# 使用网络拓扑消除冗余告警方法的研究及实现

周 飞，金可音，杨 武，杨 亮

（湖南工业大学 计算机与通信学院，湖南 株洲 412008）

**摘 要**：采用网络拓扑方法过滤网络故障中的告警信息，通过网络拓扑图消除误报、冗余的告警信息，以减少告警信息的数量，将整理后的告警信息作为事例推理技术的输入部分，进行故障定位、诊断、修复工作。实验证明该方法能缩短告警过滤时间，便于网络管理。

**关键词**：网络拓扑；事例推理；告警；故障

**中图分类号**：TP393.07 **文献标志码**：A **文章编号**：1673-9833(2011)02-0051-04

# On Research and Implementation of Redundant Alarm Elimination Based on Network Topology

Zhou Fei，Jin Keyin，Yang Wu，Yang Liang

（School of Computer & Communication，Hunan University of Technology，Zhuzhou Hunan 412008，China）

**Abstract**：Uses network topology method to filter alarm of network failures. Eliminates false alarm and redundant alarm through network topological diagram to for the reduction the number of alarms. Taking the finishing alarm as the input part of the case-based reasoning, locates the fault, diagnoses the fault and repairs the fault. The experimental results show that the approach shortens the time of alarm filtering and easy for network management.

**Keywords**：network topology；case-based reasoning；alarm；fault

## 0 引言

网络给人们的生活带来了便捷，已成为人们生活中不可或缺的一部分，如电子邮件、网上购物、网上银行、网上机票订购、网上缴费等。这些服务的提供者在运行的过程中，可能由于某些性能超标或链接问题引起故障，使得服务暂时无法供给，可能造成巨大的损失。为了将损失降到最低，需要在最短的时间内找出问题的根源，及时解决问题，恢复正常运行。良好、稳定的网络环境是保证获取网络服务的前提。

网络失效时，网络中的设备会发出告警信息[1]。在这些告警信息中有很多信息可能是由同一故障引发的，在检查的时候可以忽略或压缩重复的告警信息，减少告警信息的数量，以方便故障管理[2]。如果网络规模比较大，单靠这些杂乱无章的告警信息去检查网络故障，既费时又费力。本文提出利用网络拓扑方法来过滤误报、冗余的告警信息，将整理后的告警信息作为事例推理技术的输入部分，从而进行故障的定位、诊断、修复工作。这样，可减少因分析无关节点的告警信息所浪费的时间。

## 1 故障与告警概述

### 1.1 故障分类

按照不同的标准，网络故障可分为不同的类型。

**收稿日期**：2011-01-20

**作者简介**：周 飞（1983-），男，湖北天门人，湖南工业大学硕士生，主要研究方向为Web服务，
E-mail：afei_54@yahoo.com.cn

如根据网络故障的性质可分为物理故障和逻辑故障，根据发生故障的对象可分为线路故障、路由故障和主机故障，根据故障持续的时间可分为永久性故障、间歇性故障和短暂性故障等。

### 1.2 告警概念

在网络管理领域，故障被定义为产生异常功能的原因，故障的发生是产生告警事件的原因。告警是在特定事件发生时被管对象发出的一种反映其自身信息，并向网络管理中心发出处于异常状态信息的报告。告警表明当前有异常存在，但并不表示当前的被管设备发生了异常[3]。被管对象以发出告警信息来作为当前网络中出现故障的响应。许多告警信息只提供发出告警的时间、告警信息的发出者以及故障的外在表现，而不提供故障的发生位置及原因，从而给故障定位带来了困难[4-5]。

### 1.3 告警分类

根据特征不同，告警可以分为连通性告警和性能告警。连通性告警是指管理工作站和被管理对象的连接失败，设备不再具有连通性，无法与其通信。性能告警是指设备的连接仍然存在，但因被管对象与故障管理相关的管理信息库（management information base，MIB）对象的值超出了预设的阈值而触发的告警。

### 1.4 告警信息的收集

收集网络信息一般有异步告警和主动轮询2种方法[6]。异步告警即在发生故障时，由发生故障的设备或服务器主动向网络管理系统报告。主动轮询是由网络管理系统定期查询各设备和服务器的状态。

