文章编号:1007-5321(2020)02-0023-06 **DOI**:10.13190/j.jbupt.2019-113

基于 Rete 规则推理的告警关联性分析

杨 杨[1], 石晓丹[1], 宋 双[1], 霍永华[2], 陈连栋[3]

(1. 北京邮电大学 网络与交换技术国家重点实验室, 北京 100876; 2. 中国电子科技集团公司 第五十四研究所, 石家庄 050000;
3. 国网河北省电力有限公司 信息通信分公司, 石家庄 050022)

摘要: 针对现有规则推理算法无法实现在当前大规模复杂多变的网络环境中准确、实时地推理告警规则的问题,提出了一种改进的规则推理算法 Im_Rete. 该算法结合网络告警数据的特点,采用面向告警缺失的模糊推理策略和基于概率关联模型的事实传播策略,在提高推理准确性的同时平衡推理速度,能够更加有效地对告警进行关联分析. 通过仿真实验进行对比分析,结果表明 Im_Rete 算法在推理速度和准确性方面均具有较好的性能.

关 键 词: 告警; 关联性; 规则推理; 模糊逻辑

中图分类号: TP393.0 **文献标志码**: A

Alarm Correlation Analysis Based on Rete Rule Reasoning

YANG Yang[1], SHI Xiao-dan[1], SONG Shuang[1], HUO Yong-hua[2], CHEN Lian-dong[3]

(1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. The 54th Research Institute of CETC, Shijiazhuang 050000, China;
3. State Grid Hebei Electric Power Company Limited Information and Telecommunication Branch, Shijiazhuang 050022, China)

Abstract: With the continuous development of networks, alarm correlation analysis has received extensive attention as an important means of fault diagnosis. However, in a complex network environment, problems such as link interruption, congestion caused by network faults may result in the loss of alarm data, and the amount of transient alarms caused by fault propagation may be massive. These problems make existing rule-based reasoning algorithms are difficult to meet the accuracy and real-time requirements of root cause alarm reasoning. The algorithm based on the characteristics of network alarm uses fuzzy logic-based reasoning strategies and fact-based communication strategies based on probabilistic association models to balance the speed of reasoning while improving the accuracy of reasoning. The algorithm can more effectively correlate alarms. Finally, through simulation experiments, the experimental results show that the Im_Rete algorithm has better performance in terms of speed and accuracy.

Key words: alarm; correlation; rule reasoning; fuzzy logic

网络告警是一种特殊的由被管系统主动发送给网管中心的通知,告警数据反映了网络运行过程中某些故障等异常情况的发生,是网络故障的信息化表示. 工作人员通过监控系统实时呈现的告警数据了解网络的运行状况,进而分析、定位故障. 然而,由于网络中设备繁多,关联复杂,一台设备的故障可能产生多条告警,或者导致与该设备相连的其他设备也产生大量告警,引发告警风暴. 数量庞大的告

收稿日期: 2019-06-13

基金项目: 国家重点研发计划项目(2019YFB2103200); 中央高校基本科研业务费资助项目(500419319 2019PTB-019); 2018 年工业互联网创新发展工程项目

作者简介: 杨 杨(1981—), 女, 副教授, E-mail: yyang@bupt.edu.cn.

警信息不但不能帮助网管人员定位告警源、确定故障原因,反而会将反映故障本质的根告警淹没,加大故障诊断难度. 告警关联性分析可以在网管人员处理告警数据之前对告警进行过滤、合并和转化,进而发现根告警,减少呈现给网管人员告警的数量,辅助工作人员及时准确地定位故障[1-2].

