智能分布式通信网告警相关性模型及实现

邓 歆 孟洛明
(北京邮电大学网络与交换国家重点实验室 北京 100876)

摘 要 该文提出了智能通信网络的告警相关性分析模型。将通信网按照功能划分成不同的功能子网，针对不同网络的特点，选择适应各自网络特性的告警相关性方法，并建立了层间的网络故障传播模型。提出基于CORBA技术的分布式告警相关性模型。最后，在SDH over DWDM光传送网中，具体分析了告警相关性模型的实现和性能比较。实验证明，采用分布式的告警相关性模型可以有效提高系统的故障诊断水平。

关键词 智能通信网，故障管理，告警相关性，故障传播模型
中图分类号：TN915.07 **文献标识码**：A **文章编号**：1009-5896(2006)10-1902-05

Intelligent Distributed Alarm Correlation in Communication Networks

Deng Xin Meng Luo-ming
(*State Key Laboratory of Networking and Switching Technology*,
Beijing University of Posts and Telecommunications, Beijing 100876, *China*)

Abstract This paper presents an approach for modeling and solving the problems of intelligent fault identification and alarm correlation in large telecommunication networks. The network is initially divided into its constituting sub-networks. Different correlation technique is utilized in each sub-network according its characteristics. And the fault propagation model is used to model the functional relationship among the sub-networks. At same time, the paper also presents a distributed framework based on CORBA in alarm correlation. Finally the realization and performance of alarm correlation are discussed in SDH over DWDM systems. The experimentation has proved that the fault diagnosis efficiency is prompted by the distributed alarm correlation systems.

Key words Intelligent communication networks, Fault management, Alarm correlation, Fault propagation model

1 引言

故障诊断是网络故障管理中的重要组成部分。通信系统无法避免出现故障，快速检测和隔离故障对通信系统的鲁棒性、可靠性和可用性是至关重要的。通常，经验丰富的网络专家根据网管监控中心显示的网络失效症状来进行故障定位。随着通信系统发展得越来越大、越来越复杂，智能告警相关性分析技术成为研究的热点。采用智能告警相关性分析的优点有：降低人力资源成本、提高故障诊断效率、提高故障诊断过程的精确度。

故障诊断的核心是告警相关性分析，即通过分析网络失效时出现的外部症状——告警，隔离导致告警出现的可能的故障原因。告警相关性分析是指对告警进行合并和转化，将多个告警合并成一条具有更多信息量的告警。告警相关性可以用于故障隔离和故障诊断、选择故障处理方法、前瞻性的网络维护、网络状况趋势分析等。

本文首先比较了各种告警相关性模型的优缺点和实现难点，讨论了尚存有待解决的问题。采用CORBA技术建立分布式告警相关性模型，分析不同层网络间的根故障诊断方法。

2005-09-21收到，2006-03-07改回
国家自然科学基金(90204002)资助课题

2 告警相关性分析

告警相关性主要包括[1]：

告警压缩 Compression $[A, A, \cdots, A]\rightarrow A$ 将多个同时发生的告警缩减到一个告警中。

告警过滤 Filtering $[A, B, C, D]\rightarrow A$ 删除不符合告警相关性要求的告警。

告警计数 Count $[n*A]\rightarrow B$ 用一个新的告警替代特定数目的同时发生的告警。

告警拟制 Suppression $[A, B,$ priority$(B)<$priority $(A)]\rightarrow A$ 当高优先级的告警发生后拟制其它低优先级的告警产生。

告警布尔 Boolean $[A, B, \cdots, T, \wedge, \vee, \neg]\rightarrow C$ 用一个新的告警替代一组符合一定布尔模式的告警。

