Journal of Computer Applications
计算机应用,2016,36(S1):49-53
ISSN 1001-9081
CODEN JYIIDU
2016-06-10
http://www.joca.cn

文章编号:1001-9081(2016)S1-0049-05

基于告警日志的网络故障预测

钟 将[1],时待吾[2*],王振华[2]

(1.信息物理社会可信服务计算教育部重点实验室(重庆大学),重庆 400030; 2.重庆大学 计算机学院,重庆 400030)

(*通信作者电子邮箱 shidaiwu@cqu.edu.cn)

摘 要:收集整理某城域网络14个月的网络告警日志作为网络故障预测研究的数据集并提出一种基于告警日志的网络故障预测研究方法:首先以基于两级时间窗口的特征提取方法构建特征表征网络运行状态,并通过大量实验来选择构建特征所需的最佳参数组合,然后设计并实现了一种基于分类学习方法的自适应故障预测模型。大量的数据实验表明:对于整个网络未来6小时是否出现故障的预测准确率可以达到70%以上,明显好于基于威布尔分布的预测模型;在对网络设备故障进行预测时,分类预测的结果仍然优于基于威布尔分布的预测模型。初步研究结果表明,网络中大部分故障可通过网络运行日志数据进行预测,证明该方法具有较好的预测效果。

关键词:网络故障;网络设备;故障预测;分类预测;威布尔分布;特征构建

中图分类号:TP306.3 **文献标志码**:A

Network failure prediction based on alarm log

ZHONG Jiang[1], SHI Daiwu[2*], WANG Zhenhua[2]

(1. *Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education (Chongqing University), Chongqing* 400030, *China*; 2. *College of Computer Science, Chongqing University, Chongqing* 400030, *China*)

Abstract: This paper researched the network failure prediction upon 14 months' network alarm logs collected from a metropolitan area network. The research method is shown as below: firstly, construct features to represent network characteristics by the means of the feature construction method which is based on two levels time windows; secondly, select optimal parameter combination to create the feature files through multiple experiments; thirdly, design and build adaptive failure prediction model according to classification learning methods. Numbers of experiments show that the accuracy of predicting whether the network failure takes place in 6 hours is up to 70%, is better than the prediction result of Weibull distribution model obviously; the results of classification prediction for network equipment failure are slightly better than Weibull distribution model. Preliminary research results show that most network failures can be predicted through analyzing previous network running logs and the method proposed in this paper is verified to be with good prediction effect.

Key words: network failure; network equipment; failure prediction; classification prediction; Weibull distribution; feature construction

0 引言

随着计算机网络的普及应用,越来越多的设备接入网络,网络结构日趋复杂,难以避免各种网络故障。但在某些诸如火箭发射、军事演习等特殊应用环境,网络故障可能导致重要信息丢失甚至任务失败,造成难以预料的损失。为此,在执行关键任务前对网络状态进行评估并预测任务期间发生故障的可能性具有一定的研究意义和实用价值。

故障预测是根据系统中历史状态演变及当前的行为进行分析,从而判断是否会发生故障。故障预测研究,对于减轻网络管理和维护的负担、降低网络故障的损失具有重要意义[1]。针对信息系统的故障预测根据分析对象不同分为基于故障日志数据的预测和基于状态数据的故障预测[2]。基于故障日志数据预测的基本思想是收集系统中失效的故障日志数据,运用数据挖掘或者机器学习方法来分析故障间的潜在关系,并利用这些关系进行故障预测。Liang等[3]基于IBM BlueGene-L中的日志数据,采用时间以及空间压缩预处理,根据各种告警事件的统计量来表征系统运行状态,进而建立故障预测模型。而基于状态监控预测的基本思想是某些系统故障的出现必然会导致系统中某些状态参数的变化,因此通过监控系统运行状态参数的变化来预测系统是否可能会失效。Vaidyanathan等[4]最早提出利用随机函数进行故障预测,构建了一个半回馈马尔可夫模型,通过系统负载数据来估计相关系统变量,以此预测系统中资源何时耗尽来预测系统故障。目前针对网络故障预测的系统性研究还较少,侯晓凯[5]提出了基于神经网络的网络设备故障预测方法,该方法基于网络设备运行状态数据来建立故障预测模型并进行一定的仿真实验,但并没有在大规模、真实的网络运行环境下验证该预测模型。

