

## 一种基于结构化备份子图的路由系统失效恢复方法

王 禹\* 王振兴 张连成  
(解放军信息工程大学 郑州 450002)

**摘 要:** 鉴于当前路由系统失效恢复未能有效解决备份拓扑存储代价、冗余恢复能力以及自治域利益保护等问题, 该文在致瘫攻击易造成网络级联失效的背景下提出一种基于结构化备份子图的失效恢复方法 3R(Robust Route Recovery)。首先, 设计拓扑关键点和重要邻接点生成算法, 满足了备份子图基数小、增长率低的实际存储需求, 且具备同一子图内多点冗余恢复特性; 其次, 为充分考量自治域利益诉求, 设计基于流量权重的相邻链路排序算法, 折中路由由失效恢复与私有路由策略的双重需求; 在此基础上, 利用多次迭代生成各冗余恢复集合的备份子图。实验结果证实了方法的有效性。

**关键词:** 路由系统; 失效恢复; 结构化备份子图; 存储代价; 冗余恢复

**中图分类号:** TP393

**文献标识码:** A

**文章编号:** 1009-5896(2013)09-2254-07

**DOI:** 10.3724/SP.J.1146.2012.01669

## A Failure Recovery Method for Routing System Based on Structured Backup Subgraph

Wang Yu Wang Zhen-xing Zhang Lian-cheng  
(PLA Information Engineering University, Zhengzhou 450002, China)

**Abstract:** Current failure recovery for routing system has not effectively resolved issues including storage cost, redundant recovery and AS (Autonomous System) benefit protection. In the background of cascading failure prone to happen under paralyzing attack, a failure recovery approach 3R (Robust Route Recovery) based on structured backup subgraph is proposed. First, to reduce space complexity, two algorithms for topology keypoint and important adjacent nodes are designed to satisfy both demands of small radix and low increasing rate, as well as the redundant recovery feature for multi-node in the same subgraph. Second, considering the AS benefit request, sort for neighboring links based on traffic weight is implemented to make tradeoff between the failure recovery and private routing policy. Finally, structured backup subgraphs according to the redundant recovery sets are generated through multiple iterations. Simulation results show the effectiveness of 3R approach.

**Key words:** Routing system; Failure recovery; Structured backup subgraph; Storage cost; Redundant recovery

### 1 引言

互联网在国家经济和社会发展中的作用举足轻重, 应用于军队、电力、金融等关乎国计民生领域的路由系统更是扮演着极其重要的角色, 日益影响国家和社会的安定运行<sup>[1,2]</sup>。近年来出现了多起大规模路由系统安全事件<sup>[3-5]</sup>, 威胁到部分地区互联网的正常运行。路由系统的安全性已经逐渐被研究人员和管理者所认识, 目前针对路由系统的失效恢复研究主要集中于多路径转发、无结构备份路径与结构化备份拓扑。

YAMR<sup>[6]</sup>是一种多路径通告的多路转发协议,

为主路径上每条链路计算其备用路径, 保证链路失效时能够选择一条或多条备份路径迅速进行数据转发。类似地, MFT<sup>2</sup>-BGP<sup>[7]</sup>通过构建多转发树来实现路由恢复。然而, 由于多路径转发协议需要为每条路径计算多条冗余路径, 造成较高路由开销。

R-BGP<sup>[8]</sup>利用预计算备份路径完成路由系统恢复, 通过为最佳路径的下一跳通告最大不相交路径来解决路由的选择分发, 降低收敛的延迟, 类似方法为 D-BGP<sup>[9]</sup>。然而, 二者基于无结构的备份路径进行恢复, 只能应对已知的单点失效, 无法适用于级联失效场景, 恢复效率低且需修改 BGP 语义。

RRL<sup>[10]</sup>构建一个基于结构化备份拓扑的全局性抽象视图, 通过建立冗余拓扑子集并定义“安全节点”, 为每个子集计算备份路由表。它能够提供简单直观的恢复拓扑, 具备恢复的灵活性、较好状态增

