一种基于多层拓扑的大规模分布式系统结构脆弱性分析算法

况晓辉 李 津 赵 刚
(北京系统工程研究所信息系统安全技术国家级重点实验室 北京 100101)

摘 要 结构脆弱性是大规模分布式系统中典型的脆弱性类型之一。针对大规模分布式系统实体间复杂的依赖关系和冗余备份机制,构建了多层拓扑模型,在实体拓扑结构脆弱性分析方法的基础上,提出了基于映射-回溯思想的LDS底层结构脆弱性分析算法,并通过实现该算法验证了其有效性。

关键词 结构脆弱性,多层拓扑模型,脆弱性分析
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.8.005

Multilayer Topology Structural Vulnerability Analysis Algorithm for Large-scale Distributed System

KUANG Xiao-hui LI Jin ZHAO Gang
(National Key Laboratory of Science and Technology on Information System Security,
Beijing Institute of System Engineering, Beijing 100101, China)

Abstract Structural vulnerability is a typical type of vulnerabilities on large-scale distributed system. Aiming at the complex relation between entities and redundancy mechanism in large-scale distributed system, a new multi-topology model was proposed. Based on entity topology model structural vulnerability analysis algorithm, a new LDS low layer structural vulnerability analysis algorithm was put forward. The algorithm was verified by implementation and evaluation.

Keywords Structural vulnerability, Multi-topology module, Vulnerability analysis

1 前言

随着信息技术的不断发展,大规模分布式系统(Large Distributed System,LDS)在商业、军事和政府等领域的应用日益广泛,如网格、P2P系统以及GIG等。LDS由广域部署的众多实体构成,将高速互联网、计算机、数据库和应用软件融为一体,显著提高了资源共享和协同能力,逐渐成为重要的关键信息基础设施[1]。由于LDS特有的广域分布、异构、层叠、动态以及无法集中监控等特点,其安全性面临更严峻的挑战。其中因实体间复杂的依赖关系而引入的结构脆弱性是LDS在设计、部署过程中需研究解决的关键问题[1,2]。

结构脆弱性最早由Lu[3]、Agarwal等人[4]在研究建筑工程可靠性时提出,指复杂系统中各组成部分的依赖关系间存在的内在缺陷,对这些缺陷进行利用将导致不可预期的结果或风险。随后,人们对电力、交通等复杂系统的结构脆弱性进行了深入研究。Réka Albert, Marti Rosas-Casals等人分别研究了北美和欧洲的电力网格的结构脆弱性[5,6];Jenelius E等人对瑞典的路网结构的脆弱性进行了深入研究[7];Luca Dall' Asta对全球航空网络的结构脆弱性进行了分析,并提出了基于加权网络拓扑结构的脆弱性分析方法[8]。Shuliang Wang等人针对水处理和电力系统等基础设施的结构脆弱性问题,提出了一种脆弱性分析框架,综合考虑距离、介数、关联系数以及出入度等因素,进行长期脆弱性和关键脆弱性分析[9]。Jun Yan等人通过扩展介数的方法,提出了一种复杂网络结构脆弱性分析方法,并将其应用于电力传输网格的脆弱性分析中[10]。Yakup Koc等人针对电力传输网格提出了一种基于拓扑结构的可靠性和脆弱性分析方法[11]。但是已有方法均只针对单层拓扑结构脆弱性分析开展研究。在网络和信息系统方面,Andr' as Farag'提出了最小割算法F-Cuts来分析网络拓扑的结构脆弱性[12]。M. Kurant在双层拓扑结构的基础上,提出了启发式算法SMART-H来分析IP/WDM的结构脆弱性,并提出修正方法[13]。Zhili Zhou等人针对跨层网络的故障恢复问题,提出了一种基于混合整数线性规划的方法,在物理链路故障时快速恢复上层的逻辑链路,但并未讨论故障定位问题[14]。

相对于电力、交通、网络等复杂系统,LDS为提高抗毁性采用的冗余备份机制以及各层次间的层叠依赖关系,使其结构脆弱性分析更为复杂。而已有的研究工作均未考虑冗余备份机制和层间依赖关系,因此无法有效分析LDS的结构脆弱性。针对已有研究工作的不足,本文在故障容忍机制的基础上构建了描述层间依赖关系的多层拓扑模型,在基于权值的结构脆弱性分析算法的基础上,重点针对因层叠依赖特性引入