目前,告警关联性分析方法主要有以下几种[3-9]:基于编码的告警关联性分析,但该方法需要构建精确的网络对象模型,因此在大型、复杂的综合通信网络中难以应用;基于贝叶斯的告警关联性分析,该方法虽然可以有效克服告警事件的不确定性,但从实际环境中获取先验概率比较困难,且计算每个节点的相关概率是一个 NP-hard 问题;基于事例的告警关联性分析,但该方法对于网络变化反应不敏感,处理过程较复杂且费时;基于神经网络的告警关联性分析,该方法在告警信息包含噪声的情况下,也能较为准确地识别相关联的告警,但神经网络的学习严重依赖于学习样本,对样本数据的准确性、完整性具有较高的要求;基于规则的告警关联性分析,该方法因其表达直观、表示灵活、便于理解和推理等优点,受到广泛的应用. 基于规则的告警关联性分析方法将故障诊断领域的知识以规则的形式存放在知识库中,当网络中的告警报上来以后,它能调用相应的规则推理引擎进行启发式推理,发现根源告警. 常用的规则推理算法包括 Treat、Leaps、Rete 等,其中 Rete 作为目前效率最高的演绎推理算法成为现有规则推理引擎的主流算法. Rete 算法通过节点共享的方式降低模式匹配的时间花销,从而高效地处理大规模数据[3, 10-12]. 因此,笔者将 Rete 算法应用于告警数据的关联性分析,研究基于 Rete 规则推理的告警关联性分析.

然而,在实际复杂多变的网络环境中,由于网络故障引发的链路中断、拥塞等问题可能导致告警数据的缺失,使得现有 Rete 算法难以满足根源告警推理准确性、实时性的需求. 针对以上问题,笔者提出了一种改进的规则推理算法 Im_Rete. 该算法结合网络告警数据的特点,分别采用面向告警缺失的模糊逻辑推理策略和基于概率关联模型的事实传播策略,在提高推理准确性的同时,平衡推理速度,有效减少呈现给网管人员的告警冗余,辅助工作人员对网络故障进行及时、准确地诊断,对维护网络的稳定运行具有重要意义[13-14].

1 相关工作

Rete 算法由 Forgy[1] 提出,是一种高效的模式匹配算法. Rete 算法根据规则的条件编译生成一个树形结构的判别网络作为事实的传播路径,每个规则前件是网络中的一个节点,运行时将事实送入判别网络进行模式匹配,匹配完全的规则即被激活. Rete 的规则判别网络如图 1 所示.

Rete 网络分为 Alpha 和 Beta 网络. Alpha 网络包括 root、type、select 和 Alpha memory 节点. root 是所有事实对象(Facts)进入 Rete 网络的入口;type 节点根据事实对象的类型对其过滤,将符合条件的事实向后继节点传播;select 节点根据模式的属

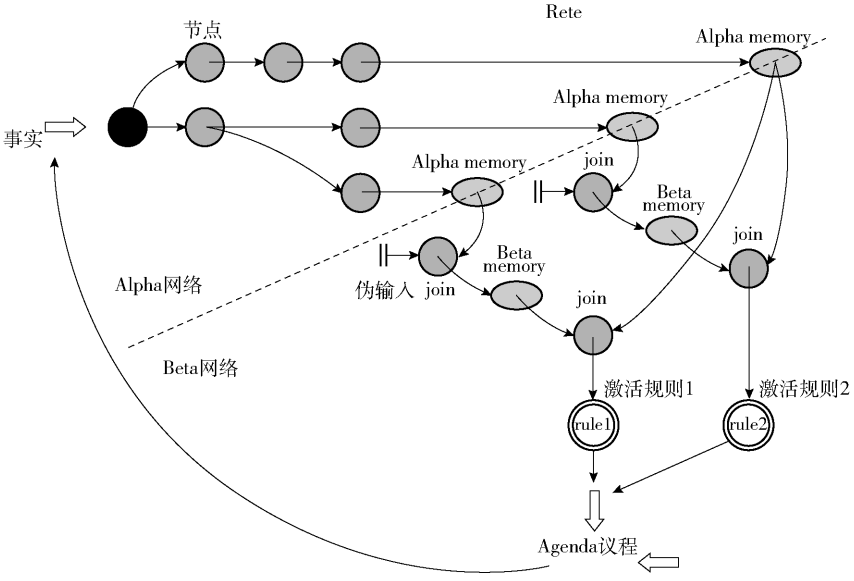

图 1 Rete 规则判别网络

性对事实进行过滤，将符合条件的事实向后继节点传播，直至 alpha memory. Beta 网络包括 beta memory 和 join 节点. join 节点是双输入节点，其中左输入通常为 beta memory 中的事实对象元组，右输入通常是一个事实对象. join 节点对事实间的属性关系进行约束，如条件符合，则对 2 个输入进行 join 连接操作，且将结果生成元组存储在 beta memory，并向后继节点传播. 当事实传播至叶子节点时，表示该节点对应的规则被完全匹配，则将该规则加入议程Agenda.

