基于 FTA 和比较模型的网络故障诊断算法

朱云鹏,陈 卓
ZHU Yun-peng,CHEN Zhuo

合肥电子工程学院 网络工程系,合肥 230037
Network Engineering Department,Electronic Engineering Institute,Hefei 230037,China
E-mail:qianlima714@tom.com

ZHU Yun-peng,CHEN Zhuo.Network fault diagnosis algorithm based on FTA and comparison model.Computer Engineering and Applications,2009,45(24):106-109.

Abstract: Aiming at the characteristic of network fault,MM* model and Fault Tree Analysis (FTA) are introduced into network fault diagnosis modeling.An algorithm is proposed which analyzes and diagnoses network fault,extracts the minimum cut sets quantificationally with Fault Tree Analysis,then detects and orients network fault with MM* model by testing the geminate nodes selected from minimum cut sets.The experimental results show that the method enhances efficiency and veracity of network fault diagnosis efficaciously.

Key words: network fault;fault diagnosis;Fault Tree Analysis(FTA);the minimum cut sets;comparison model(MM* model)

摘 要:针对网络故障特点,将 MM* 模型和 FTA 方法引入网络故障诊断建模中,设计了一种用 FTA 方法进行网络故障的系统分析与诊断,并定量求解出所有故障可能的最小割集,然后用 MM* 模型从最小割集中选取测试点对进行单点故障检测与定位的网络故障诊断算法。实验结果表明,该算法有效提高了网络故障诊断的效率和准确率,具有较好的实用性。

关键词:网络故障;故障诊断;故障树分析法;最小割集;比较模型(MM* 模型)
DOI:10.3778/j.issn.1002-8331.2009.24.032 **文章编号:**1002-8331(2009)24-0106-04 **文献标识码:**A **中图分类号:**TP393.02

1 引言

网络故障诊断以网络原理、网络配置和网络运行的知识为基础,从网络的故障现象出发,根据特定的故障检测与定位算法获取故障的详细信息并告警显示。网络故障诊断技术为网络系统正常运行提供了基本保证,是伴随着网络的可靠性、安全性的发展而发展起来的一门学科,它的出现、兴起与迅速发展,是实际应用需求与多学科理论发展共同作用的结果[1-2]。

我国计算机网络故障诊断水平相对落后,虽然在故障诊断专家系统方面开展了一定的研究,但专门针对网络故障智能诊断技术的研究还刚刚开始。国外的网络故障诊断技术正从初级向高级、从不完善向完善、从分散向集中的目标发展。一个由国际科学应用公司(SAIC)领导的小组获得美国陆军的通信/电子司令部资助,为美国国防部设计、开发和装备"联合网络管理系统"(JNMS)提供先进的故障诊断技术和保障,并提供技术支持训练、测试、保障及软件维护,预计在 2008 年 10 月前该系统正式运行。

网络故障诊断的技术难点主要包括:网络故障模型建立、网络故障关联与传播、网络故障检测与定位、网络故障表示等问题。近年来,随着网络技术与多种学科理论的融合发展,网络故障诊断技术逐步向标准化、集中式、智能化、可扩展性的方向发展[3-4]。针对网络结构和网络故障的特点,将 MM* 模型和 FTA 方法引入网络故障建模中,设计了一种用网络故障树进行 FTA 系统诊断,找出故障原因的最小集合,然后用 MM* 模型进行单点故障检测与定位的网络故障诊断算法。实验证明,该方法有效提高了网络故障诊断的效率和准确率。

2 基于 FTA 的网络故障 MM* 诊断技术

2.1 FTA 网络故障建模

故障树分析法(Fault Tree Analysis,FTA)是系统可靠性和安全分析的一种技术[5]。它采用逻辑的方法进行定性和定量分析,通过树形分支结构从故障结果开始,由顶向下寻找出所有可能导致故障的原因。FTA 把系统不希望发生的故障状态定义为"顶事件",通过分析寻找出导致顶事件故障发生的所有可能的直接原因,称为"原因事件"。接着分析寻找每一个原因事件发生的所有可能原因,以此类推,直至追踪到最后一级基本事件,也即"底事件"。各个基本事件由 AND、OR 等逻辑门连接接入上一级原因事件。

