计算机科学 1999Vol. 26№. 4

适用IP网络故障监测的智能代理研究*)

On Intelligent Agent Adapting to IP Network Fault Detecting

李 佳 石冰心 刘启文 喻 莉 李建刚

(华中理工大学电信系 武汉 430073) (武钢第一技校)

Abstract With the growing of network complexity and scale, fault modeling is becoming more difficult due to the dynamic nature and heterogeneity of network. We propose an intelligent agent for fault detecting based on adaptive learning algorithm. By segmentation measurement, MIB variable for describing network normal behavior is extracted and the deviation is detected. This information is combined in the structure of a Bayesian Graph so as to identify unknown or unpredictable faults.

Keywords Network fault management, SNMP, MIB, Bayesian Graph, Adaptive learning algorithm, Intelligent agent

1. 引言

目前的商用网管平台,如IBM的Tivoli NetView/6000、HP的OpenView,其故障管理上的实现方式均是通过配置窗口将管理员的经验转变成一系列规则集,然后通过内部解析设定规则集中包含的若干MIB(管理信息库)变量的阈值,一旦监测进程或驻留在被管对象里的代理进程发现超过阈值,就以陷阱方式向网管站报警,内置的故障管理模块对陷阱信息经过过滤和关联后定位和鉴别故障原因,并启动预定制的恢复程序。尽管传统的故障管理系统能够在一定程度上发挥作用,但仍然存在以下弊端:

a. 陷阱报文缺乏精确的临时信息导致事件关联十分困难[3],尤其是性能降级引发的潜在故障;

b. 当网络变化率增加时,管理员很难描述和维护适用各种网络行为的规则集。

鉴于上述缺陷,许多专家和学者纷纷提出很多解决方法如专家系统、有限状态机(FSM)、高级数据库技术和示例推理(CBR)。但上述方法都需要在语义上说明待检测的故障形式,而且缺乏伸缩性。此外,网络配置、应用和流量上的变化随时都可能改变故障的类型和本质,因而建立精确的故障模型是不切实际的。事实上,问题的核心是在没有特定故障模型的情况下,如何做到故障管理自动化?本文提出用于故障监测的智能代理采用自适应学习算法获知网络的正常行为参数并比较其偏差、将偏差和收集的其它信息通过贝叶斯图进行组合达到检测未知的或不可预见的潜在故障的目的。用这种方式,管理员就可以及时采取相应措施防止网络性能下降和减少停机时间。

需要指出的是,算法的实施仅需少量的特定网络的信息,因而可以无缝地在各种网络类型和结点中移植;同时其数据来自于通过SNMP(简单网管协议)收集的MIB变量值,故而具有广泛的兼容性。

目前该算法及其相关的智能故障监测代理系统已成功地在作者独立开发的商用网管平台NetHurricane中实现,其性能和效率均达到了满意的效果。

2. 算法的理论基础

2.1 贝叶斯图[6]

贝叶斯图是包含某种条件独立假设的有向非循环图(DAG),图中的结点代表随机变量,结点间的有向弧代表随机变量间的父子关系或因果关系,条件独立假设如下:

给定图$G=(N,E)$,N是结点集,E是结点间有

*)本研究得到国家"九五"重点科技攻关项目基金的资助(96-743-01-01-02)。李 佳 博士研究生,研究兴趣包括计算机网络与通信;石冰心 教授,博导,CERNET专家委员会委员;刘启文 教授,华中理工大学电信系。

向弧集，$\forall n\in N,\forall e\in E$，记 $p(n)\subseteq N$ 为结点 n 的所有父结点的集合，$d(n)\subseteq N$ 为结点 n 的所有子孙结点的集合，那么对子集 $W\subseteq\{N-(d(n)\cup\{n\})\}$，在给定 $p(n)$ 的情形下，称 W 和 n 是条件独立的，其概率关系为：

$$P[W,n|p(n)]=P[W|p(n)]P[n|p(n)] \quad (*)$$

换句话说，对于贝叶斯图中的任一结点，如果给定该结点的所有父结点，那么该结点独立于不是其子孙结点的结点。图 1 给出了贝叶斯图中的条件独立假设示例。

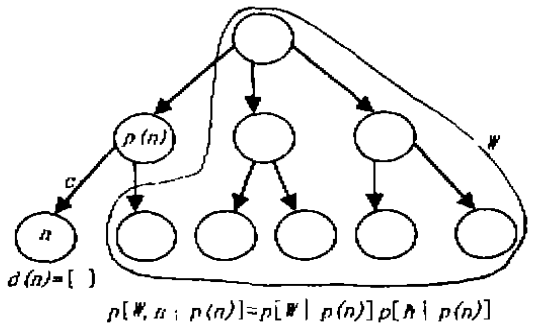

图 1　贝叶斯图中的条件独立假设

上述条件独立假设允许我们在给定某些观测信息或数据的情形下估计出贝叶斯图中结点的条件概率，本文提出的自适应学习算法将以贝叶斯图作为组合不同 MIB 变量信息的机制以达到检测网络异常的目的。

