

基于关键节点的域内路由保护算法

耿海军¹ 施新刚² 王之梁² 尹霞³ 尹少平¹

(山西大学软件学院 太原 030006)¹ (清华大学网络科学与网络空间研究院 北京 100084)²
(清华大学计算机科学与技术系 北京 100084)³

摘要 随着互联网规模的膨胀,大量的实时应用部署在互联网上,这些实时应用对网络时延提出了更加严格的要求。然而,目前互联网部署的域内路由协议无法满足实时应用对网络时延的要求,因此提高域内路由可用性成为了一项亟待解决的关键性科学问题。学术界和工业界提出利用路由保护方案来提高路由可用性,从而减少由于网络故障造成的网络中断和报文丢失。已有的路由保护方案将网络中的节点同等对待,没有考虑节点在网络中的重要程度,然而实际情况并非如此。因此,提出了一种基于关键节点的域内路由保护算法(Intra-domain Routing Protection Algorithm Based on Critical Nodes,RPBCN)。首先,建立路由可用性模型,以定量衡量路由可用性;其次,建立节点关键度模型,以定量衡量网络中节点的重要程度;最后,基于路由可用性模型和节点关键度模型,提出基于关键节点的域内路由保护方案。实验结果表明,RPBCN 在保证路由可用性的前提下极大地降低了算法的计算开销,从而为 ISP 解决路由可用性问题提供了一种全新的高效解决方案。

关键词 域内路由,路由保护,关键节点,路由可用性

中图分类号 TP309.7 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.01.032

Intra-domain Routing Protection Algorithm Based on Critical Nodes

GENG Hai-jun¹ SHI Xin-gang² WANG Zhi-liang² YIN Xia³ YIN Shao-ping¹

(School of Software Technology, Shanxi University, Taiyuan 030006, China)¹

(Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)²

(Department of Computer Science & Technology, Tsinghua University, Beijing 100084, China)³

Abstract With the expansion of the Internet, a large number of real-time applications are deployed on the Internet, which places greater demands on network delay. However, the current deployed intra-domain routing protocol cannot meet the requirements of real-time application for network delay. Therefore, improving the Internet routing availability has become an urgent problem. Academia and industry employ routing protection schemes to quickly respond to network failures and improve Internet routing availability. The existing routing protection schemes do not consider the importance of nodes in the network. However, the importance of different nodes in the network is not the same in real networks. To solve this problem, an intra-domain routing protection algorithm based on critical nodes (RPBCN) was proposed. Firstly, an Internet routing availability model is built, which can quantitatively measure the Internet routing availability. Then, a node criticality model is established, which can quantitatively measure the importance of nodes in the network. At last, RPBCN is proposed based on the Internet routing availability model and node criticality model. The experiment results show that RPBCN greatly improves the Internet routing availability while possessing low computation overhead, which provides an efficient solution for the ISP to solve the Internet route availability problem.

Keywords Intra-domain routing, Routing protection, Critical node, Internet routing availability

随着互联网的普及和其规模的逐渐扩大,互联网在人们日常生活中扮演了重要的角色,并且已经成为人们日常生活中必不可少的一部分^[1-4]。在最初阶段,互联网仅仅支持部分非实时应用^[5],如电子邮件、传输文本文件等。然而,目前大

量的实时应用数据^[6-7],如 VoIP、视频、在线游戏、股票交易等,在互联网上广泛传播,这些新型应用对路由可用性提出了更加苛刻的要求^[8]。

当网络出现故障时,目前互联网部署的域内路由协议采

到稿日期:2016-12-04 返修日期:2017-02-06 本文受国家重点基础研究发展计划(863 计划)基金资助项目(2015AA016105),国家自然科学基金资助项目(61402253,61702315)资助。

耿海军 男,博士,讲师,主要研究方向为网络体系结构、路由算法等,E-mail:ghj123025449@163.com(通信作者);施新刚 男,博士,副研究员,主要研究方向为 SDN、路由算法、网络安全等;王之梁 男,博士,副研究员,主要研究方向为数据中心、SDN、网络体系结构等;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;尹少平 男,副教授,主要研究方向为路由算法、网络安全、网络体系结构等。