2012-12-20 收到, 2013-04-19 改回

国家 863 计划项目(2009AA01A334, 2008AA01A323, 2008AA01A326)资助课题

\*通信作者: 王禹 stonchor@gmail.com

长性质；其改进方法为MRC<sup>[11]</sup>。然而，结构化备份拓扑方法通常需要计算大量恢复拓扑并修改现行协议语义。

由此，为应对潜在针对路由系统的致瘫攻击，本文借助已有中心化网络控制思想，提出了一种基于结构化备份子图的路由系统恢复方法3R(Robust Route Recovery)，在保证现有BGP协议不变的基础上，使得路由系统遭受失效后能够快速抽取预计算的备份子图，完成全局一致性路由恢复。3R具有良好的增量部署特性，并能有效应对致瘫攻击造成的级联失效场景。依照该方法生成的备份子图具备低空间复杂度、多节点冗余恢复以及自治系统(Autonomous System, AS)策略私有性保护等多重性质。

## 2 路由系统失效恢复

现有研究<sup>[12-14]</sup>已提出对路由系统进行中心化控制的思想，从而具备全局拓扑状态的实时感知能力，实现对底层网络的知悉与利用。在中心化控制模型的研究基础上，3R采用先验预计算方式构造结构化备份子图，当单AS遭受、或多AS级联失效后能够快速分发备份拓扑并实施恢复。

### 2.1 基本问题

根据Menger理论，图 $G$ 为 $k$ -连接的充要条件是对每对节点 $(u, v)$ ， $G$ 中至少存在 $k$ 条不相交的 $u-v$ 路径，该性质成为多数网络恢复研究的基础。本文意在基于中心化网络控制模型来构造结构化备份子图，保证所有AS节点具有一致性拓扑视图。目前亟需解决的主要问题可概括为：

**问题1** 传统的结构化备份子图构建方法易产生较多备份拓扑，不仅占用大量存储空间，且路由恢复时间增多。因此，首要问题应尽可能降低生成的备份子图存储代价，进而提高恢复效率。

**问题2** 网络致瘫攻击导致的AS路由失效势必引发网络负载急剧变化，在短时间内呈现级联失效场景，使得连续的单点恢复几乎无法实施。因此问题之二是令备份子图具备一定的冗余恢复能力。

**问题3** 将多个AS纳入中心化控制体系，在提升AS及整个路由系统安全性的同时势必会削弱AS个体的自身利益，因此问题之三是要一定程度上满足辖域内单自治域的利益诉求。

### 2.2 算法建立

(1)致瘫攻击下，路由系统的脆弱性主要来自其拓扑结构的不均衡性，部分关键AS及链路的级联失效将直接破坏路由系统的整体连通性。利用关键点发现算法能够找到既定拓扑中的关键AS。

#### 算法1 关键点(Key Point)发现 $KP(G)$

输入：原始拓扑 $G = (V, E)$ 。其中 $V$ 代表AS节点集合，每个 $v$ 表示一个AS，由唯一的标识编号及其拥有的前缀组成； $E$ 代表AS之间链路的集合，每条 $e$ 由起点 $v_s$ 和终点 $v_e$ 组成。

输出：关键AS集合KeyAS

步骤如下：

步骤1 从集合 $V$ 中随机抽取节点 $v$ ，对子图 $G' = (V - v, E)$ 进行DFS深度优先遍历，若 $G'$ 仍为连通图，则判断 $v$ 不是关键自治域节点。

步骤2 依次遍历节点集合，经过 $|V|$ 轮计算可获得关键自治域集合KeyAS。

由此得到KeyAS关键点集合。网络拓扑的关键节点遭受失效后将直接导致网络服务中断，它们是攻击者的重要目标，也是防御和恢复的重心。

(2)为保证备份拓扑具备最大通信效能，构建时应尽可能保留重要邻接节点间的链路，需要对负载分布情况进行评估，这里将拓扑结构与数据流量作为主要判断依据来生成重要邻接节点集合。

#### 算法2 重要邻接节点(PARTITION)集合 $PA(v)$

输入：原始拓扑 $G = (V, E)$ 与AS节点 $v$

输出：重要邻接节点集合 $RN_v$

步骤如下：

步骤1 利用函数NeighborNodes( $G, v$ )( $NN(G, v)$ )，获得 $v$ 的所有邻接节点集合 $N_v = \{n_1, n_2, \dots, n_m\}$ 。

