

# 网络事件管理系统中关联技术的选择及实现

杨洪涛, 王继龙

(清华大学信息网络工程研究中心, 北京 100084)

**摘 要:** 事件(告警)管理是网络管理的一项重要任务, 而事件关联技术是事件管理系统的核心。该文对主流事件关联技术进行对比和评述, 讨论其在实际应用中的短处, 并提出结合 RBR 和 CBR 技术实现的一种实用、高效的事件管理方案。

**关键词:** 网络事件管理; 事件关联; 基于规则的推理; 基于案例的推理

## Selection of Correlation Schemes in Network Event Management System

YANG Hongtao, WANG Jilong

(Network Research Center, Tsinghua University, Beijing 100084)

**【Abstract】** Event/alarm management is an important task in network management, and event-correlation methodologies are at the core of this task. This thesis first gives an overview of several mainstream event-correlation methodologies, compares them, and finally proposes a practical and efficient event management system solution based on RBR and CBR.

**【Key words】** Network event management; Event correlation; Rule-based Reasoning(RBR); Case-based reasoning(CBR)

随着计算机网络的规模越来越大, 有效的网络管理的重要性已经毋庸置疑。从某种角度来说, 网络管理的主要任务即监视、分析和处理网络事件。网管人员必须能够从观察到的众多事件中找出其中隐藏的问题。事件管理操作目前仍主要通过人工来完成。有调查表明, 操作人员 60%~90% 的时间仍在使用简单的测量和诊断工具来收集、监视和分析网络事件。这种人工过程不能满足网络日益增长的发展速度、复杂性和规模的需求, 网络管理人员的人工处理速度跟不上网络事件生成的速度。

因此提供一个自动化系统, 为大规模、高复杂度的网络实现自动化的事件管理, 是网络管理研究课题的一项重要任务, 这就是事件管理系统。网络事件管理系统有助于在以下几个方面应对事件“风暴”问题: (1)自动进行事件收集, 减少人工操作的负担; (2)通过事件关联技术, 区分故障根源和故障症状, 化简复杂的事件流, 使其更容易进行分析; (3)辅助故障诊断与恢复, 实现高可用性服务。

### 1 网络事件

#### 1.1 事件

网络管理领域中的事件通常定义为有关网络中正在发生的情况的信息。网络环境中受管理设备上的硬件和软件故障、安全侵害、性能下降、环境参数变动等都可能通过事件表现出来。其具体表现形式一般为软硬件系统日志、性能参数的测量、各种网络管理协议所定义的事件等可供观察、收集的信息和数据。

#### 1.2 事件关联

当网络中发生故障时, 所有感知到故障的受管理对象都可能发出告警事件。事件关联指的是将由同一个异常状况引起的所有事件组织在一起, 提出可能的问题根源。

根据对事件进行操作的方式, 事件关联可以分为以下几种类型<sup>[1]</sup>:

压缩: 将多次发生的同一个事件合并为一个单独的事件;

过滤: 如果事件的某些参数, 如优先级、类型、位置、时间不属于管理系统关心的范围, 则忽略;

抑止: 发生高优先级事件的情况下忽略低优先级事件;

计数: 相同的或类似的事件发生的次数超过阈值;

概括: 将多个局部事件综合为一个整体事件, 以便从更宏观更高层的角度观察网络事件;

时序关系: 根据事件发生的先后次序进行关联, 时序关系可以包括先、后、包含、重叠等;

逻辑组合: 使用 AND、OR、NOT 等逻辑操作符生成复杂的关联模式。

由于可观测的网络事件一般只描述了异常的现象(症状), 不可能含有对其原因的分析, 再加上以下因素的影响, 使得解决事件关联问题的难度非常大:

(1)一次故障可能使设备发出多个事件;

(2)故障可能是间歇性的, 每次发生都会发出事件;

(3)一个功能的故障可能会在每次调用该功能时都发出事件;

