网络管理中事件关联检测机制的研究

王平[1,3]，李莉[2,3]，赵宏[1,3]

（1. 东北大学 软件中心，辽宁 沈阳 110004；
2. 中国科学院 沈阳计算所，辽宁 沈阳 110004；3. 东北大学 信息学院，辽宁 沈阳 110004）

摘 要：网络事件的关联检测是网络管理需要解决的一个关键问题，本文根据分布式网络管理的特点，首次明确定义了网络事件的基本关联关系，在此基础上提出了一种基于 Petri Net 的事件关联检测机制，实现了基于事件内容的细粒度关联检测，并且在事件检测中充分考虑了时间因素，有效地提高了事件关联检测的准确性。

关键词：网络管理；网络事件；事件关联；Petri 网

中图分类号：TP393.07 **文献标识码**：B **文章编号**：1000-436X(2004)03-0073-09

Study on events correlation detecting mechanism in network management

WANG Ping[1,3], LI Li[2,3], ZHAO Hong[1,3]

(1. Software Center of Northeastern University, Shenyang 110004, China;
2. Shenyang Computing Technology Institute, Chinese Academy of Science, Shenyang 110004, China;
3. College of Information Science & Engineering, Northeastern University, Shenyang 110004, China)

Abstract: Network events correlation detecting is a key issue of network management to solve. The basic correlation of network events is first defined definitely in this paper according to the characteristics of network management. And then, A Petri net-based detecting mechanism of event correlation is proposed and fine-granularity correlation detection based on attributes of event is implemented. Moreover, time is considered in the detecting model and accuracy of event detecting is improved significantly.

Key words: network management; network event; event correlation; Petri net

1 引言

大规模分布式网络包含大量的网络实体，它们在运行过程中会产生各种各样的网络事件，这些事件潜在地展示了网络实体的运行状态和行为，例如链路断路、网络拥塞、设备失效等，有效地监视这些网络事件是实现网络管理的重要保障[1]。然而，在网络环境下，网络事件往往是相互关联的，一个简单的问题可以影响许多设备和子系统，引起大量的相关事件。由于

收稿日期：2002-12-05；**修订日期**：2003-09-18
基金项目：国家“863”计划基金资助项目（863-317-01-03-09）

网络系统需要处理大量的网络事件，导致问题诊断的时延增大，可能会造成被忽略或者误判，在某些情况下，大量的网络事件甚至会“淹没”网络管理系统，使系统瘫痪，进而给网络用户和相关的企业带来重大的损失。因此，如何有效地处理网络事件关联检测是网络管理需要解决的一个关键问题。

网络事件关联检测是一项非常复杂的任务。在网络管理领域，人们在网络事件检测方面进行了一系列的研究，取得了一定的研究成果，例如，NETFACT 系统[2]用面向对象的模型描述网元之间连接性、依赖性和包含关系；IMPACT 系统[3]采用基于模型的方法，建立网元类作为结构模型，信息类、关联类和关联规则作为行为模型来解决事件检测问题；EXCPERT[4]和 INCHARGE[5]系统建立了一种因果关系，使用 CODEBOOK 方法关联事件；文献[6]采用了基于神经网络的事件关联检测方法，以找到问题的根源。然而，这些方法都只是考虑了事件关联检测的某些问题，不够全面，主要表现在没有给出网络事件及事件基本关联关系定义，并且在网络事件检测中忽略或者简化了时间关系。

针对现有网络事件关联检测方案的不足和分布式网络管理的特点，本文在文献[7,8]的基础上，提出了一种基于 Petri net 的事件关联检测机制，该机制充分考虑了网络事件检测中的时间因素，并且可以通过 Petri net 的谓词（guard）限定事件的某些属性值，实现基于事件内容的细粒度关联检测，有效地提高了事件检测的准确性。

2 网络事件

网络事件是在某个时刻由于网络对象状态的改变而发出的消息。网络对象可以看作是一个 n 维向量，每个向量是该对象的一个属性，是时间的函数，如果网络对象的某个属性低于系统设定的阈值就触发一个事件，事件可以是网络对象直接产生，也可以由网络监视器产生。从工程的角度，事件代表系统发生的状态改变，例如网管中的链路 Up 和 Down。