到稿日期:2015-07-14 返修日期:2015-11-11
况晓辉(1975—),男,博士,研究员,主要研究方向为计算机网络、信息安全,E-mail:xiaohui_kuang@163.com;李 津(1980—),男,硕士,助理研究员,主要研究方向为信息安全;赵 刚(1969—),男,博士,研究员,主要研究方向为计算机网络、信息安全。

的 LDS 底层结构脆弱性，提出了基于映射-回溯思想的 LDS 底层结构脆弱性算法，并通过实现和测试验证了算法的有效性。

2 LDS 多层拓扑模型

LDS 多层拓扑模型包括 LDS 实体拓扑 G^u、若干个底层拓扑 G^λ 及各层间的映射关系 M 3 个要素。

2.1 实体拓扑

LDS 完成特定业务功能的复杂依赖关系可用简单无回路的有向图 $G^u=\langle V^u,E^u\rangle$ 表示，称为 LDS 的实体拓扑图。其中节点集合 V^u 表示 LDS 中的实体；边集 E^u 表示实体间的依赖关系。若实体 v_i 的功能需依赖实体 v_j 的功能，则存在边 $\langle v_i,v_j\rangle$。业务流程的起点用节点 s 表示。

定义 1 在图 $G^u=\langle V^u,E^u\rangle$ 中，若以 u 为起点到所有出度为 0 的节点间的路径均经过节点 v，则称节点 u 完全依赖节点 v，用 $\xrightarrow{c}$ 表示；若所有从 s 到节点 v 的路径均经过节点 u，且存在以 s 为起点、出度为 0 的节点为终点的路径，经过节点 u 而不经过节点 v，则称节点 u 不完全依赖节点 v，用 $\xrightarrow{nc}$ 表示；若以 s 为起点，经过节点 u 到所有出度为 0 的节点间的路径均经过节点 v，同时所有从 s 到节点 v 的路径都经过节点 u，则称节点 u 等价依赖节点 v，用↔表示。

依赖关系的定义刻画了节点间的依赖程度，其中节点 u 完全依赖节点 v 的含义是节点 v 的功能正确是节点 u 功能正确的必要条件，即若节点 v 故障，则节点 u 必然故障；同时若节点 u 故障，节点 v 功能正常还可能对业务流程具有支持作用。节点 u 等价依赖节点 v 的含义是节点 v 故障，则节点 u 必然故障；而节点 u 故障，则节点 v 的故障与否对业务流程不会产生任何影响。节点 u 不完全依赖节点 v 的含义是若节点 v 故障，则节点 u 不一定故障；同时若节点 u 故障，则节点 v 的故障与否对业务流程不会产生任何影响。

在实体拓扑模型中，故障可分为以下类型：

· 节点故障与边故障

在拓扑图中，节点和边均可能产生故障。边故障将导致相关节点间的依赖关系中断，进而可能导致该边的起始节点故障。而节点故障将导致与节点连接的所有边均故障。

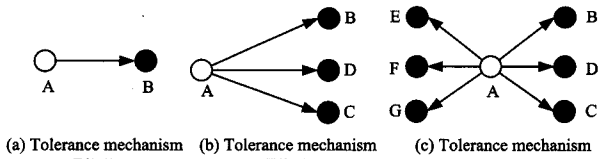
· 单点故障与组合故障

单点故障指实体拓扑模型中，某个节点或边出现故障。而组合故障指多个单点或边故障并发或顺序出现。

大规模分布式系统通常都具备故障容忍机制，以提高系统的鲁棒性。LDS 的故障容忍机制主要通过冗余备份机制实现。为刻画 LDS 的故障容忍机制，在实体拓扑结构中引入故障容忍模型，定义如下。

定义 2 故障容忍模型 $F(n,k)$，定位为 n 个实体中任意 k 个实体无故障时，则该实体集合提供的功能可用。

图 1 给出了故障容忍模型的示例。在图 1(a)中，实体 A 完全依赖实体 B。由于未采用备份机制，当实体 B 故障时，实体 A 也无法实现其功能；在图 1(b)中，实体 A 依赖的功能由 3 个互为备份的节点 B,C,D 共同承担，其中任意两个节点或边故障时，A 仍能正常工作；在图 1(c)中，实体 A 依赖的功能由 6 个节点中任意 3 个共同完成。



(a) Tolerance mechanism F(1,1)　(b) Tolerance mechanism F(3,1)　(c) Tolerance mechanism F(6,3)