(4)一次故障可能被多个网络对象同时检测到, 导致每个对象都发出了事件;

(5)一个网络对象的故障可能会影响其他对象, 而造成故障的传播。

### 2 事件关联技术

为了解决这些问题, 事件管理系统必须采用关联技术。事件关联技术是任何事件管理系统的核心, 它的目标是精简需要分析的症状和需要处理的故障的数量。目前对事件关联方法的研究可以大致分为如下几类<sup>[2-4]</sup>: (1)基于规则的推理;

**基金项目:** 国家“863”计划基金资助项目“大型计算机网络管理技术与系统”(2001AA112041)

**作者简介:** 杨洪涛(1980—), 男, 硕士, 主研方向: 网络故障管理; 王继龙, 副教授、博士

**收稿日期:** 2005-02-28 **E-mail:** yanght@mails.tsinghua.edu.cn

(2)编码方法；(3)基于案例的推理；(4)基于模型的推理；(5)人工智能方法。

### 2.1 基于规则的推理

事件管理系统是一种专家系统。最常见的专家系统的形式是基于规则推理的专家系统，它可以分为两个部分：

- 状态集合，是一组状态元素的集合，代表网络的当前状态。每个状态元素是网络中的一条信息，或推理过程中的一个假定。

- 规则集合，是以“if-then”或称“条件-动作”形式表现的专家知识规则。规则的条件部分(左端)根据状态集合的当前状态是否应用该规则。规则的动作部分(右端)含有条件满足时根据该规则所得的结论。

例如，假设链接到结点 X 的两条链路都出现故障事件则表明结点 X 出现故障，可以定义为如下规则：

link-down(X, Y) and link-down(X, Z) -> fault(X)

随着故障事件的发生，状态集合中的信息越来越多。假设某一时状态集合中同时出现了如下元素：

link-down(node-A, node-B)

link-down(node-A, node-C)

根据上述规则，此时系统推断出：

fault(node-A)

于是这条新的状态被加入状态集合。

这种基于规则的关联技术是较为传统但在实际工程应用中非常有效的技术。它的精确性在很大程度上依赖于规则的正确性，因此它需要足够的专家知识和经验来定义规则，并且随着网络的变化而随时更新这些规则。而这正是这种方法的主要缺点。

### 2.2 编码方法

编码方法的思想很简单。一个故障会导致很多症状事件。如果将一个故障导致的完整的症状集合作为识别该故障的编码，那么事件关联过程就是确定已观察到的症状符合哪个故障的编码。

编码技术按两个阶段来进行。在码本选择阶段，选择事件的一个子集进行监视，这个过程的结果被称为码本。码本是一个优化的事件子集，它必须能够用来区分一个故障，同时还要确保能够允许一定程度的噪声。在运行阶段，不断发生的事件序列被编码，并计算该编码与码本中的每条编码之间的距离，将距离最小的那条编码所对应的故障(即与观察到的症状最接近的故障)报告给网络管理人员。

与基于规则的推理方法相比，编码方法预先处理事件知识模型，将关联问题转化为故障特征的抽取和最小距离问题，这正也是编码技术中的两个难点。在实际工程中，与基于规则的方案相比，它的实现代价更大，适用范围更小。

### 2.3 基于案例的推理

上述的技术都存在一个共有的弱点，即它们不能适应网络环境的改变，这被称为“知识获取”问题。基于案例的推理试图解决这个问题，这是通过故障案例来完成的。

案例实际上即网络故障本身和排除故障的过程的特征。构造案例需要使用一种能够描述它们的语言，并利用数据库来存储和检索案例。当网络出现故障时，管理系统对当前故障进行参数化，在案例库中搜索以前出现的一个类似的案例，对找到的案例的故障排除方案进行修订，以作为当前故障的解决方案。当前故障排除后，新的解决过程被加入数据库中，使案例库逐渐丰富。

