软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2012,23(2):361−377 [doi: 10.3724/SP.J.1001.2012.03952]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# 基于多尺度主成分分析的全网络异常检测方法*

钱叶魁[1,2+], 陈 鸣[1], 叶立新[2], 刘凤荣[2], 朱少卫[2], 张 晗[2]

[1](中国人民解放军 理工大学 指挥自动化学院,江苏 南京 210007)

[2](中国人民解放军 防空兵学院,河南 郑州 450052)

## Network-Wide Anomaly Detection Method Based on Multiscale Principal Component Analysis

QIAN Ye-Kui[1,2+], CHEN Ming[1], YE Li-Xin[2], LIU Feng-Rong[2], ZHU Shao-Wei[2], ZHANG Han[2]

[1](Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China)

[2](Air Defence Forces Academy, The People's Liberation Army, Zhengzhou 450052, China)

+ Corresponding author: E-mail: qyk1129@hotmail.com

**Qian YK, Chen M, Ye LX, Liu FR, Zhu SW, Zhang H. Network-Wide anomaly detection method based on multiscale principal component analysis. *Journal of Software*, 2012,23(2):361−377.** http://www.jos.org.cn/1000-9825/3952.htm

**Abstract**: Network anomaly detection is very important in order to guarantee the reliable operation of network. Existing methods only utilize temporal correlation or spatial correlation of network traffic individually. Aiming at this deficiency, this paper considers the spatio-temporal correlation of traffic matrix together and puts forward a network-wide anomaly detection method based on MSPCA. The method utilizes the multiscale modeling ability of wavelet transform and dimensionality reduction ability comprehensively to model normal network traffic, and then analyzes residual traffic using Shewart and EWMA control charts. In addition, the MSPCA anomaly detection method is extended to online MSPCA anomaly detection method through applying gliding window mechanism. Real Internet measurement data analyses and simulation experiment analyses show that the detection performance of MSPCA algorithm is superior to PCA algorithm and KLE algorithm proposed recently. Analyses also show that the detection performance of online MSPCA algorithm is close to MSPCA algorithm, and the single step execution time of online MSPCA algorithm is very short, which can fully meet the need of real-time detection.

**Key words**: network anomaly detection; multiscale modelling; principal component analysis; traffic matrix; online detection

**摘 要**: 网络异常检测对于保证网络的可靠运行具有重要意义,而现有的异常检测方法仅仅单独利用流量的时间相关性或空间相关性.针对这一不足,同时考虑流量矩阵的时空相关性,提出了一种基于 MSPCA 的全网络异常检测方法.该方法综合利用小波变换具有的多尺度建模能力和 PCA 具有的降维能力对正常流量进行建模,然后采用 Shewart 控制图和 EWMA 控制图分析残余流量.此外,还利用滑动窗口机制对 MSPCA 异常检测方法进行在线扩展,提出了一种在线的 MSPCA 异常检测方法.因特网实测数据分析和模拟实验分析表明:MSPCA 算法的检测性能优于

* 基金项目: 国家自然科学基金(61070173); 国家高技术研究发展计划(863)(2007AA01Z418); 江苏省自然科学基金(BK2009058)

收稿时间: 2010-05-13; 修改时间: 2010-07-28; 定稿时间: 2010-10-11

PCA 算法和近期提出的 KLE 算法;在线 MSPCA 算法的检测性能非常接近 MSPCA 算法,且单步执行时间很短,完全满足实时检测的需要.

**关键词**: 网络异常检测;多尺度建模;主成分分析;流量矩阵;在线检测

**中图法分类号**: TP393 **文献标识码**: A

在当今的因特网环境下,各种异常行为(如拒绝服务攻击、蠕虫、突发流等)频繁发生.有效地检测异常行为,对于保证网络的可靠运行具有重要意义.由于网络异常行为通常具有不同的模式,且隐藏在复杂的背景流量中,因此,网络异常检测是一项极具挑战性的任务.

由于网络异常行为大都伴随着网络流量的显著变化,所以大部分研究[1,2]都是通过被动监测和分析单条链路流量的变化来检测异常.例如,Barford 等人[1]利用小波变换方法分析 IP 流和 SNMP 数据,从而揭示 4 种不同的流量异常特征.这类方法利用链路流量的时间相关性(temporal correlation),采用多尺度(multiscale)分析方法,取得了较好的检测效果.然而这类方法仅仅考虑单条链路的流量,其异常检测能力有限.其原因在于,许多异常行为影响网络中多条链路和路径,其在单条链路和路径上呈现的异常现象有时并不明显.针对这一问题,Lakhina 等人[3,4]首次采用流量矩阵作为数据源,提出了一种基于主成分分析(PCA)的全网络(network-wide)异常检测方法.这类方法利用多条链路流量之间的空间相关性(spatial correlation),将流量矩阵高维数据映射到正常子空间和异常子空间,然后在异常子空间中检测凸显的异常行为模式.然而,基于 PCA 的网络异常检测方法属于单尺度(single-scale)分析方法,它仅仅考虑了流量矩阵数据的空间相关性,并没有考虑流量矩阵数据的时间相关性.

针对现有两类方法的不足,本文试图同时利用 OD 流流量矩阵的时空相关性.为此,我们首先利用小波变换和 PCA 分别证实 OD 流流量矩阵存在的时空相关性;然后,综合利用小波变换具有的多尺度建模能力和 PCA 具有的降维能力,并采用 Shewart 和 EWMA 控制图两种残余分析方法,提出一种基于多尺度主成分分析(multiscale PCA,简称 MSPCA)的全网络异常检测方法;而且利用滑动窗口机制对 MSPCA 异常检测方法进行在线扩展,提出一种在线的 MSPCA 异常检测方法.

本文的主要贡献在于以下 3 个方面:

(1) 利用小波变换对因特网实测的 OD 流流量矩阵数据进行多尺度分析,证实其具有时间相关性,且利用主成分分析方法证实 OD 流流量矩阵数据在每个时间尺度上均具有空间相关性;

(2) 提出了一种基于 MSPCA 的全网络异常检测方法及其在线扩展;

(3) 通过因特网实测数据分析和模拟实验两种方法对算法进行了评价,证实其有效性.

本文第 1 节综述相关工作.第 2 节给出流量矩阵模型.第 3 节提出 MSPCA 异常检测方法.第 4 节提出在线扩展方法.第 5 节进行实验评价.第 6 节总结全文并提出进一步研究方向.附录给出流量矩阵的时空特性分析.

## 1 相关工作

自 1987 年 Denning[5]提出异常检测统计模型以来,网络异常检测方法的研究就一直受到学术界的广泛关注.根据异常检测范围的不同,我们可以将这些方法分为 3 类:基于主机的异常检测方法、基于单链路流量的网络异常检测方法和基于流量矩阵的全网络异常检测方法.

基于主机的异常检测方法[6−9]的基本思想是,采用主机系统的系统日志或审计记录作为异常检测数据源,应用机器学习等方法建立用户的正常行为模式,然后以某种测度来度量用户偏离正常行为模式的程度,从而检测网络入侵行为.

基于单链路流量的网络异常检测方法[1,10−12]通过被动监测和分析单条链路流量的变化来检测异常.这类方法的基本思想是,利用链路流量的时间相关性,采用小波变换等多分辨率分析方法对流量数据进行多尺度分析,将确定性信号和随机性信号分离,从而揭示各种异常行为.

基于流量矩阵的全网络异常检测是近年来兴起的一种网络异常检测方法.它主要针对单链路流量异常检

测方法的局限性,利用流量矩阵的空间相关性和时间相关性,应用各种多元统计分析方法或信号处理方法,从全网络的视角检测异常行为.Lakhina 等人[3,4]采用流量矩阵作为数据源,首次揭示了流量矩阵具有低维度特性,分析了特征流的特性,并以此为基础,提出了一种基于 PCA 的全网络异常检测方法.实验结果表明,该方法的检测性能明显优于传统的单链路流量时间序列方法;Ringberg 等人[13]进一步指出 PCA 异常检测器面临的 4 个挑战,其中包括正常子空间中主成分数对检测性能的影响、流量聚合级别对算法有效性的影响、异常流量对正常子空间的毒害等;Rubinstein 等人[14,15]则利用了 PCA 异常检测器的缺陷,提出了 4 种数据毒害机制,并提出一种基于健壮 PCA 的异常检测方法,能够有效地抵御毒害攻击.这类方法的基本思想都是利用多条链路流量之间的空间相关性,采用 PCA 方法获得流量矩阵高维数据的主成分,分别建立正常子空间和异常子空间,然后在异常子空间中检测凸显的异常行为模式.这类方法的不足之处在于,仅仅利用了流量矩阵的空间相关性,而没有利用流量矩阵的时间相关性.为此,Brauckhoff 等人[16]同时考虑流量矩阵的空间相关性和时间相关性,将 PCA 推广到 Karhunen-Loveve 变换展开式(KLE),提出了一种基于 Galerkin 的 KLE 计算方法,然后使用 KLE 建立一种预测模型并用于异常检测.实验证实,KLE 方法取得了优于 PCA 的检测性能.但是,KLE 方法仅仅利用了固定时间间隔的测量数据之间的时间相关性,不具有小波变换具有多分辨率分析能力;此外,KLE 方法同样属于离线算法,无法实时地检测异常.