步骤2 定义 $Ld_w$ 为AS节点 $w$ 的最短路径数(shortest-path betweenness)，代表节点 $w$ 的结构负载。作为一种无量纲判别方法，结构负载认为途径某节点的最短路径越多则该节点越重要，其承担的负载越多。

$$Ld_w = \frac{\sum_{k \neq k' \in V} \sigma_{kk'}(w)}{|V|(|V| - 1)} \quad (1)$$

式中 $\sigma_{kk'}$ 代表节点与 $k$ 之 $k'$ 间所有最短路径数， $\sigma_{kk'}(w)$ 代表 $k$ 之 $k'$ 间途径节点 $w$ 的最短路径数； $k$ 或 $k'$ 可以取节点 $w$ ，避免负载为零的情形。由式(1)，计算得到 $N_v$ 中各节点对应的结构负载集合 $Ld_{N_v} = \{Ld_{n_1}, Ld_{n_2}, \dots, Ld_{n_m}\}$ 。

步骤3 统计节点 $v$ 同集合 $N_v$ 中各节点在单位时段内的数据流量集合 $DT_v = \{dt_1, dt_2, \dots, dt_m\}$ ，从而获得节点在实际应用层面的负载分配情况，定义其为流量负载。

步骤4 将路由系统的全局平均结构负载 $\bar{Ld}$ 定义为结构负载重要度判断的过载阈值，同时将自治域节点 $v$ 对应的 $DT_v$ 中平均数据流量 $\bar{dt}$ 定义为流

量负载重要度判断的过载阈值。对于任一  $n_i \in N_v$ ，若同时满足结构负载  $Ld_i > \bar{L}d$  及  $dt_i > \bar{d}t$ ，则判定该节点在网络结构和业务流量层面均为重要，令  $n_i \in RN_v$ 。

依照上述步骤，循环判断  $N_v$  中每个节点从而获得  $v$  对应的  $RN_v$ 。值得注意的是，流量负载通常只反映一段时间内的节点负载特征；路由拓扑则相对稳定，由此生成的结构负载能够更加定性地反映网络负载分配，因此将二者结合可以更有效的发现重要邻接节点。

(3) 中心化控制模型面临的一大挑战即如何建立多 AS 间的协作关系。由此，通过设计基于权值的链路排序算法，加入对 AS 个体利益的考虑。

**算法 3** AS 邻接链路排序 LinkSort( $G, v$ )(LS( $G, v$ ))。

输入：原始拓扑  $G = (V, E)$  与指定 AS 节点  $v$

输出：基于权值的邻接链路序列  $P(e_v^1, e_v^2, \dots, e_v^m)$

步骤如下：

步骤 1 利用  $L(G, v)$ ，获得  $G$  中节点  $v$  的所有邻边集合  $E_v = \{e_1, e_2, \dots, e_m\}$ 。

步骤 2 依据路由系统的流量特征构造分段赋值函数，通过统计  $E_v$  中各链路单位时间内流量，利用分段函数赋予其不同权值。图 1 给出 AS1 的链路权值配置方案。

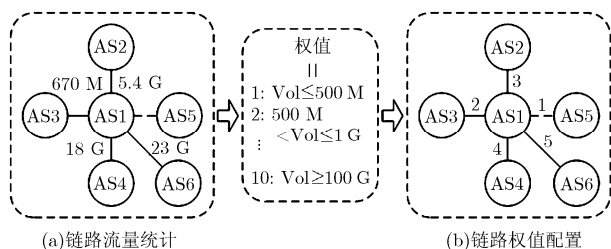


图 1 链路权值配置示例

步骤 3 根据上述权值分配，对  $E_v$  中链路进行增序排列，获得序列  $P(e_v^1, e_v^2, \dots, e_v^m)$ 。

由此获得基于权重的 AS 邻接链路序列，用于构造备份子图。LS( $G, v$ ) 着重考虑 AS 的实际利益保护，如图 1(a) 中 AS1 与 AS5 之间确有邻边，但无统计流量，可推断出于利益保护等因素，AS1 未经该链路转发数据。失效恢复时则应当充分利用该链路，折中 AS1 的利益诉求与通信恢复需求，赋予其较小权值。

