

基于分布智能传播的自动故障管理

孙朝晖, 张德运, 李庆海

(西安交通大学电子与信息工程学院, 710049, 西安)

摘要: 提出一种新的基于分布智能传播的自动故障管理系统 (AFMDIP), 该系统采用人工智能和网络分布管理技术, 引入协作代理, 提高了系统数据采集能力. 代理用神经网络和事例暂存库进行告警收集、分类和事例管理. 域内的故障首先由代理进行诊断, 域内不能解决的问题将提交给管理中心. 管理中心综合考虑各个域的信息, 进行基于事例推理的故障诊断, 并将事例传播到代理中. 后续类似故障将由代理直接完成诊断, 提高了故障管理的效率, 达到了信息和事例共享的目的. 实验证明, AFMDIP 有效降低了管理中心的带宽消耗, 提高了在大范围多故障情况下的故障诊断速度.

关键词: 故障管理; 神经网络; 基于事例推理; 代理

中图分类号: TP393 **文献标识码:** A **文章编号:** 0253 - 987X(2004)02 - 0115 - 04

Automated Fault Management Based on Distributed Intelligent Propagation

Sun Zhaohui, Zhang Deyun, Li Qinghai

(School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: A novel automated fault management system based on distributed intelligent propagation (AFMDIP) is presented by using the techniques of artificial intelligence and distributed network management. The cooperative agents are introduced to improve the ability of system's data collection. Neural networks and temporary cases database are applied by agents for alarm collection, classification and cases management. The agents first diagnose the faults in a domain, and the unsolved problems would be submitted to the management center that will diagnose the fault based on the case based reasoning after analyzing all the information from each domain, and then transmit this case to the agents. Thereafter, the consequent similar faults will be diagnosed directly by the agents, so the efficiency of the fault management is increased. The information and cases sharing can be achieved. The experiment shows that the AFMDIP efficiently reduces the bandwidth consume in the management center and speed up the fault diagnosis process under large-scale and multi-faults situations.

Key words: fault management; neural networks; case based reasoning; agent

智能故障管理的研究一般集中在专家系统上^[1], 然而它不能适应新的或不完备的数据, 不能处理概率问题, 这使它很难应用于大型动态网络. 概率方法适用于处理不完整的数据和自学习, 但是不利于故障识别^[2]. Denise^[3]首先提出了融合人工智能中的概率^[4]和符号方法来完成网络故障管理的

思想. 许多与故障管理相关的数据采集工作是单一服务器无法完成的, 如主动带宽估计, 所以数据采集的工作不能集中于网络管理中心完成. 本文提出一种基于分布智能传播的自动故障管理 (Automated Fault Management based on Distributed Intelligent Propagation, AFMDIP) 系统, 它可保证数据采集的

收稿日期: 2003 - 04 - 08. 作者简介: 孙朝晖(1976~), 男, 博士生; 张德运(联系人), 男, 教授, 博士生导师. 基金项目: 国家“八六三”网络安全管理与测评技术基金资助项目(863 - 301 - 05 - 03); 国家“九五”科技攻关基金资助项目(96 - 743 - 01 - 04 - 01).

的分布性,消除了由于数据采集对管理中心网络带宽和 CPU 时间的消耗,同时通过多个代理的相互配合可以完成并行数据包采集主动带宽估计等特殊数据采集工作.代理中实现了神经网络(NNs)和事例暂存库进行告警收集分类和事例暂存,使代理可以完成部分管理功能,减小了对管理中心 CPU 计算时间的占用.

1 AFMDIP 体系结构

AFMDIP 采用分层结构的分布协作式管理结构^[5],基本结构如图 1 所示.依赖代理间上下层关系建立多层结构,每一层都可以有多个代理,每个域也可采用多层结构,分成更小的子域.代理自身则是一个或多个物理实体构成的逻辑实体,当多个代理之间协作完成一项功能时,称为一组协作代理.

代理实现数据采集、告警接收、告警关联,以及事例暂存.代理与所管理的域直接相关,监视域内网络的运行.管理中心位于网络的核心位置,对各个网络资源实施网络管理操作,它的内部包含专家系统和数据库,功能是故障诊断、故障纠正和事例管理.分布智能传播(Distributed Intelligent Propagation, DIP)发生在各级代理与管理中心之间.AFMDIP 把人工智能用于故障管理的功能分布在管理体系的组件中,利用分布的推理和 DIP 实现高效稳定的故障管理.