为了克服网络事件的多样性造成的事件检测的困难，本文根据网络事件的特点定义了统一的描述方法，描述如下：

定义 1 网络事件：由于网络对象的状态改变而触发的消息，包含六个属性：

Event := <Event-Name>；<Event-ID>；<Source>；<TimeStamp>；
<Event-Pri>；<Variable_list>

- Event-Name∈String：事件名称；
- Event-ID∈N+，是系统中该事件区别于其它事件的唯一标识；
- Source：表示事件产生的位置；
- TimeStamp：事件产生时间；
- Event-Pri：事件的优先级。为事件定义优先级保证了紧急事件得到优先处理，使系统能够及时处理影响网络运行的重大问题，为网络的可靠运行提供了保障。
- Variable_list：是某个网络对象的某个属性或者某些属性的集合，是引起该事件的原因，其形式如下：

Variable_list:= <Var_att><Relation_Op><Value>

Relation-Op := < | > | = | != | >= | =<

Value := <Number>|<String>

Var_att：是网络对象一组属性的组合，由网络管理人员定义，表示网络对象的某方面运行状态，例如，为了检测某个端口的输入包的出错率，可定义如下：

Var_att = ifInErrors /(ifInUcastPackets + ifInNucastPkts)

在通常情况下，网络事件是重复发生的，一个事件可以发生多次，每次发生叫做事件实例。为了便于描述，本文做如下定义：

定义 2　事件实例：某种类型的网络事件发生的次数，描述如下：

$$instance(evnet,t)\begin{cases}0 & \text{事件 event 到时刻 } t \text{ 为止还没有发生}\\ i & \text{事件 event 到时刻 } t \text{ 为止共发生 } i \text{ 次}\end{cases}$$

3　网络事件的关联规则

在网络管理中，管理站接收到的事件为原始事件，这些事件是由被管的网络对象产生的，例如代理或者设备上的其他软件模块或者管理系统在轮循/监控过程中产生。在通常情况下，由于网络中几个失效可能引起许多原始事件，因此很多网络事件是相互关联的，例如，网络拥塞会导致丢包率上升，网络延时增大，关联过程可以去掉冗余信息，定位事件根源。因此，为了有效地管理网络，需要定义网络事件的关联关系，以使系统能够从大量的网络事件中迅速找到问题的根源。根据多年来从事网络管理的理论研究和工程实践的经验，本文定义了网络事件基本的关联关系，以复合事件的形式表示，而将前文定义的网络事件称为简单事件（Primitive-Event）。

定义 3　复合事件：多个网络事件按照某种关联规则组合成的事件，表示为：

Composite-Event := < Primitive-Event><Correlation-op>< Primitive-Event>|
< Primitive-Event>< Correlation-op>< Composite-Event>

Correlation-op　:=　∧ | ∨ |!| →|, n

本文定义了五种基本的网络事件关联关系，它们的含义如下：

- CE = event1∧event2

操作符“∧”表示“与”，是二元操作符，含义是两种事件 event1 和 event2 都发生，表示为：

occr (CE，t) = = TRUE
if ((instance(event1,t)>0) And (instance(event2,t)>0))

- CE = event1∨event2

操作符“∨”表示“或”，是二元操作符，含义是两种事件 event1 和 event2 至少有一个发生，表示为：

occr (CE，t) = = TRUE
if ((instance(event1,t)>0) Or (instance(event2,t)>0))

- CE = event1! event2

操作符“!”表示“非”，是二元操作符，含义是 event1 事件发生而 event2 事件不发生，表示为：

occr (CE，t) = = TRUE
if ((instance(event1,t)>0) And (instance(event2,t)= =0))

- CE = event1→ event2

操作符“→”表示“顺序”，是二元操作符，含义是 event1 事件发生在 event2 事件之前，表示为：

occr (CE，t) = = TRUE

if ((instance(event1,t)>0) And (instance(event2,t)>0)) And

(instance(event1,t).TimeStamp < instance(event2,t).TimeStamp) And

(| instance(event1,t).TimeStamp – instance(event2,t).TimeStampl)>=2_{gg} 注))[9]

- CE = event, n

操作符 ",*n*" 表示 "发生 *n* 次"，是一元操作符，含义是 event 事件实例发生 *n* 次，表示为：

occr (CE，t) = = TRUE

if (instance(event,t)>=n)