用动态路由协议应对网络故障,然而动态路由协议需要几秒甚至几十秒来完成收敛,在此过程中大量报文被丢弃^[9]。一般地,实时应用要求毫秒级的故障恢复时间,因此已有的动态路由协议无法满足实时应用对路由可用性的要求^[10-11],实时应用对路由可用性提出了新的挑战。因此,如何提高域内路由可用性成为了一项亟待解决的重大科学问题^[12]。

学术界和工业界提出利用路由保护方案来提高域内路由可用性。典型的路由保护方案包括等价多路径(Equal Cost Multiple Paths, ECMP)^[13]、无环路备选项(Loop-Free Alternates, LFA)^[14]和基于 Not-Via 地址的快速重路由方案^[15]。ECMP 是一种简单的路由保护方案,该方案为源和目的路由计算所有的等价最短路径,实现简单,易于部署,但对路由可用性的贡献有限^[16]。LFA 采用无环路条件(Loop Free Condition, LFC)和单节点保护条件(Node Protection Condition, NPC)事先为节点计算备份下一跳,当网络出现故障时,利用这些备份下一跳转发报文,然而研究表明,LFA 的故障保护率仅为 50%左右,甚至更低^[17]。针对 LFA 的故障保护率低的问题,学术界提出了基于 Not-Via 地址的快速重路由方案,该方案利用 Not-Via 地址显式地说明如何避免网络中的故障,虽然可以达到 100%单故障保护的情形,但是其计算开销较大,影响了实际部署。

通过对已有路由保护方案^[18-20]的研究,我们发现已有的路由保护方案都是在“网络中所有节点对路由可用性的贡献是相同的”这一假设条件下设计的。然而在实际网络中,这一假设条件并不总是成立。因此,本文研究了节点的特征(介数和与其相连的链路的失效概率等)与其对路由可用性贡献之间的关系,在此基础上研究了基于关键节点的域内路由保护方案,旨在尽可能地降低计算开销和存储开销,并兼顾执行效率和故障保护率。本文将网络故障限定为单节点故障情形,更加复杂的故障情形不在本文的研究范围之内。

1 网络模型和问题描述

1.1 网络模型

网络可以表示为一个有向图 $G=(V, E)$,其中 V 表示节点(路由器)的集合, E 表示边(链路)的集合。对于任意一条链路 (i, j) ,用 $w(i, j)$ 表示该链路的代价, $r(i, j)$ 表示该链路的失效概率。对于任意节点 v , $r(v)$ 表示该节点的失效概率, $N(v)$ 表示该节点的邻居节点的集合。假设源节点为 s ,目的节点为 d , $sp(s, d)$ 表示节点 s 到节点 d 的最短路径经过的链路, $sv(s, d)$ 表示节点 s 到节点 d 的最短路径经过的节点。

1.2 路由可用性模型

路由可用性表示网络转发报文的能力,本文利用路由可用性来衡量网络性能。当采用路由保护方案后,路由可用性可以得到大幅度的提升。为了定量地衡量路由可用性的提升程度,下面将对路由可用性进行定量描述。

首先定义端到端的可用性,其表示源节点将报文转发到目的节点的能力。因为本文假设网络中的故障为单节点故障,所以当某个节点被保护时,该节点的失效概率为 0,与其相连的链路的失效概率可以等价于 0。

节点 s 到节点 d 的端到端的可用性可以表示为:

$$B(s, d) = \prod_{\substack{u \in sv(s, d) \\ (u, v) \in sp(s, d)}} 1 - k(u) * r(u, v) * r(u)$$

其中, $k(u) = \begin{cases} 0, & \text{节点 } u \text{ 被保护} \\ 1, & \text{否则} \end{cases}$ 。因此,路由可用性可以表示为 $A(P) = \frac{\sum_{s, d \in V} B(s, d)}{|V| * |V-1|}$, P 表示被保护的节点的集合。

