一种基于贝叶斯网络的集成的故障定位模型

钟仕群,朱程荣,熊齐邦
(同济大学 计算机科学与技术系,上海 200331)

摘 要:故障管理是网络管理中最基本也是最重要的功能,目的是保证网络能够连续可靠地运行。故障管理可以分为两个主要的部分:故障检测和故障定位。其中故障定位是核心与难点。文中介绍了一种新的在症状收集时结合被动测试与主动探测,集成了被动诊断对网络正常的通信的影响较小以及主动探测方法可以快速有效地标识故障的优点。在诊断时采用贝叶斯网络来表示症状与故障之间的因果关系,利用不确定推理方法进行故障定位的模型。该模型包括故障推理、逼真度验证、动作选择三个模块。

关键词:故障管理;贝叶斯网络;主动探测;被动测试;不确定性推理
中图分类号:TP393.07 **文献标识码**:A **文章编号**:1673-629X(2006)12-0013-03

An Integrated Fault Localization Model Based on Bayesian Networks

ZHONG Shi-qun, ZHU Cheng-rong, XIONG Qi-bang
(Department of Computer Science and Technology, Tongji University, Shanghai 200331, China)

Abstract: Fault management is the basic and the most important function in network management. It aims to assure management networks can run continuously and reliably. Fault management includes fault detection and fault localization. Fault localization is a core component in fault management system. In this paper, Bayesian networks are proposed to model causal correlation between symptoms and faults. A novel technique that integrates the advantage of both passive diagnosis and active probing is used to detect symptoms. Probabilistic reasoning is used to locate faults in the network. The model consists of three modules: fault reasoning; fidelity evaluation; and action selection.

Key words: fault management; Bayesian networks; active probing; passive diagnosis; probabilistic reasoning

1 概 述

随着互联网在硬件、操作系统、通信、应用软件以及它们之间的依赖性方面的复杂度越来越高,网络管理的需求特别是网络故障管理的需求就越来越急迫。故障定位是故障管理的核心。故障定位过程是鉴别出引起被管网络不能正常工作的故障的过程,它是故障管理的基本组成部分,可以分为症状检测和根故障定位两个过程。故障通常指根原因,是被管网络及部件出现硬件或软件上的紊乱,使之不能提供正常的服务。症状是指与某故障有关的错误造成的网络的非正常运行的外在表现。一个 IP 网络由一组被管对象组成,如交换机、路由器、服务器、虚拟链路和物理链路等等。这些对象之间有复杂的依赖关系。很多时候,一个对象失效会对别的与它有关联的对象产生影响,比如,一个链路失效会使得不同网络层次之间的连接超时,这些依赖关系对于告警关联和故障定位过程非常重要。网络实体之间的不确定的依赖关系通常由概率来表示[1],一些普遍接受的假设是:

(1)给定故障 a,症状 b 和症状 c 可能被 a 引发的事件是相互独立的;

(2)如果故障 a 和故障 b 都可以引发症状 c,a 引发 c 和 b 引发 c 两个事件是相互独立的;

(3)各故障的发生是相互独立的。

文中利用贝叶斯网络[2]来描述所观察到的症状与故障之间的因果关系。

贝叶斯网络是不确定知识表示和处理的一个强有力工具,具有图形化的不确定推理能力。贝叶斯网络是由节点、有向弧和条件概率表构成的有向非循环图,可以定义为一个三元组(V,L,P)[3],V 是有向非循环图中的结点集,L 是结点之间的单向链接集,表示它们之间的因果关系,P 是概率集,$P=\{p(v\mid\pi(v))\mid v\in V\}$,$\pi(v)$ 是 v 的父结点。这里的症状-故障之间的贝叶斯网络如图 1 所示,V 由故障集 $F=\{f_1,f_2,\cdots,f_m\}$,和 症状集 $S=\{s_1,s_2,\cdots,s_n\}$ 组成。$P=\{p(s_i\mid f_j)\mid s_i\in S,f_j\in F,i=1,2,\cdots,n,j=1,2,\cdots,m\}$。这里,一个症状可能被多个故障引发,一个故障可能引发多个故障。假设模型是完备的,即,若用 Fs_i 表示所有可能引起症状 s_i 的故障集合,如果 Fs_i 中的故障都没发生,那么症状 s_i 一定不会出现,反之,如果出现症状 s_i,那么 Fs_i 中至少有一个故障发生。