本文提出的基于 MSPCA 的全网络异常检测方法同样采用流量矩阵作为数据源.它结合了小波变换的多分辨率分析能力和 PCA 的降维分析能力,充分利用了流量矩阵数据中蕴含的空间相关性和时间相关性.因特网实测数据分析和模拟实验均证实了 MSPCA 方法的检测性能不仅优于 PCA 方法[3],而且优于近期提出的 KLE 方法[16].此外,本文还对 MSPCA 算法进行在线扩展,不仅能够实时地检测异常,而且具有较好的检测性能.

## 2 流量矩阵模型

**定义 1(流量矩阵)**. 流量矩阵是指一个网络中所有源节点和目的节点对(即 OD 对)之间的流量需求(traffic demand).根据选择的网络节点类型的不同,可以定义不同粒度的流量矩阵:链路级、路由级和 PoP 级(point of presence)流量矩阵[17].

**定义 2(PoP 级流量矩阵)**. 假设某自治系统(autonomous system,简称 AS)有 $n$ 个 PoP 点,以一定的时间间隔(周期)连续地被动测量任意一对 PoP 点之间的流量,然后将获得的测量值排列成一个 $T\times p$ 的矩阵 $\boldsymbol{X}$,表示所有这些流量测量值的时间序列.其中,$T$ 表示测量的周期数;$p$ 表示每个周期内测量获得的流量测量值的个数,即 $p=n\times n$.第 $t$ 行表示在第 $t$ 个周期内流量测量值的向量,通常用 $\boldsymbol{x}_t$ 表示;第 $j$ 列表示第 $j$ 个 PoP 点对之间流量测量值的时间序列.矩阵 $\boldsymbol{X}$ 称为 AS 的 PoP 级流量矩阵,简称流量矩阵.本文采用流量大小(字节数、分组数和流数)作为流量测度,因此,流量矩阵的任一元素 $x_{ij}$ 表示第 $t$ 个间隔时间内第 $j$ 个 OD 对之间的流量大小.

限于正文篇幅,流量矩阵的时间相关性和空间相关性分析见附录.

## 3 MSPCA 异常检测方法

本节将充分利用流量矩阵的时空相关性,结合小波变换的多尺度建模能力和主成分分析的降维能力,对流量矩阵中的正常流量进行建模;然后采用两种残余流量分析方法实现异常检测;最后,本节对 MSPCA 异常检测算法进行时间复杂度分析.

### 3.1 正常流量建模

MSPCA[18]结合小波变换抽取信号确定性特征的能力以及 PCA 抽取多元变量共有模式的能力,很好地满足了流量矩阵中正常流量建模的要求.

基于 MSPCA 的正常流量建模方法包括以下 4 个基本步骤(如图 1 所示):

- 第 1 步:流量矩阵的小波分解.

  首先采用标准正交小波变换 $\boldsymbol{W}$ 对流量矩阵 $\boldsymbol{X}$ 进行多尺度分解,获得各个尺度的小波系数矩阵

$\boldsymbol{Z}_L, \boldsymbol{Y}_m (m=1,\ldots,L)$,然后采用 MAD 方法[19]对小波系数进行过滤,获得过滤后的小波系数矩阵:

$$\bar{\boldsymbol{Z}}_L, \bar{\boldsymbol{Y}}_m \ (m=1,...,L).$$

- 第 2 步:小波系数矩阵的主成分分析和重构.
  首先对滤波后的每个尺度的小波系数矩阵 $\bar{\boldsymbol{Z}}_L, \bar{\boldsymbol{Y}}_m (m=1,...,L)$ 进行主成分分析;然后根据碎石图(scree plot)方法[3]选择 PC 的数目;最后重构出小波系数矩阵 $\hat{\boldsymbol{Z}}_L, \hat{\boldsymbol{Y}}_m (m=1,...,L)$.
- 第 3 步:流量矩阵的小波重构.
  根据所有尺度的小波系数矩阵 $\hat{\boldsymbol{Z}}_L, \hat{\boldsymbol{Y}}_m (m=1,...,L)$, 采用小波逆变换 $\boldsymbol{W}^T$ 重构出流量矩阵.
- 第 4 步:流量矩阵的主成分分析和重构.
  具体步骤与第 2 步类似,获得重构出的流量矩阵 $\hat{\boldsymbol{X}}$.

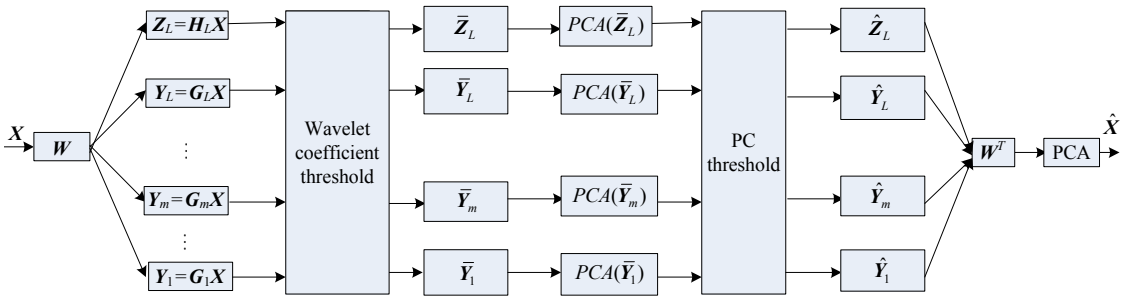



Fig.1 Normal traffic modeling method based on MSPCA

图 1 基于 MSPCA 的正常流量建模方法

### 3.2 残余流量分析

在建立正常流量的模型以后,残余流量主要由两部分组成:噪声和突发流量.其中,噪声主要是由流量模型的误差引起的,而突发流量主要是由各种异常行为引起的.为了分析残余流量,本文引入平方预测误差(squared prediction error,简称 SPE),即

$$Q_i = \sum_{j=1}^{p} (x_{ij} - \hat{x}_{ij})^2 \tag{1}$$

由于各种异常流量大小的变化差异很大,例如突发流(flash crowd)和分布式拒绝服务攻击(DDoS)的攻击行为会引起流量的急剧增加,而蠕虫(worm)流量较小且随着传播范围的扩大而逐渐增加,所以本文采用两种控制图方法[20]来分析残余流量:Shewart 和 EWMA 控制图.其中,Shewart 控制图能够很快地检测出流量的急剧变化,但在检测缓慢变化的异常流量时速度较慢;而 EWMA 控制图在选择合适的参数后能够检测变化缓慢但持续时间较长的异常流量.

#### 3.2.1 Shewart 控制图

Shewart 控制图方法直接对 SPE 的时间序列进行检测,采用 $Q$ 统计量[3]作为检测阈值,$Q$ 统计量的阈值定义如下:

$$\delta_\alpha^2 = \phi_1 \left[ \frac{c_\alpha \sqrt{2\phi_2 h_0^2}}{\phi_1} + 1 + \frac{\phi_2 h_0 (h_0 - 1)}{\phi_1^2} \right]^{\frac{1}{h_0}} \tag{2}$$

其中, $h_0 = 1 - \frac{2\phi_1\phi_3}{3\phi_2^2}, \phi_i = \sum_{j=r+1}^{p} \lambda_j^i, i = 1,2,3$, $\lambda_j$ 将流量矩阵 $\boldsymbol{X}$ 投影到第 $j$ 个主轴所捕获的方差,即第 $j$ 个特征值;$c_\alpha$是标准正态分布中的 $1-\alpha$分位数,$\alpha$通常取 0.001.如果 $SPE \geqslant \delta_\alpha^2$,则认为出现异常,其中 $\delta_\alpha^2$ 表示置信度为 $1-\alpha$时 SPE 的阈值.

3.2.2 EWMA 控制图

EWMA 控制图方法根据最近的历史数据预测时间序列下一时刻的值.在第 $t$ 时刻,残余流量的预测值记作 $\hat{Q}_t$, 第 $t$ 时刻残余流量的实际值记作 $Q_t$,第 $t$+1 时刻残余流量的预测值记作 $\hat{Q}_{t+1}$,则

$$\hat{Q}_{t+1}=\alpha Q_t+(1-\alpha)\hat{Q}_t \tag{3}$$

其中,0≤$\alpha$≤1 是历史数据的相对权重,亦称为平滑指数.关于$\alpha$值的选取,我们将在实验部分讨论.

通过公式(3)迭代求取实际值和预测值之差的绝对值$|Q_t-\hat{Q}_t|$, 称为 EWMA 过程统计量.EWMA 控制图的控制极限可以渐近表示为

$$UCL=\mu_s+L\times\sigma_s\sqrt{\frac{\alpha}{(2-\alpha)T}} \tag{4}$$

其中,$\mu_s$ 表示 EWMA 过程统计量的均值;$\sigma_s$ 表示 EWMA 过程统计量的均方差;$\alpha$表示平滑指数;$L$ 表示控制图常数,其大小直接影响检测结果;$T$ 表示时间序列的长度.若$|Q_t-\hat{Q}_t|\geqslant UCL$, 则认为出现异常.

3.2.3 算法复杂度分析

在 MSPCA 异常检测算法中,主要的计算开销是流量矩阵的小波变换以及小波系数矩阵和流量矩阵的主成分分析.在算法实现时,小波变换采用 Mallat 算法[21],其时间复杂度为 $O(T)$;主成分分析算法的时间复杂度为 $O(Tp^2)$.所以,MSPCA 异常检测算法总的时间复杂度为 $O(Tp^2+Tp)$,即 $O(Tp^2)$.