下面通过一个例子来说明如何计算端到端的可用性。图 1 给出了节点 s 到节点 d 的最短路径, $sp(s, d) = \{(s, a), (a, b), (b, c), (c, d)\}$, $sv(s, d) = \{s, a, b, c, d\}$, 假设节点的失效概率均为 0.1。当采用最短路径转发报文时,节点 s 到节点 d 的端到端的可用性 $B(s, d) = 0.9^6 * 0.8 * 0.99 * 0.7 = 0.29$;当节点 a 被保护时, $B(s, d) = 0.9^4 * 1 * 1 * 0.99 * 0.7 = 0.45$;当节点 b 被保护时, $B(s, d) = 0.9^5 * 1 * 1 * 0.7 = 0.41$;当节点 a 和 b 同时被保护时, $B(s, d) = 0.9^3 * 1 * 1 * 1 * 0.7 = 0.51$;而当节点 s, a, b, c, d 都被保护时, $B(s, d) = 1 * 1 * 1 * 1 * 1 = 1$ 。

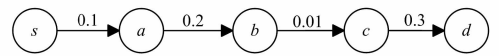


图 1 路由可用性实例

Fig. 1 An example for explaining the routing availability

1.3 问题描述

从上面的例子可以看出,通过采用路由保护方案可以提高端到端的可用性,进而提高路由可用性。然而,不同节点对端到端的可用性的贡献是不相同的,并且保护节点的数量和路由可用性的大小不呈正比关系。因此,在设计路由保护方案时应该对节点区分对待,优先保护对路由可用性贡献较大的节点,从而在保证路由可用性最大化的同时降低网络开销。该问题可以描述为:给定一个网络拓扑结构 $G=(V, E)$ 和路由可用性目标 Ω ,选择一组节点 P 进行保护,从而使 $A(P) \geq \Omega$,该问题可以形式化表示如下。

输入:网络拓扑结构 $G(V, E)$ 和路由可用性目标 Ω

输出:保护节点的集合 P

目标:Minimize $|P|$

条件: $V \supseteq P$ 并且 $A(P) \geq \Omega$

2 RPBCN 算法

2.1 算法的总体框架

从上节的描述可知,网络中不同节点对路由可用性的贡献是不同的,基于该结论研究了基于关键节点的域内路由保护算法,该算法的基本框架如下:

- (1)选择需要保护的节点集合 P 。
- (2)每个节点为集合 P 中的节点计算保护路径。
- (3)当网络中没有出现故障时,所有节点按照默认路由转发报文;当网络中出现故障时,受该故障影响的节点按照备用路径转发报文。

2.2 算法描述

为了实现上述算法,需要解决以下 3 个问题:

- (1)选择哪些节点进行保护;
- (2)最后一跳问题;
- (3)如何为选择的节点计算保护路径。

问题 1:选择哪些节点进行保护

为了解决该问题,利用节点关键度来衡量节点的重要程度,下面详细描述节点关键度的具体内容。

节点关键度:对于任意的节点 $v \in V$,节点 v 的关键度表示该节点在网络中的重要程度,用 $C(v)$ 表示,即:

$$C(v) = Bw(v) * r(v) * \sum_{u \in N(v)} r(v, u)$$

其中, $Bw(v) = \sum_{s, d \in V, s \neq d} \frac{x(s, d, v)}{x(s, d)}$ 表示节点的介数, $x(s, d)$ 表示节点 s 和节点 d 之间最短路径的数量, $x(s, d, v)$ 表示节点 s 和节点 d 之间经过节点 v 的最短路径的数量。

从上述定义可以看出,如果该节点的介数越高,且与其相连的链路的失效概率越高,则该节点的关键度越高。下面通过一个例子来解释节点的关键度。图 2 给出了一个包含 4 个节点的网络拓扑结构,每条边对应两个数值,第一个数值表示该链路对应的代价,第二个数值表示该链路的失效概率,假设所有节点的失效概率均为 0.1。通过计算可知, $Bw(a) = Bw(c) = 8$, $Bw(b) = Bw(d) = 6$, 则 $C(a) = 8 * 0.2 * 0.1 = 0.16$, $C(b) = 6 * 0.3 * 0.1 = 0.18$, $C(c) = 8 * 0.4 * 0.1 = 0.32$, $C(d) = 6 * 0.5 * 0.1 = 0.3$, 因此在该拓扑结构中,节点 c 的关键度是最高的。