使用贝叶斯网络对 IP 网络建模需完成下面两个重要

收稿日期:2006-03-17
作者简介:钟仕群(1982-),女,广东人,硕士研究生,研究方向为容错技术、网络管理;朱程荣,副教授,硕士生导师,研究方向为容错技术;熊齐邦,教授,硕士生导师,研究方向为网络管理。

的过程：

①确定被管实体之间的依赖关系及其变化，当一个实体 a 需要另一个实体提供服务来实现自身的功能时，称 a 依赖 b。

②测量依赖值，即先验概率：贝叶斯推理的结果很大程度上依赖于先验概率，要应用贝叶斯公式，必须先获取该值。过去的管理信息统计数字是获取先验概率的主要来源，此外，网管专家的经验和测试实验也是获取先验概率的主要手段。

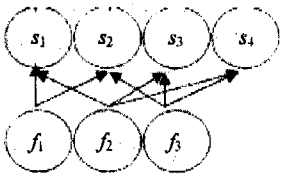


图 1 贝叶斯网络模型

图中故障引发症状的概率如下所示：

$p(f_1)=0.0097\%, p(f_2)=0.0097\%, p(f_3)=0.0097\%$

$p(s_1 \mid f_1)=0.9,\ p(s_1 \mid f_2)=0.3,\ p(s_2 \mid f_1)=0.85$

$p(s_2 \mid f_3)=0.17, p(s_3 \mid f_2)=0.44, p(s_3 \mid f_3)=0.25,$

$p(s_4 \mid f_2)=0.35, p(s_4 \mid f_3)=0.69$

在症状检测阶段，常用的方法主要有两种：

(1)被动诊断(passive diagnosis)[4]：当代理检测到所负责资源的某种状态时，发出告警，通知管理者；

(2)主动探测(active probing)：管理者每隔一段时间请求被管对象的属性。

在被动方法中，通过对被动收集到的症状进行处理，从而推断出故障发生的根源。在主动的方法中，通过构建一系列的探测动作检测网络中的故障。这两种方法各有利弊，被动诊断对网络正常的通信的影响较小，但是通过这种方法发现故障根源需要很长的时间，尤其是症状丢失率比较高的时候。另一方面，虽然主动探测方法可以快速有效地标识故障，但是在包含成千上万个网元的大型 IP 网络中，通过费力搜索引起某个功能失效的原因来定位未知故障是一个非常耗时和艰难的过程。文献[5]中提出了一种改进的主动探测方法，首先配置少量的轮询器(探针)周期运行，而在获取一定信息的时候再根据需要选择开销最小的轮询器集进行探测，从而减少了探测对网络正常通信所造成的影响。但是，如果只使用主动方法，对于有些间歇性发生的问题，可能会检测不到。

文中提出了一种结合被动与主动方法的故障检测方法。如果基于被动方法得到的信息不能充分解释问题，那么系统会选择优化的探测动作来发现在被动诊断中没有得到但又能够解释问题的最关键的症状。