(4) 基于上述算法的支撑，建立失效恢复算法 3R(Robust Route Recovery)。

**算法 4** 路由系统失效恢复 3R( $G$ )

输入：原始拓扑  $G = (V, E)$

输出：备份子图集合  $G_{\text{backup}} = \{G_1, G_2, \dots, G_m\}$ 。  
具体步骤如表 1 所示。

表 1 路由系统失效恢复 3R 步骤

	$G = (V, E)$ ; //初始化 $G$
	$i = 1$ ; //初始化变量 $i$
1	Do
	$G_i = G$ ;
	$K = \text{KP}(G_i)$ ; //发现关键点集合
2	While( $K \neq V$ )
	$V' = V - K - (\text{Gp}_1 + \text{Gp}_2 + \dots + \text{Gp}_{i-1})$ ; // $V'$ 代表当前非关键节点集， $\text{Gp}_i$ 为备份子图 $G_i$ 对应的冗余恢复节点集
	$n = \text{MD}(V')$ ; //发现度最高节点 $n$
	$RN_n = \text{PA}(n)$ ; //获得重要邻接点集合
	$PN_n = \text{LS}(RN_n)$ ; //按照节点度递增排列
3	For( $j = 1; j ++; v_j \in PN_n$ )
	If( $v_j \notin \text{KP}(G_i)$ )
	$P(e_{v_j}^1, e_{v_j}^2, \dots, e_{v_j}^m) = \text{LS}(G, v_j)$ ;
	$G_i = G_i - (e_{v_j}^1 + e_{v_j}^2 + \dots + e_{v_j}^{m-1})$ ;
	EndIf
	$K = K \cup v_j$ ; //将节点 $v_j$ 加入关键点集，并纳入 $G_i$ 的冗余恢复集合
	EndFor
	EndWhile
	Store $G_i$ ;
4	$\text{Gp}_i = \text{LN}(G_i)$ ;
	$i = i + 1$ ;
	While( $(\text{Gp}_0 \cup \text{Gp}_1 \cup \dots \cup \text{Gp}_{i-1}) \neq V$ )

注：Gp 是 Group 的缩写，MD 是 FindMaxDegree 的缩写，LN 是 LeafNode 的缩写。

重要步骤描述如下：

步骤 1 利用 Do-While 循环获得多个备份拓扑子图，直至所有 AS 落入拓扑子图对应的冗余恢复集合。

步骤 2 利用 While 循环获得单个备份拓扑子图。关键点集合  $K$  作为一个判断标识，其目的是对整个节点集合进行判断，将符合条件的部分节点及链路生成为一个备份子图。

步骤 3 利用 For 循环依次判断  $PN_n$  中每个节点。若某节点不为关键点，则使用 LS() 对其所有邻边依照权重进行排序，仅为目前生成的备份拓扑子图保留最大权重链路。

步骤 4 利用 LN( $G_i$ ) 求得备份子图  $G_i$  的叶子节点，即冗余恢复节点，将其存储于  $\text{Gp}_i$ ，当这些节点出现独立或级联失效，依照  $G_i$  进行路由恢复，保证路由系统中剩余节点的正常通信。

可知，当节点数目为  $n$  时，3R 的最坏时间复杂度为  $O(n^4)$ ，然而由于备份拓扑为预先计算生成，因此并不影响失效恢复的实际效率；单个备份子图的空间复杂度为  $O(n^2)$ ，由于所有备份子图均存储于中心控制平台，仅在失效恢复时将对应的备份子图分发至各 AS，因此并不额外占用 AS 的存储空间。

### 3 备份子图构造实例

为进一步阐述上述结构化备份子图生成算法，以 8 个自治域节点组成的路由系统为例进行分析，图 2(a)为路由系统的初始拓扑。旨在简化说明过程，每条链路上的数字表示业已量化的链路权值。

首先运用  $KP(G)$ ，发现原始拓扑中的关键节点集为空。根据分析，蓄意致瘫攻击主要对象为连接度较高节点，因此  $MD()$  将此拓扑中度最大的 AS5 作为首要遭袭对象；鉴于致瘫攻击对邻接 AS 造成的级联失效作用，运用  $PA()$  划分重要邻接节点集，为简化处理，包含 AS5 所有邻接点，则  $RN_5 = \{AS1, AS2, AS4, AS5, AS6, AS8\}$ ；依照连接度增序对各节点进行依次判断，若当前不为关键点，仅保留该点的最大权重临边，并将其纳入关键点集合，则对于 AS5 仅保留同 AS6 之间链路。对 AS4 仅保留其同 AS8 之间链路。此时  $RN_5$  中所有节点均已为关键点，循环结束。由此获得图 2(c)中的备份子图  $G_1$ ，对应的冗余恢复节点集合  $G_{p_1} = \{AS1, AS2, AS4, AS5\}$ ，用于该集合节点独立或级联失效后整个路由

