# 一种基于时间序列的自适应网络异常检测算法

吕军晖 周 刚

(北京航空航天大学 软件开发环境国家重点实验室,北京 100191) (国家数字交换系统工程技术研究中心,郑州 450002)

金 毅

(北京航空航天大学 软件开发环境国家重点实验室,北京 100191)

**摘 要**:传统的网络管理工具通常是根据预先设定的阈值进行网络流量异常检测,这种方法虽然简单,但不能根据网络状况进行自适应的动态调整.分析了基于时间序列的 Holt-Winters 异常检测方法,结合建立的历史流量的正常模型,改进了 Holt-Winters 模型的基值以及平滑因子参数的获取过程,加快了算法的启动时间,缩短了算法对网络环境的自适应时间.改进的 Holt-Winters 算法相较于原来的 Holt-Winters 算法以及阈值检测方法检测的正确率更高、误报率更低.

**关 键 词**:异常检测;时间序列分析;Holt-Winters 模型

**中图分类号**:TP 393

**文献标识码**:A **文 章 编 号**:1001-5965(2009)05-0636-04

# Adaptive aberrant network traffic detection algorithm based on time series forecast

Lü Junhui

(State Key Laboratory of Software Development Environment, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Zhou Gang

(National Digital Switching System Engineering & Technological Research Center, Zhengzhou, 450002, China)

Jin Yi

(State Key Laboratory of Software Development Environment, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

**Abstract**: The traditional network management tools usually detect aberrant network traffic according to the preset threshold. This method is straightforward, but it has poor adaptability. Therefore, A mature aberrant detection method called Holt-Winters based on the time series forecast was described. But it needed a long time to adapt the real network environment when the algorithm model applied. To solve these problems, based on the statistics of huge history network flow model, an increased Holt-Winter algorithm was proposed to calculate the base values and the model parameter values, which made the algorithm started faster. The result shows that the increased Holt-Winters algorithm has improved the detection accuracy and reduced the false alarm rate compared with threshold method and traditional Holt-Winters model.

**Key words**: aberration detection; time series analysis; Holt-Winters models

随着互联网的广泛普及,网络管理的核心任务从用量管理转向安全管理.随着网络规模的扩大,各种网络攻击造成的损失也随之增大,网络攻击的手法也不断更新,因此网络安全日益成为人

**收稿日期**:2008-08-10

**基金项目**:国家 973 计划资助项目(2005CB321901)

**作者简介**:吕军晖(1983—),女,山东莱阳人,硕士生,lvjh@nlsde.buaa.edu.cn.

们普遍关注的焦点.

网络流量异常检测方法分为以下 4 种:①阈值检测方法;②统计检测方法;③基于小波的检测方法;④面向网络安全的检测方法.在阈值检测方法中,一般是根据历史数据建立一个正常的参数基线,即一个容许的范围(可以是 2 个或者 3 个标准差),一旦超出此范围就判断为异常,如文献[1].统计检测方法在实际中有多种算法,最常见的是 GLR(Generalized Likelihood Ratio)测试,例如 Thottan 和文献[2]的方法,它考虑 2 个相邻的时间窗 $R(t)$ 和 $S(t)$以及二者合并组成的窗口 $C(t)$,每个窗口都采用自回归 AR(Auto-Regressive)模型拟合,计算各窗口序列残差的联合似然比,当该值超过预先设定的阈值 $T$ 时,两个窗口 $R(t)$和 $S(t)$的边界就被认定为异常点.文献[3]在 2000 年 12 月提出了应用时间序列算法 Holt-Winters 算法进行自适应的异常行为检测.在基于小波的方法中,利用小波变换把流量观测值序列分解成近似系数和细节系数,流量中的奇异性可以在细节系数中检测出来.面向网络安全的检测方法通过过程模型来描述所期望的网络特征,即正常行为特征,如果当前特征与所期望的特征有显著偏差时产生告警,使用的模型如马尔可夫模型.

本文对 Holt-Winters 算法进行分析,并对算法的初始值以及平滑参数的选取进行了优化.目的是实现一个实时性高、自适应能力快的网络流量异常检测算法.

## 1　Holt-Winters 算法

本论文基于的实验环境是某信息中心的大型网络,网络环境如图 1 所示.

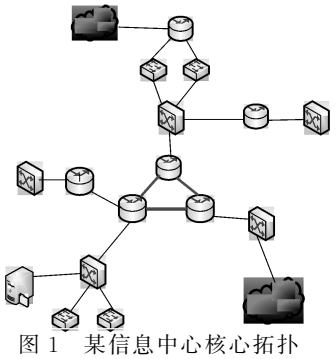

图 1　某信息中心核心拓扑

文献[4]提出尽管网络的流量行为是非常不确定的,但是通过观察可以发现,每个流量参数在一周各天的观测值都呈现出周期性趋势,这在该大型业务网络中也得到验证.