Rete 算法作为规则推理引擎的核心，受到了国内外学者的广泛关注. 例如，Sottara 等[6]对 Rete 规则的语法逻辑进行了扩展，即根据规则的逻辑操作符构造一个语法树，并在该树的基础上建立 Rete 判别网络，逻辑符作为网络中的一个判别节点参与匹配操作，从而减少额外的规则拆分开销，增强 Rete 算法的通用性；Xiao 等[7]将 Beta 内存进行单元划分，每个单元设置唯一标识，通过 Hash 函数进行索引，以提高模式匹配的速度；汪成亮等[8]提出了最小传输代价的 Rete 分布的算法，以解决智能环境中基于 Rete 的规则推理引擎需要将数据集中到 sink 节点，导致传感器网络中数据传输量过大的问题；Sun 等[9]采取有穷自动机理论的思想，提出了一种基于共享度模型的 Rete 网络构建方法，通过提高判别网络节点共享度，提高匹配速度；Zhao 等[16]提出了一种基于 XML 格式规则的 Rete 算法，该算法基于 XML 的规则描述方法，实现了规则描述文件和实体类调用的特定逻辑的松散耦合体系结构，以提高规则谓词的扩展能力以及规则共享性.

2　改进的规则推理算法 Im_Rete

Rete 算法的提出极大提高了规则引擎的匹配效率，为了提高根告警分析的效率，笔者将 Rete 算法应用于告警数据的关联性分析. 系统将接收到的实时告警与规则进行模式匹配，分析出相关联的告警，进而发现根告警，以辅助网管人员快速地进行故障定位和诊断. 然而，Rete 算法是一个基于网络的完全匹配算法，在应用于网络告警数据中时，由于实际网络环境复杂多变，网络故障引发的链路中断、拥塞、高时延、高丢包率等问题可能导致告警数据的缺失，使得告警序列难以精确匹配对应的规则，从而影响推理的准确性，难以满足故障诊断中根告警分析准确性需求.

针对上述问题，笔者提出一种改进的规则推理算法 Im_Rete. 该算法根据网络告警数据的特点，采用面向告警缺失的模糊推理策略，以适应网络故障带来的告警缺失问题；同时考虑到告警传播可能导致的告警风暴问题，算法参考近似化 Rete 的思想[4]，引入基于概率关联模型的事实传播策略，在提高推理准确性的同时平衡推理速度，能够更加有效地对告警进行关联性分析.

2.1　面向告警缺失的模糊逻辑推理策略

传统告警关联性分析中规则的表示如式(1)所示，其中 P_{in} 表示第 i 个规则中的第 n 个模式，P_i 表示第 i 个规则的结论.

$$P_{i1}, P_{i2}, \cdots, P_{in} \rightarrow P_i \tag{1}$$

Rete 算法是一个完全匹配算法，对于式(1)，如果 $P_{i1}, P_{i2}, \cdots, P_{in}$ 的取值都为真，该规则才可被激活. 即事实在判别网络进行传播时，如果任意某次 join 操作失败，则该规则匹配失败. 这种精确匹配的方式难以适应网络故障带来的告警缺失问题，对此采用一种面向告警缺失的模糊推理策略[15]，该策略为规则前件赋予不同的权重，如果某次 join 操作失败，该模式对规则的重要程度不高，则可忽略此次失败，从而增加推理网络的容错性[5]. 改进后的规则表示为

$$w_{i1}P_{i1}, w_{i2}P_{i2}, \cdots, w_{in}P_{in} \rightarrow P_i \tag{2}$$

其中 $w_{ij}(j=1,2,\cdots,n)$ 是模式 P_{ij} 的权重，$w_{ij} \geqslant 0$ 且 $\sum_{j=1}^{n} w_{ij} = 1$. 定义 $T(P_{ij})$ 为模式 P_{ij} 的真度，当事实与模式 P_{ij} 相匹配时，$T(P_{ij}) = 1$；否则 $T(P_{ij}) = 0$. 对于一个选定的阈值 τ，只要事实匹配的权重和不小于 τ，如式(3)所示，即可激活该规则.