CBR 技术通常包括以下步骤：

(1)案例检索：发生新故障时，根据新故障的特征，从历史案例

中检索出最接近的案例。

(2)案例修订：根据新的情况，对检索出的历史案例的解决方案进行调整，以提出新的解决方案。

(3)案例存储：将用户反馈信息，新案例。

### 2.4 基于模型的推理

模型是网络系统的一种数学表示。这种技术使用模型和从实际受管理对象上观察到的信息来推理甚至预测异常故障的发生。模型的具体方法包括故障模型、结构模型等。

故障模型预先定义可能发生的故障类型，只对这些故障进行建模。每种选定的故障插入每个组件，进行模拟，监视整个系统的行为。每次模拟产生一个特定的异常，记录整个系统的行为描述。这样就形成了故障与对应症状的一个清单，当实际发生故障症状时可以从确定发生故障的对象。

结构模型是用有向图的节点和有向边分别来代表系统中的变量和变量间的关系。例如变量通常代表症状和故障，而有向边代表故障和症状之间的关联，并为每条边定义权重或概率。利用概率方法对故障进行推断。

系统模型的建立需要专家知识，因此“知识获取”的困难也是这种技术的缺点。它的主要优势是能够表现复杂的结构化知识。

### 2.5 人工智能方法

人工智能(AI)方法是与传统的基于规则或码本的方法完全不同的一种技术。AI 系统的最大优势在于，在理想的情况下，它能够实现自学习的能力，从而消除前面几种技术对专家知识的需求。有关的具体技术诸如各种机器学习方法、数据挖掘方法等。

AI 方法的缺点在于，虽然它较少需要专家知识，但绝大多数 AI 技术需要预先准备较多的数据对系统进行训练，在实际运行的网络中这些数据的收集是一个较大的困难。此外，当网络规模较大、数据较多时，AI 系统的训练过程和执行过程的时间复杂度会迅速上升，这也是在实际运行的网络中较难接受的。并且 AI 方法天生所具有的不确定性也是工程技术人员不能接受的。这些缺点与 AI 技术的尚不成熟有关，有关研究仍然大多停留在实验室阶段，难以投入实际网络的运行。

## 3 THEM 中的事件关联选择

就关联技术本身来说，由于缺少实际的数据，因此难以进行量化的比较，但应用中需要考虑的几个因素至少包括实现复杂度、适应网络变化的能力、性能、准确性等。

一般来说，基于规则的方案实现代价较小，快速而准确，能够满足实时运行要求，适用于较少进行大范围配置变动的网络环境。难以适应网络变化的缺点使它难以应用于大规模的网络环境。而其它方案，例如基于案例的方案就对网络的变化没有如此敏感。基于案例的方法、编码方法和人工智能技术较为适合处理事件关联中的不确定性，例如它们对输入事件流中的“噪声”有更高的鲁棒性。编码方法在性能和鲁棒性角度都有优势，但它需要建立网络的非常详细的模型，实现复杂度较高，代价太大，使得它同样不完全适用于大规模网络。

从实际产品来看，行业市场上的主流解决方案，例如 Veritas 的 NerveCenter、Tavve 的 EventWatch、SMARTS 的 InCharge、NetView、HP NNM ECS 等平台多是基于规则方法的，并且主要以网络的拓扑结构为首要的网络模型。其最大好处在于只要将拓扑转换为各自的表现结构，它们就可以开始关联工作，但是它们没有学习的过程，不能够根据事件关

联过程中获得的经验对算法进行调整,因此单纯依赖它们有时就不能给出正确的关联结果。而基于案例的技术则正相反,它需要一个较长的学习过程,但随着案例的积累,它会不断地学习每个网络的个性特征,它的推理结果就会越来越精确。为此,必须将基于规则的技术和基于案例的技术结合起来,充分利用对解决事件关联问题有用的知识和经验。