## 4 在线扩展

MSPCA 异常检测方法要求在完成流量矩阵数据的测量后再进行异常检测,所以属于离线检测方法,无法满足实时在线地检测异常的需要.为此,本文提出一种在线的 MSPCA 异常检测方法.

在线 MSPCA 异常检测方法的基本原理如图 2 所示.它采用滑动窗口(gliding window)机制,并将检测过程分为两个阶段:初始化阶段和滑动阶段.在初始化阶段,选取前 $WIN$ 个测量数据构成流量矩阵,应用 MSPCA 异常检测方法计算初始阶段流量矩阵的残余流量,并应用 EWMA 控制图适时发出异常警报;在滑动阶段,每隔一个测量间隔时间,将最新的测量数据加入到滑动窗口并将最旧的测量数据剔除,保持滑动窗口长度 $WIN$ 不变,然后应用 MSPCA 异常检测方法计算最新测量数据的残余流量,并应用 EWMA 控制图适时发出异常警报.需要指出的是,由于小波变换在具体实现时通常采用二进小波变换算法——Mallat 算法,所以,为了提高小波变换的速度,滑动窗口长度应该取 2 的倍数,如本文选取 $WIN=2^9$.

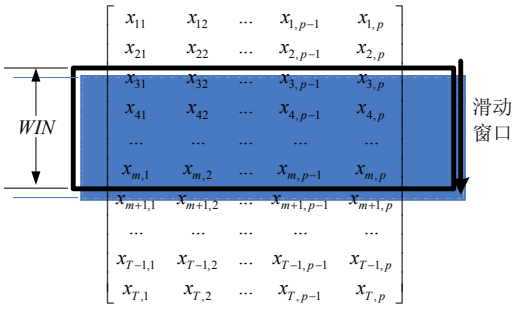



Fig.2 Principle of online MSPCA anomaly detection method

图 2 在线 MSPCA 异常检测方法的原理

时间复杂度是在线异常检测算法的重要指标.在线 MSPCA 异常检测算法单步执行时的时间复杂度是 $O(WIN\times p^2+WIN)$,即 $O(WIN\times p^2)$.若 $WIN=2^9=512$,则采用配置为 2.33GHz 的 CPU、2GB 内存的计算机,对表 1 中数据集 $F$ 执行在线 MSPCA 异常检测算法,单步运行时间小于 1s,完全满足实时检测异常的需要.

**Table 1** Abilene traffic matrix dataset

**表 1** Abilene 流量矩阵数据集

| 序号 | 持续时间 | 间隔时间(min) | 测度 | 矩阵形式 | 数据集 |
|---|---|---|---|---|---|
| 1 | 2003.12.15-12.21 | 5 | 字节数 | 2010×121 | *B* |
| 2 | 2003.12.15-12.21 | 5 | 分组数 | 2010×121 | *P* |
| 3 | 2003.12.15-12.21 | 5 | 流数 | 2010×121 | *F* |

## 5 实验评价

评价异常检测算法的检测性能主要有两种方法:因特网实测数据分析和模拟实验分析.考虑到以上两种方法各自的优缺点,本文采用这两种方法相结合的方式来评价异常检测算法的检测性能.

### 5.1 因特网实测数据分析

#### 5.1.1 数据集

本文使用的流量矩阵数据集来自于 Abilene 网络,Abilene 网络属于因特网的骨干网.它在 2003 年有 11 个 PoP 点,传送的流量大部分来自美国的大学、研究机构等非商业用户.

由于 Abilene 网络具有很高的分组速率,测量装置无法捕获流数据中的每个分组,因此,Abilene 网络使用 1% 的采样率收集网络中每个边界路由器的流数据.我们根据 BGP 和 ISIS 选路表识别出每条流的入口点和出口点,然后每隔 5 分钟计算出该时间间隔内每个 OD 对的流量大小.本文使用的流量矩阵数据集总结见表 1.需要指出的是,表 1 中的数据集来自因特网实测数据,包含了突发流量和异常流量,下面将通过实验证实 MSPCA 异常检测算法能够在突发流量背景下成功地检测出异常流量.

#### 5.1.2 评价方法

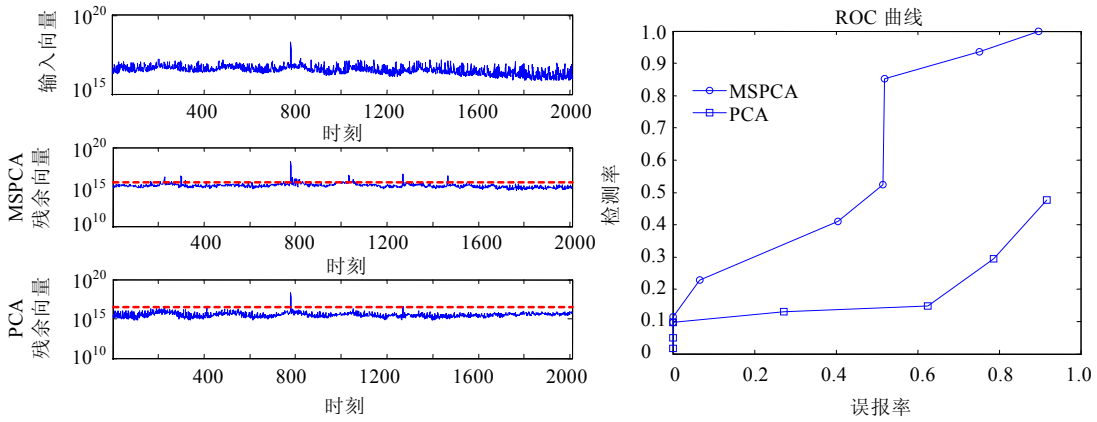
为了评价异常检测算法的检测性能,我们采用接收机工作特性(receiver operation characteristic,简称 ROC)曲线[22].ROC 曲线的 $x$ 轴坐标表示误报率(false positive rate,简称 FPR),$y$ 轴坐标表示检测率(true positive rate,简称 TPR).ROC 曲线上的每个点对应一对误报率和检测率,每条 ROC 曲线反映了检测算法在各种检测阈值条件下的误报率和检测率的折中.如果 ROC 曲线的纵坐标随着横坐标的逐渐增加而迅速到达图的左上角,则表明算法仅仅以很小的误报率取得很高的检测率,即算法具有很好的检测性能.为了定量评价算法的检测性能,人们通常以 ROC 曲线下方覆盖的区域面积作为衡量检测性能好坏的指标,算法的 ROC 曲线下方覆盖的区域面积越大,算法的检测性能就越好.

#### 5.1.3 检测性能

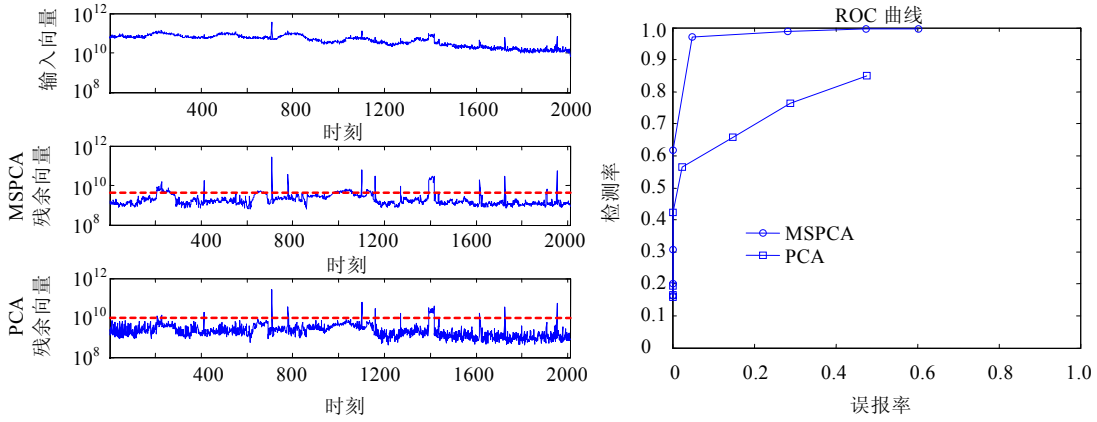
对表 1 中的数据集 *B*、数据集 *P* 和数据集 *F* 分别应用 MSPCA 和 PCA 算法.MSPCA 算法采用 Shewart 控制图和 db5 小波,检测结果及检测性能如图 3 所示.可以看出,对于 3 个不同的数据集,MSPCA 算法的检测性能均优于 PCA 算法.特别地,对于数据集 P,MSPCA 算法仅仅以小于 0.1 的误报率取得了 0.95 的检测率;对于数据集 *F*,MSPCA 算法仅仅以小于 0.1 的误报率取得了 0.85 的检测率.

对表 1 中的数据集 *B*、数据集 *P* 和数据集 *F* 分别应用 MSPCA 算法和在线 MSPCA 算法,两种算法均采用 db5 小波和 EWMA 控制图,平滑指数 $\alpha$=0.3,在线 MSPCA 算法的滑动窗口长度为 $2^9$,检测结果及检测性能如图 4 所示.可以看出,对于 3 个数据集,在线 MSPCA 算法的检测性能均与 MSPCA 算法非常接近.特别地,对于数据集 *P*,在线 MSPCA 算法仅仅以 0.3 的误报率取得了 0.85 的检测率;对于数据集 *F*,在线 MSPCA 算法仅仅以 0.25 的误报率取得了 0.85 的检测率.

