告警相关性在微波通信中的应用

丁志燕[1],徐志根[2]

(1.西南交通大学 计算机科学与技术系,四川 成都 610031;
2.西南交通大学 轨道交通国家实验室,四川 成都 610031)

摘 要:告警相关性分析有多种方法,本文所讨论的基于微波通信的告警相关性分析基于代码方法的基本思想,是建立潜在的问题(故障)和表征这些问题症状(告警)的关联矩阵,并用其进行故障定位。此方法适用范围广、速度快,能够处理较高比率的症状丢失和虚假症状,本文主要研究关联规则在微波通信告警中的具体应用。

关键词:基于代码方法;告警相关性分析;故障管理

中图分类号:TN929.11 **文献标识码**:A **文章编号**:1674-7720(2010)17-0043-03

Alarm correlation application in microwave communication

DING Zhi Yan[1], XU Zhi Gen[2]

(1.Department of Computer Science and Technology, Southwest Jiaotong University, Chengdu 610031, China;
2.State Laboratory of Rail Traffic Control and Safety, Southwest Jiaotong University, Chengdu 610031, China)

Abstract: There are many methods in alarm correlation analysis, in which the alarm analysis one based on rules can be comprehended easily and consistent with men's logic, so it applied in the communication network widely. Considering the advantages and confluence of data mining technology and correlation rule, this thesis presents an alarm correlation application in micro wave transport.

Key words: based code approach; alarm correlation analysis; fault management

在电信市场日趋开放的今天,竞争日益激烈,各种新兴电信业务不断涌现。为了提高电信企业的市场竞争力,降低企业的维护成本,减少直至避免用户服务终端受到影响,必须对整个电信网络的管理方式进行一些改进。在规模、技术及竞争相对层次较低的情况下,采取原来的处理方式是可行的。但随着数字化、集成化的发展,各种新业务、新技术被广泛应用,电信网络规模和网络结构发生了根本性的改变。传统的网络管理已经不能满足企业日益发展的需要,并会造成人力和财力的大量浪费。

在电信网络管理中,故障管理是一个重要而且难度很大的任务。尤其是通信网络,每天都会产生大量的告警信息。面对着大量告警,网络管理员很难快速进行故障定位和诊断。一个大型网站应用层故障恢复的时间中约有93%的时间花费在对故障的检测和诊断上。因此,在进行故障定位之前必须对网络产生的大量告警信息进行有效地分析和解释。网管中心的任务是在接收到网络产生的告警之后对告警进行分析。告警分析意味着对告警中包含的零散信息进行整合,并从整体上对告警作出解释。在故障管理中有些告警处理软件采用了告警关联技术,称为告警关联系统。它的主要作用是自动过滤掉冗余的告警、识别故障以及建议一些预见性的措施,因此在故障管理中极具价值。目前,很多电信网管都采用了告警关联系统作为网管智能化的一部分。

1 现阶段国内外研究方法及缺点

随着数据挖掘技术的发展,越来越多的研究人员采用数据挖掘方法分析告警数据。利用数据挖掘技术可以进行网络故障隔离和诊断、选择正确措施、进行预维护和趋势分析。最近人们已经提出了很多算法用于完成这一任务,然而现存的算法都有其自身的缺陷,不能有效挖掘告警信息。

(1)基于关联规则挖掘方法的告警分析

基于关联规则挖掘的方法在告警分析数据挖掘领域内占据了十分重要的位置，这是因为关联规则挖掘方法具有其他方法无法比拟的优点。正如参考文献[1]中总结的那样，通过这种挖掘方法得出的规则符合人的思维，容易理解，因此，目前处理告警序列的操作员乐于用这种规则的形式表达知识。而且这样的规则可以表达这一领域内的简单联系，并且有助于高效地挖掘出数据中隐藏的信息。然而，现存算法挖掘效率还比较低，并且参考文献[5]研究发现，一般关联规则挖掘方法对大规模数据库会产过多的规则，即产生所谓的规则爆炸问题，使决策者面对太多的规则而无所适从。

(2)基于神经网络方法的告警分析

神经网络方法模拟人脑神经网络，神经元是其基本处理单元。由神经元可以构成各种不同拓扑结构的神经网络。为了让神经网络实现事件关联功能，首先要对其进行训练，将网络设备上的告警信息与实际网络故障情况作为神经网络的输入和输出，不断调整神经元相互连接的权值。经过训练后的神经网络就能根据存储在神经元连接上的权值识别出特定的故障。参考文献[2,4]指出，如果目标仅仅是进行好的预测，神经网络的确具有一定功能。然而，这种方法需要有较好的训练数据，并且在当前应用中，重要的一点是发现的知识应该具有可理解性，因为电信公司不会愿意把许多黑匣子安到其系统中去。因此，神经网络方法在这方面仍需改进。