告警泛化 Generalization $[A, A\in B]\rightarrow B$ 用告警的超类代替该告警。

告警时序关系 Temporal relation 不同告警按照一定的时间先后顺序上报。

目前已经提出了很多的告警相关性方法，这些方法来源于不同的计算机领域，如人工智能、图论、神经网络、信息论和自动控制理论。图1中对目前已经提出的告警相关性方法进行分类。其中，最常用的方法有：基于规则推理[1,2]、故障传播模型[3,4]、基于编码[5,6]、贝叶斯网络[7,8]。表1中具体

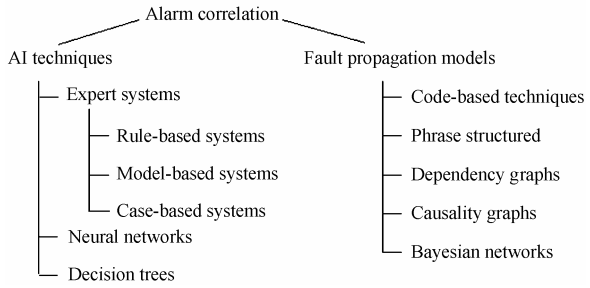

图 1　告警相关性分析模型

Fig.1 Alarm correlation models

表 1 告警相关性分析模型比较

Tab.1 Comparison among alarm correlation models

	基于规则	基于案例	基于依赖关系	基于编码	贝叶斯网络
方法分类	确定性	确定性	确定性	确定性	不确定性
构造网络模型	不需要	不需要	需要	需要	需要
适应网络变化	不能	不能	能	能	能
系统维护	难	难	较易	难	易
系统性能	低	低	较高	较高	高
学习能力	无	无	无	无	有
实现复杂度	较易	较难	较易	较难	较难
实现难点	规则发现与描述	案例描述与匹配	依赖关系的粗细粒度	构造密码本，解码	参数学习

分析了几种最常用的方法的优缺点。

告警相关性分析技术需要解决以下一些普遍的问题：

(1)告警出现的不明确性、不一致性、不完整性　不明确性是指同一个告警可能表征多个不同的故障。不一致性是指不同网络部件对网络运行状况的不同表现。例如一个网络部件认为某个网元运行正常，而另一个网络部件认为该网元发生故障。不完整性是指告警可能丢失或延迟。所以告警相关性模型最基本的任务就是将这些不明确、不一致、不完整的告警信息组成一致的网络运行视图。

(2)告警包含一些不确定内容　故障产生的一系列告警依赖于许多因素，如网络设备之间的连接关系、当前网络配置、故障发生时的服务、已存在其它故障、其它网络参数设置等等。一些瞬时故障产生的告警，也会影响故障现象准确性。

(3)多个不相关的故障同时发生造成告警集合的迭加　多个相关和不相关的故障可能在一个很短的时间内同时发生。如果不相关的故障同时发生引起告警集合的迭加，告警管理系统必须检测这些不相关的故障。

(4)同一组告警可能产生不同的故障诊断结果　当一个告警指示发生在不同网络部件的不同类型的故障，故障定位技术无法将这个告警定位到某个准确的故障。通常，因为缺少自动测试技术而无法立即寻址故障。大多数方法都事先隔离一组可能的故障假设，然后再利用有效的测试技术进行在线或下线确认。

(5)在大型通信系统中，采用集中网管模式进行定位故障和维护系统知识库是不可行　很多研究指出在大型网络中的故障定位程序应该采用分布式，由一组事件管理节点(event management nodes)共同分担数据处理的复杂度。每个管理者(manager)负责管理不同域或不同层网络协议的网络硬件和软件设备的故障定位。

3　智能分布式通信网告警相关性模型

3.1　通信网的告警相关性模型

通信网按照功能可以分为：基础媒质层、传输层、交换层、接入层、用户层。大量研究分析表明：应该针对不同网络的特点，选择适应各自网络特性的告警相关性方法。对于复杂网络的问题，还必须将多种方法组合在一起共同解决。