可以根据网络的拓扑结构,将网络划分成分层树形结构(如图 1),然后建立网络故障的 FTA 模型(如图 2)。

网络故障树构造步骤如下:

步骤 1 基于网络拓扑图构建网络的分层树形结构,每层包括设备、本层设备间的链路以及本层与上一层相连的链路;

步骤 2 将网络系统故障作为顶事件,逐级向下寻找原因事件直至底事件;

作者简介:朱云鹏(1978-),男,硕士,主要研究方向:网络安全。
收稿日期:2008-05-07 **修回日期:**2008-08-07

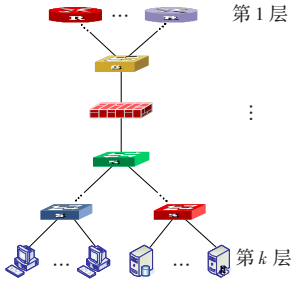


图 1　网络的分层树形结构

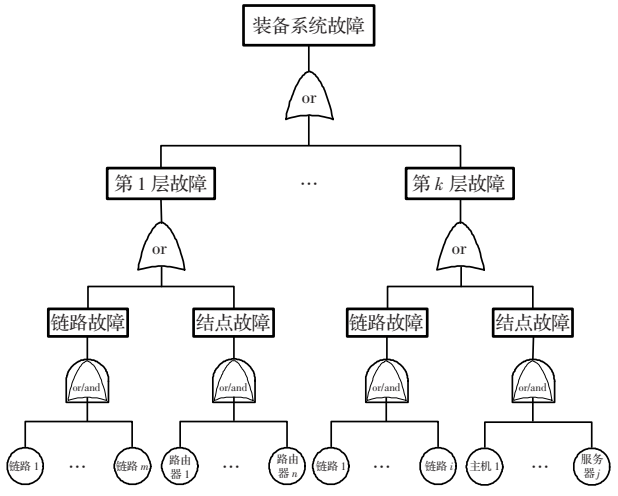


图 2　网络故障 FTA 模型

步骤 3　确定上、下级原因事件之间的连接逻辑门。若导致本级原因事件的下一级原因事件相互是串联关系，采用与门(and)连接。若是并联关系则用或门(or)连接。

为进一步对系统进行定性和定量分析,必须求解全体最小割集。割集是导致系统失效的最小的组元集合。最小割集的组合对应了系统故障的所有可能基本原因的组合。

求解最小割集的基本步骤如下:

步骤 1　从顶事件逐级向下，根据每个交叉点不同的逻辑关系,若是或门则将其每个输入事件列入不同的行,若是与门则将其输入事件列入同一行,以此类推,直至不可再分的底事件为止。所得的各个集合为故障树的割集。

步骤 2　将故障树表达的逻辑关系表示成结构函数的形式,再运用布尔代数规则中的吸收率($A+AB=A$)和分配律($A+(B+C)=AB+AC$)将结构函数等价变换,得到最小割集的组合。

根据上述步骤，求解网络故障树的最小割集的算法描述如下:

```
CutsetArray set;      //定义最小割集序列
int index;            //当前最小割集的索引
for(i=0;i<最大深度;i++)
{
for(j=0;j<第 i 层的结点数量;j++)
{
   if(结点 j 是与门)
   {
     for(k=0;k<当前结点的子结点数;k++)
        set[index]+=子结点数据;
   }
   else if(结点 j 是或门)
   {
     delete set[index] ;
     for(k=0;k<当前结点的子结点数;k++)
       {
        Cutset tmp=子结点数据;
        set.Add(tmp);
       }
   }
  if (结点 j 是底事件)
    continue;
 }
}
```

