的节点 $d$ 的LFC规则,当且仅当 $dist(x, d) < dist(c, d) + dist(c, x)$ 成立,其中 $x \neq y$ , $y$ 是计算节点 $c$ 到目的节点 $d$ 的最优下一跳。

2)NPC:如果目的节点是 $d$ ,计算节点为 $c$ ,则其邻居节点 $x$ 满足 $c$ 到目的节点 $d$ 的NPC规则,当且仅当 $dist(x, d) < dist(x, y) + dist(y, d)$ 成立,其中 $x \neq y$ , $y$ 是计算节点 $c$ 到目的节点 $d$ 的最优下一跳。

3)DC:如果目的节点是 $d$ ,计算节点为 $c$ ,则其邻居节点 $x$ 满足 $c$ 到目的节点 $d$ 的DC规则,当且仅当 $dist(x, d) < dist(c, d)$ 成立,其中 $x \neq y$ , $y$ 是计算节点 $c$ 到目的节点 $d$ 的最优下一跳。

下面将通过一个简单的例子(见图2)来解释LFA中的这3个规则。

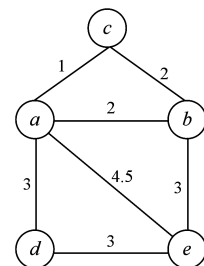


图2 LFA实例

Fig.2 Example for explaining LFA

如图 2 所示,假设  $c$  为计算节点, $c$  到目的地址  $d$  的默认下一跳为  $a$ ,  $b$  到  $d$  的最小代价等于 5,  $a$  到  $c$  的最小代价等于 2,  $c$  到  $d$  的最小代价等于 4。因为  $dist(b,d) < dist(b,c) + dist(c,d)$ , 所以结点  $b$  可以作为  $c$  到目的地址  $d$  的 LFC 下一跳。然而,因为  $dist(b,d) = dist(b,a) + dist(a,d)$ , 所以结点  $b$  不可以作为  $c$  到目的地址  $d$  的 NPC 下一跳。类似地,由于  $dist(b,d) > dist(c,d)$ , 所以结点  $b$  不可以作为  $c$  到目的地址  $d$  的 DC 下一跳。类似地, $c$  到目的地址  $e$  的默认下一跳为  $b$ 。因为  $dist(a,e) < dist(a,c) + dist(c,e)$ ,  $dist(a,e) < dist(a,b) + dist(b,e)$  和  $dist(a,e) < dist(c,e)$  都成立, 所以结点  $a$  可以作为  $c$  到目的地址  $e$  的 LFC、NPC 和 DC 下一跳。

### (3) U-turn

研究表明 LFA 方案的故障保护率较低, 基于此, 文献[43]提出利用 U-turn 方案来提高 LFA 的故障保护率。U-turn 主要根据邻居节点的无环路下一跳转发受故障影响的流量, 相对于 LFA 在单链路故障方面的保护率更高, 但是也不能完全保护所有的单链路故障。

### (4) DMPA

LFA 的实现方式的算法复杂度较高, 对此文献[44]提出利用 DMPA 算法来降低算法的复杂度。DMPA 是一种域内动态多路由算法, 分为静态算法和动态算法。与其他算法不同, 该算法只需要维护一棵以自身为根的最短路径树。当最短路径树构造完毕后, 计算节点将会计算出其到所有目的结点的备份下一跳; 当网络状态发生变化时, 执行动态 DMPA 算法来更新计算节点到所有目的节点的备份下一跳。DMPA 的计算复杂度较低, 适用于路由度量具有严格保序性的情形。

### (5) 路由偏转

文献[45]提出利用路由偏转来增加路径的多样性, 此方案在传播报文的过程中使用无环路的规则, 即将报文发送给不是最短路径上的结点来避免出现环路。在转发过程中由于该方案用标签来控制整个过程, 因此能提高网络的可用性和网络的资源利用率。但是, 此方法实现起来比较复杂, 代价高昂, 部署难度较大。下面将详细介绍路由偏转规则, 其中  $dist(n_i)$  表示始点  $n_i$  到目的点  $d$  的最小代价, 结点  $n_{i-1}$ ,  $n_i$  和  $n_{i+1}$  互为邻居。