(1)底层通信网(如 SDH，DWDM)的目标是隔离影响网络资源可用率的故障，如光缆断、设备接口故障等。因为这些类型的故障发生概率相对较小，告警相关性模型都假设通信系统在任意时间内只有一个故障发生，不支持对多个同时发生的故障的检测。底层通信网最常采用确定性模型，假设故障与症状间的依赖关系和因果关系必须百分之百准确，如基于规则的告警相关性模型和故障传播模型。

(2)高层通信网(如 IP 网)拓扑结构经常发生变化，告警包含大量不确定性的内容。高层通信网采用不确定性模型，如贝叶斯网络等。

(3)不同层网络间的功能依赖关系采用故障传播模型描述，进行根故障原因的推理。下层子网将相关性分析结果传递给向上一层子网，上层子网利用下层子网的分析结果进行新的告警相关性分析，为用户提供端到端的故障诊断功能。

本文采用故障传播模型建立不同层网络间的功能依赖关系(如图 2 所示)。故障传播模型是一个有向无环图$G=(V,E)$[9]。其中V由一组非空的节点组成，对应不同的子网。E由一组有向边(v_i,v_j)组成，表示在子网v_j依赖于子网v_i所提供的服务。且$v_i \neq v_j$。如果(v_i,v_j)属于E，则(v_i,v_i)不属于E。模型分 1 到$N+1$层Layer，表示不同层网络。

目前有很多通信网建模的方法。采用面向对象的技术，ITU-T M.3100, TMF 814.2 定义网络信息模型(management

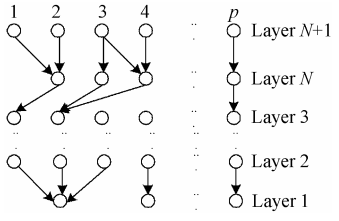

图 2　子网间的故障传播模型

Fig.2 Fault propagation model among sub-networks

information models)。网络信息模型中的被管对象间采用TMN 接口交换管理信息。通信网体系结构模型(architectural models)用于描述通信网内部结构和功能，如 ITU-T G.774 描述 SDH 管理信息模型。还有其它一些方法，如 MODEL 提供一种规范的对象描述语言。

智能通信网的告警相关性分析的过程如下：

步骤 1　网管系统通过适配器采集告警；

步骤 2　告警格式标准化，并将告警按时间窗口和所属子网分类，存储在数据库中；

步骤 3　根据通信子网的特点选择不同的告警相关性模型，并行执行告警相关性分析；

步骤 4　根据子网间的故障传播模型，将子网状态(相关告警组和可能故障)传递给上层子网；

步骤 5　采用故障传播模型对整个通信网进行根故障定位。

3.2 分布式告警相关性模型

通信网规模和结构复杂度的增加对网络管理的稳定性和效率提出了更高的要求。采用集中网管模式进行定位故障和维护系统知识库效率低，系统鲁棒性差。很多研究指出，在大型网络中的告警相关性模型应该采用分布式结构[10]。本文提出一种基于CORBA技术的分布式告警相关性模型(如图 3 所示)，CORBA为各个模块间提供消息传递服务。

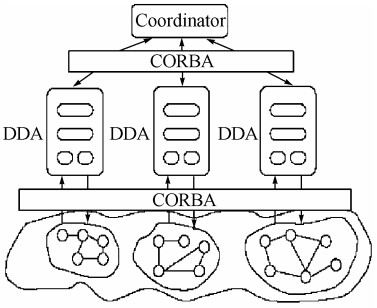

图 3 分布式告警相关性模型

Fig.3 Distributed alarm correlation

被管网络被分成几个不同的管理域(domains)，管理域是一个抽象的概念，可以是子网、网元或是网元的功能单元等。每个管理域包含一个智能代理，负责域内的告警相关性分析。智能代理也可以称为域内故障诊断代理(Domain Diagnostic Agent, DDA)，负责监控和分析域内的网络状态。智能代理包括以下 3 个功能模块：