图 1　故障容忍机制

根据故障容忍机制的定义，图 1 中 3 种情形的故障容忍模型分别是 $F(1,1)$，$F(3,1)$ 和 $F(6,3)$。在实体拓扑图中，$F(1,1)$ 为隐含的缺省模型。

2.2 底层拓扑和映射关系

底层拓扑结构 $G^\lambda=(V^\lambda,E^\lambda)$ 是简单无向图，表示 LDS 运行依赖的基础设施环境，如域名系统、网络、传输等基础设施。映射关系 M 表示从上层拓扑到下层拓扑结构的映射，用 $M(G^u)=G_N^\lambda$ 表示，包含节点映射和边映射两方面：

a)节点映射：$\forall v\in V^u$，$\exists v'\in V^\lambda$ 使得 $v'=m(v)$。

b)边映射：$\forall e=\langle v_i,v_j\rangle\in E^u$，$\exists p(v_i',v_j')\in P^\lambda$ 使得 $p(v_i',v_j')=m(e)$，且 $v_i'=m(v_i)$，$v_j'=m(v_j)$。其中，P^λ 为网络层拓扑中节点间路径集合，$p(v_i',v_j')$ 表示节点 v_i'，v_j' 间的路径。

拓扑模型的层数根据 LDS 的具体运行环境确定。若 LDS 依赖域名系统、网络基础设施，则模型分为 3 层。若只考虑网络层的路由交换机制，则模型分为两层。图 2 为两层拓扑模型示例，上层为实体拓扑层，描述 LDS 实体间的依赖关系；下层为网络层，描述网络中主机间的互联关系；中间的映射关系描述 LDS 的各实体在网络层的部署及数据传输路径。

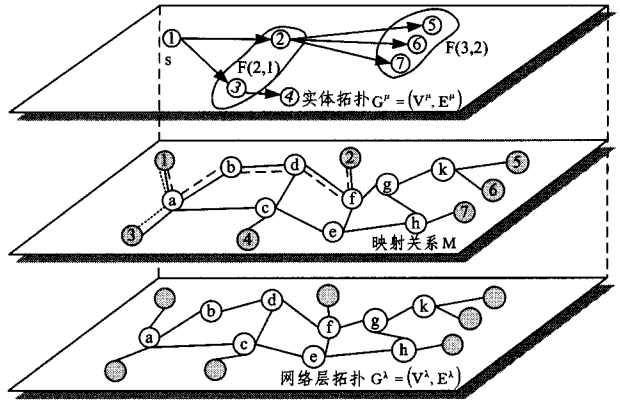


图 2　LDS 多层拓扑模型示例

在图 2 中，节点映射含义为实体组件 v 部署到网络拓扑结构中的主机 v' 上；边映射含义为实体间的通信需依赖网络层的路由交换机制。在映射过程中，若将多个实体映射到同一个主机上，则 LDS 实体拓扑模型将会发生变化，可能增加环、平行边和回路。而在基于权值的 LDS 结构脆弱性分析算法[11]的讨论中，已分析了实体间出现环、平行边和回路时的处理方法。而将一个实体映射到多个主机上，则增加了 LDS 的冗余备份机制，LDS 的实体拓扑需相应调整。因此，节点映射过程中的一对多和多对一的情况，仅影响 LDS 实体拓扑，而在上一节中已讨论了实体拓扑的构建方法。为简化模型描述，多层拓扑的节点映射仅考虑一对一映射的情况，即不存在多对一或一对多的情况。

在多层拓扑模型中，故障可能出现在多层拓扑模型的各

个层次。每个层次均可能出现节点故障、边故障、单点故障和组合故障；同时，各层间的故障因层间的映射关系存在级联效应。即底层节点或边故障可能导致上层拓扑中的节点或边故障。以图 2 为例，网络层拓扑结构中，节点 a 故障，将导致应用层拓扑中边〈1,2〉，〈1,3〉故障。

多层拓扑模型中，结构脆弱性分析的核心目的是发现 LDS 各层次中的关键节点和链路集合，这些节点或边的功能失效将导致实体拓扑模型中起点 s 失效，进而导致业务功能不可用。

3 基于多层拓扑的 LDS 结构脆弱性分析方法

3.1 算法描述

LDS 运行环境、部署方式、层间依赖关系的差异，使得分析 LDS 底层结构脆弱性十分困难。在基于权值的 LDS 结构脆弱性分析方法的基础上，采用映射-回溯的方法分析底层结构脆弱性。其核心思想是根据实体拓扑模型中节点和边的权值以及层间映射关系，计算下层拓扑中的节点和边的权值；然后选择下层拓扑中权值最大的节点，根据映射关系分析该节点功能失效后对上层拓扑的影响，从而发现底层拓扑中的结构脆弱性。