实际应用中,网络故障预测问题分为网络系统故障预测和网络设备故障预测两类。网络系统故障预测是指未来某个时段内整个网络中是否存在网络设备会发生故障。本文针对上述两类网络故障预测问题,研究真实网络环境中的告警日志,设计了基于数据挖掘的自适应预测模型。主要贡献如下:

1)针对目前网络故障预测研究缺少真实网络环境下的

收稿日期:2015-09-09;**修回日期**:2015-12-30。

基金项目:国家863计划项目(2015AA015308);中央高校基本科研业务费科研专项(CDJZR185502)。

作者简介:钟将(1974—),男,重庆人,教授,博士,CCF会员,主要研究方向:文本分析、数据挖掘、知识管理; 时待吾(1993—),男,安徽寿县人,硕士研究生,主要研究方向:数据挖掘; 王振华(1990—),男,河南林州人,硕士,主要研究方向:数据挖掘。

评估数据集,收集并整理了某城域网络14个月的告警日志,作为网络故障预测研究的评估与测试基础。

2)针对两类网络故障预测问题,分别设计了基于两级时间窗口的特征构建方法,并通过大量实验确定了故障预测特征构建中需要设定的关键参数经验值。

3)针对两类网络故障预测问题,提出了基于分类器的自适应网络故障预测模型,通过与传统概率预测模型比较表明分类预测模型具有更好的性能。

1 网络运行特征

1.1 网络及设备的运行状态

根据实际应用,网络设备的运行状态被划分为:正常运行状态、异常状态、故障状态、紧急故障状态。所谓的正常运行状态,是指网络设备运行正常,日志系统中会记录一些提示性消息。异常状态是指网络设备在运行过程中出现设备异常的状态,但这些设备异常可能不会影响设备和网络的正常运行。故障状态则是指网络设备出现一些故障,这些故障可能会对设备运行造成一定影响,但是不会导致全局性重大影响。紧急故障状态是指网络在运行过程中某台设备出现故障会导致全局性影响,需要立即处理,否则会导致核心任务失败。

网络的运行状态也可以根据网络中设备的运行状态被划分为正常运行、异常、故障和紧急故障四种状态,分别表示当前网络中所有设备都处于正常运行状态、存在处于异常状态的设备、存在处于故障状态的设备以及存在处于紧急故障状态的设备。

通过分析网络运行日志,我们发现:

1)网络设备的任意两种状态存在着相互转换的可能。

2)网络系统的任意两种状态存在着相互转换的可能。

其转换关系如图1所示。由于网络设备之间、不同故障之间相互作用的关系极其复杂,较长时间段的网络运行日志中可能包含了它们之间的依赖关系,但是难以利用领域专家的知识来精确地描述各种状态转换关系,因此本文采用数据挖掘的方法来建立针对网络设备和网络系统的紧急故障预测模型。

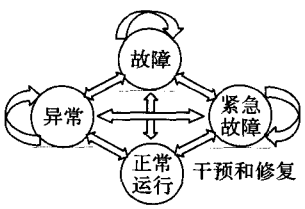

图1 网络及设备的运行状态和运行状态间的转换

1.2 网络告警日志特点

网络告警日志记录系统运行时设备的各种告警事件,包括发生告警事件的设备、告警名称、告警类型、告警级别、告警的发生时间和清除时间等信息。根据实际应用中告警事件的紧急程度,告警事件被划分为提示、次要、重要和紧急四个级别,分别对应着设备正常工作、存在异常、发生故障以及发生紧急故障四种状态。表1所示是部分网络告警日志记录的示例。