2 代理

代理的结构如图 2 所示,数据的采集告警接收是代理完成的一个首要任务,每个代理逻辑上负责一个管理域,从该域中的网络实体中获得进行故障管理的基本数据,这是进行故障管理的基础.数据采集负责给系统网络实体提交运行参数,例如流量、延

时、带宽等,这些数据的获得依靠代理向网络实体发出采集请求.告警是由网络实体主动发出的,报告自身运行状态的数据,如热启动、连接中断等,代理对告警的接收属于被动接收.协作代理在针对故障管理的特殊数据集中有独特的作用.

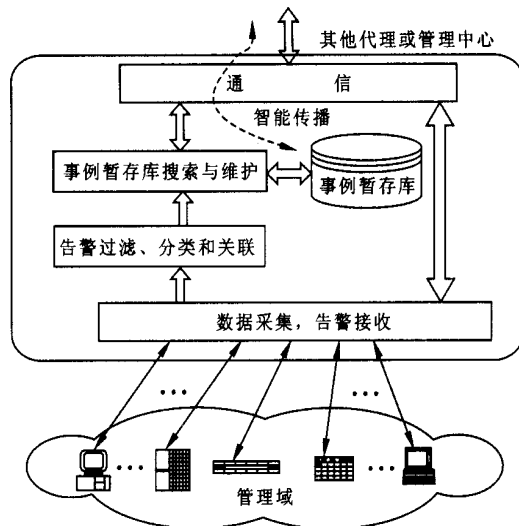


图 2 AFMDIP 的代理

带宽是进行故障诊断的一个重要依据,特别是对预测即将发生的故障有特殊的帮助作用.单一节点利用单包技术^[6]的带宽估计技术消耗带宽过大,给被测网络带来很大的负担,且测试速度也很慢.AFMDIP 利用代理之间的协作,采用包散射算法^[7]完成域间瓶颈带宽测试.对一个链路 $M = \{B_0, B_1, \dots, B_n\}$,从源端背对背发出大小为 S 的测试包,则链路的瓶颈带宽可以表示为

$$D_n = \max_{i=0, \dots, n} v_i = \frac{S}{\min_{i=0, \dots, n} \{B_i\}} = \frac{S}{B_{\text{btl}}} = v_{\text{btl}} \quad (1)$$

式中: D_n 表示两个测试包的间距; v 表示链路传输延迟.显然,包散射算法,的实施依赖于发送和接收方的协作.在 AFMDIP 中,采用一个控制代理协调两个被控代理的算法,如图 3 所示.算法的具体实现步骤如下.

- (1) 管理中心向控制代理发出测试域间瓶颈带宽的请求.
- (2) 控制代理选择 A 域的代理为发送代理, B 域的代理为接收代理,控制代理与被控代理协商测试数据包大小 S 、测试次数 n 和间隔,同步代理的时钟.
- (3) 控制代理指令接收代理开始接收测试数据,发送代理开始以 (S, n) 为参数发送测试数据.
- (4) 数据接收完毕,被控接收代理用式(1)计算

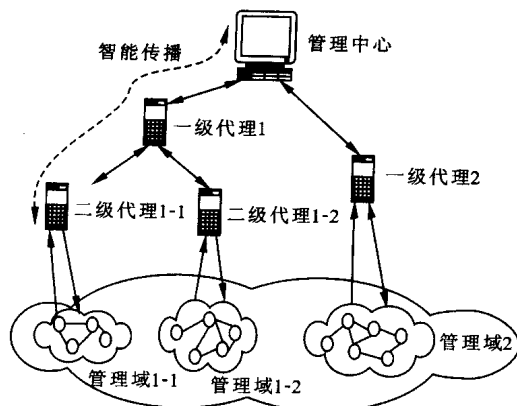


图 1 AFMDIP 体系结构

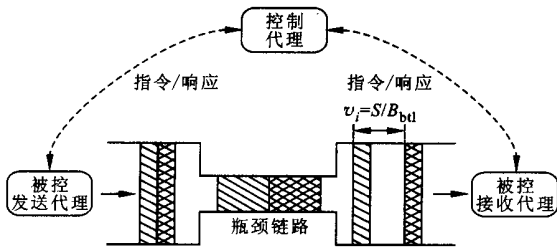


图 3 协作代理包散射带宽估计

瓶颈带宽,并提交给控制代理,由控制代理再交给管理中心.

测试 n 时间内所消耗的平均带宽为 $2nS/n = 2S/$,假定测试包大小为 800 kB,间隔为 5 s,测试 10 次,50 s 内平均带宽消耗是 320 kb/s,这在当前的网络环境下是完全可以接受的.