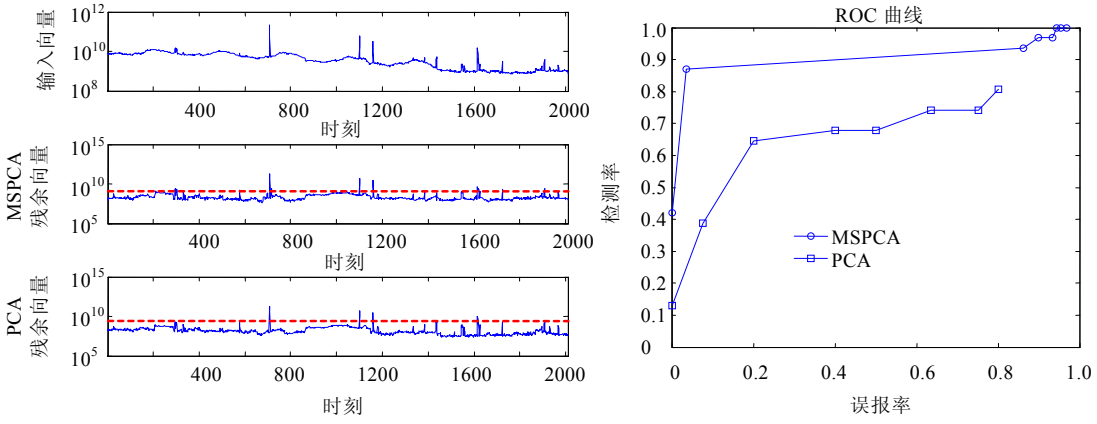
对表 1 中的数据集 *B*、数据集 *P* 和数据集 *F* 分别应用 MSPCA 算法和 KLE 算法[16].MSPCA 算法采用 Shewart 控制图和 db5 小波,KLE 算法的时间相关性幅度 $N$=2.两种算法的检测性能如图 5 所示,可以看出,对于 3 个不同的数据集,MSPCA 算法的检测性能均优于 KLE 算法.




(a) 数据集 *B*



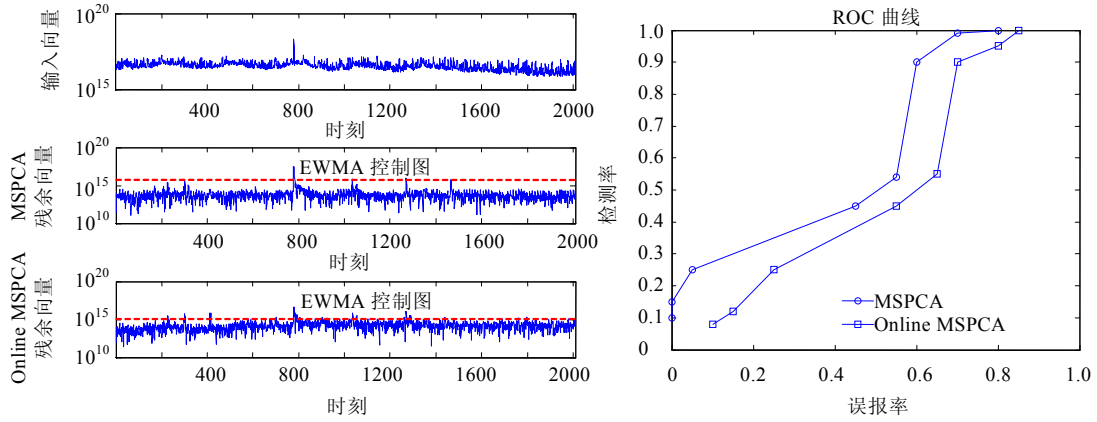

(b) 数据集 *P*



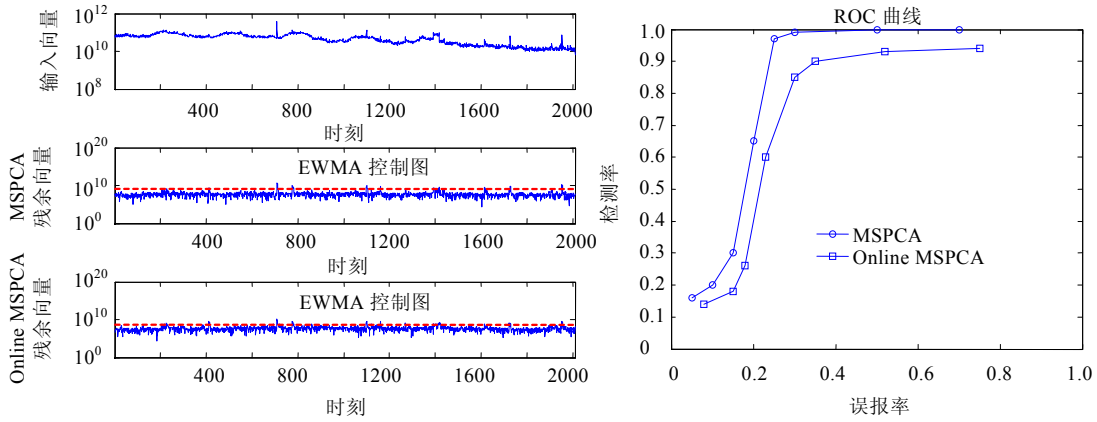

(c) 数据集 *F*

Fig.3 Detection result and performance of MSPCA and PCA algorithm for real measurement data

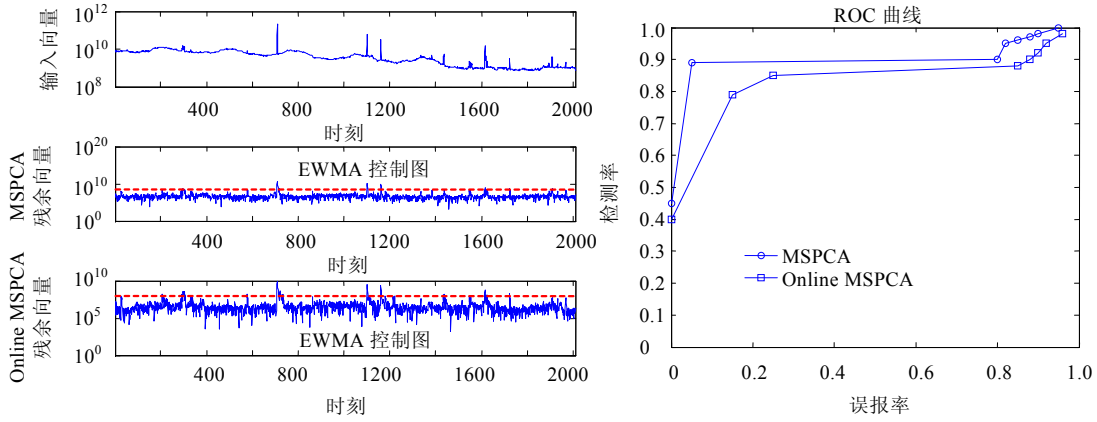
图 3 MSPCA 和 PCA 算法对实测数据的检测结果和检测性能




(a) 数据集 *B*



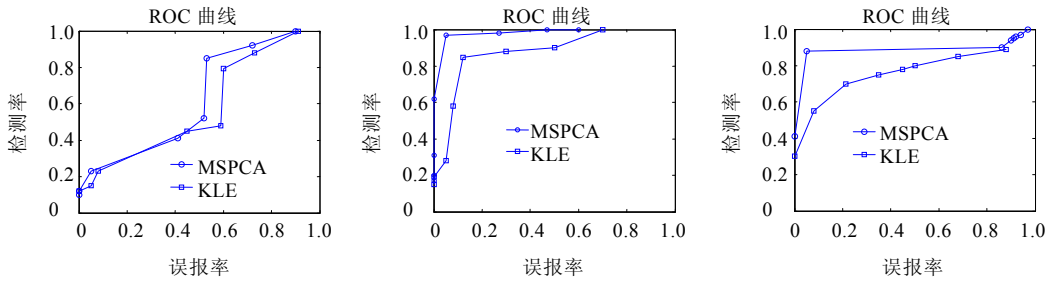

(b) 数据集 *P*




(c) 数据集 *F*

Fig.4 Detection result and performance of MSPCA and online MSPCA algorithm for real measurement data

图 4 MSPCA 和在线 MSPCA 算法对实测数据的检测结果和检测性能




(a) 数据集 *B* (b) 数据集 *P* (c) 数据集 *F*

Fig.5 Detection result and performance of MSPCA and KLE algorithm for real measurement data

图 5 MSPCA 和 KLE 算法对实测数据的检测结果和检测性能

### 5.2 模拟实验与分析

5.2.1 实验方法

为了在受控条件下模拟真实的因特网流量矩阵,本文以表 1 中实测的因特网流量矩阵为基础,采用以下 3 个步骤人工合成流量矩阵:

第 1 步.对流量矩阵中每个 OD 流量,利用小波变换抽取周期性的正常流量.本文利用 db5 小波对 OD 流量进行小波分解,获得尺度函数系数向量,然后利用小波重构算法单支重构出平滑的低频信号,滤除了包含噪声和异常的高频信号.