规则 1 结点  $n_i$  偏转集合中的结点  $n_{i+1}$  应该满足  $dist(n_{i+1}) < dist(n_i)$ 。

规则 2 结点  $n_i$  偏转集合中的结点  $n_{i+1}$  应该满足下列条件中的任何一个:

- 1)  $dist(n_{i+1}) < dist(n_i)$
- 2)  $dist(n_{i+1}) < dist(n_{i-1})$

规则 3 结点  $n_i$  偏转集合中的结点  $n_{i+1}$  应该满足下列条件中的任何一个:

- 1)  $dist(G/l_{i+1}, n_{i+1}) < dist(G/l_i, n_i)$
- 2)  $dist(G/l_{i+1}, n_{i+1}) < dist(G, n_{i-1})$

其中,  $G$  是网络拓扑,  $G/l$  表示去掉链路  $l$  后的网络拓扑。

### (6) $O_2$

文献[46]介绍了  $O_2$  方案, 此方法可以使流量被分配在不同的路径上, 从而缓解网络负担。如果网络中没有发生故

障,  $O_2$  可以平均分配网络中的流量; 如果发生故障,  $O_2$  可以缓解网络堵塞, 把网络的流量分配到不同路径中, 从而降低网络拥塞程度。但是  $O_2$  的实现复杂度较高, 并且对网络拓扑有一定的要求, 因此在现实生活中很难实现和部署。

### (7) 多路由配置方案

多路由配置路由方案 (Multiple Routing Configurations, MRC)<sup>[47]</sup> 可以在不知道网络变化原因的情况下, 完成所有单链路或者单节点故障的处理。MRC 提出为每个路由器保存多个配置图, 每个配置图包括节点和链路, 从而可以保护该配置图中未出现的节点和链路。

### (8) 分组携带故障信息

文献[48]提出了利用分组携带故障信息 (Failure-Carrying Packet, FCP) 的方案来解决网络中的故障问题。该方案的基本思想是, 当故障发生时, 转发的报文会将遇到的故障保存在报文的头部, 报文到达某个节点时会将报文头部的故障信息传给这个节点, 这个节点收到信息之后根据此信息计算出新的拓扑, 再在新拓扑的基础上计算出最优下一跳。此方案保证了只要源节点和目的节点之间存在路径, 就可以将所需要传输的信息安全送达到目的节点。如果在计算最优下一跳时出现故障, 则用与遇到普通故障时一样的方法进行处理, 即将故障信息加入报文头部, 然后在新拓扑的基础上计算最优下一跳。

此方案跳过了传统路由协议的收敛过程, 同时也意味着避免了在路由收敛过程中可能出现的路由环路等问题。但是此方案的算法复杂度较高, 相对于现在普遍使用的协议来说, 修改的地方比较多, 因此实际部署困难。

### (9) 网络故障不敏感路由

Lee 等利用网络故障不敏感路由 (Failure insensitive routing, FIR)<sup>[49-51]</sup> 来提高网络应对故障的能力。FIR 的核心思想是将路由器的接口作为分组标识故障的信息。在现有路由体系结构中, 只需要将已经计算好的转发表发送给不同的线卡即可, 而不需要改动路由协议。

### 3.2.2 非逐跳转发方式

#### (1) Not-Via

Not-Via 方案<sup>[52]</sup> 利用辅助地址计算备份路径。

为了绕开网络中存在故障的节点或者链路, 将这些节点和链路的信息存储在 Not-Via 地址中。当网络中没有故障时, 根据最短路径传输报文; 当最短路径中的元素出现故障时, 则根据 Not-Via 计算出来的备份路径转发报文。