2.2　简单网络管理协议(SNMP)[1]

SNMP 的设计目的是为了使网络管理站 NMS 能够以有效而简单的方式监视和控制网络元素，它的基本架构由三部分组成：

a. 管理站。接受应用软件实体的服务请求，构造 SNMP 报文，并向代理发送。

b. 管理信息库(MIB)。存放各种被管对象的管理参数，其中的信息由管理信息结构 SMI 定义，其信息组成形式类似于一个倒置的树，每个 MIB 变量按照从树根到该变量所经过的所有结点联合标识。

c. 代理(agnet)。驻留在各种被管对象中，维护本地的 MIB 信息，接受由管理站发来的 MIB 变量存取请求报文，经过身份校验后向管理站回送响应报文，这种报文包括管理站要求存取的 MIB 变量值或相应的错误信息；另一方面，代理也能够在某些预定义事件发生时向管理站发送陷阱(Trap)报文。

SNMP 的协议规范设定了管理站和代理交换管理信息的方式，SNMP 代理的端口号是 161，管理站的端口号是 162。

由于 SNMP 使用轮询机制(至少是周期性地)维护对网络资源的实时监视和控制，同时也采用陷阱机制报告特殊事件[1]，因此使得 SNMP 成为一种有效的网络管理协议；另一方面，由于 SNMP 是基于无连接的 UDP，因而 SNMP 提供的是不可靠的无连接服务，若想获得高可靠性，则网络管理程序应放在较高层应用中建立面向连接的操作。

SNMP 共定义了五种协议数据单元(PDU)，和本算法相关的只有 GetRequest，GetNextRequest 和 GetResponse 报文。

3. 自适应学习算法和故障监测智能代理

基于自适应学习算法的故障监测智能代理在无需建立故障模型的前提下自动检测网络异常行为，其条件是网络中的任何反常或异常行为预示着某种故障的存在，这一点在实际环境中是可以保证的，系统架构如图 2 所示。

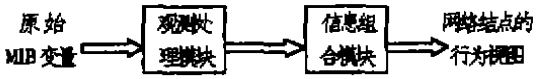

图 2　智能监测代理系统

智能监测代理分布式驻留在每个被管对象内部(如路由器、主机、Hub 等)，为了获得完整的网络运行状况视图，监测代理除定时轮询相关 MIB 变量外，还将实时的观测信息同关于网络的先验知识相组合，因而系统分为两部分：观测处理模块、信息组合模块。原始的 MIB 变量经过采样处理后用以估算该变量在给定时刻的概率，使用贝叶斯图对这些概率进行组合以提供语义上完整的网络行为视图。因此有助于在故障管理中实施时间和空间范围内的事件关联。

3.1　观测处理模块

观测处理模块采样原始 MIB 变量并转化成指示其状态的概率参数，事实上每个 MIB 变量都是反映网络流量的时序随机变量，考虑到网络行为的动态特性和 MIB 变量的频繁变化，因此必须从采样值中抽取反映每个变量行为的特征信息。

3.1.1　分段。经过观测采样获取的时序 MIB 随机变量值可视为非平稳过程，由于我们的目的是抽取反映该变量行为的相关信息，所以我们按照文[2]中的算法把这些时序 MIB 值切分成变长度的片

段，使每个片段内的数据具有类似的统计特性(如均值、方差等)，并且每个片段内的时序数据可视作平稳随机过程。实行分段有两个主要优点[2]：①由每个片段计算出的统计特性是网络流量信号的真实反映；②可以对每个片段使用以平稳随机过程为条件的信号处理技术。