第 2 步.在第 1 步产生的基准流量矩阵的每个 OD 流量上加入零均值的高斯噪声,获得不含异常的基准流量矩阵.

第 3 步.在第 2 步产生的含噪音的基准流量矩阵中,以一定的规则加入各种典型异常.

采用以上 3 个步骤对数据集 *F* 中 OD1 流量进行处理,获得的结果如图 6 所示.

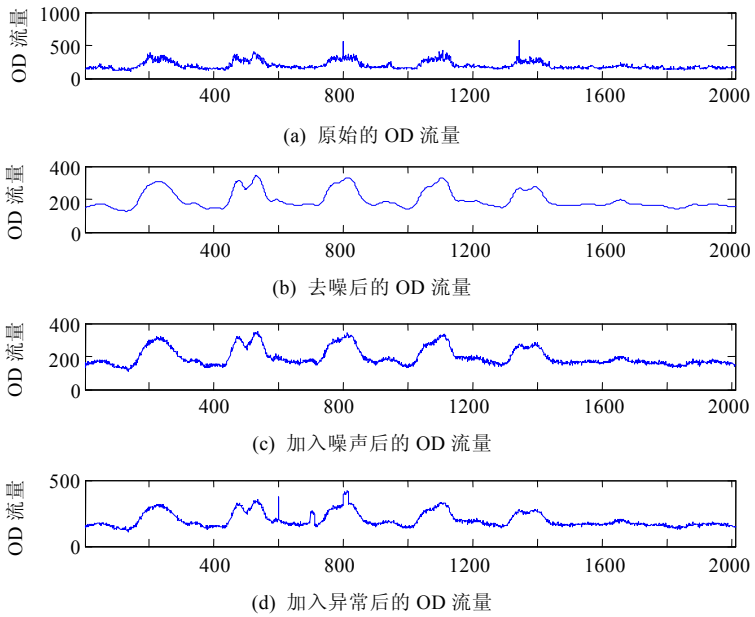



Fig.6 Three steps of synthesis traffic matrix

图 6 人工合成流量矩阵的 3 个步骤

由于本文重点关注流量大小异常的检测,所以我们模拟 4 种最常见的流量异常[22]:阿尔法(alpha)异常、(分布式)拒绝服务攻击(DoS/DDoS)、突发流(flash crowd)、入口/出口移动(ingress/egress shift)异常.这 4 种异常的具体特征见表 2.可以用 4 个参数来描述这 4 种网络流量异常:持续时间、流量变化大小、源-目的数以及形状函数.各种异常通常具有不同的持续时间,例如拒绝服务攻击通常持续 5~30 分钟;阿尔法和突发流异常可能持续任意时间;而入口/出口移动异常通常持续很多天,直到发生下次 BGP 策略变化.当网络异常出现时,可以用两种方式模拟流量大小的变化:一是通过为基准流量矩阵中部分 OD 流乘上一个乘法因子$\delta$,二是通过为基准流量矩阵中部分 OD 流加上一个常数项$\Delta$.源-目的数是指异常所涉及的 OD 流的数目,记号(1,1)表示异常涉及单个源和单个目的地,这可能是由于拒绝服务攻击或阿尔法事件;($N$,1)表示异常涉及 $N$ 个源点和 1 个目的地,这可能是由于出现了分布式拒绝服务攻击或突发流;(2,2)表示异常涉及 2 个源点和 2 个目的地,这可能是由于入口/出口移动事件引起的.形状函数用来模拟各种异常的变化行为.如阿尔法异常通常表现为流量大小的急剧上升;拒绝服务攻击通常表现为流量大小的逐渐上升;突发流事件通常表现为流量大小的迅速上升,然后又逐渐减少;而入口/出口移动表现为流量大小的阶跃变化.以上 4 个参数的可能取值见表 3.

**Table 2** Anomaly types and their characteristics

**表 2** 异常类型及其特征

| 异常类型 | 特征 |
|---|---|
| 阿尔法 | 点到点之间不寻常的高速字节传输 |
| (分布式)拒绝服务攻击 | 单源或多源对单个目的地的洪泛攻击 |
| 突发流 | 大量客户同时访问某一Web站点 |
| 入口/出口移动 | BGP策略变化引起流量出口点的变化 |

**Table 3** Anomaly parameters and their values

**表 3** 异常参数及其取值

| 参数 | 持续时间 | 流量变化 | 源-目的数 | 形状函数 |
|---|---|---|---|---|
| 可能的取值 | 分钟、小时、天 | 常数项$\Delta$,乘法因子$\delta$ | (1,1),($N$,1),(2,2) | 斜坡、指数、阶跃 |

5.2.2 检测性能

以表 1 中的流量矩阵数据集 $F$ 为基础,人工合成流量矩阵,注入 4 类不同的流量异常.其中,从第 1~500 时刻注入 10 组阿尔法异常,每组异常持续 30 分钟,增加的异常流量为原始 OD 流量均值的 50%(即$\delta$=0.5),涉及的源-目的 OD 数为(1,1),异常的形状函数为阶跃函数;从第 501~1 000 时刻注入 10 组 DDoS 攻击异常,每组异常持续 30 分钟,增加的异常流量为原始 OD 流量均值的 40%~50%(即 0.4≤$\delta$≤0.5),涉及的源-目的 OD 数为(5,1),异常的形状函数为斜坡函数;从第 1 101~1 150 时刻注入 1 组突发流异常,异常持续 250 分钟,增加的异常流量为原始 OD 流量均值的 20%~50%(即 0.2≤$\delta$≤0.5),涉及的源-目的 OD 数为(5,1),异常的形状函数为斜坡函数;从第 1 981~2 010 时刻注入 1 组入口/出口移动异常,异常持续 150 分钟,增加的异常流量为原始 OD 流量均值的 80%(即$\delta$=0.8),涉及的源-目的 OD 数为(1,1),异常的形状函数为阶跃函数.对合成的流量矩阵分别应用 MSPCA 算法和 PCA 算法,MSPCA 算法采用 Shewart 控制图和 db5 小波,检测结果及检测性能如图 7 所示.可以看出,MSPCA 算法的检测性能优于 PCA 算法.特别地,MSPCA 算法仅仅以 0.2 的误报率取得了 0.9 的检测率.

以表 1 中的流量矩阵数据集 $F$ 为基础,人工合成流量矩阵,从第 501~1 000 时刻注入 10 组 DDoS 攻击异常,每组异常持续 30 分钟,增加的异常流量为原始 OD 流量均值的 50%(即$\delta$=0.5),涉及的源-目的 OD 数为(5,1),异常的形状函数为阶跃函数.对合成的流量矩阵分别应用 MSPCA 算法和在线 MSPCA 算法,两种算法均采用 EWMA 控制图和 db5 小波,平滑指数$\alpha$=0.3,在线 MSPCA 算法的滑动窗口长度为 $2^9$,检测结果及检测性能如图 8 所示.可以看出,在线 MSPCA 算法的检测性能非常接近 MSPCA 算法.特别地,在线 MSPCA 算法仅仅以 0.25 的误报率取得了 0.8 的检测率.

采用与上面相同的方式合成流量矩阵,分别应用 MSPCA 算法和 KLE 算法[16],MSPCA 算法采用 Shewart 控制图和 db5 小波,KLE 算法的时间相关性幅度 $N$=2.两种算法的检测性能如图 9 所示,可以看出,MSPCA 算法

的检测性能优于 KLE 算法.

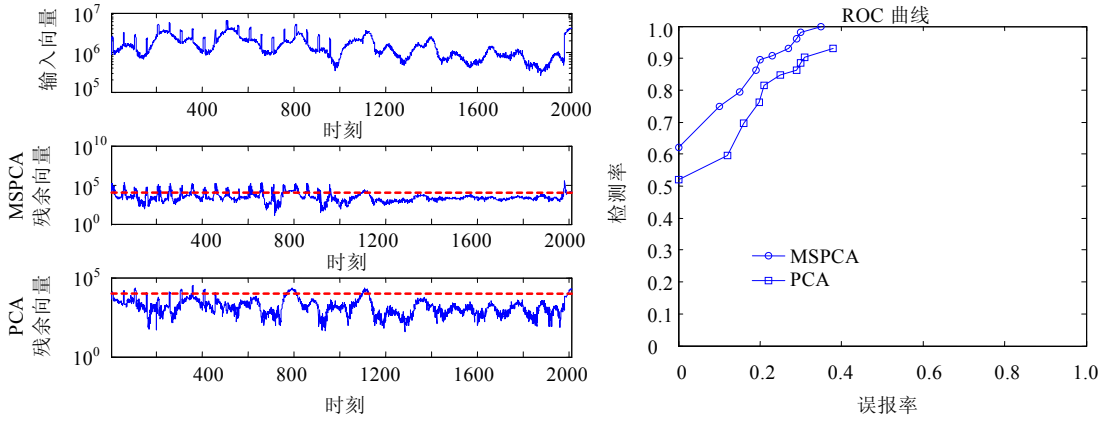



Fig.7 Detection result and performance of MSPCA and PCA algorithm for simulation experiment data