通过分析发现网络告警日志具有以下特点:

1)告警事件分为根源告警和衍生告警两大类,其中衍生告警是由根源告警引发的告警事件。

2)日志中存在大量的冗余告警记录以及大量的"闪断式"告警记录(系统短时间内自动修复并排除了该告警对应的故障)。

3)告警数量的分布具有一定的规律,故障告警事件的发生与时间具有较强的关联性,例如在工作时段发生的数量明显高于其他时段。

根据日志特点,数据的预处理过程分为三步:首先删除衍生告警,然后过滤清除间隔小于22 s的闪断式告警,最后采用基于时间间隔的过滤方法清除重复告警。其中提示、次要、重要、紧急级别告警的过滤时间阈值分别设置为15、4、3、2 min。通过采用上述过滤方法对原始的告警日志进行过滤,共过滤881 196条冗余告警记录,占原始告警记录的85%。

表1 告警日志记录数据示例

级别	告警名称	告警源	发生时间
提示	设备性能指标越限	设备36	2013-01-16T15:11:18
提示	设备性能指标越限	设备36	2013-01-16T15:11:18
次要	接口CRC校验错误	设备58	2013-01-16T15:11:20
重要	电源模块掉电	设备42	2013-01-16T15:11:27
紧急	链路断开	设备47	2013-01-16T15:11:30

1.3 网络告警分布

告警日志数据记录了每台网络设备产生的每个告警,图2是10月份每天所发生四种级别告警分布。

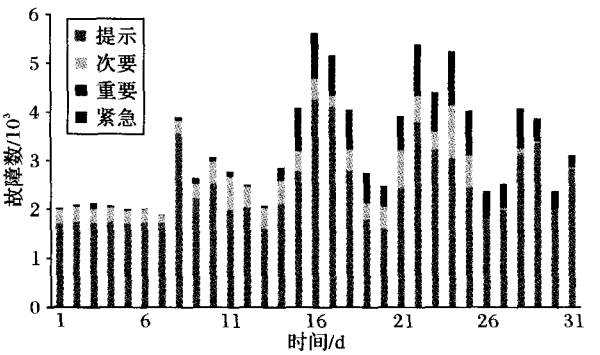

图2 10月份不同级别故障分布情况

分析告警日志记录可以发现网络运行时每天都会有不同设备发生不同级别的告警,因此可以统计某一时段的网络告警表征这一时段的网络运行状态,然后以这些统计数据构建特征集合建立预测模型。

2 基于数据挖掘的网络故障预测

本文采用与经典计算机系统故障预测方法相似的方法[6]预测网络故障,其根本思想是根据某一时刻之前一段时间的网络状态预测之后一段时间的故障发生情况,因此本文设计了如图3所示的预测系统。首先,收集网络设备的告警记录生成网络运行告警日志;其次,分析日志后过滤脏数据;然后,根据日志特点进行特征提取生成特征文件即训练数据集;之后选择分类器进行学习训练生成预测模型实现故障预测,最后根据系统反馈自适应地调整模型参数以达到更好的预测效果。

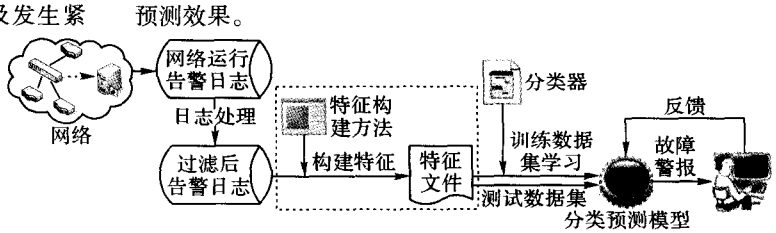

图3 网络故障预测系统

自适应的预测模型是网络故障预测系统的关键,而构建的特征是否能有效表征网络状态直接影响了模型的预测效果。所以,故障预测的关键在于网络特征的构建,也是本文的重点和创新点,最终分类器则根据不同的参数配置灵活选择。为了构建有效的决策特征以表征网络状态,本文设计了基于两级时间窗口的特征构建方法。