告警关联分类的作用是识别错误的类型,而在人工智能技术中则属于模式识别范畴.由于网络的复杂性和动态性,告警关联必须具有很强的适应能力,神经网络(Neural Network, NN)经过训练可以适应网络实体和网络拓扑的变换,因此这里采用 NN 来实现告警关联. AFMDIP 采用径向基函数网络(RBFN)完成告警关联,它是一种具有输入层、隐含层和输出层的 3 层 NN 结构.与前馈网络不同, RBFN 采用高斯传送函数,这样的隐含节点具有一个显著的作用范围. AFMDIP 的告警关联具有判别未出现过的新事例的能力. 事例暂存库(Case Cache, CC)是 AFMDIP 代理中的一个核心组件,主要作用是缓存管理中心的推理结论. 暂存库中的每个事例定义如下: Alarm Vector, 告警向量(AV); Additional Data, 附加数据(AD),由数据采集和警告接收模块产生,是 CC 的索引; Reasoning Conclusion, 推理结论(RC); Correction Method, 校正方法(CM); Agent ID, 代理 ID. CC 搜索引擎为告警收集模块产生的 AV 和 AD 查找精确匹配的事例,而不是进行推理,它是 DIP 的基础.

3 管理中心

AFMDIP 管理中心的主要职责包括下面几点:

利用代理汇报的 AV 和 AD 进行推理,采用基于事例的推理(CBR)确切定位故障^[81]; 根据事例数据库或者人工干预获得故障的纠正措施; 故障诊断和纠正的推理结果会被存入事例库,同时传送给提交故障的代理,并在事例数据库中标识哪些代理事例暂存库获得了这个事例; 提供给网络管理人员一个友好的操作界面,同时给专家干预系统提供

智能决策的基本途径.

管理中心的体系结构如图 4 所示,在 AFMDIP 中之所以采用 CBR 技术,是因为与专家系统相比它有几个特点:利用类比可以处理新的事例,例如网络拓扑的变化;新事例的加入使系统学到新的知识;通过事例整合,适用于拥有大量知识的领域;无需大量的维护;可根据以前的事例或者模拟对做出的解决方案进行评价;知识获取比专家系统的规则建立过程要节省时间.

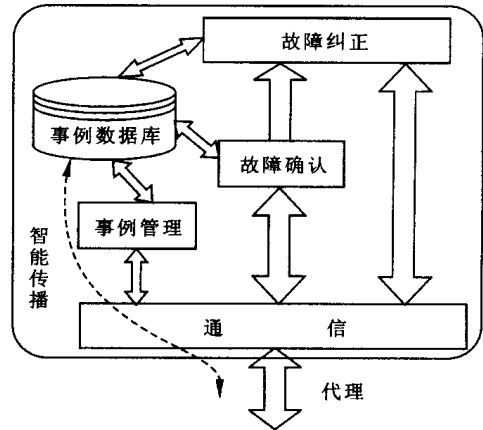


图 4 AFMDIP 的管理中心

4 分布智能传播(DIP)

各个代理在物理上是分离的,但在故障管理方面是一个有联系的有机整体,它们的纽带就是 DIP. AV 和 AD 的采集由代理完成,推理则由管理中心完成,生成的 RC 与 CM 则通过通信模块转交给提交 AV 和 AD 的代理,该事例被存入事例暂存库以备查训,且位于传送路径上的各级代理均获得了该事例.

下面定义了 DIP 操作原语.

(1) Case-Request: 第 n 层代理向第 $n - 1$ 层代理提出事例推理请求,当 $n = 1$ 的时候,请求目标为管理中心请求内容包含一个事例和相应的请求序列号,事例中 AV 和 AD 包含收集到的信息,RC 和 CM 为空,Agent ID 为本代理的标识符.

(2) Case-Response: 管理中心或 $n - 1$ 层代理向第 n 层代理发送事例推理结果,结果包含事例和相应的请求序列号,此时事例的 RC 和 CM 有效.

(3) Test-Request: 在推理过程中需要代理配合进一步取得管理域的数据的时候,管理中心向代理发送测试需求,包含测试的内容和一个测试序列号.