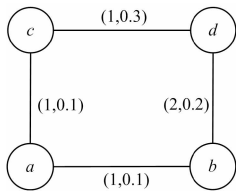


图 2 节点关键度实例

Fig. 2 An example for explaining the criticality of nodes

算法 1 描述了选择网络中需要进行保护的节点的过程。

算法 1 RPBCN

Input: $G(V, E)$, 路由可用性目标 Ω

Output: 保护节点的集合 P

1. 计算网络中所有节点的关键度
2. 按照节点关键度对节点进行降序排列
3. 将排序后的节点存储在链表 L 中
4. $P \leftarrow \emptyset$
5. While $\Delta(P) < \Omega$
6. 从链表 L 中选择第一个节点 k
7. $P \leftarrow \{k\} \cup P$
8. 计算 $\Delta(P)$
9. 从链表 L 中删除节点 k
10. EndWhile
11. Return P

按照节点关键度的大小对网络中的所有节点进行降序排列,并将其存入链表 L 中(第 1—3 行),初始化被保护节点的集合(第 4 行)。后面是一个循环,在循环中每次从链表 L 的头部选择一个节点加入到保护节点集合中,直到满足路由可用

性目标(第 5—10 行),最后返回保护节点集合 P (第 11 行)。

问题 2: 最后一跳问题

假设节点 v 到节点 u 的最优下一跳为 u , 当节点 v 为其下一跳 u 计算保护路径时,节点 v 首先假设节点 u 出现故障,然后新的拓扑结构中为其计算保护路径。然而,当节点 u 为目的地址时,如果节点 u 确实出现了故障,那么前面的假设是成立的;如果节点 u 没有出现故障,只是链路 (v, u) 出现了故障,那么前面的假设是不合理的,这就是最后一跳问题。为了解决该问题,当节点 v 为其最优下一跳节点 u 计算保护路径时,假设链路 (v, u) 和节点 u 的所有出边出现故障,然后在该新拓扑中计算保护路径,这样就可以完美解决最后一跳问题。

问题 3: 如何为节点计算保护路径

假设节点 v 为节点 u 计算保护路径,此时有两种情况:

(1) $u \in N(v)$

首先假设链路 (v, u) 和节点 u 的所有出边出现故障,然后在新拓扑上计算节点 v 到节点 u 和节点 v 到节点 u 的所有邻居节点 $N(u)$ 的最短路径。

(2) $u \notin N(v)$

首先假设节点 u 出现故障,然后在新拓扑上计算节点 $x \in N(u)$ 和节点 $y \in N(u)$ 之间的最短路径,即节点 u 的所有邻居之间的最短路径。

3 实验

本节将通过实验模拟来说明算法的性能。首先描述实验方法,然后说明实验的比较结果。

3.1 实验方法

3.1.1 实验拓扑

为了全面地评测算法的性能,在实验中采用了多种形式的拓扑结构,包括真实拓扑结构 Abilene^[21]、利用 Rocketfuel^[22]测量的拓扑结构、利用 Brite 软件¹⁾生成的拓扑结构。

(1) Abilene 是美国教育科研网络,该拓扑包括 11 个节点和 14 条边。

(2) 在 Rocketfuel 项目公开的拓扑结构中选择几个常用的拓扑作为实验对象,详细参数如表 1 所列。

表 1 Rocketfuel 的拓扑结构

Table 1 Rocketfuel topology

AS 号码	AS 名称	结点数量	链路数量
1221	Telstra	108	153
1239	Sprint	315	972
1755	Ebone	87	162
3257	Tiscali	161	328
3967	Exodus	79	147
6461	Abovenet	128	372

(3) Brite 是一个生成拓扑结构的开源软件,其参数如表 2 所列。

表 2 Brite 生成拓扑结构的参数设置

Table 2 Parameters for Brite

参数	模型	节点数量	HS	LS	链路节点比	NodePlacement	增长方式	alpha	beta	BWDist	BwMin-BwMax	模式
取值或描述	Waxman	1000	1000	100	2-20	Random	增量式	0.15	0.2	Constant	10.0-1024.0	路由器

¹⁾ <http://www.cs.bu.edu/brite>

3.1.2 评价指标

本文将 RPBCN 与 Not-Via 进行比较,评价指标包括相对计算时间和需要保护的节点比率。相对计算时间 = RPBCN 的计算时间 / Not-Via 的计算时间,需要保护的节点比率 = RPBCN 需要保护的节点数量 / Not-Via 需要保护的节点数量。本实验利用 PC 机进行实验模拟,具体配制为 CPU Intel i7,主频 1.7GHz,内存 2GB。采用 C++ 编写 RPBCN 和 Not-Via,实验结果取 100 次实验的平均值。