基于时间序列的方法对网络异常进行检测的比较成熟的方法是基于 AR 和自回归移动平均模型 ARIMA(Autoregressive Integrated Moving Average Model).根据文献[5]所描述的"具有季节周期为 $d$ 的 Holt-Winters 递归表达与 ARIMA 过程的某个大样本预测递归相符",其表达式如下:

$$(1-B)(1-B^d)Y_t = Z_t + \cdots + Z_{t-d+1} + \gamma(1-\alpha) \times (Z_{t-d} - Z_{t-d-1}) - (2-\alpha-\alpha\beta)(Z_{t-1} + \cdots + Z_{t-d}) + (1-\alpha)(Z_{t-2} + \cdots + Z_{t-d-1}) \quad (1)$$

式中,$B$ 表示后移因子;$Z_t$ 是均值为 0、方差为 $\sigma^2$ 的高斯白噪声过程;$\alpha,\beta,\gamma$ 是 Holt-Winters 算法的平滑因子.应用 ARIMA 过程进行网络流量预测已有成熟的研究,但是该大型业务网络中对流量异常的检测实时性要求较高,因此选择算法较简单、又与 ARIMA 模型相符合的 Holt-Winters 算法,从理论上具有"殊途同归"的意义.

### 1.1　算法模型

文献[6]提出了 Holt-Winters 线性季节平滑模型预测来序列数据.文献[3]提出了在开源软件 RDDtool 中应用 Holt-Winters 进行异常行为检测.文献[7]对 Holt-Winters 模型进行了改进,简化了算法平滑因子的获取过程.

Holt-Winters 算法是基于以下的模型提出的:①随时间变化的趋势;②周期性的趋势;③周期性的波动;④经过③的作用,①所呈现的规律性会逐渐演化.以上 4 点虽不能概括时间序列的所有规律性,却反映了流量的最重要的特征.Holt-Winters 算法分为 3 步对网络的流量信息进行处理:

1) 通过已知的时间序列对未来时间点的流量进行预测;

2) 测量预测值和实际流量之间的偏差;

3) 确定一个观察值是否严重偏离了预测的范围.

Holt-Winters 是基于指数平滑法的线性预测.所谓指数平滑是利用当前的预测值和当前采样值预测下一个时间点的预测值的方法.设 $\hat{y}_{t+1}$ 表示对时间点 $t+1$ 的预测结果,则有:

$$\hat{y}_{t+1} = \alpha y_t + (1-\alpha)\hat{y}_t \quad (2)$$

式中,$\alpha$ 是一个参数,区间为(0, 1),$\alpha$ 决定了当前值采样值的权重和衰减率.

假设 $y_1, y_2, \cdots, y_{t-1}, y_t, y_{t+1}, \cdots$是在某固定时间间隔内观察到的流量数据序列.Holt-Win-

ters算法将预测值分为3部分：Baseline，Linear trend以及周期影响. $t+1$ 时刻的流量预测值的计算公式如式(3)所示：

$$\hat{y}_{t+1}=a_t+b_t+c_{t-m+1} \tag{3}$$

式中，$a_t$ 表示基线；$b_t$ 表示线性趋势；$c_t$ 表示季节趋势；$m$ 表示季节的周期. 对这3部分进行更新的公式如下：

Baseline：$a_t=\alpha(y_t-c_{t-m})+(1-\alpha)(b_{t-1}+a_{t-1})$

Linear trend：$b_t=\beta(a_t-a_{t-1})+(1-\beta)b_{t-1}$

周期趋势：$c_t=\gamma(y_t-a_t)+(1-\gamma)c_{t-m}$ (4)

### 1.2 异常检测

通过衡量预测值与实际值的偏离来检测数据是否超出置信区间，采用如下公式：

$$d_t=\gamma\mid y_t-\hat{y}_t\mid+(1-\gamma)d_{t-m} \tag{5}$$

式中，$d_t$ 表示时间 $t$ 时的预测偏移；$y_t$ 的置信区间为$(\hat{y}_t-\delta_-\cdot d_{t-m},\hat{y}_t+\delta_+\cdot d_{t-m})$；$\delta_-$ 和 $\delta_+$ 是放缩比例，用来改变置信区间的大小. 通常情况下，令 $\delta_-=\delta_+=\delta$，得到一个对称的置信区间. 文献[3]提出 $\delta$ 值的合理范围为2与3之间，因此本文取$\delta=2.5$.

## 2 对Holt-Winters算法的改进

### 2.1 基值的确定

本文研究网络环境每个流量参数在一周各天的观测值都呈现出周期性趋势，因此取季节周期为一周7 d，采样间隔为5 min，每天有288个采样值，那么 $m=7\times288=2\,016$. 预先收集8周的网络流量数据，分析建立流量的正常模式.