(1)数据采集模块　负责采集管理域内的告警信息和网络配置信息，并把信息转化成统一的标准格式，存储在数据库中。

(2)告警相关性分析模块　根据数据库中的告警和配置信息，建立网络模型。根据被管管理的特点，选择合适的告警相关性分析方法，压缩告警。

(3)数据上报模块　向上层协调者上报相关性告警组。

此外，必须有一个协调者(coordinator)共享不同管理域间的信息，协调解决域间的根故障定位。协调者主要包括以下 3 个功能模块：

(1)数据采集模块　负责采集不同管理域上报的相关性告警组。

(2)根故障定位模块　根据域间的故障传播模型，遵守最小费用原则定位根故障[11]。

(3)故障上报模块　向用户上报故障，并提供用户图形界面。

4 实现原型与性能评价

4.1 实现框架

实验环境采用朗讯 ADM16 SDH 设备和 OLS80G DWDM 设备，网络结构模型如图 4 所示。DWDM 系统由 *a* ~ *f* 6 个 OADM 站组成网状结构，将 *a* ~ *b* ~ *c* ~ *f* 划分为子网 I，*b*~ *c*~ *d* ~ *e* 划分为子网 II。SDH 系统由 *A*~*B*~*C* 3 个 ADM 站组成环 *R*1，*D*~*E*~*F*~*G* 4 个 ADM 站组成环 *R*2。 其中 SDH 与 DWDM 系统的承载关系是：SDH 环 *R*1 的业务承载在 DWDM 子网 I 上，SDH 环 *R*2 的业务承载在 DWDM 子网 II 上。

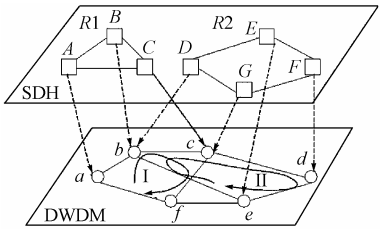

图 4　SDH over DWDM 网络结构

Fig 4 Network structures of SDH over DWDM

分布式告警相关性系统的实现框架如图 5 所示，主要包括以下几个部分：

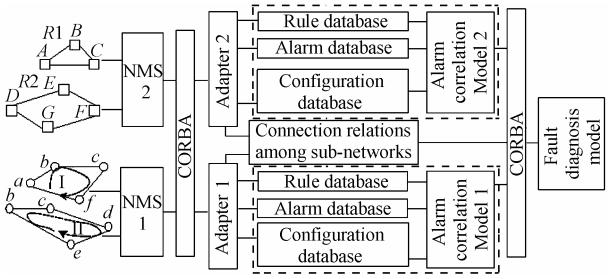

图 5　分布式告警相关性模型的实现框架

Fig.5 Framework of distributed alarm correlation

(1)适配器(adapter)　提供 CORBA 接口，采集被管网络的告警信息和配置信息，并将数据格式转化为适于数据库存储的统一格式。告警消息包括多个字段，如告警发生时间、告警清除时间、告警发生的位置信息、告警级别、告警内容描述等等。配置信息包含网元层和网络连接层的具体信息。网元层描述的是被管网络中物理或逻辑上的网元，包括子网、局站、机框、机槽、机盘、端口等等。网络连接层则描述的是网元之间的连接关系。

(2)数据库　包括告警数据库(alarm database)、配置数据库(configuration database)、规则数据库(rule database)，负责

存储和检索子网信息。网间连接关系数据库(connection relations among sub-networks)负责存储和检索子网间功能节点依赖关系。

(3)相关性分析模块(alarm correlation model) SDH 与 DWDM 系统内部采用基于规则的告警相关性分析方法，将分析结果(相关告警组和可能故障)上报给故障定位模块。通信专家在线维护和配置告警相关性规则。