网络事件是时间相关的，事件关联规则通常要与一个关联时间窗相联系才有意义。例如，事件关联规则如下定义：

当管理系统接收到链路断开的网络事件（Down）时，如果在 2 分钟内没有收到该链路的 Up 事件，则告警管理员。该事件的管理规则可以描述如下：

occr(CE) == TRUE

if((instance(Down,t)>0) And (instance(Up,t)==0) And

(t - instance(Down,t).TimeStamp)>=2))

OR ((instance(Down,t)>0) And (instance(Up,t)>0) And

(linstance(Up,t).TimeStamp – instance(Down,t).TimeStampl)>2)))

可见，网络事件的关联检测要充分考虑时间因素，以保证事件检测的正确性。

4 基于 Petri net 的网络事件关联检测方法

网络事件的关联检测过程实际是将网络子事件与关联规则相匹配的过程，因此可以用状态跃迁技术来实现。常用的状态跃迁描述方法有两种：有限状态机 FSM 和 Petri net。在文献[10,11]中，提出了基于 FSM 的事件关联检测方法，但是 FSM 用全局状态刻画变化，对于网络事件检测而言，一个子事件的产生只涉及局部状态元素，而不是全局，因此用全局状态描述变化是不必要的；另外当 FSM 的状态元素的个数太大时，FSM 全局状态不是实时可知的，从而无法确定哪些状态可以发生，因此不适合大规模网络事件检测。采用 Petri net 方法，每个发生的子事件用一个 token 表示，因此无论该子事件发生多少次，也只与一个位置有关，适合处理复杂的事件关联检测。文献[11,12]中采用了基于 Petri net 的网络事件检测方法，但是描述过于简单，并且没有考虑时间因素。本文在对相关文献进行系统分析的基础上，提出了一种基于 Petri net 的事件关联检测机制，该机制充分考虑了网络事件检测中的时间因素，实现了网络事件属性相关的细粒度并行检测，有效地提高了网络事件检测的准确性和效率。

4.1 Petri Net 的扩充

为了使 Petri net 满足网络事件关联检测的要求，本文对 Petri net 模型进行了扩充，主要表现在以下几个方面：

- 库所（place）

在本文应用的 Petri net 模型中，位置分为两种类型：主库所和辅助库所。每个主库所与一种类型的网络事件相对应，而辅助库只描述状态，没有实际意义。

注：本文提出的系统模型采用文献[9]中的全局时钟同步方案。

· 令牌（token）

相应地系统定义了两种令牌：主令牌和辅助令牌。相对于普通的 Petri Net 模型，主令牌包含更多的信息，令牌所处的位置决定了令牌的内容。辅助令牌与辅助位置相对应，不包含任何信息，在事件检测中起到一种类似并发概念中的信号量的作用。

· 流（flow）

输入弧 arc∈S*T 可以包含变量和常量，变量作为令牌的声明，包含令牌的信息；常量定义了该输入弧上一次移动的令牌数量，即事件实例。输出弧 arc∈T*S 上的函数表示对输入弧上的变量执行的操作。

· 变迁（transition）

变迁 T 上的谓词（guard）限定令牌的内容。guard 是一个逻辑表达式，其参数是该变迁 T 输入令牌（token）所代表的事件的属性，以对事件的内容进行限制，从而实现细粒度的网络事件的关联检测，提高事件关联的准确性；如果变迁 T 不包含令牌，则表示对令牌没有限制。

4.2 基于 Petri net 网络事件关联检测机制

对于前面定义的网络事件关联关系，本文定义了相应的 Petri net 模型。如图 1 为关联规则 event1∧event2 的模型，三个主库所分别代表了网络事件 event1、event2 和复合事件 event1∧event2，不包含辅助库所；从库所 event1 和 event2 到变迁 T 的输入弧不包含常量，表示每次移动的令牌数为 1，变量 Var1、Var2 分别代表两种令牌；从变迁 T 到库所 CE 的输出弧上的操作“∧”表示对两个令牌代表的事件执行的操作；变迁 T 上的谓词 guard 表示对令牌内容的限制。例如，系统定义如下检测规则：