$a_t$ 表示基线，因此，采用一周每天流量的平均值作为 $a$ 的取值. 用 $\bar{y}_{ij}$ 表示一周第 $i$ 天第 $j$ 个时刻的平均值，$a_{0j}(j=1,2,\cdots,7)$表示一周第 $j$ 天的基准值，$a_{0j}$ 计算公式如下：

$$\left.\begin{aligned}a_{0j}&=\frac{1}{288}\sum_{i=1}^{288}\bar{y}_{ij}\\ \bar{y}_{ij}&=\frac{1}{8}\sum_{t=1}^{8}y_{ij}\end{aligned}\right\} \tag{6}$$

这8个数据中可能有异常数据，会对流量的正常模式的确定产生影响，必须把这样的异常数据当作坏值(其相对误差为粗大误差)而剔除，然后再对剩余的数据求平均，得到真正的测量值，这是数据处理中的一种常用方法. 本文采用格拉布斯准则剔除异常值. 格拉布斯准则是判断测量数据粗大误差的一个准则. 具体的说，若 $\bar{y}$ 表示 $y_1$，$y_2,y_3,\cdots,y_8$ 的平均值，$v$ 表示它们的标准差，即：

$$\left.\begin{aligned}\bar{y}&=\frac{1}{8}\sum_{t=1}^{8}y_t\\ v&=\sqrt{\frac{1}{8}\sum_{t=1}^{8}(y_t-\bar{y})^2}\end{aligned}\right\} \tag{7}$$

若 $|y_t-\bar{y}|>kv$ 且 $|y_t-\bar{y}|=\max_{t=1,2,\cdots,8}|y_t-\bar{y}|$，则认为 $y_t$ 是坏值，应剔除不用，其中 $k$ 是格拉布斯准则系数，当取置信区间为95%时，对应 $k=2.03$. 每次计算只剔除一个坏值，下一次必须重新计算平均值和标准差，直到所有的数据值都满足 $|y_t-\bar{y}|<kv$.

经过对历史数据进行统计，得到了图2所示的一周7 d的正常行为模式，它代表了当前环境下，流量随时间发生变化的一种周期性趋势.

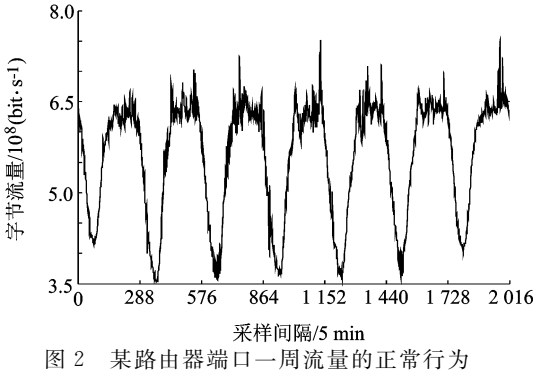


图2 某路由器端口一周流量的正常行为

由于 $b$ 表示线性趋势，可以取第 $t+1$ 周第 $j$ 天与第 $t$ 周第 $j$ 天每个流量差值的平均值作为衡量 $b$ 值的一种方式，$b$ 的计算公式如下：

$$b_{0j}=\left(\sum_{i=1}^{m}\bar{y}_{ij}/m-\sum_{i=d+1}^{2m}y_{ij}/m\right)\Big/m \tag{8}$$

$c_t$ 表示季节趋势，令 $k=1,2,3,\cdots,m$，$\bar{y}_{tk}$ 表示第 $t$ 周时刻 $k$ 取值的平均值，$c$ 计算公式如下：

$$c_{0k}=\bar{y}_{tk}-(a_{01}+(k-1)b_{01}) \tag{9}$$

$d_t$ 表示流量偏离正常值的大小，选取的计算公式如下：

$$d=v=\sqrt{\frac{1}{8}\sum_{t=1}^{8}(y_t-\bar{y})^2} \tag{10}$$

### 2.2 平滑因子值的选取

$\alpha,\beta$ 和 $\gamma$ 是Holt-Winters算法的自适应参数，Holt-Winters算法根据这3个平滑因子进行指数平滑. 一般它们都是介于0到1之间的数，取值较大表示算法的适应较快，近期观察所占权重大，取值较小则算法适应较慢，历史数据占较大的比重. 采用如下的选取依据，$\alpha$ 的取值是根据过去数据点所占的权重计算得出，具体计算方法如下：

$$\alpha=1-\exp\left(\frac{\log(1-w\%)}{n}\right) \tag{11}$$

式中，log表示自然对数；而 $w$ 表示权重的百分比

形式;$n$ 表示所取时间序列数据点的数目.举例来说,如果希望过去 45 min(每 5 min 采集一次流量数据)在计算中占 95% 的权重,那 $w=95\%$,$n=12$,计算得到 $\alpha=0.28$.