2 故障定位模型

故障定位过程包含三个模块：故障推理、逼真度验证、动作选择。完整的过程如图 2 所示。故障推理模块以被动收集到的症状 SO 作为初始输入，输出故障假设集 Φ。故障假设集 Φ 包含一组假设 $(h_1, h_2, \cdots, h_n)$。这里，每个假设包含一组可以解释所有已观察到的症状的故障。然后 Φ 被发送至逼真度验证模块，检验有没有可满足的假设 $h, h \in \Phi$。若有，则整个故障定位过程结束；否则，相应的逼真度值最高的假设 h 里的故障可引发的但又尚未观察到的症状集 SN 将会发送到动作选择模块，验证其是否发生。验证后的结果返回逼真度验证模块，若通过，则故障定位过程结束；否则，把动作选择模块的结果传入故障推理模块，开始新一轮的检测。下面将分别对这三个模块的算法进行介绍。

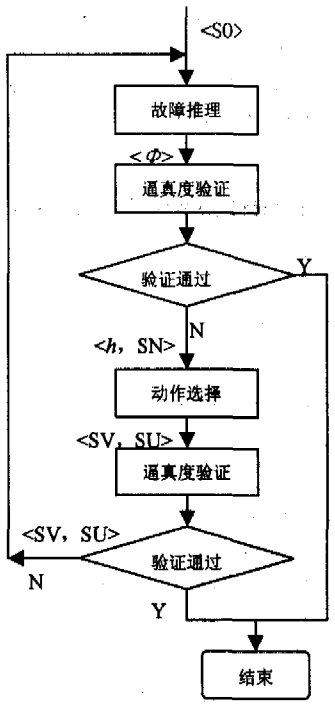


图 2 完整的故障定位过程

2.1 故障推理算法

本模块通过构建贡献函数 $C(f_i)$ 对各个 f_i 引发已知症状的贡献进行比较，该函数的定义过程如下：

a. 根据每个故障引发某个症状的概率 $p(s_i \mid f_j) \in (0,1]$，规范化为 $\hat{p}(s_i \mid f_j)$ 构建概率模型以比较各个 f_i 引发 s_i 概率。

$$\hat{p}(s_i \mid f_i)=\frac{p(s_i \mid f_i)}{\sum_{f_i \in Fs_i} p(s_i \mid f_i)}$$

b. 利用贝叶斯公式，可以计算 $p(f_i \mid s_j)$，当存在症状 s_i 时，各 f_i 发生的平均概率。

$$\hat{p}(f_i \mid s_i)=\frac{\hat{p}(s_i \mid f_i)p(f_i)}{\sum_{f_i \in Fs_i} \hat{p}(s_i \mid f_i)p(f_i)}$$，其中 $p(f_i)$ 是根据长期观察得出的 f_i 发生的概率。

c. 构造评估函数 $C(f_i)=\dfrac{\sum_{s_i \in SO} \hat{p}(f_i \mid s_i)}{\sum_{s_i \in SF_i} \hat{p}(f_i \mid s_i)}$。算法根据该函数对 F 进行搜索。该过程持续到所有已观察到的症状都被解释完为止，最后得出假设集 Φ。

推理算法如下，用 FC 表示至少能引发 SO 中的一个

症状的故障的集合,用 SK 表示还未被 h_i 解释的但已被观察到的症状集合,用 C_{max} 表示最大的 $C(f_i)$。

(1) 初始化操作:$\Phi = \varnothing; h = \varnothing; FC = \{f_j\}$,$f_j$ 至少能引发 SO 中的一个症状,$j = 1,2,3,\cdots,m; SO = \{s_i\}$,$i = 1,2,3,\cdots n; i \leftarrow 1; C_{max} = 0, max = 0$。

(2) 若 $i \leqslant n$,则作[$j \leftarrow 1$,转(3)],否则转(5)。

(3) 若 $j \leqslant m$,{则计算 $C(f_j)$[若 $C(f_j) > C_{max}$,则 $C_{max} = C(f_j), max = j$],$j \leftarrow j + 1$,转(3)}。否则转(4)。

(4) $h = h \cup \{f_{max}\}, \Phi = \Phi \cup \{h\}; h = \varnothing, i \leftarrow i + 1$,转(2)。