相关性分析的具体算法：从告警数据库中读取告警信息；按照网元进行分类，将告警定位到网元上；将告警信息去匹配规则库中的所有规则，查找出可能的故障。线路故障仅判断单个网元是无法准确判断故障点的，必须在对远端的网元发生的告警进行分析，最终确定故障点。

(4) 故障定位模块(fault diagnosis model) SDH 与 DWDM 系统间的故障传播模型如图 6 所示。其中，节点{*a-b, b-c, c-f, f-a*}表示 DWDM 子网 I 的最小光缆段；节点{*b-c, c-d, d-e, e-b*}表示DWDM子网I的最小光缆段；节点{*C-A,A-B,B-C*}表示 SDH 环 *R*1 的复用段连接；节点{*G-D,D-E,E-F,F-G*}表示 SDH 环 *R*2 的复用段连接。

故障定位算法：假定发生小故障量的可能性比发生大故障量的可能性要大[11]。具体算法：获取子网上报的相关告警组和可能故障；根据网间连接关系，建立网间故障传播图，选取故障的最小交叉点；该最小故障点必须能够解释所有的告警，具有最小成本。

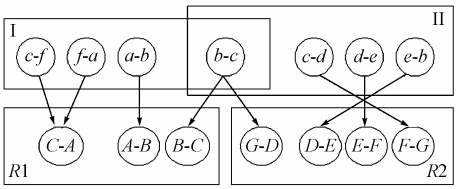

图 6　SDH over DWDM 故障传播模型

Fig.6 Fault propagation model of SDH over DWDM

4.2　案例分析

(1)案例：DWDM 子网 I 的光缆段 *b-c* 中断，引起告警风暴。据统计 SDH 系统上报 1327 个告警，DWDM 系统上报 22 个告警。

(2)要求：压缩大量不相关的告警，准确判断故障点，并上报用户。

(3)分析过程：SDH 告警相关性规则如下文所示。经过告警压缩后，相关告警数为 22 个，诊断出可能故障："SDH 环 *R*1 复用段{*B-C*}中断"和"环 R2 复用段{*G-D*}中断"。

规则 1　提取标识 SDH 系统线路故障的主要告警"信号丢失(LOS)"和"远端缺陷指示(RDI)"。

if alarm_type=' LOS' or alarm_type=' RDI' then pass (source)

规则 2　采用固定时间窗口机制，将告警分组。

if (alarm_type='LOS') is_before (alarm_type='RDI') and within 1min then group(source)

规则 3　属于同一个 SDH 复用段，且告警满足一定的时间先后关系，那么诊断故障为"SDH 复用段中断"。

if (*A*1 and *A*2) and *B* then Fault('光缆中断', alarm- startpoint, alarm- endpoint)

其中，*A*1: alarm-endpoint='LOS'；*A*2: alarm-startpoint ='RDI'；*B*: DWDMtopolink(alarm- startpoint, alarm-endpoint) =true

DWDM 告警相关性规则如下文所示。经过告警压缩后，相关告警数为 2 个，诊断出可能故障："DWDM 光缆段{*b-c*}中断"。

规则 1　提取标识 DWDM 系统线路故障的主要告警"光信号丢失(OLINEcLOS)"和"远端缺陷指示(OLINEcRFI)"。

if alarm_type=' OLINEcLOS' or alarm_type=' OLINEcRFI' then pass (source)

规则 2　采用固定时间窗口机制，将告警分组。

if (alarm_type=' OLINEcLOS') is_before (alarm_type=' OLINEcRFI') and within 1min then group(source)

规则 3　属于同一个 DWDM 光传送段，且告警满足一定的时间先后关系，那么诊断故障为"DWDM 光缆中断"。

if (*A*1 and *A*2) and *B* then Fault('光缆中断', alarm-startpoint, alarm-endpoint)

其中，*A*1: alarm-endpoint='OLINEcLOS' ；*A*2: alarm-startpoint ='OLINEcRFI'；*B*: DWDMtopolink(alarm- startpoint, alarm- endpoint)=true