综合以上考虑,作者在 THEM(Tsinghua Event Management)系统项目中采用了 CBR 和 RBR 结合的方案。

THEM 事件管理系统具有如图 1 所示的基本结构。其基本组成部分是知识存储(案例库/规则库)、事件收集、RBR/CBR 事件关联部分等。

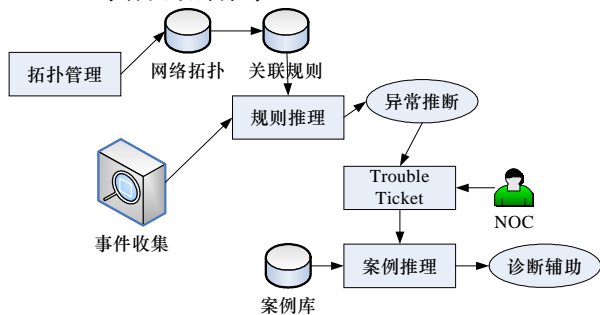


图 1 系统结构

事件收集同时采用轮询和通知的方法,内容主要包括:

(1)基于 ICMP 的网络节点连通性、性能参数;(2)Web/Mail/文件等重要服务可用性;(3)应用程序日志;(4)基于 SNMP 的 MIB 变量轮询、trap 收集;(5)网络设备和应用服务器的 syslog。

所有收集到的事件进入一个当前事件池。直到发生相对应的 Clear 事件才从事件池中删除一个事件(例如 linkDown 事件对应的 Clear 事件是 linkUp)。

### 3.1 规则关联及其构造

基于 RBR 的事件关联模块所创建的规则内容包括了前面讨论到的压缩、过滤、抑止、计数、概括、时序、逻辑等。它们的来源主要分为两大部分:

(1) 基于网络拓扑所创建的规则。拓扑规则是关联规则中的一个重要部分,这部分融合了基于关系模型方法的优点,同时在一定程度上解决 RBR 适应网络变化的问题。

THEM 以图 2 所示的对象结构来描述网络的层次结构、服务与被服务关系、节点与链接关系等,如:

```
link1 ConnectedTo nodeA
serviceX ResideIn nodeA
```

经由这种 OO 表达,将拓扑抽象为有向图,使故障判断转化为图的连通问题。这样就可以将图的运算运用在规则中。

本文注意到,现有基于拓扑模型的方案中通常不考虑环境因素,这是不恰当的。为此 THEM 所采用的广义拓扑描述中还考虑了受管理对象所处的环境,例如一些网络设备位于同一个机房中,环境温度的异常会对各设备同时造成影响。

(2) 根据实际网络运行状况而从有经验的网络运营人员获得的专家知识,以及基于受管理网络设备、主机的功能及特性所创建的规则。后者主要来自设备的使用手册和生产厂商在各种产品文档中对产品的管理策略所作的推荐,这方面文献[6]是一个典型的例子,它讨论了对受管理网络设备的性能基准测量、日志和 trap 关联的推荐方案。

规则运算采用前向链模式做规则匹配。匹配计算实时进行,每当事件发生时,扫描事件池中满足规则左端的状态元

素。当条件满足时,执行条件右端。新形成的状态元素再用来测试其它规则的条件,形成链。

在中等规模的校园网络中,基于 RBR 的事件关联能够每天的数万个原始事件归并为小于 100 个含有综合信息的、供网络管理人员监督的事件。

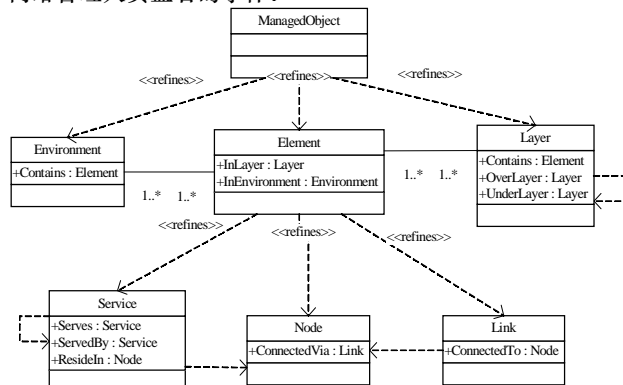


图 2 用以描述拓扑的对象结构

### 3.2 通过 Trouble Ticket 系统应用历史经验

THEM 事件管理系统中包括一个 Trouble Ticket(TT)工作流子系统。TT 系统采用 CBR 方法将系统中积累的历史知识应用到新问题的解决过程中,其基本思路是从案例库中检索与目前情况接近的案例,按相似度排序,通过可视化界面展示给用户。