系统的恢复。

之后，仍从原始拓扑出发，剩余节点中 AS8 度为最高，经计算仅保留其同 AS4 间链路；由 AS8 获得的重要邻接节点集  $RN_8 = \{AS4, AS5, AS6, AS7, AS8\}$ ，目前只需考虑 AS6 和 AS7，分别对二者进行邻接链路权重排序和去边处理，获得如图 2(e)的备份子图  $G_2$ ，对应的冗余恢复集合  $G_{p_2} = \{AS2, AS3, AS6, AS7, AS8\}$ 。至此  $G_{p_1}$  与  $G_{p_2}$  已涵盖路由系统所有节点，备份子图生成完毕。开销方面，假设路由系统包含  $n$  个 AS，则备份子图空间复杂度为  $O(n^2)$ ，事实上考虑到当前路由系统的无标度特性，实际开销要远小于  $O(n^2)$ 。

## 4 仿真实验分析

### 4.1 备份子图个数

为验证路由系统失效恢复方法 3R 的空间复杂度、扩展性及冗余恢复性，本节利用已有的互联网拓扑模型和拓扑产生器生成仿真路由系统拓扑，在此基础上，针对生成的备份子图个数进行分析。

**4.1.1 数量分布特征** 本文利用 BRITE<sup>[15]</sup>拓扑产生器，依照 Waxman<sup>[16]</sup>和 GLP<sup>[17]</sup>模型分别生成 AS 级仿真拓扑共 15 种类型，每类含 100 个拓扑。拓扑中节点数目范围设定为 8~256，其中 Waxman 模型的平均节点度为 6，GLP 为 4.2。图 3 中 wa 表示 Waxman 模型，glp 表示 GLP 模型。