由于各层间的依赖关系复杂，不同的依赖关系结构脆弱性算法也存在一定差异。而绝大多数 LDS 均具有依赖网络层基础设施的特性，因此本文以实体-网络双层拓扑模型为基础，描述基于多层拓扑的 LDS 结构脆弱性分析方法。

为计算网络层拓扑中节点和边的权值，在多层拓扑模型基础上，引入以下定义。

定义 3 在实体拓扑 G^μ 中，若存在一条包含边 e_1 和 e_2 且起点为 s 的路径，则称 e_1 和 e_2 互为关联边。

定义 4 在实体拓扑 G^μ 中，若边集$\{e_1,e_2,\cdots,e_n\}$为故障容忍模型 $F(n,k)$的 n 条边，则称集合$\{e_1,e_2,\cdots,e_n\}$中的边为 k 阶等价边。

对于网络层拓扑中的节点，若是直接映射的节点，则其权值等于实体拓扑中对应节点的权值；否则，节点的权值为映射到该节点的边集合中去除关联边和等价边后的权值之和。网络层边的权值为映射到该节点的边集合中去除关联边和等价边后的权值之和。

基于多层拓扑的 LDS 结构脆弱性分析算法如下：

S 表示 G^λ 中的边集合；

T 表示 G^λ 中的节点集合；

$p_i(v_i',v_j')$表示应用层拓扑中 $e_i=(v_i^\mu,v_j^\mu)$在网络层拓扑中的映射路径；

$M(e_{i,j}^\lambda)$表示映射路径包含边 $e_{i,j}^\lambda=(v_i^\lambda,v_j^\lambda)$的应用层拓扑边的集合；

1)首先去除集合 $M(e_{i,j}^\lambda)$中的冗余关联边。

对于每一个集合 $M(e_{i,j}^\lambda)$

for k=1 to $|M(e_{i,j}^\lambda)|$

  for n=k+1 to $|M(e_{i,j}^\lambda)|$

    if(m_k,m_n 为关联边)&& $w^\mu(m_k)\geqslant w^\mu(m_n)$

      从集合 $M(e_{i,j}^\lambda)$中去除 m_n

    else

      从集合 $M(e_{i,j}^\lambda)$中去除 m_k

经过上述算法，得到去除冗余关联边的集合 $\overline{M}(e_{i,j}^\lambda)$。

2)其次，去除集合 $\overline{M}(e_{i,j}^\lambda)$中的冗余等价边。

对于每一个集合 $\overline{M}(e_{i,j}^\lambda)$，遍历应用层拓扑中的故障冗余机制；

若集合 $\overline{M}(e_{i,j}^\lambda)$存在子集$\bar{N}(e_{i,j}^\lambda)\subseteq\overline{M}(e_{i,j}^\lambda)$，$\bar{N}(e_{i,j}^\lambda)$中的边为故障容忍模型 $F(n,k)$中的 k 阶等价边，且$|\bar{N}(e_{i,j}^\lambda)|>n-k+1$，则从集合中随机选择$|\bar{N}(e_{i,j}^\lambda)|-(n-k+1)$条边，并将它们从 $\overline{M}(e_{i,j}^\lambda)$中移除。

去除冗余等价边后，得到集合$\overline{\overline{M}}(e_{i,j}^\lambda)$。

3)计算网络层拓扑中边和节点的权值。

$e_{i,j}^\lambda$的权值为集合$\overline{\overline{M}}(e_{i,j}^\lambda)$中所有边权值的和：

$w^\lambda(e_{i,j})=\sum w^\mu(e)$，其中 $e\in\overline{\overline{M}}(e_{i,j}^\lambda)$。

节点 v_i^λ的权值为以 v_i^λ为顶点的边的权值之和的 1/2。

4)遍历网络层拓扑 $G^\lambda=(V^\lambda,E^\lambda)$，查找权值最大的节点，用 $v_{\max}^\lambda$表示。将 $v_{\max}^\lambda$加入集合 T；将与 $v_{\max}^\lambda$连接的边对应的 $\overline{\overline{M}}(e_{i,j}^\lambda)$中所有的元素加入到集合 S；在 $G^\lambda=(V^\lambda,E^\lambda)$中移除 $v_{\max}^\lambda$及连接 $v_{\max}^\lambda$的边。