(5) 输出 Φ 至逼真度评估模块。

2.2 逼真度评估算法

由于网络拥塞和网络噪音等可能造成症状丢失和虚假症状以及被动测试方法症状获取范围的局限性,网管人员难以从故障推理算法中得出根故障,逼真度评估就是对这些假设的信任度进行衡量,看其是否满足事先设置的逼真度阈值 THREASHOLD,若满足,则得出根故障,否则,选择合适的探测动作,获取更多的系统状态信息,再进行推理。

假设 h 的信任度计算函数 $FD(h)$ 如下所示,根据已观察到的症状集 SO 对 h 的信任度进行计算。

$$FD(h) = \frac{\prod_{s_i \in Sf_i, f_i \in h}(1 - \prod_{f_i \in h}(1 - p(s_i \mid f_i)))}{\prod_{s_i \in SO}(1 - \prod_{f_i \in h}(1 - p(s_i \mid f_i)))}$$

如果 Φ 满足 THREASHOLD 的 h,那么整个故障定位过程结束;否则,选择信任度最高的 h,列出 h 中的故障可能引发的但又尚未观察到的症状集 SN,输出至动作选择模块,验证系统是否存在这些症状。

2.3 动作选择模块

动作选择模块的任务是选择一组开销最小的探针至服务器或被管网元[5]来探测系统中是否具有 SN 中的症状。传统的主动检测方法是周期性地运行已定义好的探针集,这在规模比较大的网络中,会影响正常的网络流量。探针是在特定机器上执行的一个程序或命令,比如常见的 ping,traceroute 或一些专门的网络管理工具。

这里探针与症状之间是多对多的关系,一个探针可以验证多个症状是否存在,一个症状可以通过多个探针来验证,探针与症状之间的关系可以用一个三元组 (A,S,E) 表示。$A = \{a_i\}$ 是探针的集合,S 是症状的集合,如前面所定义。$E = \{w_{ik} \mid w_{ik}$ 是使用探针 a_i 来验证 s_k 所需的开销,$w_{ik} > 0\}$,若 a_i 和 s_k 无关联,则 $w_{ik} = 0$。对于有些症状,可能需要使用多个动作才能验证,这里采用一个虚拟节点 v_j 表示这些动作集,并把其抽象为一个普通节点以构造二部图,v_j 的权重 $w(s_i, v_j)$ 是结合的动作集的总开销,可用 v_j 里的一个探针验证的症状也可由 v_j 验证。图 3 的症状

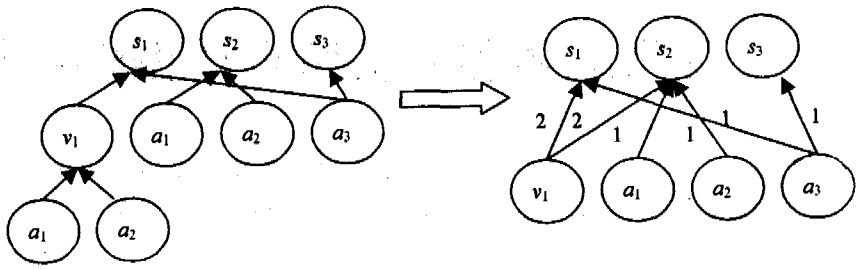


图 3　症状 - 探针关联图

- 探针图表示症状集 $\{s_1, s_2, s_3\}$ 和探针集 $\{a_1, a_2, a_3\}$ 之间的验证关系。这里,假设单个动作验证某个症状的开销都是 1。症状 s_1 可由探针 a_1 和 a_2 的联合来验证,所以创建 $v_1 = \{a_1, a_2\}, w(s_1 \mid v_1) = 2, w(s_2 \mid v_1) = 2$。