假定图 2 的 FTA 模型中连接逻辑门已确定,T_0 表示顶事件,I、L、N 表示原因事件,l 为链路,R 为路由器,h 为席位主机,S 为服务器,则图 2 可抽象成图 3 故障树简图。

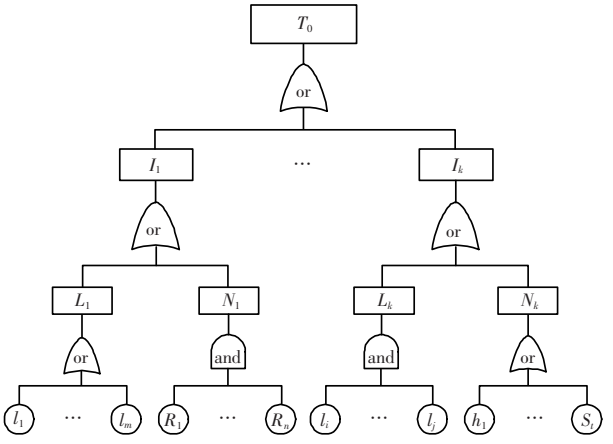
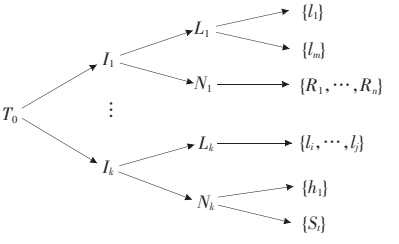


图 3　故障树的符号简图

根据求解最小割集的算法对故障树进行结构处理:



整理并化简得结构函数:$T_0=l_1+l_m+R_1\cdots R_n+\cdots+l_i\cdots l_j+h_1+S_t$。

故障树的最小割集为:$K_1=\{l_1\}$,$K_2=\{l_m\}$,$K_3=\{R_1,\cdots,R_n\}$,$\cdots$,$K_{n-2}=\{l_i,\cdots,l_j\}$,$K_{n-1}=\{h_1\}$,$K_n=\{S_t\}$。由此可得,最小割集是网络中可能导致故障的网络元素的最小集合。下一步用网络故障的 MM* 诊断模型进行单点故障定位时，比较测试的结点将从最小割集中选取,或者根据求解结构函数的结构树从叶子结点向根结点方向依次组合选取。

2.2　网络故障 MM* 诊断建模

MM* 是一种基于比较的故障诊断模型[6],MM* 模型通过给一对处理器$\{u,v\}$发送相同的测试任务然后比较它们的响应以此进行故障诊断,这种比较是由与 u 和 v 相连的第三个处理器 w 来执行的,w 被称为 u 和 v 的比较器。MM* 模型将网络中的结点视为处理器,每个结点都可以作为与它直接相连的任意两个结点的比较器,通过比较和分析对两个直接相连的结点的测试结果便可诊断出故障结点。

2.2.1　基本理论

把计算机网络看作一个图,网络中各个设备(如:终端主机

和路由器、交换机、防火墙、IDS 等网络设备)作为图中的结点,各设备之间的连接路径作为图的边。图 $G=(V,E)$指两个集合 V、E,集合 V 称为图的顶点集,往往被用来代表实际系统中的个体,集合 E 被称为图的边集,多用于表示实际系统中个体之间的关系或相互作用。若$\{x,y\}\in E$,就称图 G 中有一条从 x 到 y 的弧(有向边),记为 $x\rightarrow y$,其中顶点 x 叫做弧的起点,顶点 y 叫做弧的终点。记 G 中顶点数为 $v(G)=|V|$,边数为 $\varepsilon(G)=|E|$,分别叫做图 G 的阶和规模,显然有 $\varepsilon(G)\leqslant v(G)(v(G)-1)$。