Rule1 := {(CE= Discard∧Delay) And (Discard.source = Delay.source)}

即要求检测丢包率和延时都超过系统设定的阈值的网络对象，按照图 1 关于 CE=event1∧event2 的描述，规则 Rule1 的 Petri Net 模型如图 2 所示。

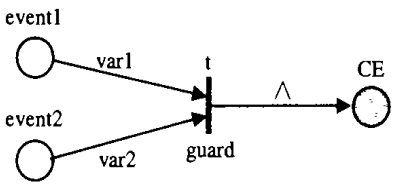


图 1　CE= event1∧event2 的 Petri net 模型

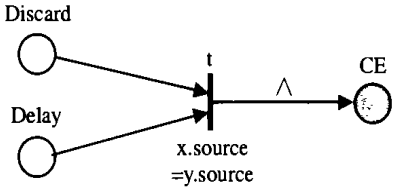


图 2　Rule1 的 Petri net 模型

图 3 为关联规则 event1∨event2 的 Petri net 模型，与 event1∧event2 的模型类似，差别在于复合事件 CE 的产生条件不同，所以该模型有两个变迁 t1 和 t2。例如，系统定义如下检测规则：

Rule2:={ CE = DeviceDown∨LinkDown }

即检测网络中的链路失效或者网络设备失效，Rule2 的 Petri net 模型如图 4 所示，模型中的变迁没有谓词，表示对令牌的内容没有限制。

图 5 为关联规则 event1→event2 的 Petri net 模型。为了表示事件 event1、event2 的时间关系，将这两个事件的产生时间作为两个事件 T_{event1} 和 T_{event2}，同时设置了一个辅助库所 H1 作为 T_{event1} 和 T_{event2} 的互斥资源（信号量），因此事件 event1→event2 转化为(T_{event1}!T_{event2})∧(event1∧event2)。该模型中的所有输入弧都不包含常量，表示每次移动的令牌数为 1；变迁

t3、t4、t5 没有谓词 guard，变迁 t1、t2 的谓词 guard1、guard2 根据实际的需要定义。

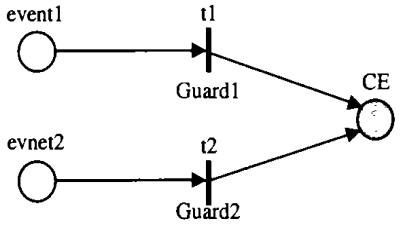


图 3 CE=event1∨event2 的 Petri net 模型

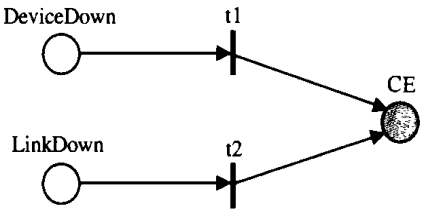


图 4 Rule2 的 Petri net 模型

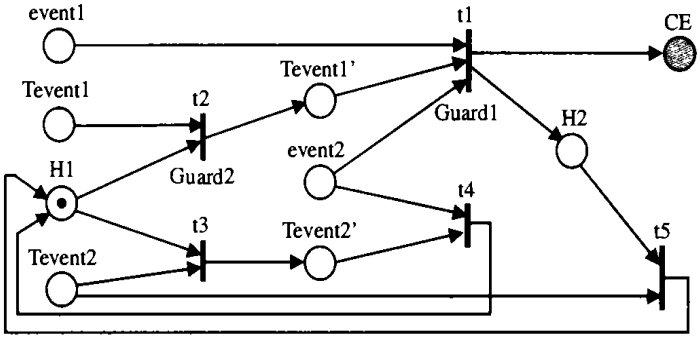


图 5 CE = event1→event2 的 Petri net 模型

关联规则 event1!event2 的 Petri net 模型如图 6 所示。该关联规则一般与一个时间段相关，其通常形式是 event1!event2 in(T_{begin}, T_{end})，其中 $T_{begin} < T_{end}$。事件 CE=event1!event2 的产生条件是在时间 T_{begin} 到 T_{end} 内，只发生事件 event1，而事件 event2 不发生。类似于关联规则 event1→event2，该模型设置两个时间事件 T_{begin} 和 T_{end}，事件 event1!event2 in(T_{begin}, T_{end})可以转化为(T_{begin}∧T_{end}∧event1)!event2。该模型设置了一个辅助库所 H，H 是事件 T_{begin}、event1 和 event2 的互斥资源，其作用是使在时间 T_{begin} 之前发生的事件 event1 和 event2 无效，保证所有的事件发生在时间 T_{begin} 之后。变迁 t1、t2、t3、t4、t5、t6、t8 没有谓词 guard，变迁 t7 的谓词 guard 根据实际的需要定义。