根据 SDH 与 DWDM 系统间的故障传播模型(如图 6 所示)，经过分析，诊断出根故障是："DWDM 光缆段{*b-c*}中断"。其中，"SDH 环 *R*1 复用段{*B-C*}中断"和"环 *R*2 复用段{*G-D*}中断"受 DWDM 系统光缆中断的影响，并不是真正的故障点。

最后，在用户图形界面上报故障"DWDM 光缆段{*b-c*}中断"，如图 7 所示。具体的故障内容包括：故障系统代号，故障区间，故障源，故障描述，故障发生时间等。

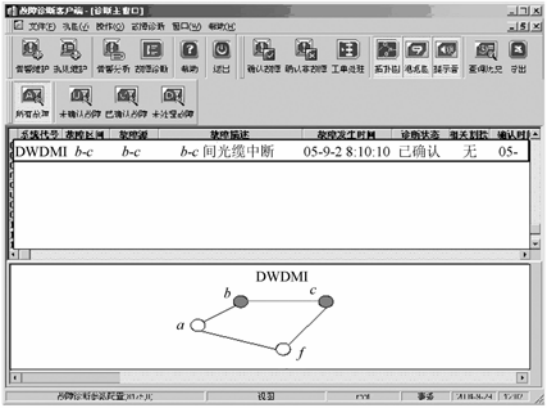

图 7　故障诊断结果

Fig.7 Fault diagnosis results

4.3　性能评价

表 2 给出了集中式和分布式告警相关性模型的性能比较结果。表 2 中使用时间进度条表示在各个模块所需要的时间(单位：s)。时间值是根据大量测量数据平均统计计算出，具有一定的代表性。分析得出：分布式模型提高了系统的故障诊断水平。即使在发生告警风暴的情况下，也可以确保在实际网络故障发生的 1min 内准确定位根故障。随着网络规模

的扩大，分布式告警相关性模型更具有其优越性。

表 2 集中式与分布式告警相关性模型的性能比较

Tab.2 Performance comparisons between centralized and distributed alarm correlation

	集中式告警相关性模型	分布式告警相关性模型
告警采集	30s	10s
告警相关性分析	40s	25s
根故障定位	10s	15s
故障上报GUI	10s	10s
总计	90s	60s

同时，定义两个参数：告警相关率CR_i和故障定位准确率HR，用于衡量告警相关性模型的执行效率E。其中，告警相关率CR_i表示在SDH和DWDM系统的告警压缩程度；故障诊断率HR表示根据网间故障传播模型，定位根故障的准确程度。所以执行效率E等于所有子网的告警相关率CR_i与根故障诊断率的乘积。

$$E=\prod_{i=1}^{n}\mathrm{CR}_i\times\mathrm{HR}$$

$$\mathrm{CR}_i=\frac{\text{相关告警的数量}}{\text{实际告警总数}}$$

$$\mathrm{HR}=\frac{\text{诊断出的根故障数}}{\text{实际故障总数}}$$

根据实验室多次测量结果统计平均，取SDH告警相关率$CR_1\geqslant 97.2\%$，DWDM告警相关率$CR_2\geqslant 90\%$，根故障诊断率$HR\geqslant 94\%$，计算得执行效率$E\geqslant 82.2\%$。

5 结束语

告警相关性分析作为计算机科学和信息技术的分支，在近十年中得到广泛的研究和应用。告警相关性分析是一组实时的告警分析程序，对告警进行合并和转化，将多个告警合并成一条具有更多信息量的告警。告警相关性分析已经成为现代通信网广泛采用的网络管理技术。告警相关性分析主要支持以下网络管理的任务：