(3)基于案例推理方法的告警分析

案例推理是基于集中存储的认知模型，其基本思想是将以前解决问题的经验以案例的形式存放在案例库中，当遇到问题时就从案例库中查找同类案例的求解，从而获得当前问题的解决方法。参考文献[3]开发了三个模块对告警关联方法进行模拟：一个模块用于生成故障和告警，另一个模块用于定义网络配置，最后一个模块再进行告警过滤和关联。但是这种方法是基于经验和事例来解决问题的，所以对于网络处理反应不敏感，不适应要求实时性高的告警处理。

(4)基于代码方法的告警分析

代码方法的基本思想是建立潜在的问题(故障)和表征这些问题症状(告警)的关联矩阵并用其进行故障定位。参考文献[6]提出一种综合方法。该方法结合小代码书和简单专家规则的优点进行告警分析，取得了一定成果。使用代码方法简单、适用范围广、速度快，能够处理较高比率的症状丢失和虚假症状。此方法适合微波通信小心的故障管理系统。

(5)其他方法

除上述所列方法外，还有其他方法，如聚类方法、模糊逻辑等。聚类是把一组个体按照相似性归成若干类别。参考文献[7]通过聚类算法预测出一些告警集合的发生可以导致哪些告警集合的随后发生。参考文献[8]在进行告警数据分析时采用了遗传算法生成相关性规则的预测模式，用来对故障进行预测。对融合算法的研究也逐渐进入了人们的视野。根据当前专家系统不能适应网络日益发展的需要，提出一种综合智能解决方法，将神经网络和基于案例的推理进行结合从而完成对告警数据的分析。将遗传算法和神经网络进行结合，通过实验证明，该方法在网络学习和训练效率上高于传统的BP算法、标准遗传算法和一般的自适应遗传算法。

2 告警相关性在微波通信中的应用

由于通信告警在逻辑上具有告警相关性，单个的故障告警往往会触发一系列的相关联的告警，导致产生大量告警信息，使对故障的判断和定位变得困难。例如：在微波通信中，在网络管理客户端上对同一个MPT进行收发频率的配置，如果配置的收发频率和MPT真实的收发频率不一致，会出现Incompatible Frequency Alarm，同时会导致Incompatible Shifer Alarm告警的产生，这就是由于两个告警之间的关联性，一个告警的产生，导致另一个告警的产生。如果网络中同时发生多个故障，告警的情况就会变得更为复杂。网络管理员面对这些大量的告警信息是很难找出故障发生的根本原因，从而无法修复所发生的故障。

告警相关性分析的目标是为网络中某个设备故障抑制不必要或不相关的告警，为网络管理员提供更准确的故障告警信息，找到产生故障告警的根源，以实现快速、准确的故障定位。告警相关性分析，一定的告警可以抑制比它级别低的告警，同时也可以被比它级别高的告警抑制。

告警相关性分析的过程，就是比较所有出现的通信告警之间的优先级关系，抑制告警级别低的告警，使其不上报给网络管理系统，只向上发送最高级别的告警，以减少告警上报的数量，有利于告警根源的准确判断。告警抑制功能用来减少故障告警的上报数量，硬件告警能够抑制所有的通信告警，被抑制的告警将不再上报给网络管理系统。如出现MPT Card Fail Alarm，则所有的通信业务将中断，也就不会出现通信告警。高级别的通信告警会抑制低级别的告警，被抑制的通信告警将不再被上报给网管系统显示。如出现Demodulator Fail告警，就不会在上报High BER告警。

告警处理过程模型如图1所示。

3 告警相关性处理流程图

告警相关性是告警处理的重要组成部分，告警管理模块从微波通信接收和发射设备中获得通信告警相关信息，并在告警管理模块中完成告警的处理。告警相关性组件只能利用检测到的告警状态去做告警相关性处理。告警相关性处理流程如图2所示。