$$\sum_{j=1}^{n} W_{ij} T(P_{ij}) \geqslant \tau \tag{3}$$

Im_Rete 算法采用面向告警缺失的模糊推理策略，基于模糊 c-均值(FCM，Fuzzy c-means)聚类为规则前件每个模式设置权重 W_{each}，并设置匹配阈值 τ. 告警事实在判别网络传播的过程中，当某次 join 连接操作失败时，如果该规则模式的最小 W_{each} 小于 $(1-\tau)$，则忽略此次失败. 当传播至终端节点(叶子节点)时，如果 W_{total} 于事先设定的匹配阈值 τ，则激活该规则，否则规则激活失败. 其中规则权重的确定对推理的准确性具有重要意义，为了更加准确地确定规则权重，引用 FCM 算法对告警模糊化获得告警对根告警的模糊隶属度的方法确定权值[17].

1）告警量化

告警的每个属性从不同角度反映告警的重要程度. 因此,对告警进行模糊化其实就是将告警的各属性值整体进行综合模糊化,告警属性量化是进行告警模糊化的前提. 选取以下几个属性:

① 告警节点. 告警节点所连接的链路数目大小反映节点位置的重要程度,链路数目越大,重要程度越高.

② 告警级别. 告警级别由厂商以及专家预先定义,分别用1~5依次表示告警的级别,数字越大,告警级别越严重.

③ 告警类型. 根据TCP/IP协议模型,低层为上层提供服务. 若低层发生故障,故障将会传播至使用该低层服务的高层,从而引发较高层产生次生告警,因此低层告警相对重要程度较高.

2）模糊权值的确定

根据一条告警与根告警的接近程度,定义语言变量评价模糊集 $F=\{A_5,A_4,A_3,A_2,A_1\}$,接近根源告警的程度依次降低. 因此对告警 J 进行模糊化,就是求 J 对于 F 的模糊隶属度向量. FCM实现将 n 个向量 $\boldsymbol{u}_i(i=1,2,\cdots,n)$ 划分成 $c(c$ 取告警等级数5)个模糊簇,然后每个告警以[0,1]区间某个取值隶属于该聚类.

隶属度矩阵:

$$\boldsymbol{U}=\{u_{ij}\in[0,1]\mid 1\leqslant i\leqslant c,1\leqslant j\leqslant n\} \tag{4}$$

隶属度向量归一化处理:

$$\sum_{i=1}^{c}u_{ij}=1,\ \forall j=1,2,\cdots,n \tag{5}$$

目标函数:

$$J(\boldsymbol{U},c_1,c_2,\cdots,c_c)=\sum_{i=1}^{c}J_i=\sum_{i=1}^{c}\sum_{j=1}^{n}u_{ij}^m d_{ij}^2 \tag{6}$$

其中:$c_i(i=1,2,\cdots,c)$ 为第 i 个聚类中心,$m\in[1,\infty)$ 为加权指数,d_{ij} 为元素 j 至聚类中心 c_i 的欧氏距离. 构造新的目标函数:

$$\begin{aligned}&\bar{J}(\boldsymbol{U},c_1,c_2,\cdots,c_c,\lambda_1,\lambda_2,\cdots,\lambda_n)=\\&J(\boldsymbol{U},c_1,c_2,\cdots,c_c)+\sum_{j=1}^{n}\lambda_j\left(\sum_{i=1}^{c}u_{ij}-1\right)=\\&\sum_{i=1}^{c}\sum_{j=1}^{n}u_{ij}^m d_{ij}^2+\sum_{j=1}^{n}\lambda_j\left(\sum_{i=1}^{c}u_{ij}-1\right)\end{aligned} \tag{7}$$

其中 $\lambda_j(j=1,2\cdots,n)$ 是 $J(\boldsymbol{U},c_1,c_2,\cdots,c_c)$ 约束式的拉格朗日乘子. 对式(7)求导,可得

$$c_i=\frac{\sum_{j=1}^{n}u_{ij}^m x_j}{\sum_{j=1}^{n}u_{ij}^m} \tag{8}$$

$$u_{ij}=\frac{1}{\sum_{k=1}^{c}\left(\frac{d_{ij}}{d_{kj}}\right)^{2/(m-1)}} \tag{9}$$

c_i、u_{ij} 即为目标函数取得最小值的必要条件.