在获取网络信息时，一般将异步告警与主动轮询结合起来，以便能够获取更加全面的信息，防止告警信息的丢失。

## 2 告警过滤的常用方法

告警过滤是指将非故障性、误报、冗余的告警信息去除，保留发生故障的潜在原因。告警相关性分析可以过滤掉一些告警信息，减少操作人员看见的告警数量，有助于维护人员找出问题的潜在原因，有助于故障的实时诊断和故障的定位[7]。

常用的消除冗余告警事件的方法有如下几种[8]。

告警压缩。在短时间内，收到大量重复的告警信息，可用一个事件加上这个事件发生的次数来代替。

选择性抑制。针对特定的告警时间，按照一定的原则，暂时禁止其他告警信息的出现，如高优先级告警信息存在时，抑制低优先级告警信息。

过滤。根据事先制定的参数去除符合条件的告警信息，如某个节点发出了告警信息，但是其某个参数与预先设定的阈值相差较大，则过滤掉。

缩放。在特定的网络环境下，生成一个事件的副本，通过提升副本中的某些值（如优先级）来抑制原来的事件。

泛化。根据关联操作的上下文，将某一类具有共性的事件提升为更高级的事件，如某处电缆断开导致大量告警产生，找到这些具有共同路径、同时发生的告警事件，对其进行泛化，用“某一连接断开导致故障发生”来代替之前发生的告警信息，即电缆出现故障。

特殊化。特殊化是与泛化相反的操作，是用较低管理层上的具体事件来代替当前事件，该操作是建立在演绎推理基础上的。

事态关系。事态关系是指事件发生和结束的时间及其先后次序，如在 $A$，$B$ 事件发生后，$C$ 事件才发生，这样可在关联时去除 $C$ 的告警信息。

## 3 网络拓扑信息库的建立

### 3.1 网络拓扑信息的获取

网络管理系统可通过异步告警或主动轮询的方式获取网络中的所有结点，实现网络拓扑的自动发现。网络管理系统为了获取所有的网络结点，需要能够访问到如下信息：管理工作站代理的子网掩码，管理工作站路由表中缺省路由器的地址，来自缺省路由器及网络中其他路由器、结点的简单网络管理协议（simple network management protocol，SNMP）信息。根据获取的网络拓扑结构信息，建立网络拓扑信息库。

### 3.2 连接矩阵

网络拓扑信息库主要由关联表构成。本研究首先将获取到的网络拓扑信息转化成网络连接矩阵，再生成关联表。

连接矩阵反映出各设备之间的连接关系，设备之间有直接连接用1表示，无直接连接用0表示。由于设备间的连接是无方向的，所以最后完成的连接矩阵是一个对称矩阵。

### 3.3 关联表

本研究设计了一个关联算法，根据所获取的连接矩阵，将其转化为一个关联关系表，以便关联关系的查询及消除冗余的告警消息。

由于连接矩阵为对称矩阵，故只需扫描对角线以上的部分即可得到每个设备所关联的设备。如 $\boldsymbol{A}$ 为连接矩阵，$a_{ij}$ 为连接矩阵的元素，$b_{ij}$ 为设备关联数组（$i, j \leq$ 设备数目），其关联计算步骤如下：

1）判断 $i$ 与 $j$ 的大小，如果 $i<j$，且 $a_{ij}$=1，则 $a_{ij}$ 的 $j$ 值添加到 $b_{ij}$ 中，继续扫描后面的元素。

2）执行 $i$++ 操作，进入到下一行扫描，如果 $i \geq$ 设备数目，跳转到步骤 4）。

3）如果 $i>j$，执行 $j$++ 操作，直到 $i<j$，然后跳转到步骤 1）。

4）结束扫描，整理设备关联数组 $b_{ij}$。

经过关联算法运算后，$b_{ij}$ 中存放的是每个设备中有直接关联的节点，从这些节点中取出相关节点就可以组成关联表，其步骤如下：

1）将每个设备数组 $b_{ij}$ 中所包含的 $a_{ij}$ 按照行元素 $i$ 从小到大的顺序排序。

2）将排序好的 $b_{ij}$ 中的元素再按列元素 $j$ 从小到大的顺序排序。

3）如果 $b_{ij}=j$，并且 $b_{ij}\neq 0$，则跳转到 $b$ 的 $j$ 行。

4）如果 $b_{jk}\neq 0$，则将 $k$ 值添加到 $b_{jk}$ 中（$k \leq$ 设备数目）；否则 $i$, $j$ 增加，跳转到步骤 3）。