2.1　用于故障预测的时间窗口

本文使用两级时间窗口中各种告警事件的统计量描述网络运行特征,并以此作为故障预测的决策特征。假设当前时刻为 t,预测未来 Δ 时间内紧急故障的发生情况,定义三种时间窗口[7-8],三者的关系如图 4 所示。

定义 1　预测时间窗 W_p。是指$(t, t+\Delta]$的时段,故障预测即预测在 W_p 时段内出现的紧急故障。

定义 2　观测时间窗 W_o。是指时刻 t 之前的 n 个等长时间窗口,通常单位观测时间窗口的时长与预测时间窗口时长大小相等。

定义 3　样本时间窗 W_s。是指每个单位观测时间窗中包含 Δ/δ(可以被整除)个长度为 δ 的子时间窗。

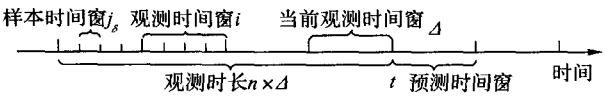

图 4　预测时间窗口、观测时间窗口和样本时间窗口的示意图

在使用分类方法进行网络故障预测时,需要数量化表示网络系统以及网络设备的运行特征。我们利用时间窗口中各种告警事件的统计特征来表示该时段内网络系统或者网络设备的运行特征,本文的预测模型基于这些统计特征建立。

2.2　针对网络系统故障的特征构建

在针对网络系统故障建立分类预测模型过程中,特征项的选取起着至关重要的作用。为了保障模型的预测效果,需要构建特征数据尽可能地准确表征网络运行状态。本文针对告警日志分析后发现:网络设备以及网络系统的任意两种状态间都存在着转换可能,则网络故障之间存在着一定程度的关联关系,表现在告警日志里告警事件之间的关联,所以统计每个观测窗口内各个级别、类型告警事件的数量作为第一类特征项。为了更精确地表示网络故障发生情况,统计每个样本窗口内各个级别、类型告警事件的数量作为第二类特征项。将所有样本窗口中各个级别、类型告警事件的统计分布特征即均值与方差作为第三类特征项。同时考虑到如果网络中长时间没有故障事件发生,那么即将发生故障事件的概率会比较大,因此提取当前时间窗口与上一故障时间窗口之间间隔的单位时间窗口个数作为第四类特征项。另外在日志分析中发现紧急告警的出现具有一定的时间相关性,所以本文选择预测时间窗口中点对应的时间(选取小时)作为第 5 类特征项。综上所述,在针对网络整体的故障预测模型提取特征时,定义了如表 2 所示的五类特征提取规则。根据以上定义的 5 类特征提取规则共提取 $113+37(n\Delta/\delta+1)$ 个特征项后运用特征筛选方法如信息增益度量对特征项进行筛选[9],降低特征空间的维度。

2.3　针对网络设备故障的特征构建

针对网络设备故障的预测是预测某一网络设备在预测时间窗口内是否会出现故障。在针对网络设备故障预测模型构建特征时,考虑到网络设备的任意两种状态间均存在着相互转换的可能性以及网络设备故障之间存在着一定程度的关联关系,这种关联关系同样表现为告警日志里告警事件之间的关联。因此,借鉴针对网络系统故障预测模型建立特征的思想,分别统计各时间窗口中每台设备不同级别、类型的告警数量(网络设备 87 台,告警级别 4 种,告警类型 32 种)作为特征项,得到的特征项如表 3。