设 $F=\{A_5,A_4,A_3,A_2,A_1\}$ 模糊语言评价集中对应的权重分别为 $\{w_5,w_4,w_3,w_2,w_1\}$,则对于模糊隶属度向量为 $(u_{5j},u_{4j},u_{3j},u_{2j},u_{1j}\mid j=1,2,\cdots,n)$ 的告警 J,其权值如下:

$$V_{al}=\frac{u_{5j}w_5+u_{4j}w_4+u_{3j}w_3+u_{2j}w_2+u_{1j}w_1}{w_5+w_4+w_3+w_2+w_1} \tag{10}$$

2.2 基于概率关联模型的事实传播策略

传统Rete算法在事实匹配阶段将事实传播给节点的每个后继节点,该方法采用完全匹配的方式,效率较低,难以适应告警风暴时根源告警推理实时性的需求. 而Im_Rete算法参考近似化Rete的思想,引入基于概率关联模型的事实传播策略[4],在提高推理准确性的同时平衡推理速度,能够更加有效地对告警进行关联性分析. 基于概率关联模型的事实传播策略是指Im_Rete算法在事实传播给后继节点的过程中基于概率关联模型进行近似化处理以达到提高推理效率的方法. Im_Rete算法通过获取事实传播给后继节点的概率,并对关联概率较低的传播过程进行剪枝,以提高匹配效率.

如图2所示,定义某一事实fact传播至节点 $(i-1)$ 的概率为 $p(i-1)$,fact与节点 $(i-1)$ 匹配成功的概率为 $p_{\text{pass}}(i-1)$,fact在节点 $(i-1)$ 与 i 之间的传播概率为 $p_{\text{sp}}(i-1,i)$,则fact传播至节点 i 的概率 $p(i)$ 为

$$p(i)=p(i-1)p_{\text{pass}}(i-1)p_{\text{sp}}(i-1,i) \tag{11}$$

$$p_{\text{pass}}(i-1)=\frac{\text{match}(i-1)}{\text{total}(i-1)} \tag{12}$$

$$p_{\text{sp}}(i-1,i)=\frac{\text{match}((i-1)\cap i)}{\text{match}(i-1)} \tag{13}$$

其中:$\text{match}(i-1)$ 表示与节点 $(i-1)$ 匹配成功的事实数,$\text{total}(i-1)$ 表示传播至节点 $(i-1)$ 的总事实数;$\text{match}((i-1)\cap i)$ 表示与节点 i 和 $(i-1)$ 均匹配成功的事实数. 上述变量可根据历史数据进行统计获取,在进行实时匹配时按照 $p(i)$ 概率的大小,即当概率大于预先设置的概率阈值时,选择后续分支进行传播,以提高事实传播的速率,减少不必要存储. 其中概率阈值的设置对推理效果具有重要影响,设置得过大会导致过剪枝,无法匹配到对应的规则,影响推理的准确性;设置得过小会导致事实传播策略回退至完全传播,从而影响匹配速率.

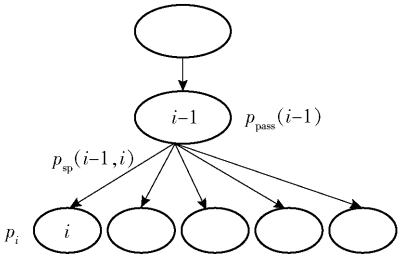

图 2　基于概率关联模型的事实传播策略

3　仿真实验结果与分析

实验选取 Rete[1]、Rete_SDM[9]算法和所提出的 Im_Rete 算法进行对比，所采用的数据来自于某地区电力通信网网管系统导出的告警数据. 仿真实验使用的操作系统为 Windows7，运行环境 CPU 为 2.2 GHz Intel Core i3，内存为 8 GB，编程语言为 Java1.7，IDE 为 MyEclipse2017. 在不同的规则数和事实数下分别运行 Rete、Rete_SDM 和 Im_Rete 算法多次，记录每次算法的运行时间，统计平均值，算法运行结果如图 3 ~ 5 所示. 需要说明的是，结果中的运行时间消耗不包括告警数据预处理的时间以及构建 Rete 网络的时间.