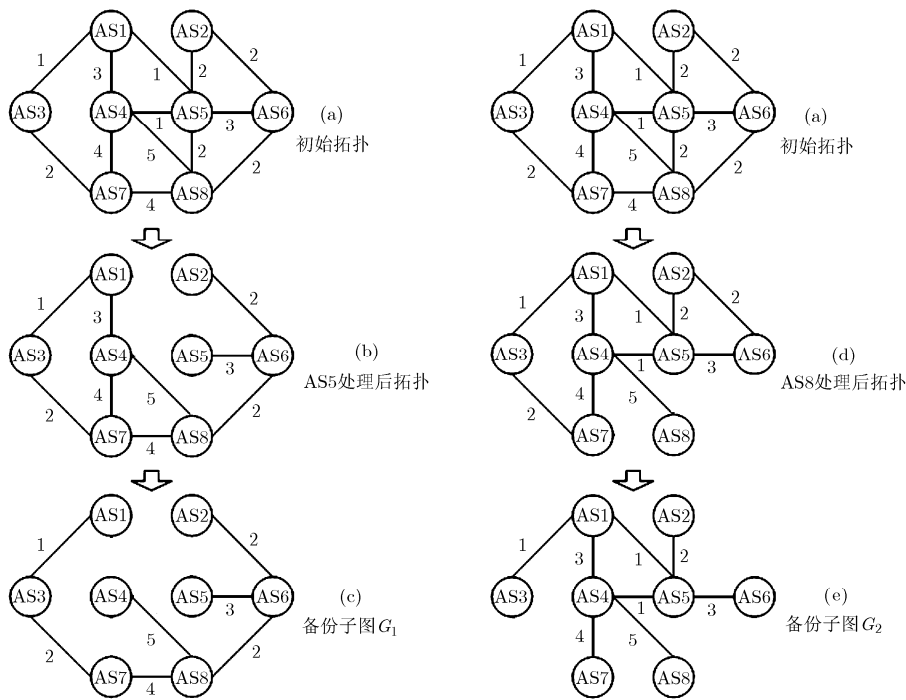


图 2 一个路由系统备份拓扑子图构造实例

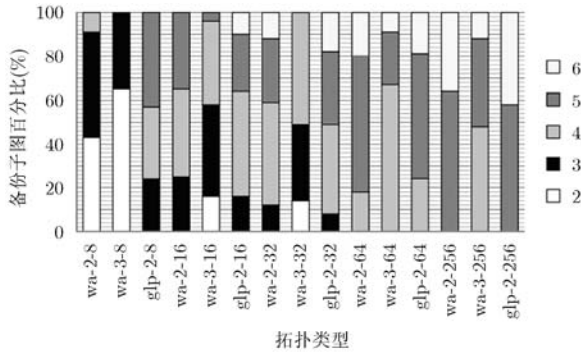


图 3 仿真拓扑下生成的备份子图个数分布

为链路随机赋予 1~5 的权重, 综合代表流量与拓扑结构属性。图 3 给出了针对 15 种拓扑类型, 基于 3R 得到的最小备份子图个数分布。拓扑类型表示为模型-链路-节点的形式, 如 wa-2-8 代表节点数为 8, 链路/节点(L/N)比率为 2 的 Waxman 模型网络。表 2 给出由 Waxman 模型生成的平均备份子图个数。可知, 在具有相同节点数目时, L/N 率较高的备份子图个数较少, 最大差幅为 22.5%(节点数为 32)。分析可知, 节点间连接增多势必导致节点相关度的提高, 使得冗余恢复集合规模扩大, 由此产生较少的备份子图个数。

表 2 各 Waxman 拓扑的平均备份子图个数

拓扑类型	wa-2-8	wa-2-16	wa-2-32	wa-2-64	wa-2-256
	wa-3-8	wa-3-16	wa-3-32	wa-3-64	wa-3-256
子图数目	2.66	4.10	4.41	5.02	5.36
	2.35	3.33	3.37	4.42	4.64

表 2 表明, 由 Waxman 仿真拓扑生成的备份子图, 节点数为 256 时所需平均子图个数仅为 5~6, 证明 3R 产生的备份拓扑子图具备较低的空间复杂度, 可充分满足子图存储空间及路由分发性能两方面的需求。

**4.1.2 增长及冗余性质** 表 3 显示了基于 GLP 模型的 L/N 率为 2 的平均备份子图个数。结合表 2 中 Waxman 模型生成的备份子图数据, 绘制各类型网络对应的备份子图增长态势, 见图 4。观察 Waxman 仿真拓扑的平均备份子图个数可以发现, L/N 率为 2 时, 节点数为 16 与 32 对应子图个数均为 5, 节点数为 64 与 256 时子图个数均为 6。在节点数目成倍增长的同时, 相应备份子图个数增幅却极其滞缓。Waxman 中 L/N 率为 3 及 GLP 模型亦如此。

该结果表明, 伴随路由系统规模的增大, 基于 3R 生成的备份子图个数增长非常缓慢。即 3R 算法

表 3 L/N 率为 2 的 GLP 拓扑平均备份子图个数

拓扑类型	glp-2-8	glp-2-16	glp-2-32	glp-2-64	glp-2-256
子图数目	3.79	4.37	4.69	4.95	5.42

具备良好的增长特性, 能有效控制备份子图数量, 由此验证了算法的可扩展性。更重要的, 对于给定节点数目, 备份子图数量越少则意味着每个子图中包含的冗余恢复节点越多, 即备份子图数量同冗余恢复能力成反比。由图 4 可得, 对比于原始单节点失效路径生成方法, 3R 在 Waxman 及 GPL 模型下的备份子图生长曲线均平缓得多; 根据表 2 与表 3 可知, 对于节点数为 64 的网络拓扑, 其对应的每个备份拓扑包含大致 10 个叶节点, 即能够同时满足这些节点失效后的路由恢复, 从而证明该算法具有较好的冗余恢复特性。

级联效应造成的多点失效场景, 其短间隔连续失效特性使得传统方法效率低下, 而 3R 能利用极少的备份拓扑完成存活节点间的通信恢复。由于备份子图数量增幅缓慢, 可将其设为常数  $k$ , 当 AS 节点数目为  $n$  时, 3R 计算单个备份子图的空间复杂度为  $O(n^2)$ , 则备份子图的整体存储开销为  $k \times (n^2) \sim O(n^2)$ 。

## 4.2 备份路径长度

考量 3R 算法空间复杂度的另一个重要指标为备份路径长度。

**4.2.1 相异生成算法的比较** 3R 生成的备份子图去除了原始拓扑中部分链路, 减少了可选路径。本节通过生成仿真拓扑, 分析单节点失效情形下的备份路径长度分布, 并与典型的最优备份路径以及 RRL 备份路径进行比对。

利用 BRITE, 基于 Waxman 和 GLP 模型各生成 100 个仿真拓扑, 每个拓扑 L/N 为 64/32。分别依照 3R, RRL 以及最优化方法对所有原始路径计算备份路径, 以获得相应的平均备份路径长度, 结果见图 5。表 4 总结了各拓扑类型对应的平均路径长度。可知, 对于 Waxman 和 GLP 拓扑模型, 利用任一生成方法获得的路径长度相仿, GLP 对应的拓扑长度略小于 Waxman, 证明两类模型对于备份拓扑长度影响甚微。