表 2　针对网络系统故障预测模型的特征提取规则

特征类别	特征项	特征项数量
1	每个单位观测时间窗口内 4 个级别、33 种类型告警事件数量	$37n$
2	每个样本时间窗口内 4 个级别、33 种类型告警事件数量	$37n\Delta/\delta$
3	每个样本时间窗口内 4 个级别、33 种类型告警事件数量的均值与方差	37×2
4	当前时间窗口与上一故障时间窗口之间间隔的单位时间窗口的个数	1
5	预测时间窗口的中点对应的时间(选取小时)	1

表 3　针对网络设备故障预测模型的特征提取规则

特征类别	特征项	特征项数量
1	每个单位观测时间窗口内每台设备发生的 4 个级别、32 种类型告警事件数量	$87\times(32+4)\times n$
2	每个样本时间窗口内每台设备发生的 4 个级别、32 种类型告警事件数量	$87\times36\times(n\times\Delta/\delta)$
3	所有样本时间窗口中每台设备发生的 4 个级别、32 每种类型告警事件数量的均值和方差	$87\times(32+4)\times2$
4	每个设备上一次出现故障的时间窗口与当前时间窗口之间的单位时间窗口个数	87
5	预测时间窗口中点对应的时间(选取小时)	1

根据以上 5 类规则共提取 $9\,484+3\,132n(\Delta/\delta+1)$ 个特征项。

3　实验与性能评估

本文收集某城域网络 2013 年 1 月 10 日至 2014 年 3 月 11 日共 14 个月的网络设备告警日志作为预测研究的数据集(http://pan.baidu.com/s/1eRcSrPS)。首先,我们确定了预测模型的评价指标;然后,依据评价指标研究构建特征时的参数选择问题,确定了构建特征的参数;最后,展示了实验结果并给出分析。实验过程中,为了与分类预测模型进行对比,本文采用两参数威布尔分布理论[10]从概率统计的角度建立预测模型,通过最小二乘估计法对威布尔分布的两个参数进行估计,得到威布尔分布对应的失效概率密度函数等可靠性特征量,对网络设备进行可靠性分析实现网络设备故障预测、网络系统故障预测。

3.1　故障预测的评价指标

本文实验在对预测模型的预测效果进行对比评估时,主要采用了预测的准确率(Precision)、召回率(Recall)和 F- 值

(*F*-Measure)作为评价指标[2],这些指标的具体计算方式如式(1)~(3)所示:

$$\text{准确率} = \frac{\text{正确预测的故障数}}{\text{正确预测的故障数} + \text{非故障预测为故障数}} = \frac{TP}{(TP + FP)} \quad (1)$$

$$\text{召回率} = \frac{\text{正确预测的故障数}}{\text{正确预测的故障数} + \text{没有预测到的故障数}} = \frac{TP}{(TP + FN)} \quad (2)$$

$$F\text{-值} = \frac{2 \times \text{召回率} \times \text{准确率}}{\text{召回率} + \text{准确率}} = \frac{2 \times TP}{2 \times TP + FP + FN} \quad (3)$$

3.2 实验结果及分析

3.2.1 参数选择实验

在特征提取时,需要确定观测窗口数量和样本窗口大小两个参数,为此进行多组对比实验,如图5所示是使用Bayes Net算法进行故障预测时不同预测时间窗下准确率随观测窗口数量、样本窗口大小变化情况。

由图5可知:

1)预测未来一段时间内网络是否出现故障(预测时间窗已确定),样本窗口大小不变时,预测准确率随观测窗口数量的增加总体呈下降趋势;观测窗口数量不变时,预测准确率随样本窗口的增大总体呈上升趋势,但幅度不大。

2)样本窗口大小和观测窗口数量确定时,预测时间窗口越大,预测准确率越高。

针对网络设备故障预测进行实验分析(预测时间窗为6、12 h)同样得到上述结论。综合以上分析,在进行故障预测研究时,根据预测时间窗的大小确定观测窗口数量和样本窗口大小,观测窗口数量默认设置为1~3,样本窗口大小适中(一般取10~60 min)。