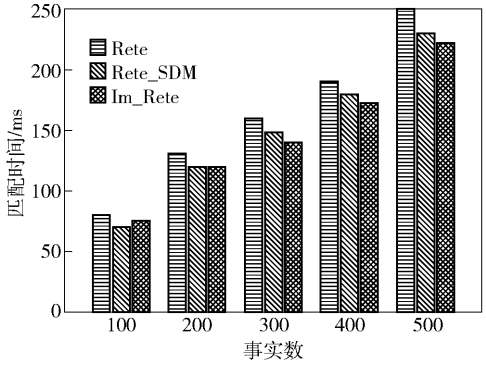

图 3　算法运行时间对比(规则数:200)

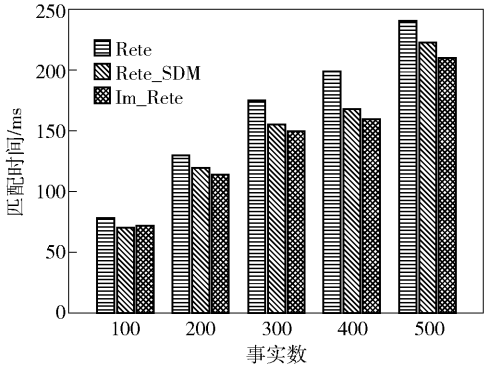

图 4　算法运行时间对比(规则数:400)

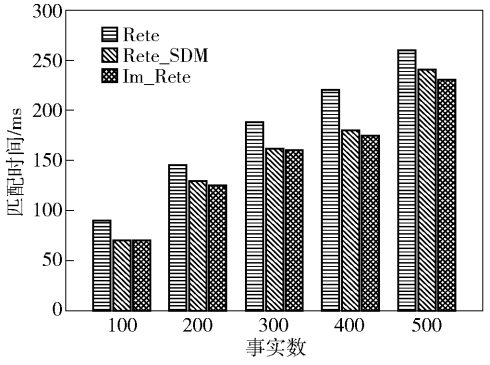

图 5　算法运行时间对比(规则数:600)

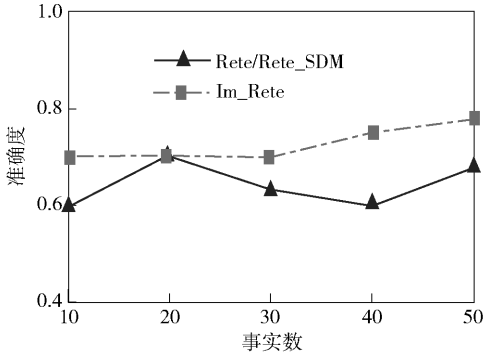

图 6　算法推理准确度对比($\tau = 0.65$)

在推理准确度方面，选取该电力通信网 50 次故障期间产生的告警数据进行仿真分析，如图 6 ~ 8 所示. 在不同匹配阈值的条件下，Im_Rete 算法推理准确度均高于 Rete 和 Rete_SDM 算法. 由于实际网络环境复杂多变，网络故障引发的链路中断、拥塞、高时延、高丢包率等问题都可能导致告警数据的缺失，Im_Rete 算法结合网络告警的特点，采用了面向告警缺失的模糊推理策略，当规则中匹配的模式权重超过匹配阈值时即可激活该规则，从而提高根告警分析的容错性.

其中匹配阈值的选取对于推理的准确性具有重要影响，匹配阈值过小会导致匹配到的规则过多，从而掩盖真实的根告警；匹配阈值过大会导致推理策略回退至完全匹配，从而影响推理的准确性. 阈值的选取需要结合具体场景进行反复实验确定.

在推理速度方面，如图 3 ~ 5 所示，在不同规则数的条件下，Im_Rete 算法的推理速度均优于传统 Rete 算法，与 Rete_SDM 算法基本一致. 这是因为 Im_Rete 算法采用的面向告警缺失的推理策略会带来额外的开销，在一定程度上会影响算法的推理速度，对此，Im_Rete 算法在 Rete_SDM 算法共享度模型[9]的基础上采用了基于概率关联模型的事实传

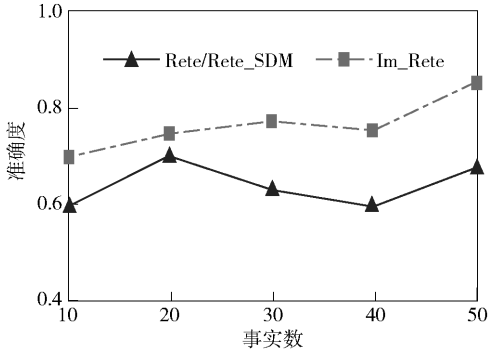

图7 算法推理准确度对比($\tau=0.75$)