下面用一个例子 (见图 3) 来形象地解释 Not-Via 的执行过程。

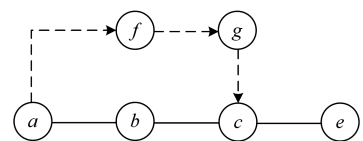


图 3 Not-via 实例

Fig. 3 Example for explaining Not-via

如图 3 所示, 若  $a$  和  $e$  分别为源节点和目的节点, 其原本的路径为  $(a, b, c, e)$ 。若  $b$  节点发生故障, 则将报文封装, 并根据 Not-Via 地址, 经过  $f$  和  $g$  节点将报文发送到  $c$  节点,

到了  $c$  节点之后对报文解除封装,然后将其正常转发到  $e$ 。

Not-Via 不仅可以提高路由的可用性,而且可以工作在链路权重非对称的网络中。但是,Not-Via 的实现复杂度比较高,很难实际部署。

### (2)HLP

针对 Not-Via 实现复杂度较高的问题,文献[53]提出了将 LFA 和 Not-Via 结合的快速重路由方案 HLP。HLP 的执行过程为:首先计算所有节点对之间符合 LFA 规则的下一跳集合,然后计算网络中的关键链路,最后利用 Not-Via 方案保护关键链路。HLP 不仅降低了 Not-Via 的计算开销,而且与 Not-Via 有着相同的故障保护率。

### (3)Tunnels

Bryant 等<sup>[54]</sup>提出了一种基于隧道(Tunnels)的 IP 快速重路由方案,但是此方案在寻找可靠、有效的中转点时的性能还需要提升。针对此问题,文献[54]提出了计算隧道终点的启发式算法。

### (4)MPLS 路径保护方案

MPLS 路径保护方案<sup>[55]</sup>的原理与 Not-Via 方案的原理类似,都是为每条链路分配两个地址,分别为普通的 IP 地址和 MPLS 地址,在发生故障时启用 MPLS 隧道以绕开发生故障的链路或结点。MPLS 方案可以提供快速转发分组,缩短数据流的切换时间。此方案缩短了交换时间,但适用范围有限,只适用于支持 MPLS 协议的网络。

### (5)段路由

段路由(Segment Routing,SR)<sup>[56-60]</sup>是为了支持具有严格服务等级协议(Service Level Agreement,SLA)保证的应用而提出来的。SR 的核心思想是利用一连串的分段来构建端到端的路径。因为大部分网络供应商已经支持 SR,所以可以根据 SR 来实现基于 IP 的快速重路由机制。

## 4 域内路由可用性提高方案的比较

表 1 总结了提高域内路由可用性的各种方案的优缺点。

表 1 提高路由可用性的各方案的优缺点

Table 1 Advantages and disadvantages of the schemes for improving routing availability

		优势	劣势
被动保护方案	改变路由协议参数	不需要修改路由协议,实现简单,容易部署,加快了路由收敛速度	稳定性差,容易引起路由震荡,给路由器带来额外的负担
	修改链路权重	不产生环路、提高了路由可用性	适用范围有限,只能处理可以预见的故障,无法处理突发故障
路由保护方案	ECMP	实现简单、容易部署	对路由可用性贡献较小
	LFA	实现简单、容易部署	对路由可用性贡献较小,对网络拓扑有一定的要求
	O <sub>2</sub>	减缓网络堵塞、分担流量冲击	实现复杂度较高、对网络拓扑有一定的要求
	逐跳转发	利用无环路规则避免路由环路,提高路由可用性	实现复杂度较高、难以部署
	MRC	多个配置图可以保护部分节点和链路	消耗大量资源、需要大量配置
	FCP	避免路由环路	实现复杂度较高、对路由协议改动较大,难以部署
	DMPA	复杂度比较低,容易部署	对路由可用性贡献较小
非逐跳转发	Not-Via	路由可用性高	实现复杂度较高,对路由协议改动较大,难以部署
	Tunnels	路由可用性高	实现复杂度较高,要求路由器支持直接转发
	段路由	路由可用性高,转发方式灵活	对路由协议改动较大
	MPLS	适用于对实时性要求较高的应用	部署开销大,只适用于支持 MPLS 协议的网络