通过实际网络环境测试发现,取 $\alpha=0.28$,$\beta=0.0035$,$\gamma=0.1$ 会取得比较好的异常检测效果.

## 3　实验结果分析

为验证采用改进 Holt-Winter 算法的有效性,在图 1 所示的实际网络环境下收集流量数据进行异常检测,并将改进的算法与集成于 RDDtool 中的 Holt-Winters 算法、以及原有针对该大型业务网络中的阈值检测方法进行比较.

图 3 中,对历史数据应用公式(6)、式(7)进行计算得到的某网络端口输入字节速率在周日表现出的正常流量模型(虚线).可以看出,这一天流量波动的幅度较大,通过对该端口流量以及相关设备状态进行核查,网管人员认为产生的异常事件有 8 个.

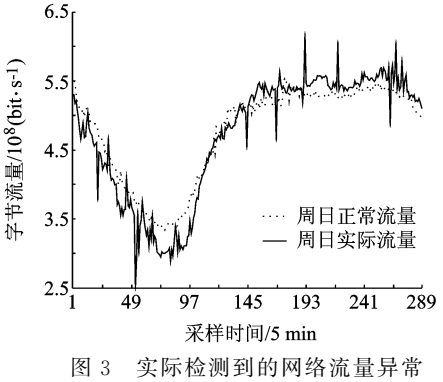


图 3　实际检测到的网络流量异常

采用改进的 Holt-Winters 算法、集成于 RDDtool 中的 HoltWinters 算法,以及传统的阈值算法对该天的采集序列进行异常检测,得到了如表 1 所示的结果.

**表 1　告警情况统计**

| 异常统计个数 | 改进 Holt-Winters | Holt-Winters | 阈值检测 |
|---|---|---|---|
| 检测异常总数 | 9 | 7 | 10 |
| 误报个数 | 2 | 2 | 4 |

本文改进的 Holt-Winters 算法检测出的异常为 9 个,其中误报的有 2 个,也就是实际检测的异常有 7 个,达到了较好的效果.集成于 RDDtool 中的 Holt-Winters 算法检测出的异常为 7 个,但是其中误报的有 2 个,也就是说实际检测的异常有 5 个.但是一天的刚开始发生的异常事件,原始的 Holt-Winters 算法并未检测出来,这也证明了本文提出的改进 Holt-Winters 算法不需要一定时间的适应,即能产生较好的异常检测的效果.在实际网络中的测试也证明了改进的算法的适应性很快,得到了预期的效果.阈值检测方法相比较另外两种算法而言,虽然检测出的实际异常为 6 个,但是由于误报率太高,给网管人员进行告警确认、故障排查带来了很大的干扰作用.

## 4　结　论

本文提出了针对 Holt-Winters 模型进行改进的算法.本算法的特点是通过对实际网络环境中的历史数据进行统计分析,得到算法基值,并给出了适合于该网络环境的平滑因子的取值,使得改进 Holt-Winters 算法应用于实际网络时适应性快,在采集的前几个周期内就能达到较好的效果,算法的启动时间较短.与阈值检测方法相比,提高了报告异常的准确度.进一步的研究工作可尝试算法分析误报率的原因.

### 参考文献(References)

[1] Lawrence Ho L, Cavuto D J, Papavassiliou S, et al. Adaptive and automated detection of service anomalies in transaction-oriented WAN's: Network analysis, algorithms, implementation and deployment[J]. IEEE Journal of Selected Areas in Communications, 2000, l8(5): 744－757

[2] Hood C S, Ji C. Beyond thresholds: an alternative method for extracting information from network measures[C]// Proceedings of IEEE Globecom Conference. Phoenix: Arizona, 1997:487－491

[3] Brutlag J. Aberrant behavior detection in time series for network monitoring [C]// Proceedings of the USENIX Fourteenth System Administration Conference LISA XIV. California: USENIX Assoc, 2000: 139－146

[4] Ho L L, Cavuto D J, Papavassiliou S. Adaptive and automated detection of service anomalies in transactionoriented WAN's: network analysis, algorithms, implementation, and deployment [J]. IEEE Journal of Seletected Areas in Communications, 2000, 18 (5): 744－757

[5] Brockwel P J, Davis R A. Introduction to time series and forecasting [M]. New York: Springer, 2002: 326－328

[6] Chatfield C, Yark M. The Holt-Winters forecasting: some practical issues [J]. The Statistician, 1988, 37: 129－140

[7] Bermudez J D, Segura J V, Vercher E. Holt-Winters forecasting: an alternative formulation applied to UK air passenger data [J]. Journal of Applied Statistics, 2007, 34(9): 1075－1090