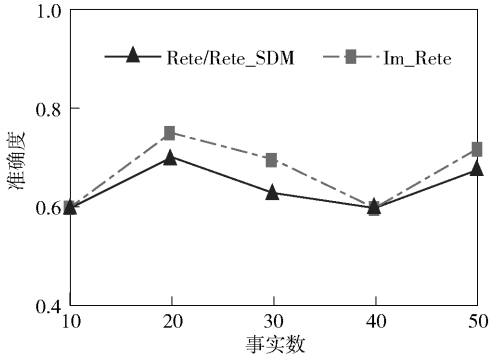

图8 算法推理准确度对比($\tau=0.85$)

播策略,虽然会损失一部分推理精度,但可以提高匹配过程中事实的传播速度,在推理的准确度和速度之间获得良好的平衡,从而更好地适应网络根告警分析实时性、准确性的需求.

4 结束语

针对现有 Rete 规则推理算法的不足,结合网络告警数据的特点,提出了一种改进的规则推理算法 Im_Rete. 该算法分别采用面向告警缺失的模糊逻辑推理策略和基于概率关联模型的事实传播策略,以适应网络故障带来的告警缺失以及告警风暴等问题,可以更加快速、准确地对告警进行压缩和过滤,发现根源告警,最后通过仿真实验进行对比分析,结果表明 Im_Rete 算法在根告警分析方面具有较好的性能.

参考文献:

[1] Forgy C L. Rete: a fast algorithm for the many pattern/many object pattern match problem[J]// Expert systems. IEEE Computer Society Press, 1991: 547-559.

[2] 李文璟, 王智立. 网络管理原理及技术[M]. 北京:人民邮电出版社, 2008.

[3] Xiaodong G, Yang G, Jun H. Rete algorithm: current issues and future challenge [J]. Computer Science, IEEE, 2012, 39(11): 8-12.

[4] 顾小东. 基于 Rete 算法的大规模规则推理引擎研究与应用[D]. 南京:南京大学, 2013.

[5] 王瑞. 规则推理在故障诊断中的应用研究[D]. 福州:福州大学, 2013.

[6] Sottara D, Mello P, Proctor M. A configurable Rete-OO engine for reasoning with different types of imperfect information[J]. IEEE Transactions on Knowledge & Data Engineering, 2010, 22(11): 1535-1548.

[7] Xiao D, Zhong X. Improving Rete algorithm to enhance performance of rule engine systems [C]// International Conference on Computer Design and Applications. [S. l.]: IEEE, 2010: 572- 575.

[8] Cheng L W, Xin W. Distributed Rete algorithm in smart environment [J]. Journal of Computer Applications, 2016, 36(7): 1893-1898.

[9] Sun X, Yan X M, Shang Y M, et al. An improved Rete algorithm using shared degree model[J]. Acta Automatica Sinica, 2017, 43(9): 1571-1579.

[10] Guo C, Xiong W, Hao L. An improved Rete algorithm with branch filtration [J]. Procedia Engineering, 2017, 174: 767-772.

[11] Yao J. An efficient approach for rule matching in production system based on multi-agent[C]// International Conference on Systems and Informatics. [S. l.]: IEEE, 2017: 378-381.

[12] Guo J Y, Hwang C, Chen M S. Using GPU to shorten the match time of rule reasoning based on Rete algorithm [C]// International Symposium on Computer, Consumer and Control. [S. l.]: IEEE, 2016: 883-886.

[13] Zhang Y H. Design and implementation of telecommunication network alarm analysis based on big data technology association [J]. Telecom Engineering Technics and Standardization, 2016, 29(4): 18-23.

[14] Huang Q. Research on alarm correlation analysis model of IT centralized monitoring system [J]. Science and technology products, 2017(5): 179-179.

[15] Qu G X. Research and practice on correlation analysis technology based on fuzzy scene[J]. Wireless Internet Technology, 2016(14): 115-118.

[16] Zhao N, Bai L F. Research of the rule engine based on XML[J]. AER-Advances in Engineering Research, 2016, 67: 1787-1793.

[17] 刘珍. 多域分布式网络的告警模糊关联规则挖掘[D]. 成都:电子科技大学, 2015.