根据症状 - 探针二部图,可以把选择符合要求的开销最小的探针集的问题建模为最小权重覆盖问题。所以动作选择算法搜索一个 A_i,A_i 包含了能够覆盖需验证的症状集 SN 中的所有症状的动作,并且总开销和最小。即搜索 A_i,A_i 满足以下两个条件:(1) $\forall s_j \in SN, \exists a_i \in A_i, w_{ij} > 0$;(2) $\sum_{a_i \in A_i, s_j \in SN} W_{ij}$ 最小。这个过程是个 NP - 完全问题,这里采用贪心选择算法来获取最优解。贪心的标准是选择当前具有最大的相对覆盖率的探针。相对覆盖率 $R_i = \frac{|S_{a_i}|}{\sum_{s_j \in S_{a_i}} W_{ij}}$,$S_{a_i}$ 是 a_i 可以验证的症状集,$S_{a_i} \subseteq SN$。

3 结束语

评估一种故障定位技术的两个因素是下述性能:定位出故障所花时间和检测率。文中提出的基于贝叶斯网络的集成的故障定位算法检测的方法集成了被动诊断和主动探测两种方法,推理上采用不确定性推理方法能够在最短的时间内准确定位故障。由于 IP 网络是一个复杂的动态变化的网络,下一步可以继续研究如何在贝叶斯网络中反映出这种动态变化并进一步优化定位算法。

参考文献:

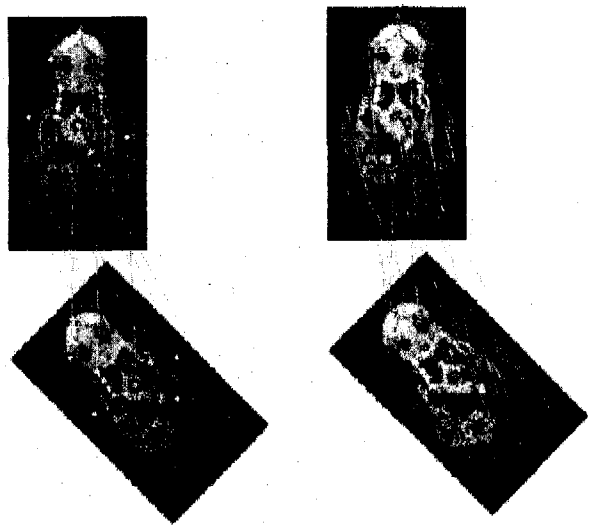
[1] Katzela I, Schwartz M. Schemes for fault identification in communication networks[J]. IEEE Transactions on Networking, 1995,3(6):733 - 764.

[2] Kant L, McAuley A, Morera R, et al. Fault localization and self - healing with dynamic domain configuration[C]//Military Communications Conference, 2003. [s. l.]:[s. n.], 2003:977 - 981.

[3] Ding Jianguo, Kramer B, Xu Shihao, et al. Predictive Fault Management in the Dynamic Environment of IP Networks. IP Operations and Management[C]//2004. Proceedings IEEE Workshop. [s. l.]:[s. n.], 2004:233 - 239.

[4] STEINDER M, SETHI A S. Increasing robustness of fault localization through analysis of lost, spurious, and positive symptoms[C]//In Proc. of IEEE INFOCOM. New York, NY:[s. n.], 2002.

(下转第 18 页)



(a)Scott 算法匹配结果($\sigma = 300$)　　(b) 改进算法匹配结果(σ_1=300，σ_2=3)

图 1　物体平面旋转匹配

$$LOC2 = LOC1 \times INV(T) \tag{7}$$

其中，

$$T = \begin{bmatrix} \cos\theta & -\sin\theta & n\sin^2\theta \\ \sin\theta & \cos\theta & -n\cos\theta\sin\theta \\ 0 & 0 & 1 \end{bmatrix} \tag{8}$$