(1)通过与告警内容密切相关的告警抑制(过滤)分析，减少呈现给网络运维人员的告警信息量。

(2)通过告警的聚合和一般化，提高呈现给网络运维人员的告警的语意性。

(3)网络故障的实时隔离，故障原因诊断和有效故障处理的建议。

(4)预测网络行为和网络趋势分析。

(5)根据历史告警日志文件，进行长期的告警相关性分析和网络行为趋势分析。

事实上，告警相关性已经分析超越了故障管理的领域，在安全管理和性能管理中得到应用，如网络入侵检测。告警相关性分析主要应用领域包括：网络监控、故障诊断、安全保护、性能监控。本文只讨论了告警相关性在故障诊断中的应用。

告警相关性分析的最新技术发展方向包括：多代理技术、基于拓扑结构的知识密集型分析、多层次网络(协议)间的相关性分析、高速告警相关性引擎、模糊相关性分析、自动告警规则发现等等。本文重点讨论了分布式多代理技术和多层次网络间的相关性分析，并结合 SDH over DWDM 光传送网的具体案例，分析了告警相关性模型的设计和实现，并提供用户图形界面显示，具有很强的操作性，并在实际网络管理系统中得到应用。

参 考 文 献

[1] Sterritt R, Bustard D, McCrea A. Autonomic computing correlation for fault management system evolution. Proceedings of IEEE International Conference on Industrial Informatics, India, 21-24 Aug. 2003: 233−247.

[2] Burns L, Hellerstein J L, Ma S, Perng C S, *et al*.. Towards discovery of event correlation rules**.** Proceedings of IEEE/IFIP International Symposium on Integrated Network Management, Seattle, WA, USA, 14-18 May 2001: 345−359

[3] Chao C S, Yang D L, Liu A C. An automated fault diagnosis system using hierarchical reasoning and alarm correlation. Proceedings of IEEE Workshop on Internet Applications, San Jose, CA, USA, 26-27 July 1999: 120−127.

[4] Ekaette E U, Far B H. A framework for distributed fault management using intelligent software agents**.** Proceedings of IEEE CCECE 2003. Canadian Conference on Electrical and Computer Engineering, Canada, 4-7 May 2003, vol.2: 797−800.

[5] Lo Chi-Chun, Chen Shing-Hong, Lin Bon-Yeh. Coding-based schemes for fault identification in communication networks**.** Proceedings of Military Communications Conference, MILCOM 1999 IEEE, Atlantic, NJ, USA, 31 Oct.-3 Nov. 1999, vol.2: 915−919.

[6] Albaghdadi1 M, Bruce Briley, Martha Evens, *et al*.. A framework for event correlation in communication systems. Proceedings of MMNS2001, Florence, Italy, LNCS2216, 2001: 271−284,

[7] Ekaette E U, Far B H. A framework for distributed fault management using intelligent software agents**.** Proceedings of IEEE CCECE 2003. Canadian Conference on Electrical and Computer Engineering, Canada, 4-7 May 2003, vol.2: 797−800.

[8] Steinder M, Sethi A S. End-to-end service failure diagnosis using belief networks. Network Operations and Management Symposium (NOMS), Florence, Italy, 2002: 375−390.

[9] Choi Jaesung, Choi Myungwhan, Lee Sang-Hyuk. An alarm correlation and fault identification scheme based on OSI managed object classes**.** Proceedings of ICC '99. IEEE International Conference on Communications, Vancouver, BC, 6-10 June 1999, vol.3: 1547−1551.

[10] Li H, Yang S, Baras J S. On system designs for distributed, extensible framework for network monitoring and control. Tech. Rep. CSHCN TR 2001-12, Center for Satellite and Hybrid Communication Networks, University of Maryland, 2001.

[11] Bouloutas A T, Calo S, Finkel A. Alarm correlation and fault identification in communication networks. IEEE Transactions on Communications, Feb-Apr 1994, vol.42(2/3/4): 523−533.

邓　歆：　女，1977 年生，博士生. 研究方向为通信软件与网络管理.
孟洛明：　男，1955 年生，教授. 研究方向为通信软件与网络管理.