被动恢复方案主要是从加快路由收敛过程方面进行改进,比如加快收敛过程,缩短中断时间等;但是在改进收敛过程的同时,也要注意路由的稳定性,因为链路的频繁断开可能会引起路由动荡。

基于逐跳转发的路由保护方案与目前的路由协议有着相同的转发方式,因此部署比较简单,实用性很强;但是需要考虑资源消耗和复杂度的问题。

与逐跳转发方案不同,基于非逐跳转发的路由保护方案需要借助辅助机制来实现报文的转发,因此很难在互联网中实际部署。

## 5 下一步的研究方向

### 5.1 路由算法的复杂度

路由算法的复杂度是网络处理故障能力的标尺。目前已有算法的复杂度普遍较高,因此很难在实际中部署。如何降低路由算法的复杂度,是亟需解决的一个关键问题。

### 5.2 保护方案的适用性

在提出提高路由可用性的方案时,应该考虑其与目前路由协议的兼容性。目前有些方案的适用范围有限、与路由协

议不符或者改动较大,这样就无法满足现有网络的需求,从而不能应用到具体的网络中。

### 5.3 增加链路可靠性

当网络中的链路频繁出现故障时,会导致路由不稳定等问题。因此,可以通过提高链路可靠性、适时调整数据的传递效率、减少链路断开次数来提高路由可用性。

### 5.4 基于关键节点的路由保护方案

目前已有的路由保护算法大部分复杂度都比较高,而且很难部署,很少考虑网络节点的重要程度。而实际网络中,节点的重要程度是不同的。相关研究<sup>[61-62]</sup>已表明网络中的故障有高度集中的特征,因此在研究中不能将节点一概而论,需要特殊节点特殊对待,在此基础上再进一步研究路由可用性及其相应的算法。

**结束语** 本文首先说明了提高域内路由可用性的必要性;然后总结了已有提高域内路由可用性的方法,将已有方法分为被动恢复方案和路由保护方案,根据报文转发方式的不同又将路由保护方案进一步分为逐跳转发方法和非逐跳转发方法;接着详细介绍了每种方法的优缺点;最后讨论了下一步的研究方向。