3.1.3 网络链路故障模型

为了简化实验过程,本文采用一种简单的网络链路故障模型,即假设网路中节点和链路的失效概率均为 0~0.01 之间的随机数。

3.2 相对计算时间

图 3 给出了 RPBCN 算法在真实拓扑和测量拓扑中的相对计算时间和路由可用性之间的关系。从图 3 中可以看出,当路由可用性为 94% 时,除 Abilene 外,在其余拓扑结构中,RPBCN 的计算时间在 Not-Via 的计算时间的 10% 以下;在 Abilene 拓扑中,RPBCN 的计算时间大约是 Not-Via 的计算时间的 25% 左右,这是因为 Abilene 的拓扑较小,连通性较差,而其余拓扑的拓扑密度相对较大,连通性较好。当路由可用性是 100% 时,除 Abilene 外,在其余拓扑结构中 RPBCN 的计算时间在 Not-Via 的计算时间的 30% 以下,在 Abilene 拓扑中 RPBCN 的计算时间大约是 Not-Via 的计算时间的 80% 左右。

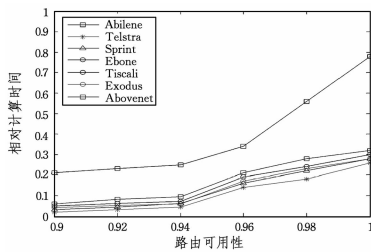


图 3 真实拓扑和测量拓扑中的相对计算时间

Fig. 3 Relative computation time on real and measured topologies

图 4 给出了当网络拓扑大小为 1000 时相对计算时间和网络节点平均度之间的关系。从图 4 中可以看出,随着网络节点平均度的增加,相对计算时间逐渐减少。在所有的模拟拓扑结构中,RPBCN 的性能明显优于 Not-Via 的性能。

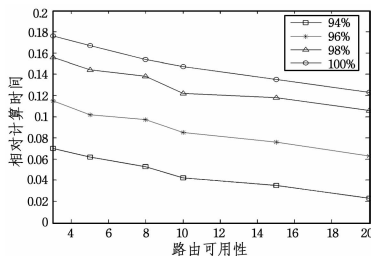


图 4 测量拓扑中的相对计算时间

Fig. 4 Relative computation time on generated topologies

3.3 需要保护节点比率

图 5 给出了在真实拓扑和测量拓扑中,算法 RPBCN 需要保护的节点的数量随着路由可用性的变化规律。从图 5 中可以看出,在 Abilene 拓扑中,RPBCN 在保护大约 80% 的节点的情况下路由可用性才能达到 100%,而在其余拓扑中

RPBCN 仅仅需要保护 20% 以下的节点,此时路由可用性便可达到 100%,因此大大降低了算法的开销。

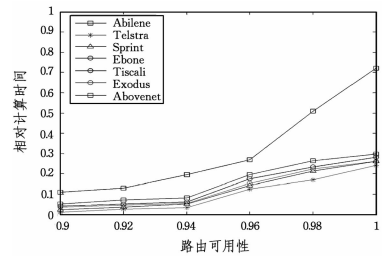


图 5 真实拓扑和测量拓扑中的需要保护的节点比率

Fig. 5 Backup-nodes for Real and measured topologies

图 6 给出了当网络拓扑大小为 1000 时网络节点平均度和需要保护的节点比率之间的变化规律。从图 6 中可知,随着网络节点平均度的增加,RPBCN 需要保护的节点的数量逐渐减少,这是因为随着网络节点平均度的增加,网络的连通性逐渐提升,算法的性能也得到明显的提升。