TT 系统的 ticket 来源有两个:(1)根据关联规则的设定,一部分事件会进入 TT 系统,成为需要运营人员处理的 ticket;(2)TT 系统支持一般 NOC Ticket 系统所具有的工作流功能[6],即它还有人工输入的 ticket,来源主要是 NOC 热线收到的用户故障报告。

对于第一类 ticket,即规则关联系统自动输入的事件,由于它的属性是固定的,甚至是可以量化的数值属性,因此采用如下余弦公式计算案例间的相似度<sup>[8]</sup>:

$$G_{case} = \frac{\sum_{i=1}^m \omega_i^n \omega_i^{p_k} \left( 1 - \left( \frac{(x_i - y_i)}{R_i} \right) \right)}{\sqrt{\sum_{i=1}^m (\omega_i^n)^2 \sum_{i=1}^m (\omega_i^{p_k})^2}} \quad (1)$$

其中  $1 - \left( \frac{(x_i - y_i)}{R_i} \right)$  代表新案例和原案例在第 i 个属性上的相似性;  $\omega_i^n$  为新案例的第 i 个属性的权重;  $\omega_i^{p_k}$  为历史案例 k 的第 i 个属性的权重。

但是 NOC Ticket 系统的第二类 ticket,即人工输入的自由文本描述,是半结构化的。它的属性不能视为量化属性,而是由故障描述、相关日志、测试结果、解决过程、结论等自由文本描述的属性构成的,并且很难将这些属性转化为结构化表示。对此类 ticket,THEM 将信息检索(IR)技术应用到 CBR 的案例检索过程中。

其基本流程为:在预处理阶段,首先根据案例库生成专业词表(terms)。在 IR 研究中通常认为名词和名词性短语承载有文字中主要语义。对历史案例的自由文本属性做分词,标注网络管理领域内涉及的名词及短语,并对词表中每个 term 做所有历史案例的倒排表索引。

新案例发生时,根据新案例属性中出现的词表中的 term,对倒排表进行查询和求交计算结果。并根据 tf · idf 算法确定案例相似度<sup>[7]</sup>排序。

(下转第 213 页)

### 3 实验结果与分析

我们在 ORL 人脸数据库<sup>[6]</sup>上测试了算法效果。ORL 人脸数据库有 40 个人的图像, 每个人都有 10 张不同表情、不同姿态与不同光照条件的人脸图像, 每张图像的分辨率都是  $92 \times 112$  像素, 每个像素为 256 个灰度级。图 2 是 ORL 人脸数据库中的部分实例。



图 2 ORL 人脸数据库的部分实例

每个人随机取 5 张照片用于训练集, 剩下的 5 张照片用于测试集。首先实验了式(5)中参数  $\alpha$  对识别性能的影响, 然后实验了我们的算法与 PCA<sup>[1]</sup>、LDA<sup>[5]</sup>以及 PCA+LDA<sup>[4]</sup>的对比情况, 在实验中识别率均采用首选正确识别率。