对照上述结果可知, 由于最优备份路径选择移除单失效节点外整个拓扑中的最短路由, 因此长度最短。RRL 在计算层中节点时未予优化, 易于造成节点聚集。而 3R 在利用 PA( $v$ ) 构建重要邻接节点集合时有意筛去了负载较低节点, 一定程度上降低了

表 4 平均备份路径长度

拓扑类型	wa-3R	glp-3R	wa-RRL	glp-RRL	wa-opt	glp-opt
路径长度	4.06	3.96	4.31	4.30	3.74	3.61

单个子图含有的节点个数，因此 3R 的平均备份路径要略短于 RRL 算法，意味着存储代价小于后者。

**4.2.2 相异拓扑构成的影响** 本节针对不同拓扑构成(相异节点数及链路数)，验证其对备份路径长度的影响。利用 BRITE 基于 Waxman 模型分别生成 L/N 为 64/32, 96/32 以及 256/128 的仿真路由系统，分别运用 3R 算法和最优路径选择算法获得备份拓扑子图，其备份路径长度分布结果如图 6。

将 3R 备份路径长度与最优路径长度进行比对，表 5 给出了各类网络拓扑对应的平均备份路径长度。易于发现，对于具备相同拓扑构成的仿真网络，基于最优路径算法生成的路径长度均小于 3R 算法。

然而，具有相同节点数目时，链路数目越多的拓扑产生的平均备份路径长度越短。分析可知，L/N 率的提高会增强节点间的连接度，从而提供更多的冗余恢复路由，降低了平均备份路径长度。此外，相同 L/N 率情况下，较大规模的网络包含较多节点，

则节点间距离也相应增大，其所需的备份路径长度也越大。

### 5 结束语

互联网规模的急剧扩展和实时应用的诸多需求对路由系统的失效恢复提出更高要求，本文提出了一种基于结构化备份子图的路由系统失效恢复方法 3R，其生成的备份拓扑具备较低的存储代价及较好的冗余恢复特性。3R 利用 KP()和 PA()分别计算拓扑中关键点与重要邻接点，减少备份子图个数的同时缩短备份路径长度，并具备多点冗余恢复能力；运用 LS()依照流量权重对相邻链路进行排序，实施失效恢复时尽量保护 AS 自身利益。最后，通过仿真实验对 3R 方法生成的备份子图个数及路径长度进行了多角度的比对分析，验证了该方法的优越性。考虑域间路由系统时，鉴于 3R 需要掌握 AS 间私有信息，必须保证中心控制节点的安全性，因此其组成构建以及路由恢复策略是未来的重要研究内容。

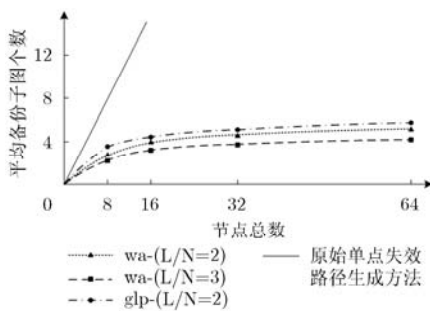


图 4 备份子图增长态势

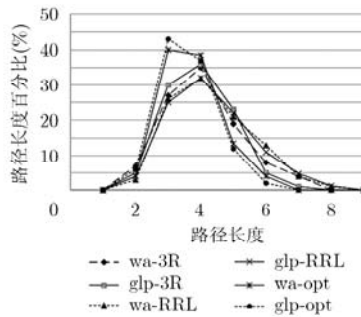


图 5 不同备份拓扑方法的路径长度分布

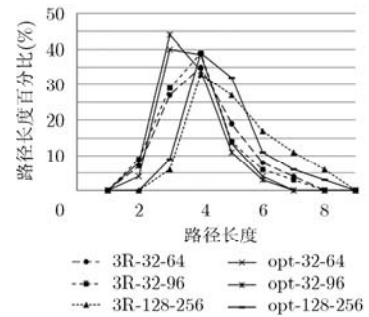


图 6 不同 L/N 率下的备份路径长度

表 5 平均备份路径长度

拓扑类型	3R-32-64	3R-32-96	3R-128-256	opt-32-64	opt-32-96	opt-128-256
路径长度	4.06	3.91	5.12	3.74	3.57	4.75

### 参考文献

[1] 刘志辉, 孙斌, 谷利泽, 等. 一种防范 BGP 地址前缀劫持的源认证方案[J]. 软件学报, 2012, 23(7): 1908-1923.  
Liu Z H, Sun B, Gu L Z, et al. Origin authentication scheme against BGP address prefix hijacking[J]. *Journal of Software*, 2012, 23(7): 1908-1923.