比较模型[7-8]可表示为一个加权图 $M=(V,C)$,其中 V 为结点集,C 为加权边的集合。如果边$(u,v)_w\in C$,则边上的权为 w,表示比较器 w 对处理器 u、v 进行比较,比较结果表示为 $r((u,v)_w)$。其中,若 u 和 v 的结果一致,则 $r((u,v)_w)=0$,否则 $r((u,v)_w)=1$。比较结果的汇总称为症候,记为 r。

2.2.2 模型建立

在 MM* 模型中,满足$(w,u)\in E$ 以及$(w,v)\in E$ 的结点 w 都可以作为 u、v 的比较器,因此一对结点的比较器可以有多个。考虑到网络故障的特性和网络测试必须有链路保障,首先作以下基本假设:

(1)相对于瞬时故障,在一定时间域内网络中所有故障都是永久故障;

(2)能接收到测试任务的故障结点能对测试任务作出响应;

(3)对于两个故障结点,相同的输入不会产生相同的输出;

(4)无故障结点总能给出正确比较,而故障结点给出的比较结果不可信。

由此,MM* 模型描述的可能的故障情况如表 1 所示:

表 1 MM* 模型中 u、v、w 的状态

被测结点 u 和 v 的状态	比较器 w 的状态	$r((u,v)_w)$
均无故障	无故障	0
至少一个有故障	无故障	1
任何情况	有故障	0 或 1

令结点状态正常时为 0,故障时为 1,则由比较结果推断结点状态的算法如下:

```
if (r((u,v)w)=0)
        {
        if (w=0) then u=0 and v=0;
        else if(w=1) then u=1 or v=1;
        }
else if(r((u,v)w)=1)
        {
        if (w=0) then u=1 or v=1;
        else if(w=1) then u=0/1,v=0/1;
        }
```

当 $r((u,v)_w)=1$,$w=1$ 时,u、v 的状态之所以存在多种可能是因为比较器 w 本身可能有故障,w 状态的不确定增加了故障诊断的复杂度。对 MM* 模型进行优化,将接入的诊断结点机作为固定、唯一的比较器 w,且 w 的状态为正常。这样,无须考虑 w 的状态,则表 1 可简化为表 2:

表 2 由比较结果推断 u、v 的状态

$r((u,v)_w)$	被测结点 u 和 v 的状态
0	均无故障
1	至少一个有故障

由此,算法可简化为:

```
if (r((u,v)w)=0) then u=0 and v=0;
else if(r((u,v)w)=1) then u=1 or v=1
```

因为网络元素很多,盲目选取测试点将严重影响故障诊断的效率。所以,直接用 FTA 方法求解出的可能导致网络故障的最小测试点集合中选择合适的测试对象 u 和 v,将减少比较测试的次数,有效提高诊断的效率。

2.3 故障测试与定位

FTA 模型求出网络故障树的最小割集,再用 MM* 模型从最小割集中选取测试点进行比较测试。网络测量方面的研究提供了很多有效的测试手段,较为实用的是 Windows 操作系统下的 Ping 和 Tracert 命令。

Ping 命令是一个测试程序,在检查网络故障中广泛使用。使用 Ping 命令来查找问题所在或检验网络运行情况时,如果执行 Ping 成功,则大体上就可以排除网络访问层、网卡、MODEM 的输入输出线路、电缆和路由器等存在的故障,减小了故障可能的范围;如果执行 Ping 成功而网络仍无法使用,那么问题很可能出在网络系统的软件配置方面;若执行 Ping 不成功,则故障可能是网络链路不通、网络适配器配置不正确或 IP 地址不可用等。

Tracert 将包含不同生存时间(TTL)值的 Internet 控制消息协议(ICMP)回显数据包发送到目标,以测试到达目标采用的路由。Tracert 诊断程序要求每个路由器在转发数据包之前将数据包上的 TTL 值递减 1,当数据包上的 TTL 到达 0 时,路由器应该将“ICMP 已超时”的消息发送回源系统。Tracert 先发送 TTL 为 1 的回显数据包,并在随后的每次发送过程将 TTL 递增 1,直到目标响应或 TTL 达到最大值,最后通过回送的“ICMP 已超时”的消息来确定路由。

