基于知识的面向对象事件关联系统的设计

吴剑章[1]
(东南大学计算机系，南京 210096)

【摘要】 本文根据当前网络管理的发展的要求，分析并建立了基于知识的面向对象的事件关联系统，并通过仿真技术给出了系统的性能。

【关键词】关联; 面向对象; 差错
中图分类号：TP393

Knowledge Based Object Oriented Evnet Correlation

Wu Jianzhang
(SouthEast University NanJing 210096)

【Abstract】According to network management development, a Knowledge based object oriented event correlation system is introduced in this paper.

【Key words】correlation ; object oriented; fault

1 概述

当今，为了提供快速、可靠和更加丰富的网络服务，需要网络在规模、复杂程度，带宽资源上进一步扩展，例如，在一个高速通信网络中，通常包含成千上万的来自不同厂商的网络互连设备，使用不同的传输媒体，并且宽带技术被频繁使用。但是随之而来的问题是在网络运行管理中，一旦网络发生故障，与故障相关的逻辑或物理成员将产生大量重复、相关的报警信息，并通过高速网络迅速蔓延，虽然报警信息有助于分析故障原因，但是被事件风暴淹没的管理中心根本无法实施物理监控和故障诊断。因此，必须使用事件关联技术，过滤重复、冗余的报警信息，关联相关事件，帮助管理者尽快完成故障恢复工作。

本文结合传统的事件关联方法，采用面向对象技术，组播技术提出一种基于知识的事件关联方法。

2 事件与事件关联

2.1 事件内容与事件类型

作者简介：吴剑章，助教，主要研究方向：网络管理，群通信等
定稿日期：2000-06-28

事件是局部系统出现异常状态或某条件得以满足时，由故障源、故障周边设备或监测系统发出的报警信息。

事件形式通常表现为短小的文本信息，内容包括：

- 事件报送设备；
- 故障症状；
- 事件发送起始时戳；

事件通常分为：

- 独立事件：通常表示性能，安全异常事件，如流量超过警戒值或设备复位。
- 复合事件：每次状态迁移都会触发事件，即有可能多个事件表示同一故障。

2.2 关联规则

满足下列规则的都属于相关事件：

- 来自相同事件源的异步事件，描述相同故障引发的不同症状或不同过渡状态；
- 来自不同事件源的异步事件，描述相同故障引发的相同或不同症状；
- 来自不同事件源的异步事件，描述不同故障引发的相同或不同症状，但是所有故障都来源于同一原始故障。

通过事件关联，将使独立、不完整的报警信息转变为综合、详细的故障状态描述。

2.3 事件关联系统设计原则

- 事件关联系统的基本要素包括对不同事件源的事件进行过滤、累计、压缩、概括、分类、模式匹配；
- 事件关联系统必须考虑网络时钟不同步、网络传播延迟、报警信息丢失等客观因素；
- 事件关联系统必须具有良好的扩展性，并且能够灵活应付网络配置和拓扑的变化；
- 理想的系统应该具有分布性，否则将导致性能下降甚至产生瓶颈。

根据上面对事件关联原则和系统设计原则的讨论，下面本文将给出基于知识的事件关联系统。

3 基于知识的面向对象事件关联系统

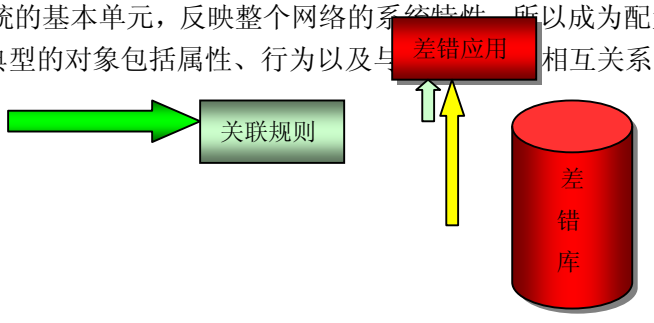
3.1 系统架构

如图 1，当网络发生故障时，事件关联系统通过事件输入接口获取事件报告，首先对事件报告进行解码，并添加辅助信息以产生内部事件卡片，第一个报送的故障事件触发关联引擎搜索被管理对象关系库，定位故障源或使用测试工具确认被定位的故障源，并以此为中心，根据关系库提供的对象关系确定故障波及范围和传播路线，最终生成故障关联规则.故障关联规则在生命期内可以对故障引发的后继事件进行归并、压缩等关联操作，未被关联的事件即被丢弃。关联规则的生命期通常为故障产生至恢复或一个关联周期。

3.2 面向对象的网络对象系统模型

- 网络对象

网络对象作为网络系统的基本单元，反映整个网络的系统特性，所以成为配置、诊断、监测等网络管理任务关注的焦点。典型的对象包括属性、行为以及与[illegible]相互关系。