针对网络系统故障、网络设备故障特征提取时选择的样本窗口大小、观测窗口数量两个参数均如表4所示,本文中预测时间窗口大小分别为1 h、4 h、6 h、12 h。

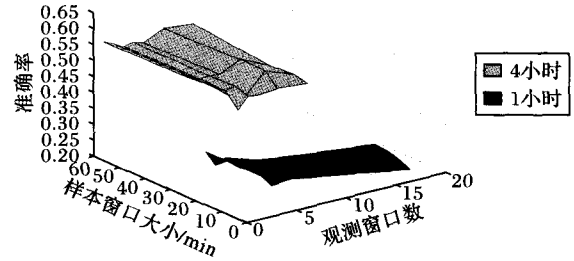

图5 准确率随观测窗口数量、样本窗口大小变化

表4 不同预测时间窗,样本时间窗大小与观测窗口数量参数设定

预测时间窗口 Δ/h	样本窗口大小 δ/min	观测窗口数量 n
1	10	3
4	40	2
6	60	1
12	90	1

3.2.2 针对网络系统故障的预测结果

本文分别选择RIPPER、Bayes Net和Random Forest[11]算法建立分类预测模型,依据3.2.1节所选定的观测时间窗口数量、样本窗口大小2个参数针对网络系统故障生成4个特征文件,每个数据集被分为用来训练和学习生成模型的训练数据集和用以测试模型性能的测试数据集,本次实验采用十轮交叉验证的方法,根据3.1节选定的预测评价指标对预测效果进行对比,基于分类预测的三种分类器和基于威布尔分布的结果对比如图6所示。

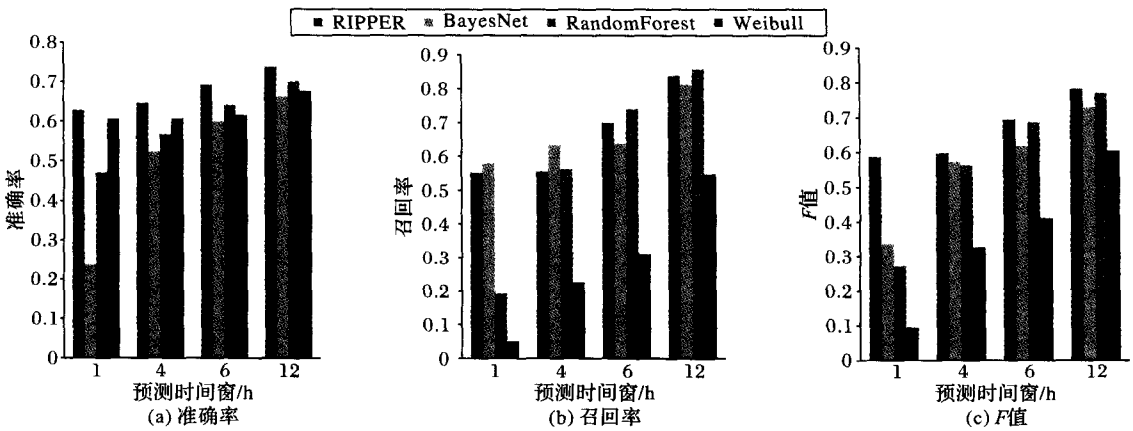

图6 网络系统故障预测模型在不同预测窗口下准确率、召回率、*F*值

实验表明:1)基于分类的预测模型具有更好的预测性能,说明分类预测方法比基于威布尔分布的传统预测方法更适合对网络系统故障进行预测。2)当预测时间窗口大于等于6 h的时候,故障预测模型具有更好的预测性能,准确率达到70%以上、召回率达到80%以上。3)三种分类算法中,RIPPER算法稳定性和性能总体更优。

3.2.3 针对网络设备故障的预测结果

某一设备发生故障次数越少,日志记录越少,分类预测效果越差。因此,实验过程中选择出现故障次数较多的设备83,出现次数较多的设备0作为预测对象,运用分类预测及概率统计的方法分别对这两台设备建立故障预测模型。