5)利用剪枝算法在 $G^\mu=\langle V^\mu,E^\mu\rangle$中依次移除 S 中的元素，得到子图 $G'^\mu=[V'^\mu,E'^\mu]$。若起始节点 s 不在 V'^μ 中，则集合 $T\subseteq V^\lambda$ 为网络层拓扑的结构脆弱点；否则，重复步骤 4)。

在网络层拓扑的结构脆弱性分析算法中，将步骤 4)改为选择权值最大的边，也可得到脆弱性分析结果。此时，集合 $T\subseteq E^\lambda$。

3.2 算法讨论

大规模分布式系统通常都具备故障容忍机制，以提高系统的鲁棒性。在 LDS 实体-网络拓扑模型中，LDS 的故障容忍机制可分为应用层故障容忍机制和网络层故障容忍机制两种类型。LDS 的实体层故障容忍机制主要通过冗余备份机制实现，而其网络层故障容忍机制通过动态路由或多路径路由实现。由于网络层故障容忍机制的复杂性，在多层拓扑模型中没有引入网络层的故障容忍模型。因此网络层拓扑的结构脆弱性分析算法的分析结果是当前路由方式下的结构脆弱性，它可能因网络层故障容忍机制而得到自动修复。因此在算法分析结果的基础上，还需通过其他方法进行进一步分析和验证，利用基于故障注入的脆弱性分析环境进行分析和验证是有效的方法之一。

4 模拟分析与验证

基于 Jgraph 和图论算法实现库，利用 Java 语言实现了基于多层拓扑的 LDS 结构脆弱性分析算法。在 CPU 为 2.33GHz、内存为 1.5GB 的 Windows XP 上对算法的性能进行了分析和验证。其中实体拓扑图通过随机生成有向图后去除其中的回路得到。实体拓扑图的节点数量为 500，平均最短路径长度为 6，结构脆弱性节点 36 个，脆弱性边 60 条。网络层拓扑利用课题组研究并实现的大规模网络拓扑框架生成，分为自治域、路由和端系统 3 层，且端系统和网络节点的比例为 4∶1。通过随机方法确定端系统和实体拓扑中节点的

关系，实现实体拓扑到网络层拓扑的映射。为避免单个测试样本的特殊性对算法分析结果的影响，每类的拓扑生成 10 个样本，统计结果取平均值。

图 3 显示了算法运行时间随网络层拓扑节点数目的变化情况。从图中可以看出，算法的运行时间随节点数量呈线性变化，根据算法描述可知，算法的执行时间与路径的长度有关，而路由层的节点数量随拓扑规模变化较小，因此算法开销随网络层规模变化不显著。在实体拓扑图权值已知的情况下，网络层拓扑结构脆弱性分析算法运算开销较小，算法的运算开销随节点数量呈线性增长，在 2500 个节点时，算法运行时间为 120s；5000 个节点时，也仅需 251s。

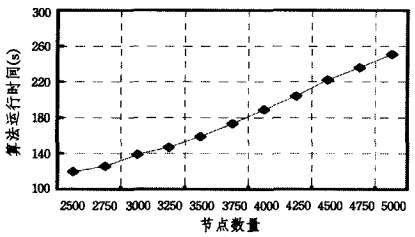


图 3　算法运行时间随节点数目的变化情况

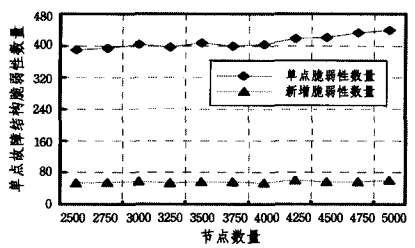


图 4　结构脆弱性数量随网络层节点数量的变化情况

图 4 显示了网络层单点故障结构脆弱性和新增结构脆弱性随节点数量的变化情况，其中新增单点结构脆弱性指实体拓扑中多条非结构脆弱性边映射到网络拓扑中而形成的新的脆弱性。从图中可以看出，网络层单点故障结构脆弱性远高于实体拓扑中的单点故障结构脆弱性。其中 2500 个节点的网络层拓扑中，存在 390 个单点故障结构脆弱性，而实体拓扑中单点故障结构脆弱性仅为 96 个。同时，网络层单点故障结构脆弱性数量随节点数量增加而缓慢增加，原因是网络拓扑中单点结构脆弱性主要源于实体拓扑中脆弱性边的映射。而网络层节点间平均路径随节点数量扩大而增加，从而使实体拓扑中的脆弱性边映射到网络层而形成的脆弱性边的数量随之增加，因而网络层单点故障结构脆弱性呈缓慢增加趋势。而由于网络层拓扑符合无尺度特性，使得实体拓扑中的单点故障结构脆弱性并未随着网络规模的扩大而分布化，因映射累积而形成的新的脆弱性数量始终保持在 55 左右。从整体角度看，对网络层的依赖使得 LDS 的结构脆弱性数量呈上升趋势，说明层叠依赖特性导致 LDS 的结构脆弱性更为严峻。