图 7 MSPCA 和 PCA 算法对模拟实验数据的检测结果和检测性能

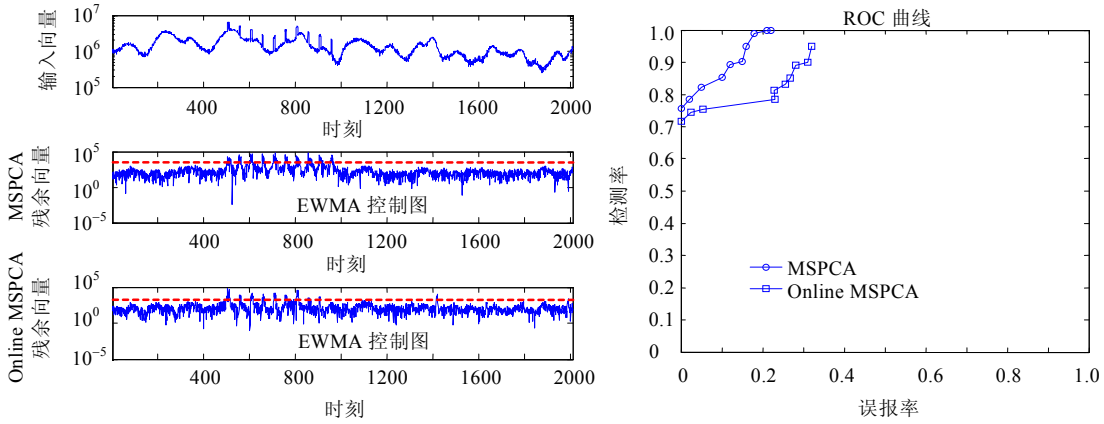



Fig.8 Detection result and performance of MSPCA and online MSPCA algorithm for simulation experiment data

图 8 MSPCA 和在线 MSPCA 算法对模拟实验数据的检测结果和检测性能

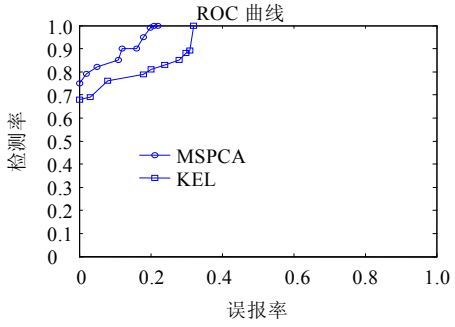



Fig.9 Detection result and performance of MSPCA and KLE algorithm for simulation experiment data

图 9 MSPCA 和 KLE 算法对模拟实验数据的检测结果和检测性能

5.2.3 参数分析

为了验证不同的小波算法是否对 MSPCA 算法的检测性能有影响,本文对第 5.2.2 节合成的流量矩阵数据

应用 MSPCA 算法.当采用不同的小波算法时,检测结果和检测性能如图 10 所示.可以看出,当 MSPCA 算法采用不同的小波算法时,产生的检测性能几乎相同.在线 MSPCA 算法中,最重要的参数是滑动窗口长度 *WIN*.为了验证不同的滑动窗口长度是否对在线 MSPCA 算法的检测性能有影响,本文对第 5.2.2 节合成的流量矩阵数据应用在线 MSPCA 算法.当采用不同的滑动窗口长度时,检测结果和检测性能如图 11 所示.可以看出,当在线 MSPCA 算法采用的滑动窗口越长,算法的检测性能越好.但是,随着滑动窗口长度的增加,在线 MSPCA 算法单步执行所需的时间越长.因此,在选择滑动窗口长度的取值时,应该寻求检测性能和检测时间的折中.

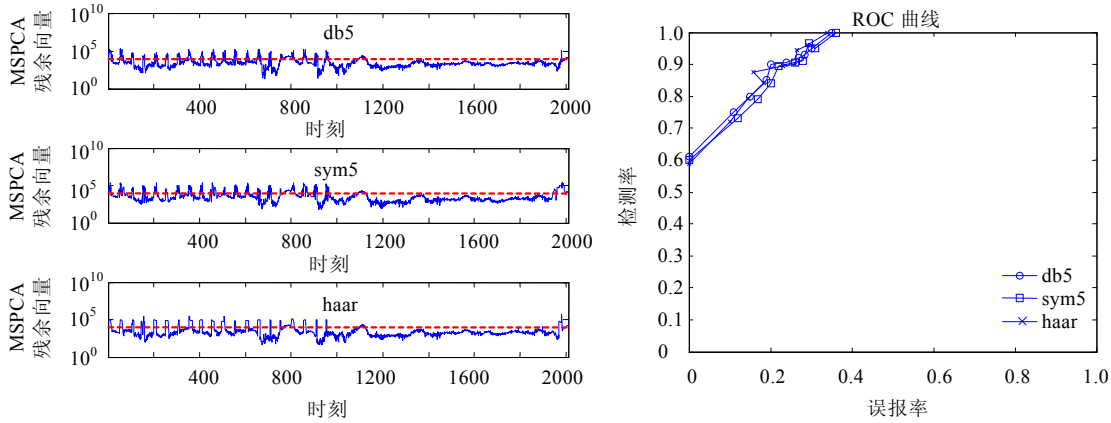



Fig.10 Detection result and performance of MSPCA algorithm with different wavelet algorithms

图 10 MSPCA 算法采用不同小波算法时的检测结果和检测性能

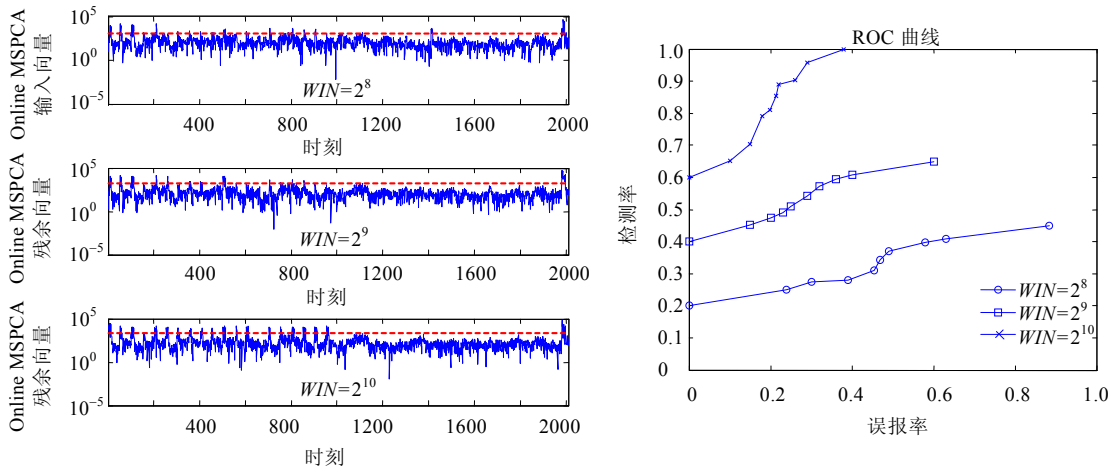



Fig.11 Detection result and performance of online MSPCA algorithm with different sliding window lengths

图 11 在线 MSPCA 算法采用不同滑动窗口长度时的检测结果和检测性能

### 5.2.4 敏感性分析

MSPCA 算法可以采用 Shewart 控制图或 EWMA 控制图.为了分析这两种不同的残余流量分析方法对异常流量大小的敏感性,我们在第 1 500~1 700 时刻之间注入 DDoS 攻击流量,不断改变异常流量的大小,两种 MSPCA 算法的检测率和误报率如图 12 所示,其中,横坐标表示乘法因子$\delta$.可以看出,随着异常流量的增大,两种 MSPCA 算法的检测率均增加,误报率均减小.当异常流量较小时,EWMA 控制图获得的检测性能优于 Shewart 控制图;当异常流量较大时,Shewart 控制图获得的检测性能优于 EWMA 控制图.因此,EWMA 控制图适合于检测较小的异常流量,而 Shewart 控制图适合于检测较大的异常流量.

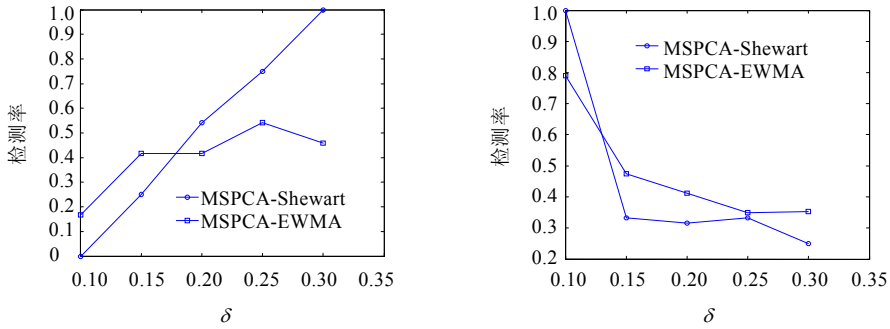



Fig.12 Detection performance of online MSPCA algorithm with different anomaly traffic volumes

图 12 MSPCA 算法对不同大小异常流量的检测性能

## 6 结 论

现有的异常检测方法仅仅单独利用流量的时间相关性或空间相关性.针对这一不足,本文同时考虑流量矩阵的时空相关性,综合利用小波变换具有的多尺度建模能力和 PCA 具有的降维能力,采用 Shewart 控制图和 EWMA 控制图两种残余流量分析方法,提出了一种基于 MSPCA 的全网络异常检测方法.并且利用滑动窗口机制对 MSPCA 异常检测方法进行在线扩展,提出了一种在线的 MSPCA 异常检测方法.因特网实测数据分析和模拟实验分析表明:MSPCA 算法的检测性能优于 PCA 算法和近期提出的 KLE 算法;在线 MSPCA 算法的检测性能非常接近 MSPCA 算法,且单步执行时间较短,完全满足实时检测的需要.此外,实验分析还证实 EWMA 控制图适合于检测较小的异常流量,而 Shewart 控制图适合于检测较大的异常流量.下一步,我们将在异常检测的基础上进一步研究异常分类的方法以及如何针对不同类型的异常采取相应的防御措施.