故障检测与定位的流程如图 4 所示,其基本步骤如下:

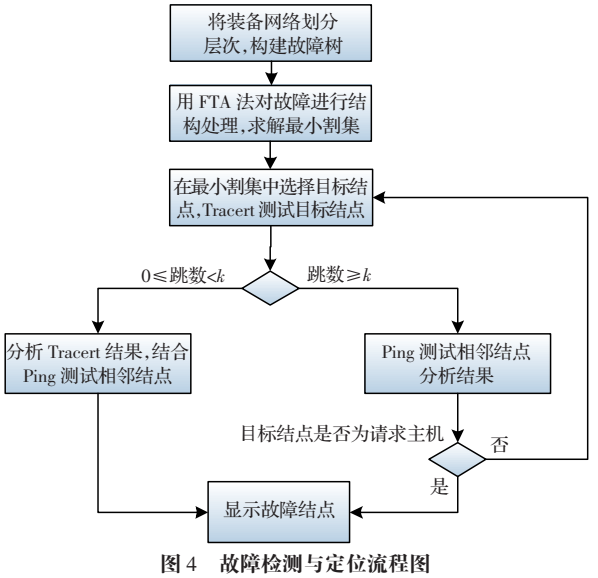


图 4 故障检测与定位流程图

步骤 1 将装备网络按其拓扑结构划分为 k 层,构建网络故障树;

步骤 2 用 FTA 方法对故障树进行结构处理,求解出最小割集作为 MM* 测试预选的网元结点对;

步骤 3 从最小割集中选择测试目标结点(一般为发出故障定位请求的主机或管理软件所在服务器),从该主机执行 Tracert 命令;

步骤 4 判断 Tracert 结果,如果跃点跳数$\geqslant k$ 则进入步骤

5,如果 0≤跃点跳数<k 则进入步骤 7;

步骤 5　Ping 测试目标结点的相邻结点,并分析故障原因;

步骤 6　判断目标结点是否为发出故障定位请求的主机,如果是则进入步骤 8,否则返回步骤 3;

步骤 7　分析 Tracert 中断原因,Ping 测试目标结点的相邻结点以及目标结点到 Tracert 中断那层的中间各结点,分析故障原因;

步骤 8　显示故障结点。

Tracert 和 Ping 命令被作为具体的测试手段集成到基于 FTA 的 MM* 诊断算法中,诊断程序对 Tracert 和 Ping 的测试结果进行分析,通过结果解析函数实现网络故障的最终定位。

3　实验与分析

3.1　实验方法及实验环境

实验中共选取三种故障诊断算法进行比对测试:(1)只用 Ping 和 Tracert 诊断;(2)基于 MM* 模型诊断;(3)基于 FTA 的 MM* 模型诊断。实验环境如图 5 所示,系统接入互联网的出口带宽为 100 M,装备网络带宽为 10 M。三种诊断方法定位出不同类型的网络故障所用的时间(单位:s)如表 3 所示。