从算法描述可以看出，组合故障结构脆弱性分析过程实质可分解为多次单点故障结构脆弱性分析。因此，上述分析结果也适用于组合故障结构脆弱性分析算法。

结束语　结构脆弱性是复杂系统典型的脆弱性之一。对于不同的复杂系统，其结构脆弱性分析方法存在明显差异。本文针对大规模分布式系统的层叠依赖特性，在已有研究工作的基础上，提出了基于映射-回溯思想的 LDS 底层结构脆弱性分析算法，并在算法实现的基础上测试和验证了算法的有效性，有效解决了具有冗余备份和层叠依赖特性的 LDS 的结构脆弱性分析问题。

参 考 文 献

[1] Helsinger A, Ferguson W, Lazarus R. Exploring large-scale, distributed system behavior with a focus on information assurance [C]// IEEE Computer Society. 2001: 1273-1286

[2] Qiang W Z, Zou D Q, Jin H. Research on Privacy Preservation Mechanism for Credentials and Policies in Grid Computing Environment[J]. Journal of Computer Research & Development, 2007, 44(1): 11-19(in Chinese)
羌卫中，邹德清，金海. 网格环境中证书和策略的隐私保护机制研究[J]. 计算机研究与发展，2007，44(1)：11-19

[3] Lu Z, Yu Y, et al. A theory of structural vulnerability [J]. Structural Engineer, 1999, 77(18): 17-24

[4] Agarwal J, Blockley D I, Woodman N J. Vulnerability of 3D trusses[J]. Structural Safety, 2001, 23(3): 203-220

[5] Albert R, Albert I, Nakarado G L. Structural vulnerability of the North American power grid[J]. Phys. Rev. E Statistical Nonlinear & Soft Matter Physics, 2004, 69(2): 292-313

[6] Rosas-Casals M, Valverde S, Solé R. Topological vulnerability of the European power grid under errors and attacks[J]. International Journal of Bifurcations and Chaos, 2007, 17(7): 2465-2475

[7] Jenelius E, Petersen T, Mattson L. Importance and exposure in road network vulnerability analysis [J]. Transportation Research, 2008, 40: 537-560

[8] DallAsta L, Barrat A, Barth′elemy M, et al. Vulnerability of weighted networks [J]. J. Stat. Mech, 2006, 25(4): 04006

[9] Wang S, Hong L, Chen X. Vulnerability analysis of interdependent infrastructure systems: A methodological framework[J]. Physical A: Stat. Mech. Its Appl., 2012, 391(11): 3323-3335

[10] Yan J, He H, Sun Y. Integrated security analysis on cascading failure in complex networks[J]. IEEE Trans. Inf. Forensics Security, 2014, 9(3): 451-463

[11] Koc Y, Raman A, Warnier M, et al. Structural Vulnerability Analysis of Electric Power Distribution Grids[J]. arXiv preprint arXiv: 1506. 08641, 2015

[12] Farago A. A graph theoretic model for complex network failure scenarios[C]// INFORMS. 2006

[13] Kurant M, Thiran P. Survivable Mapping Algorithm by Ring Trimming (SMART) for large IP-over-WDM networks[C]// Proceedings of BroadNets. San Jose, California, USA, 2004: 25-29

[14] Zhou Z, Lin T, Thulasiraman K, et al. Cross-Layer Network Survivability Under Multiple Cross-Layer Metrics[J]. Journal of Optical Communications and Networking, 2015, 7(6): 540-553

[15] Zhao Gang, Kuang Xiao-hui, Li Jin, et al. A Structural Vulnerability Analysis Algorithm for Large-Scale Distributed System [J]. Journal of Computer Research & Development, 2011, 48(5): 906-912(in Chinese)
赵刚，况晓辉，李津，等. 一种基于权值的大规模分布式系统结构脆弱性分析算法[J]. 计算机研究与发展，2011，48(5)：906-912