(1)告警管理进程从微波通信接收和发射设备中获得告警的状态。

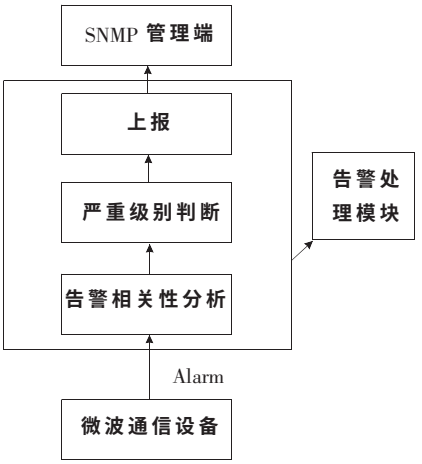

图 1 告警处理过程模型

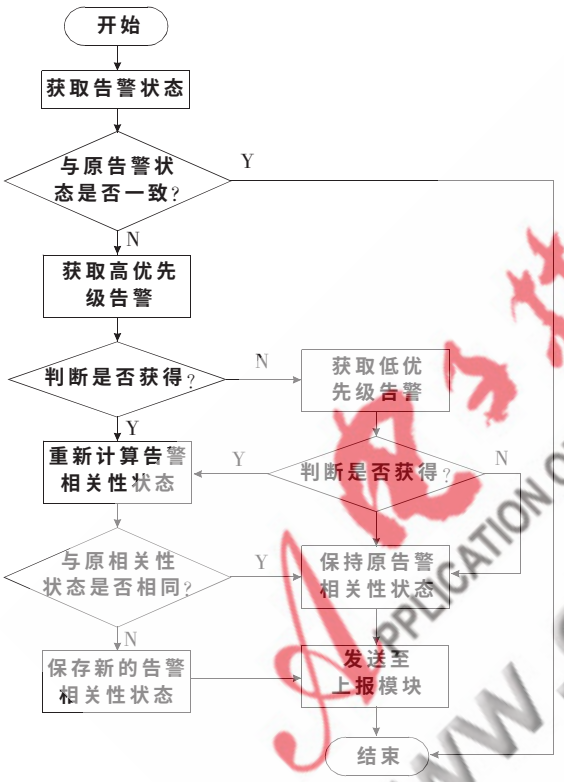

图 2 告警相关性关系处理流程

(2)如果检测到的告警状态和老的告警不相同,则保存新的检测到的告警,并且转到(3),否则什么都不做。

(3)计算是否有比这个告警级别高的告警,如果有,则重新计算告警相关性状态,保存并发送到告警上报模块;如果没有,则计算是否有比此告警级别低的告警,如果有,则重新计算告警相关性状态,保存并发送到告警上报模块。

4 实验结果

实验结果如图 3 所示。

本文提出的告警相关性分析模型与其他模型比较具有以下优点:(1)更可靠,易于实现;(2)便于修改告警相关性规则;(3)自适于网络配置信息的改变;(4)适用于

图 3 显示结果

微波通信设备的故障诊断,但由于组成微波通信网的设备很复杂,生产厂商型号、规格的不同,为得到一个通用相关性模型,使它适用于各种电信网络,还需继续研究。

参考文献

[1] KICIMAN E, FOX A. Detecting and localizing anomalous behavior to discover failures in component-based internet services[R]. Technical Report, Stanford, 2004.

[2] CHEN M S, HAN J, YU P S. Data mining: an overview from database perspective [J]. IEEE Transactions on Knowledge and Data Engineering, 1996,8(6):866-883.

[3] WIETGREFE H. Investigation and practical assessment of alarm correlation methods for the use in GSM access networks [C]. In: R. Stadler and M.Ulema,Editors, Proc. Network Operation and Management Symposium, 2002:391-404.

[4] 郑庆国,吕卫锋.通信网络中的告警相关性研究[J].计算机工程与应用,2002(2):11-14.

[5] KLEMETTINEN M, MANNILA H, TOIVONEN H. Interactive exploration of interesting findings in the telecommunication network alarm sequence analyzer TASA [J]. Information and Software Technology, 1999,41:557-567.

[6] KLEMETTINEN M. A knowledge discovery methodology for telecommunication network alarm databases[D]. Finland: Department of Computer Science, University of Helsinki, 1999.

[7] MANNILA H, TOIVONEN H. Discovering generalized episodesusing minimal occurrences [C]. In: Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining(KDD'96).关联规则挖掘在电信网络告警分析中的应用研究 Portland,Oregon:AAAI Press,1996:146-151.

[8] 胡一飞.计算机网络中告警数据处理技术的研究[J].福建电脑,2005(11):32-33.

(收稿日期:2010-03-08)

作者简介:

丁志燕,男,1981 年生,硕士研究生,主要研究方向:网络与通信。