5）扫描设备数组 $b_{ij}$，即得到与该设备 $i$ 相关联的其它所有设备。

6）将所有的 $b_{ij}$ 组织起来，即为所需要的设备关联表。

## 4　告警过滤算法

本研究在得到关联表以后，将收到的告警信息与关联表中的关联设备进行比较，消除冗余或误报的告警信息，这里主要针对连通性故障。告警过滤计算步骤如下（$p$ 为告警数目，$i$, $j$ 为设备数目）：

1）将告警信息送入到 $C_a$ 数组中，并对告警序号进行排序，去除相同的告警信息。

2）将 $C_{ap}$ 中的元素与关联表 $b_{ij}$ 中的元素进行比较，如果 $C_{ap}\neq 0$，并且 $b_{ij}$=$C_{ap}$，则跳转到关联表的 $j$ 行；否则跳转到步骤 4）。

3）如果 $b_{jp}\neq 0$，用其去比较 $C_a$ 中的元素，相同则将其消除；否则跳转到 $p$+1 元素比较。

4）将 $i$, $j$, $p$ 自增，跳转到步骤 2），如果比较完毕则跳转到步骤 5）。

5）对 $C_a$ 中的元素进行整理输出，即为可能导致故障的潜在原因。

## 5　实验仿真

实验环境为 Windows server 2003，软件版本为 VS 2005，通过 SNMP 中 MIB 数据库的信息，获取实验环境网络拓扑图（见图 1）。网络管理中心通过主动轮询的方式获取到6条分别由D/4, E/5, F/6, G/7, H/8, J/10 发出的告警信息，运用网络拓扑方式进行网络故障定位。需要注意的是，设备编号时，后一节点的编号要比前一节点的编号大。

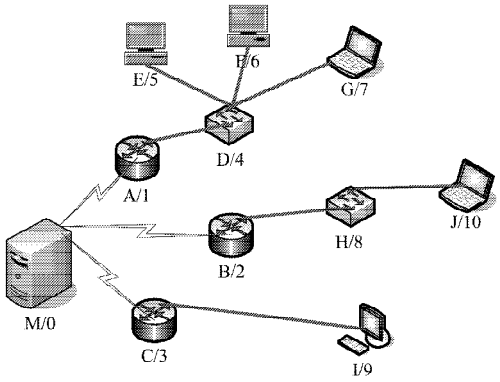


**图 1　网络拓扑图**

Fig.1　Network topology diagram

根据网络拓扑结构，可得出网络设备的连接矩阵。设

$$a_{ij}=\begin{cases}0 & \text{设备间没有连接，}\\ 1 & \text{设备间有直接连接，}\end{cases}$$

则连接矩阵如下：

$$A=\begin{pmatrix}0&1&1&1&0&0&0&0&0&0&0\\1&0&0&0&1&0&0&0&0&0&0\\1&0&0&0&0&0&0&0&0&0&1\\1&0&0&0&0&0&0&0&0&1&0\\0&1&0&0&0&1&1&1&0&0&0\\0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0\\0&0&0&0&0&0&0&0&0&0&1\\0&0&0&1&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&1&0&0\end{pmatrix}。$$

由网络设备间的连接矩阵，再根据关联算法，可得出设备间的关联关系，如表 1 所示。

**表 1　关联表**

Table 1　Association table

| 设备号 | M/0 | A/1 | B/2 | C/3 | D/4 | H/8 |
|---|---|---|---|---|---|---|
| 关联设备号 | A/1~J/10 | D/4,E/5,F/6,G/7 | J/10,H/8 | I/9 | E/5,F/6,G/7 | I/10 |

将收到的 6 条告警信息（D/4, E/5, F/6, G/7, H/8, J/10）作为一个事件，根据故障的外在表象，查找关联表，将同在本告警事件中且有关联关系的被关联的设备去掉，最终剩下的设备（D/4,H/8）可能就是导致本次故障的潜在原因。