3.1.2 特征抽取。目前经典的检测网络异常的方法是"阈值法"，为相关的 MIB 变量设定上、下限阈值，一旦所检测到的 MIB 变量值超出由上、下限阈值确定的区间，便视为异常。然而相对于网络的动态性和异质性，这种方法具有极大的局限性。首先，阈值本身依赖于网络流量，如果设置不正确，就可能发生在已经出现网络异常的情形下阈值不被超出(阈值过高)或阈值被频繁超过而引发不必要的"事件风暴"(阈值过低)；其次，即使正确设置了阈值，暗示故障前兆的 MIB 变量的微小变化也容易被忽略，从而延误故障诊断和恢复的时间。

为克服以上弊端，我们抽取片段数据的相关信息来判定当前 MIB 变量的行为是否正常。为方便研究，不妨设$\{Y_t\}$为当前随机 MIB 变量的时间序列，注意到 MIB 变量具有随网络环境不同其值发生变化的特点，同时又便于检测 MIB 变量的微小变化，我们以二阶自回归过程作为$\{Y_t\}$的线性模型，记为 AR(2)。

$$Y(t)=aY(t-1)+bY(t-2)+\theta(t) \quad (1)$$

这里 $Y(t)$是 MIB 变量在 t 时刻的值，a、b 为表示其特征的自回归系数，$\theta(t)$是白噪声序列，根据采样获得的 MIB 变量值可以容易得出特征值 a、b。

3.1.3 行为学习。特征模型(1)提供了检测微小变化的能力，但它首先被用来建立对应每个 MIB 变量正常行为的采用概率分布形式的描述，

为了做到这一点，必须准确地知道从整体上说网络的每部分功能何时是异常的，通过用来报告问题的工具(如 syslog 等)产生关于网络故障类型的报告(如停机、链路断)，从学习的观点看，将这些报告作为"标签"，并以此估计在网络功能失效的情况下 MIB 变量异常行为的概率，只要遵循如下判据：

如果 AR(2)是平稳随机过程，且当前随机 MIB 变量对应的特征值 a，b 满足下列条件：$a+b<1$；$b-a<1$；$-1<a<1$；则该 MIB 变量行为视为正常，否则即为异常。

3.2 信息组合模块

信息组合模块将经过处理的 MIB 变量参数组合成高层次的描述网络行为视图的参数，这些参数能够激活本地的控制程序或向网管站报警。

贝叶斯图中的结点实际上是随机变量，考虑到故障监测的特殊性，将随机变量分为两类：一类是其值直接通过监测获取，如 MIB 变量；另一类必须经过估计，称之为内部变量。由于智能监测代理一般驻留在路由器中，其网络协议栈由 IF(接口驱动)、IP 和 UDP 组成，故定义内部变量为 if、ip 和 udp，分别对应于 MIB II 中的同名变量组。逻辑上它们分别描述不同类型的网络功能，为方便研究，记 nf 泛指网络功能。定义 Network 为待监测的整个网络，其它的网络功能也能在贝叶斯图中加以扩充，具体的贝叶斯图模型如图 3 所示。图中的直线指示结点间的因果关系(父子关系)，例如网络接口层 IF 直接影响从属于该层的 MIB 变量结点，也就是说 IF 层的故障将导致在相关的 MIB 变量值中有所反映，这里用于故障监测的贝叶斯图模型是对 RFC1213 设定的 MIB II 结构的直接映象，由于每种网络功能都用独立的组件描述，因此贝叶斯图所需的条件独立假设是很容易满足的。

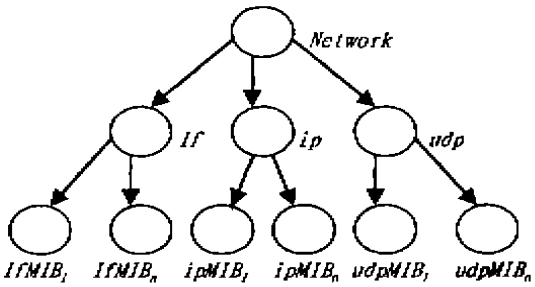

图 3 智能监测代理的贝叶斯图模型

内部变量有两种离散状态：正常(normal)和异常(abnormal)，而 MIB 变量是连续的，估算以下后验概率：

$$p(network=normal/abnormal|MIBs) \quad (2)$$

$$p(nf=normal/abnormal|MIBs) \quad (3)$$

这里 MIBs 代表多个 MIB 变量，(2)和(3)表示在已知 MIB 变量值的前提下，内部变量 network、nf 正常或异常的概率。注意到贝叶斯图的单向连通性，(2)和(3)可由 2.1 中的概率关系(*)推出，当然还必须估算下列先验概率：