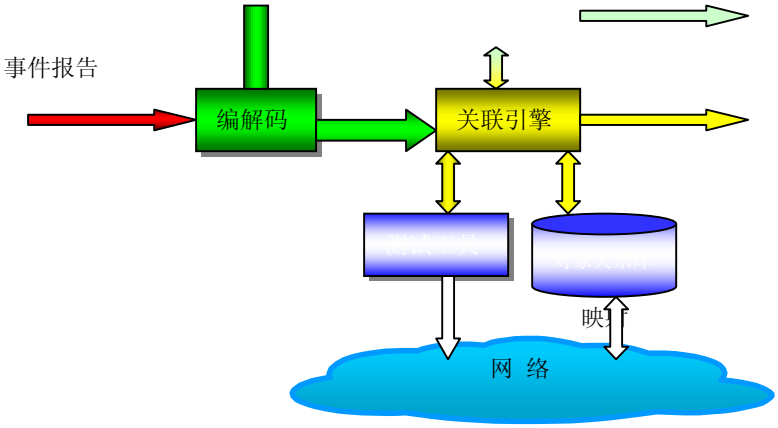


图 1 事件关联系统结构

- 对象的类型

网络对象的类型包括：

原始对象：表示不依赖其他对象而存在的网络实体，例如主机、设备、线路等；

派生对象：表示不能单独存在，必须依赖其他对象而存在的网络实体，例如应用程序、线路带宽等；

- 对象属性

对象属性包括对象的配置信息和状态。对象的配置信息不仅反应对象的特性，还提供本对象与其他对象之间的联系；另外，对象在同一故障下可能发生多次状态迁移，不同状态体现出不同的症状，总之，对象属性可以为事件相关提供重要依据。

- 对象行为

对象行为体现为对象对外部条件的响应，包括自身的处理和对象之间的互操作。

图 2 即为一个典型的面向对象的网络模型。

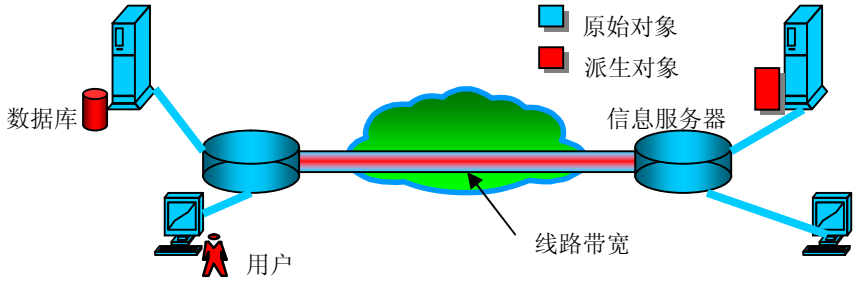


图 2 面向对象的网络对象模型

3.3 基于知识的关联系统

关联系统的知识包括网络对象关系库和故障码集。

差错管理系统首先通过拓扑发现确定所有的网络资源，再使用面向对象技术将所有网络资源映射为网络对象，网络对象的属性和行为由清单管理生成。在面向对象的网络对象系统模型中，对象关联分为三级：

- 一级：通过对象分类技术，完成同宿原始、派生对象关联；
- 二级：通过网络拓扑结构，完成原始对象关联；
- 三级：通过网络服务，完成原始对象之间、派生对象之间及异宿原始对象与派生对象关联。

通过三级关联，关联引擎可以在外部事件触发下，根据关联对象库动态模拟实际网络行为，预测或确定网络故障产生的影响，并以此生成关联规则。网络对象和对象关联关系共同组成网络对象关系库。

3.4 关联算法

- 因果图

因果图表示由起因(网络故障)所导致的结果(所有的报警事件)，事件在因果图中可以表示为症状，其中症状可能是由故障直接引发的，或者是间接的。

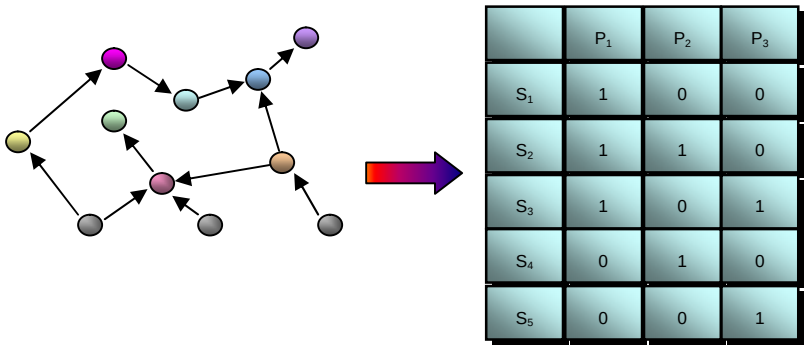


图 3　　因果图和故障编码

图中显示三个灰色故障导致多个直接或间接症状(S 表示症状,P 表示故障),可见通过已知故障可以推导出所有症状，同样如果绘制逆向因果图，也可以由症状判断故障。通常事件关联系统是基于知识的模型，假设在已知所有故障类型和相关症状的前提下，通过因果图可以得到所有故障的数据编码，对于未知的故障类型和症状，将通过下面介绍的 CBR 技术获取。