依据3.2.1节所选定的参数分别针对设备83、设备0的故障生成四个特征文件,根据3.1节选定的预测评价指标对预测效果进行对比,三种分类器和威布尔分布的结果对比分别如图7所示。

根据图7可以看出,基于概率统计的威布尔分布预测模型与分类预测模型的预测效果总体相当,说明不同设备的告警之间存在一定的独立性;相比分类预测模型,基于威布尔分布的预测模型的性能波动较大,说明基于分类的预测模型稳定性更好。

综上所述,在进行特征提取时若预测时间窗口较大,则观测窗口数量设置较小(一般设置为1~3),效果较好;样本窗口大小适中(一般取10~60 min),预测效果较好。针对网络系统故障的预测准确率可以达到70%以上,明显好于概率预

测模型,RIPPER 算法进行分类预测时总体效果最优;针对网络设备故障的预测效果不是很理想,那些与该设备无关的其他设备的告警数据作为特征,会干扰分类器的分类效果,针对故障较少的网络设备进行故障预测时,三种分类算法中 Bayes Net 更为合适,针对故障较多的网络设备进行故障预测时,Random Forest 算法更为合适。

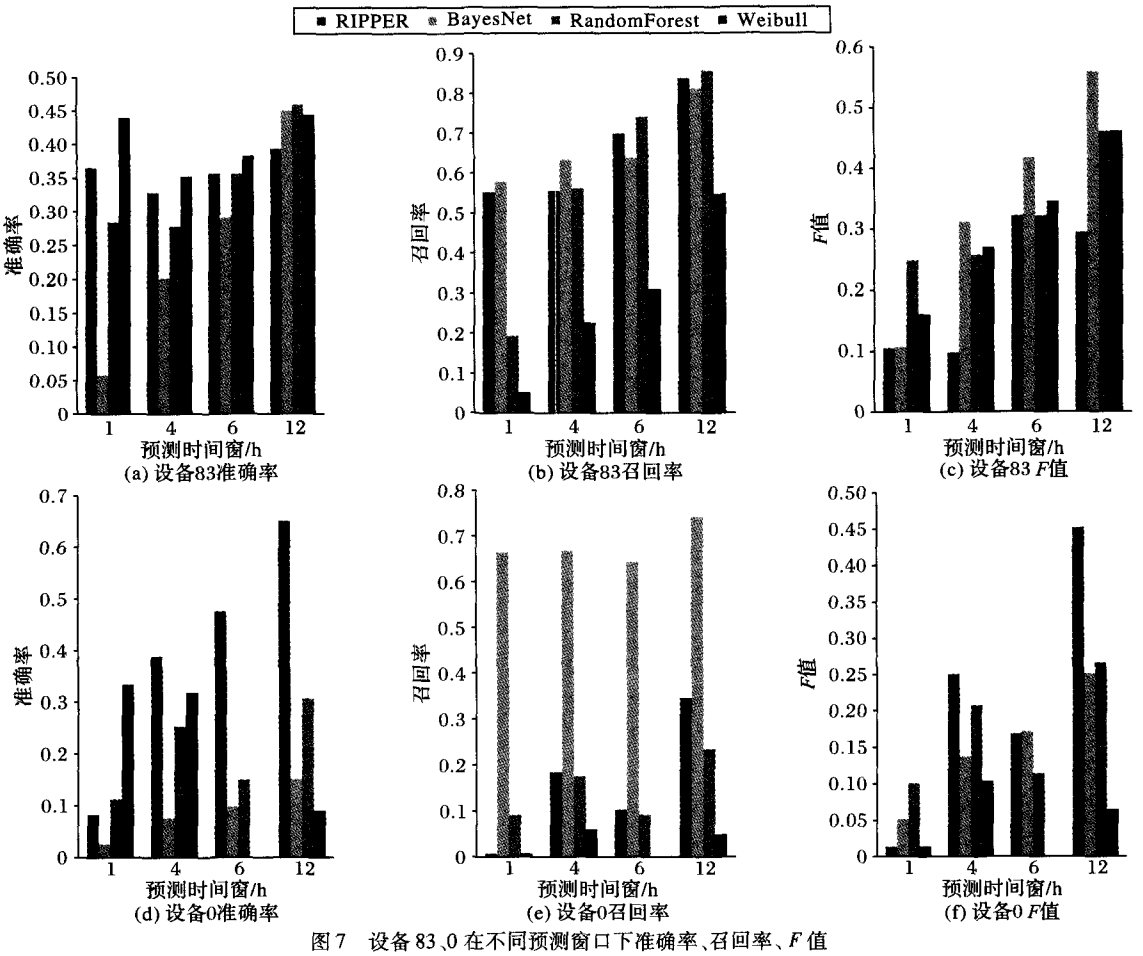

图 7　设备 83、0 在不同预测窗口下准确率、召回率、F 值

4　结语

本文通过分析网络运行告警日志,提出基于两级时间窗口的特征提取方法,设计并实现了基于分类的针对网络系统故障、网络设备故障的预测模型,故障预测的准确率高达 70% 以上,说明了网络设备以及网络系统的任意两种状态间都存在着相互转换的可能性,网络故障可以通过采用数据挖掘的方法分析处理网络运行日志进行有效预测;与基于威布尔分布的预测模型的对比实验的结果表明:不论是针对网络系统故障还是网络设备故障,基于分类的预测模型的性能总体上更优。

在未来的研究工作中,可以从以下几个方面进行改进:根据专家建议收集更加有效的告警类型数据,如设备 CPU 利用率、板卡温度等;结合网络设备的特点对特征提取的规则进行改进;采用类似 AdaBoost 的提升算法,通过组合多个不同的分类器来实现分类效果的改进。

参考文献:

[1] VICHARE N M, PECHT M G. Prognostics and health management of electronics[J]. IEEE Transactions on Components and Packaging Technologies, 2006, 29(1): 222 - 229.

[2] SALFNER F, LENK M, MALEK M. A survey of online failure prediction methods[J]. ACM Computing Surveys, 2010, 42(3): 10.

[3] LIANG Y, ZHANG Y, JETTE M, et al. BlueGene/L failure analysis and prediction models[C]// Proceedings of the 2006 International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2006: 425 - 434.