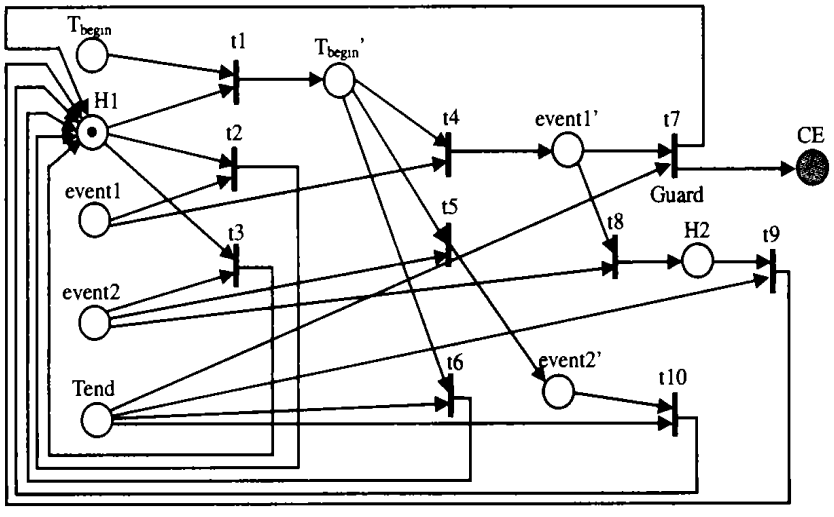


图 6 CE=event1!event2 的 Petri net 模型

关联规则 event,n 的 Petri net 模型如图 7 所示。该管理规则与 event1!event2 类似，通常也与一个时间段相关，其形式为 event,n in(T_{begin}, T_{end})，其中 $T_{begin} < T_{end}$。该模型同样设置两个时间事件 T_{begin} 和 T_{end}，事件 event, n in(T_{begin}, T_{end})转化为(T_{begin}! T_{end})∧(event∧event∧…∧event)。该模型设置了一个辅助库所，作为事件 event 和 T_{begin} 的互斥资源，使得在时间 T_{begin} 之前发生的事件 event 无效。输入弧 arc∈（event * t3）上包含一个常量 n，表示该输入弧每次移动的令牌数为 n 个；变迁 t1、t2、t4 没有谓词，变迁 t3 的谓词 guard 根据实际的需要定义。

通过基本事件关联关系的 Petri net 模型的组合，可以很容易地构造复杂的网络事件关联关系模型。例如事件关联关系(event1∧event2)∨event3 可以分解为两个基本的事件关联关系 CE1=event1∧event2 和 CE2=CE1∨event3，因此通过这两个基本事件关联关系 Petri net 模型的组合可以构造出(event1∧event2)∨event3 的 Petri net 模型，如图 8 所示。

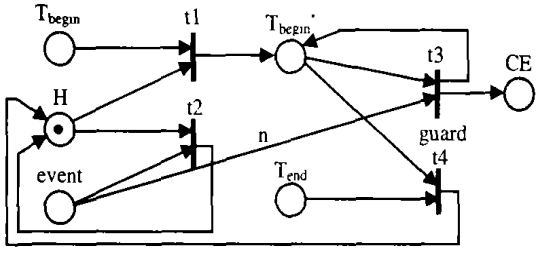


图 7　CE= (event, n)的 Petri net 模型

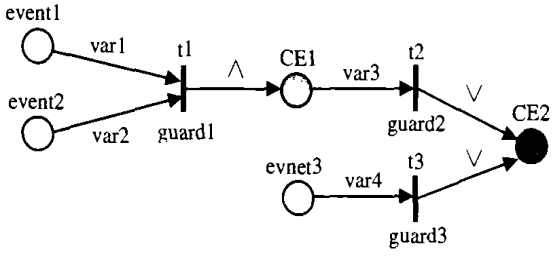


图 8　CE= (event1∧event2)∨event3 的 Petri net 模型

5　系统模型

网络事件检测是实现网络管理任务的基础，本文根据大规模网络管理的特点，提出了一种基于事件检测机制的分布式网络管理系统模型，该模型的结构如图 9 所示，主要包括以下部分：