图 3 为式(5)中参数  $\alpha$  对人脸识别率的影响的曲线图。

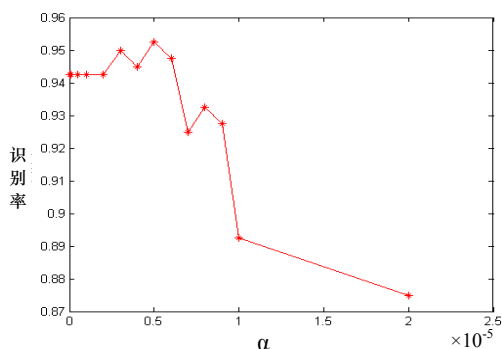


图 3 参数  $\alpha$  对识别率的影响

在实验中, 识别特征维数为 39。从图中可以看出参数  $\alpha$  对算法性能的影响是比较大的。当  $\alpha$  小到接近于 0 的时, ILDA 算法就相当于传统的 LDA 算法, 随着  $\alpha$  的增加, 算法

的性能慢慢变好, 但到了某个临界值后再增加  $\alpha$ , 算法的性能又开始变差了, 这是由于将距离大的类惩罚得太厉害了的缘故。从图 3 中可看出当  $\alpha$  值在  $0.5 \times 10^{-5}$  左右时, 算法的性能最好。

图 4 为识别率随维数变化的曲线图。从图 4 中可看出 ILDA 算法在各种特征维数下的识别率都较传统算法优越。

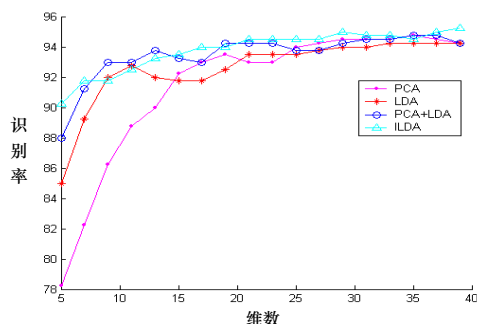


图 4 特征维数与识别率的关系

### 4 总结

通过对 ORL 人脸数据库的测试表明 ILDA 算法的性能是非常好的, 并且 ILDA 算法的训练与识别的实现也很简单, 相信在其的模式识别的研究领域中也有一定的意义。

#### 参考文献

- 1 Turk M A, Pentland A P. Face Recognition Using Eigenfaces [C]. Proceedings of CVPR '91, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1991-06-03 : 586-591.
- 2 Barrett W A. A Survey of Face Recognition Algorithms and Testing Results [C]. Conference Record of the Thirty-First Asilomar Conference on Signals, Systems & Computers, 1997-11-02: 301-305.
- 3 Yu Bing, Jin Lianfu, Chen Ping. A New LDA-based Method for Face Recognition[C]. Proceedings of 16<sup>th</sup>International Conference on Pattern Recognition, 2002-08-11: 168-171.
- 4 Belhumeur P N, Hespanha J P, Kriegman D J. Eigenfaces vs Fisherfaces: Recognition Using Class Specific Linear Projection [J]. IEEE Trans. on Pattern Analysis and Machine Intelligence, 1997, 19 (7): 711-720.
- 5 Chen L F, Liao H Y M, Ko M T, et al. A New LDA-based Face Recognition System Which Can Solve the Small Sample Size Problem [J]. Pattern Reco., 2000, 33 (10): 1713-1726.
- 6 AT&T Lab. The ORL Database of Faces[Z]. <http://www.uk.research.att.com/facedatabase.html>.

(上接第 199 页)

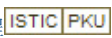
### 4 结束语

本文对网络事件管理系统中的事件关联技术进行对比和评述, 讨论了它们在实际应用中的优缺点, 并提出使用 RBR 和 CBR 结合的一种实用、高效、准确的事件管理方案, 在两种技术上扬长避短, 在 RBR 技术中注重拓扑以减小创建规则的代价, 在 CBR 中通过 IR 方法增强对半结构化属性的处理, 在实际应用中取得了很好的效果。

#### 参考文献

- 1 Aboelela E, Douligeris C. Switching Theory Approach to Alarm Correlation in Network Management, Local Computer Networks[C]. Proceedings of 25<sup>th</sup> Annual IEEE Conference, 2000.
- 2 Gardner R D, Harle D A. Methods and Systems for Alarm Correlation[C]. Proceedings of IEEE Globecom '96, 1996.