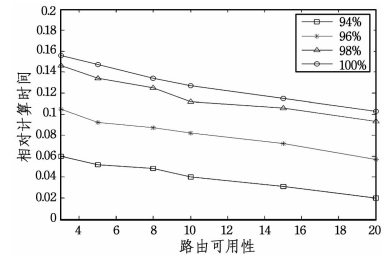


图 6 模拟拓扑中的需要保护的节点比率

Fig. 6 Backup-nodes for generated topologies

从图 3—图 6 可以看出,需要保护的节点比率的数值比相对计算时间的数值小,这是因为 RPBCN 算法需要一些额外的计算时间,如初始化操作、计算节点关键度、节点排序等,然而这些操作所需要的时间远远小于计算保护的路径的时间。

结束语 针对已有路由保护方案没有很好地权衡路由可用性和计算开销的问题,本文提出了一种基于关键节点的域内路由保护方案,该方案考虑了节点关键度属性,根据该属性依次保护网络中的节点,直到路由可用性达到目标。该方案在保证路由可用性的前提下,大大降低了算法的计算开销。

本文在实验中采用了一种简单的链路故障模型来模拟实验,因此为了更加准确地说明算法的有效性,下一步将研究网络中的链路故障模型,从而进一步改进算法。另外,本文仅讨论了网络中的单节点故障情形,下一步将研究如何将本文的算法应用在多故障和并发故障情形中。

参考文献

- [1] Internet Users[OL]. <http://www.internetworldstats.com/top20.htm>.
- [2] GENG H J, SHI X G, YIN X, et al. Algebra and algorithms for multipath QoS routing in link state networks[J]. Journal of Communications and Networks, 2017, 19(2): 189-200.
- [3] Reaching 50 million users[OL]. <http://visual.ly/reaching-50-million-users>.
- [4] 第 38 次中国互联网络发展状况统计报告[R]. 中国互联网信息中心, 2016.
- [5] CLARK D. The design philosophy of the DARPA Internet pro-

- tocols [J]. ACM SIGCOMM Computer Communication Review, 1988,18(4):106-114.
- [6] GOODE B. Voice over internet protocol (voip)[J]. Proceedings of the IEEE,2002,90(9):1495-1517.
- [7] DREW P,GALLON C. Next-generation VoIP network architecture[R]. Multiservice Switching Forum,2003.
- [8] KRIST P. Scalable and Efficient Multipath Routing:Complexity and Algorithms[C]//2015 IEEE 23rd International Conference on Network Protocols (ICNP). IEEE,2015:376-385.
- [9] ZHENG J,XU H,ZHU X,et al. We've Got You Covered:Failure Recovery with Backup Tunnels in Traffic Engineering[C]//IEEE 24rd International Conference on Network Protocols (ICNP). IEEE,2016:1-10.
- [10] YANG B,LIU J,SHENKER S,et al. Keep forwarding: Towards k-link failure resilient routing[C]//IEEE Conference on Computer Communications. IEEE INFOCOM,2014:1617-1625.
- [11] PAL S,GADDE R,LATCHMAN H A. On the reliability of voice over ip (voip) telephony[C]//The SPRING 9th International Conference on Computing, Communications and Control Technologies. Orlando,Florida,USA,2011.
- [12] YALLOUZ J,ROTTENSTREICH O,BABARCI P,et al. Optimal Link-Disjoint Node-"Somewhat Disjoint" Paths[C]//2016 IEEE 24rd International Conference on Network Protocols (ICNP). IEEE,2016:1-10.
- [13] MOY J. rfc 2328:Ospf version 2[OL]. <http://tools.ietf.org/html/rfc2328>.
- [14] ATLAS A K,ZININ A. Basic Specification for IP Fast Reroute: Loop-Free Alternates[OL]. <http://www.heise.de/netze/rfc/rfcs/rfcs5286.shtml>.
- [15] SHAND M. Ip fast reroute using not-via addresses[J]. Cisco Systems Conference Dapricot,2003,137(654):29-42.
- [16] SRIDHARAN A,GUERIN R,DIOT C. Achieving near-optimal traffic engineering solutions for current ospf/is-is networks[J]. IEEE/ACM Transactions on Networking (TON),2005,13(2):234-247.
- [17] FRANCOIS P,BONAVENTURE O. An evaluation of ip-based fast reroute techniques [C] // ACM Conference on Emerging Network Experiment and Technology. ACM,2005:244-245.
- [18] KWONG K W,GAO L,GUÉRIN R,et al. On the feasibility and efficacy of protection routing in IP networks[C]//Proc. IEEE INFOCOM. 2010:1235-1243.
- [19] VO H Q,LYSNE O,KVALBEIN A. Routing with joker links for maximized robustness[C]//IFIP Networking Conference. 2013:1-9.
- [20] CHO S,ELHOURNAI T,RAMASUBRAMANIAN S. Independent directed acyclic graphs for resilient multipath routing [J]. IEEE/ACM Trans. on Networking,2012,20(1):153-162.
- [21] Advanced networking for research and education[OL]. <https://www.internet2.edu/products-services/advanced-networking>.
- [22] SPRING N,MAHAJAN R,WETHERALL D,et al. Measuring isp topologies with rocketfuel [J]. IEEE/ACM Transactions on Networking,2004,12(1):2-16.