事件/规则编辑器：是提供给网络管理员的用户接口，管理员通过事件编辑器定义新的网络事件和事件的关联规则，或者修改系统中原有的事件和规则；

事件/规则分析器：其作用是对网络管理员定义的网络事件和关联规则进行语法分析，如果正确，则交给事件/规则编译器进一步处理；

事件/规则编译器：将网络管理员定义的网络事件和管理规则转化成系统命令（如 Petri net 模型），并存储在事件/规则库中；

网络监视器/事件产生器：网络监视器监视网络中各种网络对象的运行情况，当发现网络对象的状态异常或者发生故障时，则以事件的形式报告给网络管理系统；

事件检测器：接收事件产生器发送的事件，并按照系统定义的事件描述进行检测，将符合条件的事件传递给事件关联分析器。事件检测器处理的是简单网络事件，具有过滤功能，可以消除冗余的信息；

事件关联分析器：根据系统定义

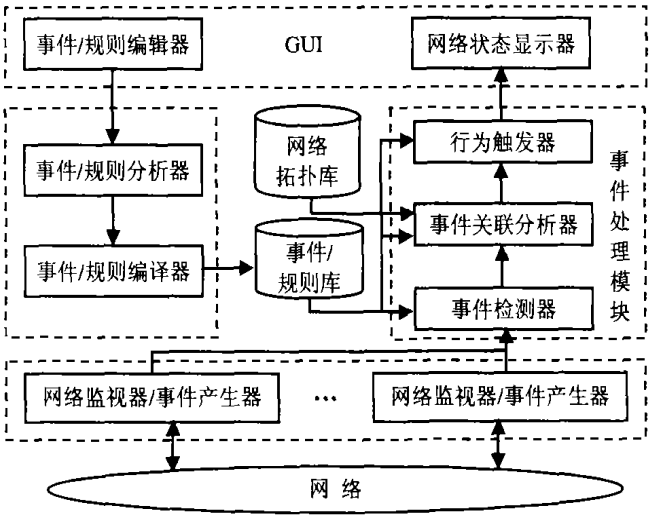


图 9　系统模型

的事件关联规则和网络结构信息，对网络事件进行关联检测，以发现问题的根源；

行为触发器：当网络事件的检测结果满足系统定义的某条规则时，则该规则定义的系统行为被触发，系统行为有很多种，例如，将网络中存在的问题报告给网络管理员；通过网络状态显示器展示网络的运行状况；或者更进一步地触发新的网络规则，实现网络管理的动态配置，以提高系统的灵活性。

6 结论

网络事件的关联检测是网络管理需要解决的一个关键问题，本文针对这个问题进行了深入的研究，主要表现在：

(1) 根据网络管理的特点，给出了网络事件的定义，并首次明确提出了网络事件的基本关联关系，为网络管理的相关研究提供了理论参考；

(2) 提出了一种基于 Petri net 的网络事件并行检测机制，实现了基于事件内容的细粒度关联检测，并在事件检测中考虑了时间因素，保证了事件检测的准确性；

(3) 提出了一个基于事件检测机制的网络管理系统模型。

通过本文提出的基于 Petri net 的事件关联检测机制，网络管理系统可以提供更加精确的告警信息视图，使管理人员能够准确快速定位问题的根源。本文提出的事件关联检测方法已经在实际的系统得到应用，取得了良好的效果。

参考文献：

[1] ERFANI S, LAWRENCE V B, MALEK M, *et al*. Network management: emerging trends and challenges[J]. Bell Labs Technical Journal, 1999, 4 (4):3-22.

[2] HOUCK K,CALO S, FINKEL A. Towards a practical alarm correlation system[A]. 4th IEEE on Integrated Network Management[C]. 1995.

[3] JAKOBSON G. Real-time telecommunication network management: extending event correlation with temporal constraints[A]. 4th IEEE on Integrated Network Management[C].1995.

[4] NYGATE Y A. Event correlation using rule and object based techniques[A]. 4th IEEE on Integrated Network Management[C]. 1995.