[2] Lippert K J and Seger R A. The story behind network defense[C]. 8th International Conference on Information Technology: New Generations, Las Vegas, USA, Apr. 11-13,

2011: 909-913.

[3] Theodoridis G, Tsigkas O, and Tzovaras D. A novel unsupervised method for securing BGP against routing hijacks[C]. 27th International Symposium on Computer and Information Sciences, Paris, France, Oct. 3-4, 2012: 21-29.

[4] Geoff H, Mattia R, and Grenville A. Securing BGP-A literature survey[J]. *IEEE Communications Surveys & Tutorials*, 2011, 13(2): 199-222.

[5] André M. Anomaly detection in enterprise networks[D].

- [Ph.D. dissertation], University of Porto, 2011.
- [6] Ganichev I, Dai B, Godfrey P B, *et al.* YAMR: yet another multipath routing protocol[J]. *ACM SIGCOMM Computer Communication Review*, 2010, 40(5): 14–19.
- [7] 胡乔林, 彭伟, 陈新, 等. MFT<sup>2</sup>-BGP: 基于多转发树的无中断域间路由协议[J]. *计算机学报*, 2012, 35(10): 2023–2036.  
Hu Q L, Peng W, Chen X, *et al.* MFT<sup>2</sup>-BGP: achieving disruption-free inter-domain routing protocol using multiple forwarding trees[J]. *Chinese Journal of Computers*, 2012, 35(10): 2023–2036.
- [8] Kushman N, Kandula S, Katabi D, *et al.* R-BGP: staying connected in a connected world[C]. 4th USENIX Symposium on Networked System Design & Implementation, Cambridge, USA, Apr. 11–13, 2007: 341–354.
- [9] Wang F and Gao L. Path diversity aware interdomain routing[C]. 28th IEEE International Conference on Computer Communications, Rio de Janeiro, Brazil, Apr. 19–25, 2009: 307–315.
- [10] Hansen A F, Kvalbein A, Cicic T, *et al.* Resilient routing layers for recovery in packet networks[C]. International Conference on Dependable Systems and Networks, Yokohama, Japan, June 28–July 1, 2005: 238–247.
- [11] Kvalbein A, Hansen A F, Cicic T, *et al.* Fast IP network recovery using multiple routing configurations[C]. 25th IEEE Conference on Computer Communications, Barcelona, Spain, Apr. 23–29, 2006: 1–11.
- [12] Hong Y. A practical system for centralized network control[D]. [Ph.D. dissertation], Carnegie Mellon University, 2010.
- [13] 曲延盛, 李伟, 罗军舟, 等. 可信可控网络中的 QoS 资源控制模型[J]. *软件学报*, 2011, 22(11): 2782–2794.  
Qu Y S, Li W, Luo J Z, *et al.* Resource control model for QoS in the trustworthy and controllable network[J]. *Journal of Software*, 2011, 22(11): 2782–2794.
- [14] John P J, Ethan K B, Arvind K, *et al.* Consensus routing: the internet as a distributed system[C]. 5th USENIX Symposium on Networked Systems Design and Implementation, San Francisco, USA, Apr. 16–18, 2008: 351–364.
- [15] Medina A, Lakhina A, Matta I, *et al.* BRIT: an approach to universal topology generation[C]. 9th International Workshop on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, Cincinnati, USA, Aug. 15–18, 2001: 346–353.
- [16] Waxman B M. Routing of multipoint connections[J]. *IEEE Journal on Selected Areas in Communications*, 1988, 6(9): 1617–1622.
- [17] Bu T and Towsley D. On distinguishing between internet power law topology generators[C]. 21th IEEE Conference on Computer Communications, New York, USA, June 23–27, 2002: 638–647.
- 王 禹: 男, 1984 年生, 博士生, 研究方向为路由系统安全与 IPv6 安全.
- 王振兴: 男, 1959 年生, 教授, 博士生导师, 研究方向为路由系统安全与 IPv6 安全.
- 张连成: 男, 1982 年生, 讲师, 研究方向为路由系统安全.