(上接第 151 页)

部分一致约简。易见,由方法 2 所求得的部分一致约简与方法一求得的结果一致。

综上可知,在该决策问题中,市场潜力是使对象的决策不变的属性。该案例使用了两种不同的求解方法,所用的时间也不同。从计算的过程来看,方法一的过程较复杂,总共需要计算 $15(2^4 - 1)$ 次带偏好度量的直觉模糊优势类,相对而言,方法 2 所用的时间较少。因此在求部分一致约简时,利用方法 2 求解具有明显的时间优势。

结束语 本文在直觉模糊序决策信息系统下,通过考虑隶属度、非隶属度和犹豫度在评价机制中的重要性,并对其赋以一定的权重,建立了一个不协调的带偏好度量的直觉模糊序决策信息系统,并通过加权得分函数引入新的直觉模糊序关系,通过分析部分一致约简的性质得到了对应的判定定理,建立了获取这种约简的具体方法;同时通过实例证明了这种方法的可行性和有效性,并且提高了效率。

参 考 文 献

- [1] ZADEH L A. Fuzzy Sets [J]. Information and Control,1965,8(3):338-353.
- [2] VLACHIOS I K,SERGIADIS G D. Intuitionistic fuzzy information-Applications to pattern recognition [J]. Pattern Recognition Letters,2007,28(2):197-206.
- [3] ZHOU L,WU W Z. On characterization of intuitionistic fuzzy rough sets based on intuitionistic fuzzy implicators [J]. Information Sciences,2009,179(7):883-898.
- [4] LI X P,WANG G J. The Extension Operations of the Intuitionistic Fuzzy Sets [J]. Fuzzy Systems and Mathematics,2002,16(1):40-46. (in Chinese)
李晓萍,王贵君. 直觉模糊集的扩张运算[J]. 模糊系统与数学,2002,16(1):40-46.
- [5] 徐泽水. 直觉模糊信息集成理论及应用[M]. 北京:科学出版社,2008.
- [6] PAWLAK Z. Rough Sets: Theoretical aspects of reasoning about data [M]. Kluwer Academic Publishers,1992.
- [7] JERZY W,GRZYMALA-BUSSE,PAWLAK Z,et al. Rough sets [J]. Communications of the ACM,1995,38(11):88-95.
- [8] 徐伟华. 序信息系统与粗糙集[M]. 北京:科学出版社,2013.
- [9] ZHANG W X,MI J S,WU W Z. Knowledge Reductions of Inconsistent Information systems[J]. Chinese Journal of Computers,2003,26(1):12-18. (in Chinese)
张文修,米据生,吴伟志. 不协调目标信息系统的知识约简[J]. 计算机学报,2003,26(1):12-18.
- [10] WANG J,MIAO D Q. Rough Set Theory And Its Application: A Survey [J]. Pattern Recognition and Artificial Intelligence,1996(4):337-344. (in Chinese)
王珏,苗夺谦. 关于 Rough Set 理论与应用的综述[J]. 模式识别与人工智能,1996(4):337-344.
- [11] HU M,GUO Y T,XU W H. The "Logical Or" Rough Set Theory of Variable Precision and Grade Based on Dominance Relation in Intuitionistic Fuzzy Information System[J]. Operations Research and Fuzziology,2016,6(2):66-77. (in Chinese)
胡猛,郭艳婷,徐伟华. 优势关系下直觉模糊信息系统的变精度与程度“逻辑或”粗糙集[J]. 运筹与模糊学,2016,6(2):66-77.