**致谢** 感谢南京航空航天大学陈松灿教授在本文的研究过程中给予的指导和帮助,感谢瑞士苏黎世联邦工学院 Daniela Brauckhoff 博士提供的 KLE 算法代码.

**References**:

[1] Barford P, Kline J, Plonka D, Amos R. A signal analysis of network traffic anomalies. In: Proc. of the ACM SIGCOMM Internet Measurement Workshop. New York: ACM Press, 2002. 56−67. [doi: 10.1145/637201.637210]

[2] Hussain A. Measurement and spectral analysis of denial of service attacks [Ph.D. Thesis]. Information Sciences Institute, 2005.

[3] Lakhina A, Crovella M, Diot C. Diagnosing network-wide traffic anomalies. In: Proc. of the ACM SIGCOMM. New York: ACM Press, 2004. 65−76. [doi: 10.1145/1030194.1015492]

[4] Lakhina A, Crovella M, Diot C. Characterization of network-wide anomalies in traffic flows. In: Proc. of the ACM Internet Measurement Conf. New York: ACM Press, 2004. 34−45. [doi: 10.1145/1028788.1028813]

[5] Denning D. An intrusion-detection model. IEEE Trans. on Software Engineering, 1987,13(2):222−232. [doi: 10.1109/TSE.1987.232894]

[6] Xie Y, Yu SZ. Anomaly detection based on Web users' browsing behaviors. Journal of Software, 2007,18(4):967−977 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/967.htm [doi: 10.1360/jos180967]

[7] Li Y, Fang BX, Guo L, Chen Y. A network anomaly detection method based on transduction scheme. Journal of Software, 2007, 18(10):2595−2604 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2595.htm [doi: 10.1360/jos182595]

[8] Lin GY, Guo SQ, Huang H, Cao TJ. An anomaly detection model based on dynamic behavior and character patterns. Chinese Journal of Computers, 2006,29(9):1553−1560 (in Chinese with English abstract).

[9] Wu SY, Tian XG. Method for anomaly detection of user behaviors based on hidden Markov models. Journal on Communications, 2007,28(4):38−43 (in Chinese with English abstract).

[10] Dainotti A, Pescape A, Ventre G. NIS04-1: Wavelet-Based detection of DoS attacks. In: Proc. of the IEEE GLOBECOM. New York: IEEE Press, 2006. 1−6. [doi: 10.1109/GLOCOM.2006.279]

[11] Zhang L. Functional singular value decomposition and multiresolution anomaly detection [Ph.D. Thesis]. Chapel Hill: University of North Carolina, 2007.

[12] Lu W, Ghorbani AA. Network anomaly detection based on wavelet analysis. EURASIP Journal on Advances in Signal Processing, 2009,12(5):1234−1249. [doi: 10.1155/2009/837601]

[13] Ringberg H, Soule A, Rexford J, Diot C. Sensitivity of PCA for traffic anomaly detection. In: Proc. of the ACM SIGMETRICS. New York: ACM Press, 2007. 78−89. [doi: 10.1145/1269899.1254895]

[14] Rubinstein BIP, Nelson B, Huang L, Joseph AD, Lau SH, Taft N, Tygar JD. Compromising PCA-based anomaly detectors for network-wide traffic. Technical Report, EECS-2008-73, Berkeley: UC Berkeley, 2009. 1−16.

[15] Rubinstein BIP, Nelson B, Huang L, Joseph AD, Lau SH, Rao S, Taft N, Tygar JD. Stealthy poisoning attacks on PCA-based anomaly detectors. In: Proc. of the ACM SIGMETRICS. New York: ACM Press, 2009. [doi: 10.1145/1639562.1639592]

[16] Brauckhoff D, Salamatian K, May M. Applying PCA for traffic anomaly detection: problems and solutions. In: Proc. of the INFOCOM. New York: IEEE Press, 2009. 46−53. [doi: 10.1109/INFCOM.2009.5062248]

[17] Zhou JJ, Yang JH, Yang Y, Zhang H. Research development on traffic matrix estimation. Journal of Software, 2007,18(11): 2669−2682 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2669.htm [doi: 10.1360/jos182669]

[18] Donoho DL, Johnstone IM, Kerkyacharian G, Dominque P. Wavelet shrinkage: asymptopia? Journal of the Royal Statistical Society, Series B, 1995,57(2):301−369. [doi: 10.2307/2345967]

[19] Bakshi BR. Multiscale PCA with application to multivariate statistical process monitoring. AIChE Journal, 1998,44(7):1596−1610. [doi: 10.1002/aic.690440712]

[20] Bersimis S, Psarakis S, Panaretos J. Multivariate statistical process control charts: An overview. Quality and Reliability Engineering Int'l, 2007,23(5):517−543. [doi: 10.1002/qre.829]

[21] Mallat SG. A theory for multiresolution signal decomposition: The wavelet representation. IEEE Trans. on Pattern Analysis and Machine Intelligence, 1989,11(7):674−693. [doi: 10.1109/34.192463]

[22] Soule A, Salamatian KE, Taft N. Combining filtering and statistical methods for anomaly detection. In: Proc. of the ACM Internet Measurement Conf. New York: ACM Press, 2005. [doi: 10.1145/1330107.1330147]

**附中文参考文献**:

[6] 谢逸,余顺争.基于 Web 用户浏览行为的统计异常检测.软件学报,2007,18(4):967−977. http://www.jos.org.cn/1000-9825/18/967.htm [doi: 10.1360/jos180967]

[7] 李洋,方滨兴,郭莉,陈友.基于直推式方法的网络异常检测方法.软件学报,2007,18(10):2595−2604. http://www.jos.org.cn/1000-9825/18/2595.htm [doi: 10.1360/jos182595]

[8] 林果园,郭山清,黄皓,曹天杰.基于动态行为和特征模式的异常检测模型.计算机学报,2006,29(9):1553−1560.

[9] 邬书跃,田新广.基于隐马尔可夫模型的用户行为异常检测新方法.通信学报,2007,28(4):673−678.

[17] 周静静,杨家海,杨扬, 张辉.流量矩阵估算的研究进展.软件学报,2007,18(2):2669−2681. http://www.jos.org.cn/1000-9825/18/2669.htm [doi: 10.1360/jos182669]

## 附录. 流量矩阵的时空特性分析

流量矩阵的时空相关性是基于流量矩阵的全网络异常检测方法有效性的前提条件.为此,本文应用小波变换对流量矩阵进行多尺度分析,揭示其时间相关性;在每个尺度上,应用主成分分析方法对小波系数矩阵进行单尺度主成分分析,揭示其在各个时间尺度上的空间相关性.

1. 多尺度分析

$T\times p$ 的流量矩阵 $\boldsymbol{X}$ 是由 $p$ 个 OD 流量构成的多元时间序列,而每个 OD 流量都是许多不同的用户群行为共同作用的结果,那么这些 OD 流量在不同的时间尺度下是否具有不同的特征呢?为了回答这个问题,我们引入小波分析方法.

小波基函数是由同一母函数$\psi(t)$经过伸缩和平移后得到的一组函数序列,可以记作

$$\psi_{su}(t)=\frac{1}{\sqrt{s}}\psi\left(\frac{t-u}{s}\right) \tag{5}$$

其中,$s$ 和 $u$ 分别表示伸缩和平移因子.

在实际应用中,伸缩和平移因子通常被二进离散化,此时,小波函数族表示为

$$\psi_{mk}(t)=2^{-m/2}\psi(2^{-m}t-k) \tag{6}$$

其中,$m$ 表示伸缩因子,它决定小波在频域中的位置,即尺度;$k$ 表示平移因子,它决定小波在时域中的位置.

公式(6)表示的小波基函数可以被设计为相互标准正交,如 Daubechies 小波.

任何信号通过向小波基函数进行投影都可以被分解为不同频率的成分.与滤波器 $\boldsymbol{H}$ 的卷积表示向尺度函数的投影,与滤波器 $\boldsymbol{G}$ 的卷积表示向小波函数的投影,则不同尺度下的系数可以表示如下:

$$\boldsymbol{a}_m=\boldsymbol{H}\boldsymbol{a}_{m-1},\boldsymbol{d}_m=\boldsymbol{G}\boldsymbol{a}_{m-1} \tag{7}$$

其中,$\boldsymbol{d}_m$ 表示尺度为 $m$ 的小波函数系数向量,$\boldsymbol{a}_m$ 表示尺度为 $m$ 的尺度函数系数向量.如果将原始数据 $\boldsymbol{x}$ 看作最细尺度上的尺度函数系数向量,则公式(7)可以表示为

$$\boldsymbol{a}_m=\boldsymbol{H}_m\boldsymbol{x},\boldsymbol{d}_m=\boldsymbol{G}_m\boldsymbol{x} \tag{8}$$

其中,$\boldsymbol{H}_m$ 表示应用 $\boldsymbol{H}$ 滤波器 $m$ 次;$\boldsymbol{G}_m$ 表示应用 $\boldsymbol{H}$ 滤波器 $m$–1 次,且应用 $\boldsymbol{G}$ 滤波器 1 次.