[4] VAIDYANATHAN K, TRIVEDI K S. A measurement-based model for estimation of resource exhaustion in operational software systems [C]// Proceedings of the 1999 10th International Symposium on Software Reliability Engineering. Piscataway: IEEE, 1999: 84 - 93.

[5] 侯晓凯,李师谦,王杰琼,等. 一种基于神经网络的网络设备故障预测系统[J]. 山东理工大学学报(自然科学版),2014, 28(6):29 - 34.

[6] LIANG Y, ZHANG Y, XIONG H, et al. An adaptive semantic filter for blue gene/L failure log analysis[C]// IPDPS 2007: Proceedings of the 2007 IEEE International Parallel and Distributed Processing Symposium. Piscataway: IEEE, 2007: 1 - 8.

[7] OLINER A J, AIKEN A, STEARLEY J. Alert detection in system logs[C]// ICDM'08: Proceedings of the Eighth IEEE International Conference on Data Mining. Piscataway: IEEE, 2008: 959 - 964.

[8] LIANG Y, ZHANG Y, XIONG H, et al. Failure prediction in IBM blue gene/L event logs[C]// Proceedings of Seventh IEEE International Conference on Data Mining. Washington, DC: IEEE Computer Society, 2007: 583 - 588.

[9] GAO Z, XU Y, MENG F, et al. Improved information gain-based feature selection for text categorization[C]// Proceedings of the 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems. Piscataway: IEEE, 2014: 1 - 5.