[5] YEMINI S, KLIGER S. High speed and robust event correlation[A]. IEEE Communications[C]. 1996.

[6] WIETGREFE H, TOCHS K, *et al*. Using neural networks for alarm correlation in cellular phone networks[A]. The International Workshop on Applications of Neural Networks in Telecommunications[C]. 1997.

[7] WANG P, LI X M, ZHAO H. A scalable hierarchical architecture for distributed network management[A]. International Conference on Computer Networks and Mobile Computing[C]. IEEE Computer Society Press, 2001. 21-26.

[8] 王平, 赵宏, 李莉. 一种面向分布式网络管理的自适应可扩展模型[J]. 通信学报, 2002, 23(12):118-128.

[9] SCHWIDERSKI S. Monitoring the Behavior of Distributed System[D]. Selwyn College, Computer Lab, University of Cambridge, 1996.

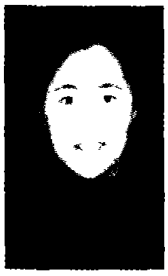
[10] GEHANI N, JAGADISH H V, SHMUELI O. Advanced Database Concepts and Research Issues, Lecture Notes Computer Science[M]. BeHin: Springer Verlag, 1993. 454-469.

[11] AL-SHAER E. Event filtering framework: key criteria and design trade-offs[A]. The 21st IEEE International Conference on Computer Software and Applications[C]. Washington D C, 1997. 88-93.

[12] AL-SHAER E. Active management framework for distributed multimedia systems[J]. Journal of Network and Systems Management (JNSM), 2000, 8(1): 49-72.

作者简介：

王平（1973-），男，辽宁法库人，东北大学博士，主要研究方向为网络管理，分布式多媒体。



李莉（1975-），女，山东齐河人，东北大学博士，主要研究方向为网络管理。

赵宏（1954-），男，河北河间人，东北大学教授、博士生导师，主要研究方向为网络管理、网络安全、分布式多媒体等。

第十四届中国计算机学会网络与数据通信学术会议

征 文 通 知

中国计算机学会网络与数据通信专委会和开放系统专委会定于2004年10月在西安召开第十四届中国计算机学会网络与数据通信学术会议（会议通知另发），现将会议征文的有关事项通知如下：

一、学术会议主题及征文范围

本届会议的主题是：**研究信息网络关键技术，营造安全可靠网络环境**

征文范围包含：开放系统及其互联技术；新一代网络结构与协议；网络智能化、网络管理；网络信息系统模型；网络计算与应用；网络环境下的信息安全；无线通信网络；电子商务系统以及光纤通信技术。

二、提交会议论文的有关要求

1. 欢迎围绕以上主题提交研究论文，字数一般不要超过6000字。录用的论文将在西北大学学报（增刊）（国内核心期刊）上发表，评选的优秀论文将推荐在国家权威期刊上发表。

2. 稿件格式要求请在下面列出的查询网址中查询，不符合格式要求的论文恕不录用。

3. 应征文章请寄两份打印稿，同时须用电子邮件的附件发来（或用软盘寄来）电子稿，电子稿件请用Word文件格式（.doc文件）。

4. 请随同稿件一起，用另纸写明文章题目，所属主题，作者姓名（最多四人），职务/职称，所属单位，详细通信地址，邮编，电话，E-mail地址。

5. 已经发表的论文请勿报送。如因一稿多投带来任何问题，责任由投稿者自负。

6. 论文收寄地址：西安市太白北路229号西北大学现代教育技术中心学术年会筹备组 宋峰 收

邮编：710069　　发送电子稿的邮件地址：cetc@nwu.edu.cn。

7. 提交论文截止日期为2004年6月30日（以寄出邮戳日期为准）。会议组委会将于2004年7月31日前发出论文录用通知和参加会议邀请信。

三、联系方式

通信地址：西安市太白北路229号西北大学现代教育技术中心学术年会筹备组

邮编：710069　　电话：029-88302758　　传真：029-88303857

电子邮件：cetc@nwu.edu.cn　查询网址：http://www.nwu.edu.cn/xsnh/index.htm　联系人：宋峰　刘瑞献

欢迎各会员单位的联系人将此通知转发给有关单位和个人。

第十四届中国计算机学会网络与数据通信学术会议筹备组