(4) Test-Response: 代理对管理中心测试请求的

回应,包含测试结果和测试序列号。

(5) Case-Cache-Request: 代理向本地 CC 请求精确匹配的事例,发送的数据包包含事例和请求序列号,事例中 AV 和 AD 包含收集到的信息,RC 和 CM 为空。

(6) Case-Cache-Response: CC 向代理报告搜索情况,在报告的事例中如果 RC 和 CM 有效,则说明找到了匹配的事例;如果无效,则说明未能找到。

(7) Case-Cache-Update: 代理收到 Case-Response,根据事例内容,向代理本地 CC 发送指令,并更新暂存库。

下面将根据原语定义来定义 DIP 的基本流程。

首先, n 级代理根据收集到的数据和告警进行告警过滤和关联,CC 搜索引擎向 CC 发送 Case-Cache-Request。CC 进行匹配后向代理发送 Case-Cache-Response,如果事例搜索成功,则将 RC 和 CM 用于故障的纠正;否则,代理向上 $n-1$ 级代理发送 Case-Request。 $n-1$ 级代理的 CC 搜索引擎发送 Case-Cache-Request,重复 n 级代理的操作。依次类推,直到 $n=0$,事例被提交给管理中心,管理中心进行 CBR。过程中如果需要进一步的数据查询,管理中心直接向提交事例的 n 级代理发出 Test-Request,代理以 Test-Response 回应。管理中心完成推理后,沿着事例提交路径将结论发送给各级代理, n 级代理执行事例的 CM,其余的各级代理将事例通过 Case-Cache-Update 送入本地 CC。

假定 A 、 B 两个 n 级代理都属于 $n-m$ 级代理 ($m < n$) 管理域,则 A 进行了事例 a 的智能扩散后,如果 B 遇到同样问题,则在 $n-m$ 级代理处获得事例的处理方案,而不是完全依靠管理中心。在减少了管理中心的压力的同时,事例的学习过程也贯穿在整个分布系统之中,达到事例的共享目的。

5 故障管理系统的应用

实验中,AFMDIP 在管理中心下采用 4 个代理,连接逻辑方式如图 1 所示,均用 100 Mb/s 以太网接入网络,每个代理负责管理一个子域,含一个 C 段地址。网络故障告警接收采用主动测试和接收 Trap 两种,设定的告警主动测试目标包括域内主机是否启动,Web、Ftp 和 DNS 服务器是否正常工作,以及沿途路由器的状态。系统采用两种工作方式,第 1 种是本文提出的 AFMDIP 系统,另外一种是采用单一管理中心进行故障诊断,所有的告警接收和故障诊断均由管理中心负责。图 5 给出的是两种系统

管理中心在 24 h 中的带宽占用情况。从图中可以看出,AFMDIP 系统的管理中心带宽消耗一直维持在 10 Mb 以下;在单一管理中心的情况下,带宽消耗则在 30 ~ 45 Mb 范围内波动,基本达到了 PC 机网络速度的极限。管理中心带宽消耗反映了其直接负责处理事务的多少,单一管理中心由于负责了故障的收集和所有的诊断工作,因此消耗了大量带宽。CPU 也忙于处理大量的网络数据,用于故障诊断计算的时间必然受到影响。图 6 为两种系统故障诊断耗时的对比图。可见,在并发故障较少的情况下,AFMDIP 比单一管理中心花在系统故障诊断的时间要多,这是由于 AFMDIP 系统在智能传播和事例库维护上要消耗时间;在网络规模扩大而并发故障增加后,由于故障事例在代理中的缓存以及代理对故障的事先判断起到显著作用,AFMDIP 系统的故障诊断时间就显著低于单一管理中心的。

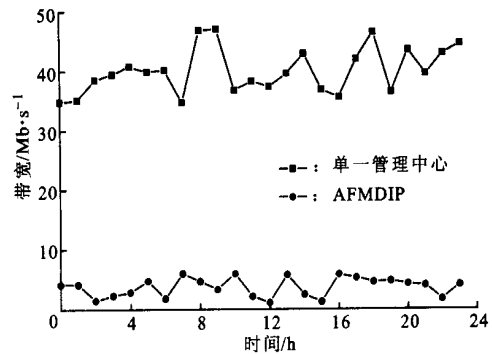


图 5 带宽消耗

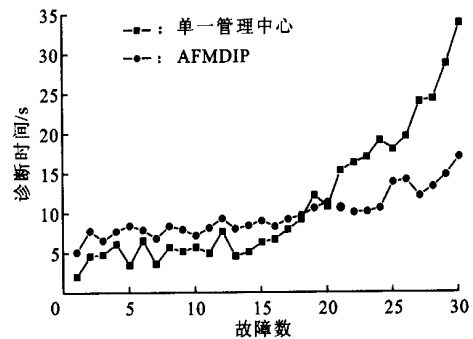


图 6 故障诊断时间

6 结论

神经网络和 CBR 是两种各有特点的人工智能技术,单独将其应用在网络故障管理当中都有很多的缺点。综合两者的优点,利用 DIP 技术,可充分发

(下转第 148 页)