## 参 考 文 献

- [1] CLARK D. The design philosophy of the DARPA internet protocols[J]. *Acm Sigcomm Computer Communication Review*, 1988, 18(4):106-114.
- [2] ALBERT R, JEONG H, BARABÁSI A L. Internet: Diameter of the World-Wide Web[J]. *Nature*, 1999, 401(6):130-131.
- [3] TURKLE S. Life on the Screen: Identity in the Age of the Internet[J]. *Science*, 1997, 23(2):123-149.
- [4] VARSHNEY U, SNOW A, MCGIVERN M, et al. Voice over IP [J]. *Communications of the Acm*, 2002, 45(1):89-96.
- [5] GOODE B. Voice over internet protocol (voip) [J]. *Proceedings of the IEEE*, 2002, 90(9):1495-1517.
- [6] DREW P, GALLON C. Next-generation voip network architecture [C]// *Proceedings of Multiservice Switching Forum*. New York: IEEE Press, 2003:1-19.
- [7] YALLOUZ J, ROTTENSTREICH O, BABARCZI P, et al. Optimal Link-Disjoint Node-“Somewhat Disjoint” Paths [C]// *Proceedings of International Conference on Network Protocols (ICNP)*. New York: IEEE Press, 2016:1-10.
- [8] KWONG K W, GAO L, ZHANG Z L. On the feasibility and efficacy of protection routing in IP networks [J]. *IEEE/ACM Transactions on Networking*, 2011, 19(5):1543-1556.
- [9] GOPALAN A, RAMASUBRAMANIAN S. IP Fast Rerouting and Disjoint Multipath Routing With Three Edge-Independent Spanning Trees [J]. *IEEE/ACM Transactions on Networking*, 2016, 24(3):1336-1349.
- [10] ANTONAKOPOULOS S, BEJERANO Y, KOPPOL P. Full Protection Made Easy: The DisPath IP Fast Reroute Scheme [J]. *IEEE/ACM Transactions on Networking*, 2015, 23(4):1229-1242.
- [11] XU A, BI J, ZHANG B. Failure Inference for shortening traffic Detours [C]// *Proceedings of IEEE/ACM International Symposium on Quality of Service (IWQoS)*. New York: IEEE Press, 2016:1-10.
- [12] TAPOLCAI J, RETVARI G, BABARCZI P, et al. Scalable and Efficient Multipath Routing: Complexity and Algorithms [C]// *Proceedings of International Conference on Network Protocols (ICNP)*. New York: IEEE Press, 2015:376-385.
- [13] ZHENG J Q, XU H, ZHU X J, et al. We’ve Got You Covered: Failure Recovery with Backup Tunnels in Traffic Engineering [C]// *Proceedings of International Conference on Network Protocols (ICNP)*. New York: IEEE Press, 2016:1-10.
- [14] YANG Y, XU M, LI Q. Tunneling on demand: A lightweight approach for IP fast rerouting against multi-link failures [C]// *Proceedings of IEEE/ACM International Symposium on Quality of Service (IWQoS)*. New York: IEEE Press, 2016:1-6.
- [15] ANTONAKOPOULOS S, BEJERANO Y, KOPPOL P. Full Protection Made Easy: The DisPath IP Fast Reroute Scheme [J]. *IEEE/ACM Transactions on Networking*, 2016, 23(4):1229-1242.
- [16] MARKOPOULOU A, IANNACCONE G, BHATTACHARYYA S, et al. Characterization of failures in an operational ip backbone network [J]. *IEEE/ACM Transactions on Networking*, 2008, 16(4):749-762.