其中 n 为图像的高度。

$INV(T)$ 是变换矩阵 T 的逆矩阵。

这里，以逆时针旋转 $\theta = 45°$ 得到的图像与原图像 18 对特征点进行匹配为例，给出实验结果(见表 1)。

表 1　第一组图像特征点匹配实验结果

	总点数	匹配点数	正确匹配点数	错误匹配点数	没有匹配点数
Scott 算法	18	17	10	7	1
改进方法	18	18	18	0	0

图 1 中，用白色的“*”表示所有参加匹配的特征点，当两幅图像中的特征点正确匹配时，用黑色“☆”覆盖这些特征点，绿色直线连接两幅图像中相应匹配的特征点(包括错误匹配的特征点)。

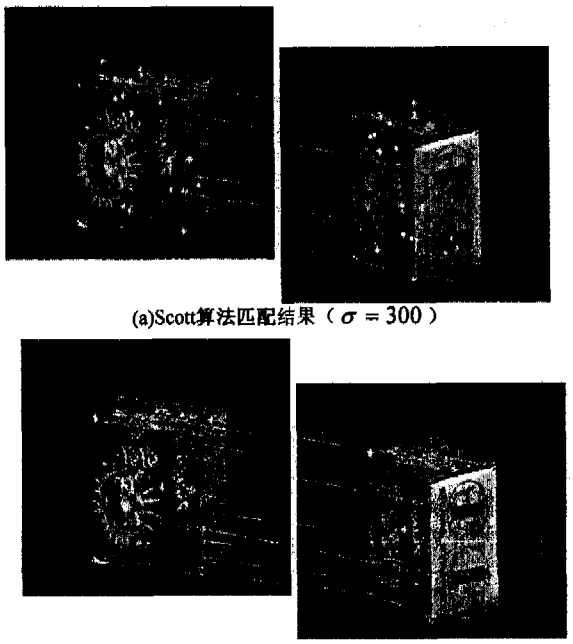
图 2 为物体立体旋转匹配结果。

从标准图像库(Amsterdam Library of Object Images (ALOI):Object. nr:. 730)中取出序列图像，图像大小为 768×576，选取 35 对特征点进行两两匹配。

这里，以原图像与顺时针旋转图像进行匹配为例，给出实验结果(见表 2)。

4　结　论

对彩色图像进行特征点匹配时，在 Scott 图像特征点匹配算法中引入 HSV 颜色空间下的色调 H 的局部累加直方图，并提出以上改进方法。实验结果表明：改进后的图像特征点匹配算法大大提高了原 Scott 图像特征点匹配算法的匹配精确度，不仅对物体平面旋转具有很高的匹配精确度，对物体立体旋转也具有较高的匹配精确度。



(a)Scott算法匹配结果（$\sigma = 300$）

(b) 改进算法匹配结果（σ_1=300，$\sigma_2 = 18$）

图 2　物体立体旋转匹配

表 2　第二组图像特征点匹配实验结果

	总点数	匹配点数	正确匹配点数	错误匹配点数	没有匹配点数
Scott 算法	35	30	20	10	5
改进方法	35	33	32	2	1

参考文献：

[1] Scott G L, Longuet - Higgins H C. An algorithm for associating the features of two patterns[C] // Proc Royal Society. London:[s.l.],1991:21 - 26.

[2] Pilu M. A Direct Method for Stereo Correspondence based on Singular Value Decomposition[C] // IEEE, CVPR97. [s.l.]: [s.n.],1997:261 - 266.

[3] Castleman K R. Digital Image Processing[M]. New York: Prentice - Hall, 1996.

[4] 刘忠伟，章毓晋. 利用局部累加直方图进行彩色图像检索[J]. 中国图象图形学报，1998，3(7)：533 - 537.

[5] 黄朝兵，余胜生，周敬利，等. 基于多邻域统计矩直方图的彩色图像检索[J]. 小型微型计算机系统，2005，26(6)：1061 - 1064.

(上接第 15 页)

[5] Rish I, Brodie M, Odintsova N, et al. Real - time Problem Determination in Distributed Systems using Active Probing[C] // In Proceedings of 2004 IEEE/IFIP Network Operations and Management Symposium (NOMS 2004). Seoul, Korea: [s.n.],2004.