速度为 29.4 m/s^2 、脉宽为 10 ms 的方波冲击脉冲,系统得到的控制波形.可以看出,基于自适应逆控制的冲击振动控制在控制信号的低频能力上有很大的改进,冲击波形的光滑度明显提高,波形的起伏由频域自调整算法的 0.4 m/s^2 下降到约 0.2 m/s^2 ,由吉卜斯现象引起的波形振荡明显减弱.在矩形波的高电平由原来的 0.3 m/s^2 下降到约 0.05 m/s^2 ,说明了快速批处理 X 滤波 LMS 算法在冲击振动控制中提高了冲击波形的控制精度.

3 总 结

基于自适应逆控制的冲击振动控制是一种全新的控制方法,本文提出了一种基于快速批处理 X 滤波 LMS 算法的冲击振动自适应逆控制算法.该算法能够根据不同的负载特性自适应地调节逆控制器参数,其收敛过程对输入信号的自相关矩阵依赖小.试验表明,该方法实时性好,收敛速度快,与传统的频域自调整冲击振动控制方法相比,克服了易产生

溢出等问题,改善了系统的低频响应,冲击波形的波动降低了约 50% ,提高了冲击波形的控制精度.

参考文献:

- [1] Page M. Signal processing for vibration control [A]. IEE Colloquium on DSP in Instrumentation, London, 1992.
- [2] Widrow B, Walach E. 自适应逆控制[M]. 刘树棠, 韩崇昭, 译. 西安:西安交通大学出版社,2000.
- [3] Shynk J. Frequency-domain and multirate adaptive filtering [J]. IEEE Transactions on Signal Processing, 1992, 9(1): 14~37.
- [4] Boroujeny F B, Chan K S. Analysis of the frequency-domain block LMS algorithm [J]. IEEE Transactions on Signal Processing, 2000, 48(8): 2 332~2 342.
- [5] Haykin S. Adaptive filter theory [M]. 4th ed. Upper Saddle River, NJ: Prentice-Hall, 2002. 320~366.

(编辑 刘 杨)

(上接第 118 页)

挥神经网络在模式识别方面及 CBR 在事例推理方面的能力,并取得了满意的效果.在 AFMDIP 体系结构下,后续的研究集中在:利用神经网络解决代理内的告警关联、数据采集内容和手段等问题;DIP 在各级代理与管理中心之间的安全高效通信问题;利用 CBR 在管理中心进行故障诊断和事例表达的通用化问题.

参考文献:

- [1] Baras J S. Automated network fault management [A]. Proceedings of the 1997 MILCOM Conference [C]. Monterey, USA: IEEE, 1997. 1 244~1 250.
- [2] Patton R J, Chen J, Siew T M. Fault diagnosis in nonlinear dynamic systems via neural networks[A]. Proceedings of the International Conference on CONTROL [C]. Coventry, UK: IEE, 1994. 1 346~1 351.
- [3] Guerer D W, Khan I, Ogler R, et al. An artificial intelligence approach to network fault management [EB/OL]. <http://citeseer.nj.nec.com/105695.html>, 2003-02-01
- [4] Russell P N S. Artificial intelligence: A modern approach

[M]. Upper Saddle River, New Jersey: Prentice-Hall, 1995.

- [5] Yong Z. Research on the key technologies of distributed cooperative network operation management architecture [D]. Xi'an: School of Electronics and Information Engineering, Xi'an Jiaotong University, 2002.
- [6] Jacobson V. Pathchar: A tool to infer characteristics of Internet paths [EB/OL]. <http://lists.debian.org/debian-user/1997,2003-02-20>.
- [7] Dovrolis C, Ramanathan P, Moore D. What do packet dispersion techniques measure? [A]. 20th Annual Joint Conference of the IEEE Computer and Communications Societies [C]. Anchorage, AK, USA: IEEE, 2001. 905~914.
- [8] Lewis L. Case-based reasoning approach to the management of faults in communications networks[A]. Proceedings of the 12th Annual Joint Conference of the IEEE Computer and Communications Societies [C]. San Francisco: IEEE, 1993. 1 422~1 429.

(编辑 苗 凌)