- [17] HOU M J, WANG D, XU M W, et al. Selective protection: A Cost-Efficient Backup Scheme for Link State Routing [C]// *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*. New York: IEEE Press, 2009:68-75.
- [18] MOY J. RFC 2328: OSPF Version 2 [S]. USA: Soc Internet Society, 1998.
- [19] BASU A, RIECKE J. Stability issues in OSPF routing [J]. *Acm Sigcomm Computer Communication Review*, 2001, 31(4):225-236.
- [20] CLAD F, MERINDOL P, VISSICCHIO S, et al. Graceful router updates in link-state protocols [C]// *Proceedings of International Conference on Network Protocols (ICNP)*. New York: IEEE Press, 2013:1-10.
- [21] FRANCOIS P, BONAVENTURE O. Avoiding Transient Loops During the Convergence of Link-State Routing Protocols [J]. *IEEE/ACM Transactions on Networking*, 2007, 15(6):1280-1292.
- [22] PAL S, GADDE R, LATCHMAN H A. On the reliability of voice over ip (VoIP) telephony [C]// *Proceedings of International Conference on Computing, Communications and Control Technologies*. New York: IEEE Press, 2011:1-8.
- [23] XU M W, HOU M J, WANG D, et al. An efficient critical protection scheme for intra-domain routing using link characteristics [J]. *Computer Networks*, 2013, 57(1):117-133.
- [24] XU A, BI J, ZHANG B B, et al. Failure Inference for shortening traffic Detours [C]// *Proceedings of IEEE/ACM International Symposium on Quality of Service (IWQoS)*. New York: IEEE Press, 2017:1-10.
- [25] KWONG K W, GAO L, ZHANG Z L. On the feasibility and efficacy of protection routing in IP networks [J]. *IEEE/ACM Transactions on Networking*, 2011, 19(5):1543-1556.
- [26] PENG Q, WALID A, LOW S H. Multipath TCP algorithms: theory and design [C]// *Proceedings of the ACM SIGMETRICS/International Conference on Measurement and Modeling of Computer Systems*. 2013:305-316.
- [27] GRAN E G, DREIBHOLZ T, KVALBEIN A. NorNet Core-A multihomed research testbed [J]. *Computer Networks*, 2014, 61(C):75-87.
- [28] ATLAS A, KEBLER R, KONSTANTYNOWICZ M, et al. An Architecture for IP/LDP Fast-Reroute Using Maximally Redundant Trees [S]. USA: ISOC Internet Society, 2015.
- [29] ENYEDI G, CSASZAR A, ATLAS A, et al. Algorithms for computing Maximally Redundant Trees for IP/LDP Fast-Reroute [S]. USA: ISOC Internet Society, 2013.
- [30] XU M W, LI Q, PANG L T, et al. The model and algorithm on network failure and self-healing Routing [J]. *Scientia Sinica*, 2010, 40(7):943-953. (in Chinese)  
徐明伟, 李琦, 潘凌霄, 等. 网络故障及自愈路由模型和算法 [J]. *中国科学: 信息科学*, 2010, 40(7):943-953.
- [31] XU M W, YANG Y, LI Q. Survey of Intra-Domain Self-Healing Routing [J]. *Acta Electronica Sinica*, 2009, 37(12):2753-2761. (in Chinese)  
徐明伟, 杨莞, 李琦. 域内自愈路由研究综述 [J]. *电子学报*, 2009, 37(12):2753-2761.
- [32] LI Q. Availability and Scalability Issues in Internet Routing: A Weak Forwarding Correctness Approach [D]. Beijing: Tsinghua University, 2013. (in Chinese)