$$p(network=normal/abnormal) \quad (4)$$

$$p(nf=normal/abn|network=normal/abn) \quad (5)$$

$$p(MIB\ variable|nf=normal/abnormal) \quad (6)$$

根据管理员的先验知识和监测的 MIB 变量值估算(4)和(5)，而(6)中的条件概率必须依据 3.1.3 的判

据估算。

由于智能代理驻留在本地监测，从而使通过历史的或当前的监测数据集估算后验概率成为可能。

在国家"九五"重点科技攻关项目基金的资助下，基于上述自适应学习算法的故障监测智能代理已成功地在拥有自主开发版权的 NetHurricane 网管平台上实现，开发工具采用 Visual C++5.0 和 Delphi 4.0 C/S、Windows 95&NT 环境下的 SNMP 协议库使用 ACE + Comm 公司提供的符合 WinSnmp2.0 规范的动态库 WSnmp32.dll，以后我们将把智能监测代理模块移植到实现路由器核心软件模块的实时操作系统 VxWorks 环境中。

4. 实验结果

为了验证自适应学习算法的正确性及性能，以华中地区网的一部分作为实验对象，其中的路由器2(Router2)承担着内部子网间的流量路由任务，运行在子网 2 中 PC 上的智能监测代理以 15 秒的周期轮询 Router2，通过发送 SNMP 查询原语(get、getnext)收集可用的 MIB 变量值。为便于比较，同时采用"阈值法"对同一故障类型进行监测，

智能监测代理的实验结果表明在报告故障前约 12 分钟，智能监测代理已经检测到暗示故障的网络异常行为。与传统"阈值法"比较。设定相关 MIB 变量的上、下限阈值后进行了三次实验，时段分别为 1 小时、4 小时和 1 周，前两个时段对应智能监测代理，后一个时段对应"阈值法"，直接检测阈值的超出比例，结果表明，智能监测代理优于传统"阈值法"。

结论与展望 业已表明，在不建立特定故障模型的前提下使用自适应学习算法可以检测网络故障，贝叶斯图提供了使用先验知识判定和学习 MIB 变量行为的理论框架。智能监测代理通过辨识 MIB 变量与正常行为值的偏差并以概率形式关联信息的方法完成故障的早期检测。

本文的工作只是迈向自动网络故障管理的第一步，将来的努力涉及扩大实验范围、研究行为学习阶段 AR(2)的特征值优化算法，同时延伸贝叶斯图以包括更多的信息类型或 MIB 组，并组合不同层结点的观测信息，通过扩展，贝叶斯图能够估算带有不完整信息的结点的异常概率。

参 考 文 献

1 李佳，等．网络管理系统中的自动拓扑发现算法．华中理工大学学报，1998(1)

2 Appel U，Btandt A V. Adaptive Sequential Segmentation of Piecewise Stationary Time Series. Information Sciences，1983，29：27～56

3 Jakobson G，Weissman M D. Alarm Correlation. IEEE Network，1993(Nov.)：52～59

4 谢希仁．计算机网络．大连：大连理工大学出版社，1996

5 周明天，汪文勇．TCP/IP 网络原理与技术．北京：清华大学出版社，1993

6 Spiegelhalter D J，David A P. Bayesian Analysis in Exper Systems. Statistical Science，1993，8(3)：219～288

(上接第 87 页)

力。它也需要有实践环节以及其它环节如学生在自己房间里面对计算机辅助教育的学习，等等，但有关课堂教育将会解体的种种断言都是毫无根据的。

是远程教育还是近程教育？ 我们已经明确地回答，近程教育决不会让位给远程教育。远程教育仅仅是对于偏远地区或者水平尚有特提高地区有价值，不会成为教育的主角。这也正如计算机辅助教育的种种手段一样，它们是辅助性的，而不会是主导性的。如果人类对自己后代的教育，真正实现人工智能化，那人类在人工智能方面就真正达到了大大超越于今天的水平，但这就不是下一个世纪的事了。

参 考 文 献

1 Task Force，ACM & IEEE'91 curriculum. ACM Inc，1991

2 Allegre C. French Strategy for Science Education. Sciences，1998，281(5376)：515

3 Doyle J，et al. Strategic Directions in Artificial Intelligence

4 苏运霖．21 世纪大学教育(待发表)

5 苏运霖．关于计算机科学中加强连续数学教育的问题．计算机科学，1995(4)