在得到导致故障发生的潜在原因后，根据故障

的外在表现，采取对应的措施解除故障，使网络恢复正常运行。

根据前面的网络拓扑信息，模拟大型网络，将网络拓扑方法与一般方法（如压缩、选择性抑制、缩放、泛化等）过滤告警信息所花费的时间进行比较，结果见图2。

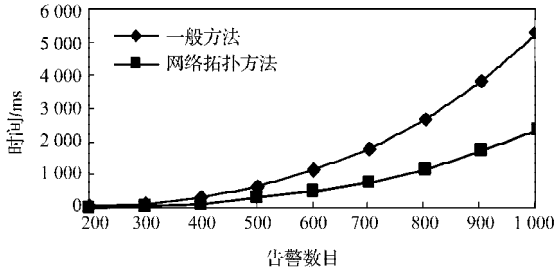


**图2 网络拓扑方法与一般方法过滤告警花费时间比较**

Fig. 2 The comparison of alarm filtering time between network topology method and general method

## 6 结语

利用网络拓扑方式进行告警过滤，可在大量告警信息送入到事例推理输入端前就消除冗余、误报的告警信息，这就避免了将一些错误的告警信息送入事例推理中去[9-10]。通过实验验证，利用网络拓扑方法可将告警过滤时间缩短到一般方法进行告警过滤所花费时间的44%，减少了因分析无关网络节点信息而浪费的时间，直接将可能导致告警发生的网络结点信息送入事例推理系统中，传输给管理员最直接的信息，便于网络管理。

关于网络拓扑告警过滤方法，可在以下问题上做进一步的深入研究：

1）将网络拓扑方法与基于事例推理技术的事件关联结合起来，在运用网络拓扑过滤后的告警信息送入到事例推理器后，能够快速地找出故障的解决办法；

2）进一步完善关联算法，增加对性能性事件的关联效果。

**参考文献：**

[1] 刘增新. 基于关联技术的网络故障诊断与定位系统的研究[D]. 北京：华北电力大学，2009.
Liu Zengxin. Research on Network Fault Diagnosis and Location System Based on Correlation Technology[D]. Beijing：North China Electric Power University，2009.

[2] Mani Subramanian· Network Management Principles and Practice[M]. 王 松，周 靖，孟纯城，译. 北京：清华大学出版社，2003：117-130.
Mani Subramanian· Network Management Principles and Practice[M]. Wang Song，Zhou Jing，Meng Chuncheng，Translators. Beijing：Tsinghua University Press，2003：117-130.

[3] 李 岚. 基于事件关联的网络事件管理的研究和设计[D]. 南昌：南昌大学，2005.
Li Lan. Study of Network Event Management Based on Event Correlation[D]. Nanchang：Nanchang University，2005.

[4] 石 磊. 网络故障定位与检测技术研究[D]. 南京：南京理工大学，2006.
Shi Lei. Network Fault Location and Detection Technology [D]. Nanjing：Nanjing University of Science，2006.

[5] 金瑞琪. 网络智能故障定位系统的研究[D]. 哈尔滨：哈尔滨工程大学，2005.
Jin Ruiqi. Research of Network Intelligent Malfunction Localization System[D]. Harbin：Harbin Engineering University，2005.

[6] Janet Kolodner. Case-Based Reasoning[M]. San Mateo：Morgan Kaufmann Publishers，1993：22-23.

[7] 田 可. 局域网络故障诊断技术的研究与实现[D]. 北京：华北电力大学，2005.
Tian Ke. Research and Implement of Network Fault Diagnosis in Local Area Network[D]. Beijing：North China Electric Power University，2005.

[8] 张 新. 分层分布式网络故障管理研究[D]. 西安：西安电子科技大学，2007.
Zhang Xin. Study of the Hierarchical and Distributed Network Fault Management[D]. Xi’an：Xi’an University of Electronic Science and Technology，2007.

[9] 张文雯. 基于事件关联技术的互联网故障诊断研究[D]. 南京：南京理工大学，2004.
Zhang Wenwen. Research on Event Correlation Based Internet Fault Diagnosis[D]. Nanjing：Nanjing University of Science，2004.

[10] 李 鹏. 基于事件关联的网络故障管理研究[D]. 长沙：中南大学，2008.
Li Peng. Research on Event Correlation Based Network Fault Management[D]. Changsha：Central South University，2008.

（责任编辑：徐海燕）