- 李清. 基于弱转发的互联网路由可用性和扩展性研究[D]. 北京:清华大学, 2013.
- [33] LEE S, YU Y, NELAKUDITI S, et al. Proactive vs Reactive Approaches to Failure Resilient Routing[C] // Proceedings of IEEE International Conference on Computer Communication (INFOCOM). New York: IEEE Press, 2004: 1-11.
- [34] GENG H J. Research on Routing Metric based Intra-Domain Multipath Routing [D]. Beijing: Tsinghua University, 2015. (in Chinese)  
耿海军. 基于路由度量的域内多路径路由研究[D]. 北京: 清华大学, 2015.
- [35] NARVAEZ P. Routing Reconfiguration in IP Networks[D]. Massachusetts: Massachusetts Institute of Technology, 2000.
- [36] NARVAEZ P, SIU K, TZENG H. New dynamic algorithms for shortest path tree computation[J]. IEEE/ACM Transactions on Networking (TON), 2000, 8(6): 734-746.
- [37] NARVAEZ P, SIU K, TZENG H. New dynamic spt algorithm based on a ball-and-string model[J]. IEEE/ACM Transactions on Networking (TON), 2001, 9(6): 706-718.
- [38] FRANCOIS P, SHAND M, BONAVENTURE O. Disruption free topology reconfiguration in OSPF networks[C] // Proceedings of IEEE International Conference on Computer Communication (INFOCOM). New York: IEEE Press, 2007: 89-97.
- [39] FORTZ B, THORUP M. Optimizing OSPF/IS-IS weights in a changing world[J]. IEEE Journal on Selected Areas in Communications, 2002, 20(4): 756-767.
- [40] NUCCI A, SCHROEDER B, BHATTACHARYYA S, et al. IGP Link Weight Assignment for Transient Link Failures[C] // Proceedings of the International Teletraffic Congress. New York: IEEE Press, 2003: 321-330.
- [41] FERGUSON D, MOY J, COLTUN R. RFC 2740: OSPF for IPv6[S]. USA: ISOC Internet Society, 1999.
- [42] ATLAS A, ZININ A. Basic specification for ip fast reroute: Loop-free alternates[S]. USA: ISOC Internet Society, 2008.
- [43] ATLAS A. U-turn alternates for IP/LDP fast-reroute[S]. USA: ISOC Internet Society, 2006.
- [44] GENG H, SHI X, WANG Z, et al. A hop-by-hop dynamic distributed multipath routing mechanism for link state network [J]. Computer Communications, 2018, 116: 225-239.
- [45] YANG X, WETHERALL D. Source selectable path diversity via routing deflections[C] // Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM). 2006: 159-170.
- [46] SCHOLLMEIERS G, CHARZINSKI J, KIRSTADTER A, et al. Improving the resilience in IP networks[C] // Proceedings of IEEE HPSR. New York: IEEE Press, 2003: 91-96.
- [47] KVALBEIN A, HANSEN A F, GJESSING S, et al. Fast ip network recovery using multiple routing configurations[C] // Proceedings of IEEE International Conference on Computer Communication (INFOCOM). New York: IEEE Press, 2007: 1-11.
- [48] LAKSHMINARAYANAN K, CAESAR M, RANGAN M, et al. Achieving convergence-free routing using failure-carrying packets[J]. Acm Sigcomm Computer Communication Review, 2007, 37(4): 241-252.
- [49] NELAKUDITI S, LEE S, YU Y, et al. Fast Local Rerouting for Handling Transient Link Failures[J]. IEEE/ACM Transactions on Networking, 2007, 15(2): 359-372.
- [50] ZHANG B, WU J, BI J. RPPF: IP fast reroute with providing complete protection and without using tunnels[C] // Proceedings of IEEE/ACM International Symposium on Quality of Service (IWQoS). New York: IEEE Press, 2013: 1-10.
- [51] YANG B, LIU J, SHENKER S, et al. Keep forwarding: Towards k-link failure resilient routing[C] // Proceedings of IEEE International Conference on Computer Communication (INFOCOM). New York: IEEE Press, 2014: 1617-1625.
- [52] ENYEDI G, RÉTVÁRI G, SZILÁGYI P, et al. IP Fast ReRoute: Lightweight Not-Via without Additional Addresses[C] // Proceedings of IEEE International Conference on Computer Communication (INFOCOM). New York: IEEE Press, 2009: 2771-2775.
- [53] GENG H, SHI X, YIN X, et al. An efficient link protection scheme for link-state routing networks[C] // Proceedings of IEEE International Conference on Communications (ICC). New York: IEEE Press, 2015: 6024-6029.
- [54] XU M, YANG Y, LI Q. Selecting Shorter Alternate Paths for Tunnel-based IP Fast ReRoute in Linear Time[J]. Computer Networks, 2012, 56(2): 845-857.
- [55] BANERJEE G, SIDHU D. Comparative analysis of path computation techniques for MPLS traffic engineering [J]. Computer Networks, 2002, 40(1): 149-165.
- [56] SOMMERS J, ERIKSSON B, BARFORD P. On the prevalence and characteristics of MPLS deployments in the open Internet [C] // Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM). New York: ACM Press, 2011: 445-462.
- [57] CHRIS B, GAURAV A, ANIL N, et al. Maximally Redundant Trees in Segment Routing[J]. Chinese Journal of Engineering Design, 2016, 94(1): 33-42.
- [58] CIANFRANI A, LISTANTI M, POLVERINI M. Incremental Deployment of Segment Routing Into an ISP Network: a Traffic Engineering Perspective[J]. IEEE/ACM Transactions on Networking, 2017, 25(5): 3146-3160.
- [59] HARTERT R, VISSICCHIO S, SCHAUS P, et al. A Declarative and Expressive Approach to Control Forwarding Paths in Carrier-Grade Networks[J]. Acm Sigcomm Computer Communication Review, 2015, 45(5): 15-28.
- [60] GENG H J, LIU J Q, YIN X. Single Node Failure Routing Protection Algorithm Based on Segment Routing [J]. Journal of Tsinghua University (Science and Technology), 2018, 58(8): 710-714. (in Chinese)  
耿海军, 刘洁琦, 尹霞. 基于段路由的单节点故障路由保护算法[J]. 清华大学学报(自然科学版), 2018, 58(8): 710-714.
- [61] HOU M J. Research on Internet Routing Protection [D]. Beijing: Tsinghua University, 2015. (in Chinese)  
侯美佳. 互联网路由保护研究[D]. 北京: 清华大学, 2015.
- [62] GENG H J, SHI X G, WANG Z L, et al. Intra-domain Routing Protection Algorithm Based on Critical Nodes [J]. Computer Science, 2018, 45(1): 183-187. (in Chinese)  
耿海军, 施新刚, 王之梁, 等. 基于关键节点的域内路由保护算法[J]. 计算机科学, 2018, 45(1): 183-187.