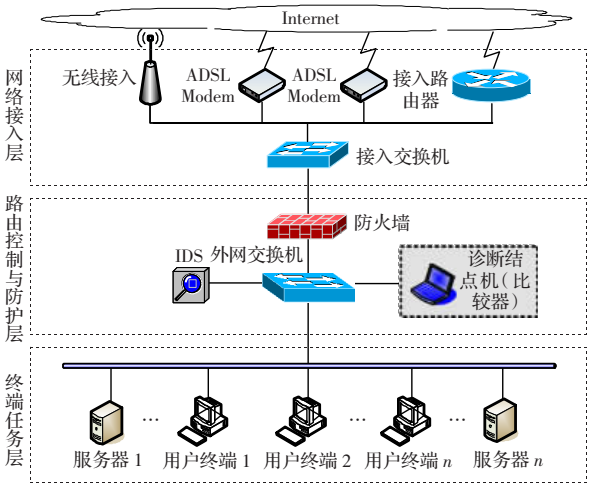


图 5　实验环境示意图

表 3　三种诊断方法定位故障所用时间统计　　s

定位的故障点	只用 Ping 和 Tracert 诊断	基于 MM* 模型诊断	基于 FTA 的 MM* 诊断
定位到链路故障	8	3	1
定位到主机故障	36	20	10
定位到交换机故障	46	25	12
定位到防火墙故障	60	28	15
定位到路由器故障	56	30	20
定为无故障	120	80	50

3.2　实验结果及数据分析

对图 6 中三种故障诊断算法的时间性能曲线进行比较分析:算法 1 只用 Ping 和 Tracert 进行故障诊断,耗时最长;算法 2 将接入的诊断结点机作为比较器,采用 MM* 模型选择不同

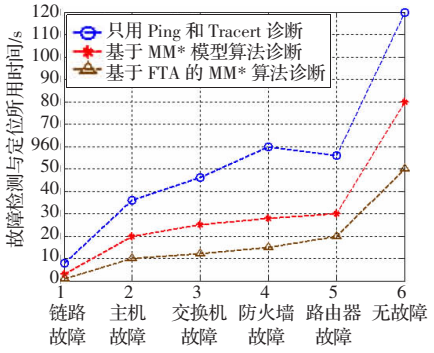


图 6　三种故障诊断算法的时间性能比较曲线

的结点对,然后结合 Ping 和 Tracert 进行比较测试,较算法 1 减少了故障诊断时间,但由于结点对的选择没有针对性,存在无用的比对测试,响影了诊断效率;算法 3 首先用 FTA 方法找出所有可能故障的最小网元集合,再从中筛选出结点对采用优化的 MM* 模型进行比较测试,明显提高了故障诊断效率和单次故障诊断的准确率。

4　结束语

基于 FTA 的 MM* 诊断算法首先用 FTA 方法对装备网络作系统的可靠性和安全分析,将网络按照树形结构进行分层,然后根据分层结构构建网络故障树,采用逻辑的方法定量计算,求解最小的可能导致故障的网元集合,为 MM* 模型提供比较测试的结点。MM* 模型是一种优化的具有实用价值的比较诊断模型,可以提供多项式时间的算法来判定故障结点。该文将接入的诊断结点机作为比较器,直接选取经 FTA 方法求解的最小割集中的网元进行比较测试,消除了测试过程中选取结点机的盲目性和随意性,大大提高了诊断效率和诊断准确度。诊断程序通过对集成的 Tracert 和 Ping 等测试结果的分析,实现网络故障的精确定位。通过实验和测试,证明该算法能有效提高网络故障诊断效率,具有较强的实用性。

参考文献:

[1] 方耿.网络维护与故障诊断[M].北京:冶金工业出版社,2004.

[2] 王道平,张义忠.故障智能诊断系统的理论与方法[M].北京:冶金工业出版社,2001.

[3] 李千目,戚湧,张宏,等.基于粗糙集神经网络的网络故障诊断新方法[J].计算机研究与发展,2004,11(10).

[4] 曾声奎,Pecht M G,吴际.故障预测与健康管理(PHM)技术的现状与发展[J].航空学报,2005(5).

[5] 郑明.计算机系统脆弱性评估方法研究[D].哈尔滨:哈尔滨工业大学,2005.

[6] 陈蜀宇.系统级网络故障诊断研究[D].重庆:重庆大学,2000.

[7] 彭宇,洪炳熔,乔永强.基于通用比较模型的 t-可诊断系统的特征化及并行诊断算法[J].计算机学报,2000,23(7):126-133.

[8] 阳惠,杨小帆.在 MM* 比较模型下 Möbius 立方体的一个快速诊断算法[J].计算机学报,2007,30(7):1126-1131.