- 选举算法

选举算法主要完成故障定位，包括确定故障类型和故障源，算法描述如下：

(1) 对在一个关联周期内的事件通过对象关系库的三级关联产生一个事件集；

(2) 对事件集编码产生故障码；

(3) 与事先定义的故障码比较，选择汉明距离最小的故障码,并将此故障定为实际故障(必要时可用测试工具进一步确认)；

(4) 故障码进行纠错后,还原出的事件即为故障相关事件,被排除的事件在相关周期内可加入其他故障选举；

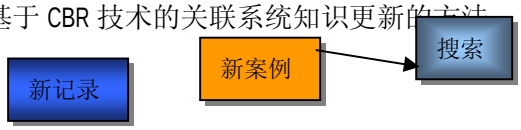
3.5 分布关联

为了减小因网络拓扑结构变化对关系数据库的影响，可以将网络按地理域或路由域划分为不同区域，每个区域建立自己的关系库，这样即可以保证本区域的变动不影响其他区域，而且通过分布关联计算可以提高系统的收敛速度。关联引擎分布在网络中不同的地理位置，事件报送可能是杂乱无章的网状报送，这样可能应该获取报告的未得到事件报告。解决方法是建立不同级别、类型的广播组，即可以避免事件风暴，又可以实现分布关联计算。

3.6 关联系统知识库的维护

在实际网络运行中,网络拓扑可能发生变动，网络服务可能更加丰富和完善，因而网络故障类型也在增加。那么系统预生成的关系对象库中的三级关联和故障码也要随之发生变化，为了保持模型与实际系统的一致，通常采用基于事实的推理方法(CBR)。

CBR 以历史的经验作为解决问题的依据，然而新问题常常带有不同于以往问题的特性，所以新的方法会被引入，并且将为以后的问题解决提供建议。所以，CBR 重要的特点是解决问题的过程也是一个学习的过程。下图给出基于 CBR 技术的关联系统知识更新的方法



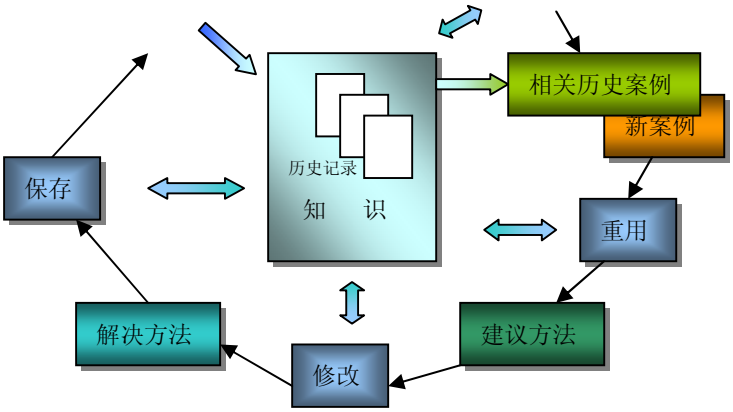


图 4 知识维护循环链

本方法包括四个过程：

- 在历史记录中查询与新事件近似的事件；
- 重用历史事件的解决方法为新问题解决提供建议；
- 诊断新事件与已往问题的差异作相应的修改并形成解决方案；
- 保存本次事件描述和解决方法为将来问题解决提供依据。

4 系统性能评价

在差错管理中通过使用事件关联系统，可以很好的抑制事件风暴，向管理员提供简练、有效的信息，下面是一个典型的故障关联的例子：如图 2 当广域连接线路发生间歇性时钟信号丢失时，将导致线路丢包发生，TCP 连接的性能随之下降，大量的报文丢失使 TCP 认为发生网络拥塞，又因为时钟丢失间歇发生，造成 TCP 窗口保持很小，这将引发多种症状,包括事件风暴。

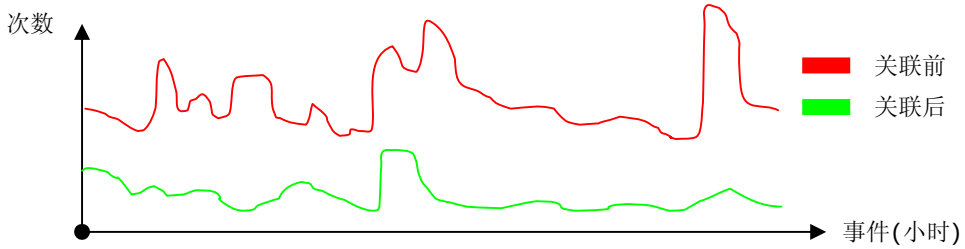


图 5 关联系统性能

由图 5 可见，经过事件关联，类似上述网络故障造成的突发事件风暴得到了很好的控制。

5 结束语

事件关联是现代网络管理中的一项重要技术，我们采用面向对象的事件关联技术，通过仿真运行的结果看出，本系统可以很好的抑制了突发网络故障所引起事件风暴，帮助管理员迅速定位故障，恢复网络正常运行。

参考文献

1.Network Fault Detection: A Simplified Approach to Alarm Correlation.

2.High Speed & Robust Event Correlation.

3.Model_Based Alarm Correlation in Cellular Phone Networks.