- 3 Ketschau H J, Bruck S, Schefczik P. LUCAS — An Expert System for Intelligent Fault Management and Alarm Correlation [C]. Network Operations and Management Symposium, 2002.
- 4 Melchioris C, Tarouco L M R. Troubleshooting Network Faults Using Past Experience[C]. IEEE/IFIP Network Operations and Management Symposium, 2000.
- 5 Cisco Systems, Inc. Cisco Network Monitoring and Event Correlation Guidelines[Z]. 1999.
- 6 Johnson D. NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist[S]. RFC 1297, 1992.
- 7 Salton G, Buckley C. Term-weighting Approaches in Automatic Text Retrieval[J]. Information Processing and Management, 1988, 24(5): 513-523.

作者: 杨洪涛, 王继龙, YANG Hongtao, WANG Jilong  
作者单位: 清华大学信息网络工程研究中心, 北京, 100084  
刊名: 计算机工程   
英文刊名: COMPUTER ENGINEERING  
年, 卷(期): 2006, 32 (4)  
被引用次数: 3次

## 参考文献(7条)

1. Salton G; Buckley C Term-weighting Approaches in Automatic Text Retrieval 1988 (05)
2. Johnson D NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist 1992
3. Cisco Systems Inc Cisco Network Monitoring and Event Correlation Guidelines 1999
4. Melchior C; Tarouco L M R Troubleshooting Network Faults Using Past Experience [外文会议] 2000
5. Kettschau H J; Bruck S; Schefczik P LUCAS—An Expert System for Intelligent Fault Management and Alarm Correlation 2002
6. Gardner R D; Harle D A Methods and Systems for Alarm Correlation [外文会议] 1996
7. Aboelela E; Douligieris C Switching Theory Approach to Alarm Correlation in Network Management, Local Computer Networks 2000

## 本文读者也读过(10条)

1. 李岚 基于事件关联的网络事件管理的研究和设计 [学位论文] 2005
2. 胡鹏 面向SLA的网络运行态势及链路性能分析技术的研究与实现 [学位论文] 2010
3. 张涛, 高海波, 李昕, 洪文学 通信网络关联信息可视化 [期刊论文] - 燕山大学学报 2010, 34 (2)
4. 朱伽 一种面向多系统的日志审计系统的设计与实现 [学位论文] 2009
5. 李波 网络管理系统中事件管理子系统的设计与实现 [学位论文] 2006
6. 钟向群, 沈昌祥, 戴英侠, ZHONG Xiangqun, SHEN Changxiang, Dai Yingxia 金融IT服务运行风险模型及其应用 [期刊论文] - 计算机工程 2005, 31 (17)
7. 李广福 基于SNMP和Syslog的校园网安全管理系统 [学位论文] 2010
8. 叶玲肖 基于SYSLOG的集中日志管理系统的设计与实现 [学位论文] 2011
9. 顾清 基于日志采集的分布式网管系统设计与实现 [学位论文] 2008
10. 李鹏 基于事件关联的网络故障管理研究 [学位论文] 2008

## 引证文献(3条)

1. 高爱国, 王卓, 张桂香, 吕博 事件关联技术在移动网络管理中的研究与应用 [期刊论文] - 高师理科学刊 2009 (4)
2. 曹海 基于时间Petri网的事件关联检测机制研究 [期刊论文] - 计算机应用 2008 (5)
3. 王保义, 郭雅薇, 史占成, 张少敏 基于依赖搜索树的电力通信网络告警关联方法的研究 [期刊论文] - 继电器 2008 (6)

本文链接: [http://d.g.wanfangdata.com.cn/Periodical\\_jsjgc200604070.aspx](http://d.g.wanfangdata.com.cn/Periodical_jsjgc200604070.aspx)