根据公式(8)中不同尺度对应的尺度函数系数向量 $\boldsymbol{a}_m$ 和小波函数系数向量 $\boldsymbol{d}_m$,可以单支重构出不同尺度下的低频和高频信号成分;而且根据所有尺度对应的尺度函数系数向量 $\boldsymbol{a}_m(m=1,\ldots,L)$和最粗尺度 $L$ 对应的小波函数系数向量 $\boldsymbol{d}_m(m=L)$,可以重构出原始信号.

对表 1 中数据集 $F$ 中每列 OD 流量进行小波分析,其中,第 1 列和第 121 列的 OD 流量原始信号和对应的小波分解结构如图 13 所示.可以看出,尺度函数系数明显大于小波函数系数.因此,这两个 OD 流量原始信号中确定性成分完全由低频信号构成,而随机性成分则由高频信号构成.为了进一步分析这两个 OD 流量原始信号中确定性成分和随机性成分的具体特性,我们根据不同尺度对应的尺度函数系数向量和小波函数系数向量,单支重构出不同尺度下的低频和高频信号成分,如图 14 所示.可以看出,低频成分 $a_5$ 具有显著的周期性,且周期约为 1 天,它们是正常流量呈现出的周期性波动现象;其他高频成分中除了噪音成分以外,还包含一些突发的随机性信号,它们是各种不同频率的异常流量.

为了将信号中确定性成分和随机性成分分离,本文采用中位绝对偏差(median absolute deviation,简称 MAD)方法[19]对所有尺度的小波系数向量进行过滤.根据过滤后所有尺度的小波系数向量,我们重构出 OD 流量原始信号,如图 15 所示.可见,重构信号保留了原始信号中确定性的变化趋势,滤除了各种随机性的异常信号成分.对表 1 中 3 个流量矩阵数据集的所有 OD 流量进行同样的分析,可以获得类似的结论.

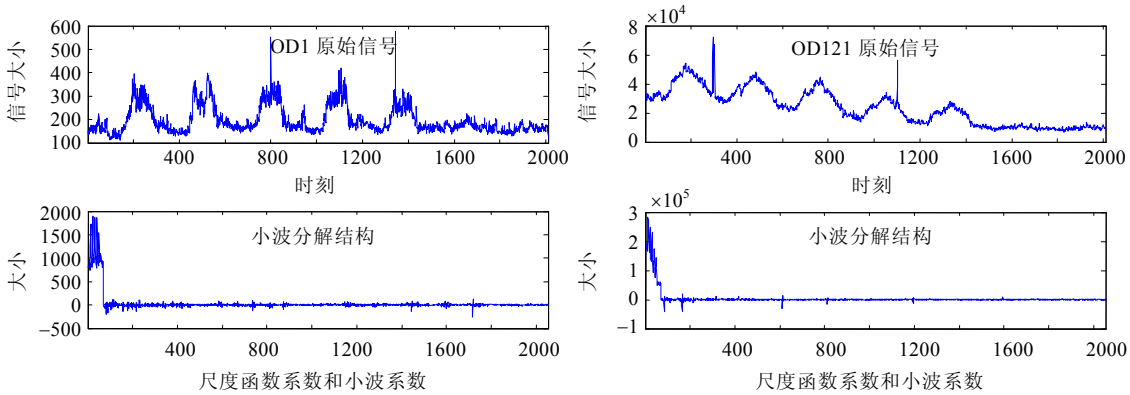



Fig.13 Original signal and wavelet decomposition structure of OD1 (left) and OD121 (right) traffic

图 13 OD1(左)和 OD121(右)流量原始信号及其小波分解结构

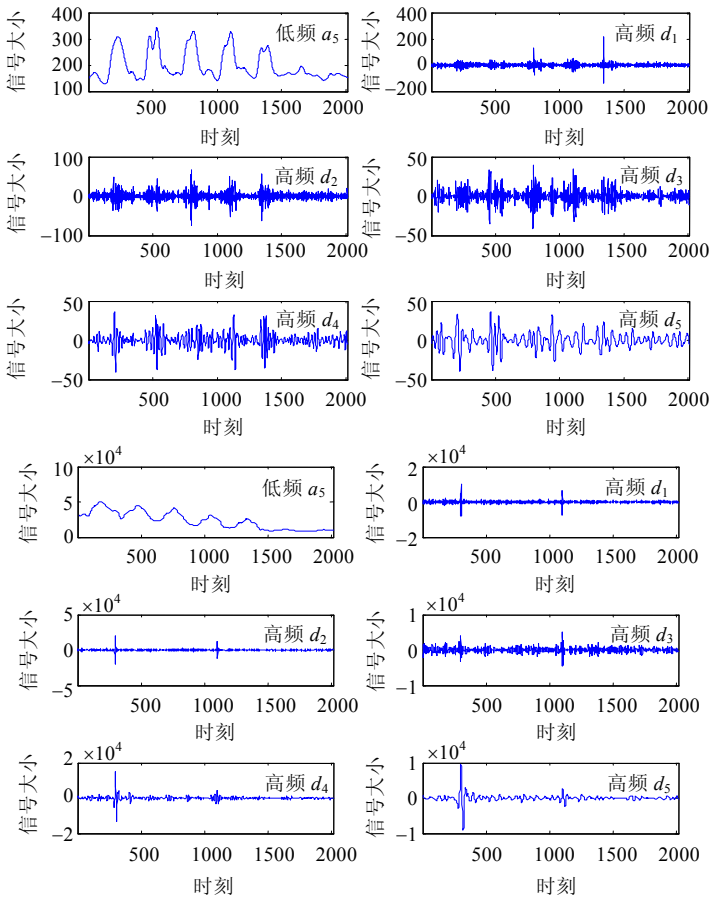



Fig.14 Low frequency and high frequency components of OD1 (up) and OD121 (down) traffic signal

图 14 OD1(上)和 OD121(下)流量信号的低频和高频成分

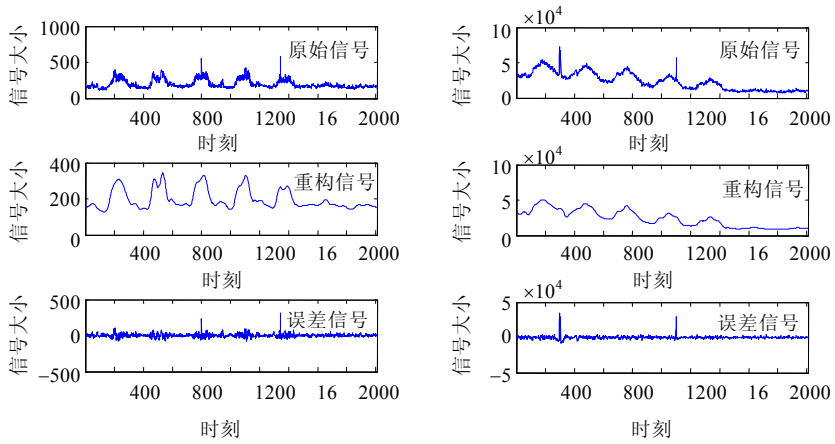



Fig.15 Original signal and wavelet reconstruction of OD1 (left) and OD121 (right) traffic

图 15 OD1(左)和 OD121(右)流量原始信号及其重构

2. 单尺度主成分分析

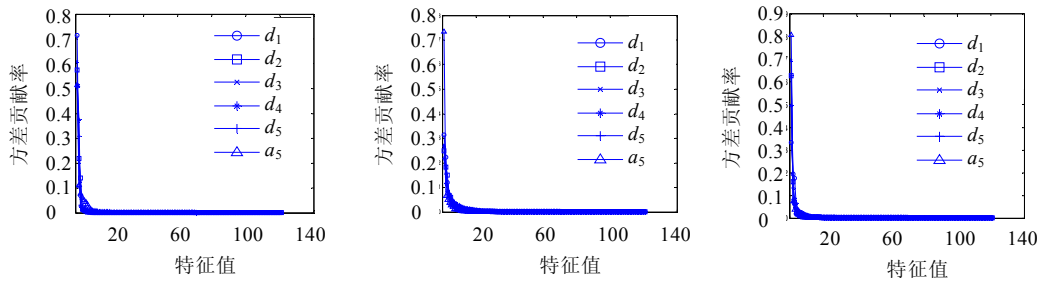
为了在各个时间尺度上对流量矩阵 $\boldsymbol{X}$ 进行单尺度主成分分析,本文对流量矩阵 $\boldsymbol{X}$ 的每列应用同样的标准正交小波变换 $\boldsymbol{W}$,获得各个尺度上的小波系数矩阵,其中,

$$\boldsymbol{W}=[\boldsymbol{H}_L,\boldsymbol{G}_L,\boldsymbol{G}_{L-1},\ldots,\boldsymbol{G}_m,\ldots,\boldsymbol{G}_L]^T \tag{9}$$

$\boldsymbol{G}_m$ 表示尺度为 $m=1,\ldots,L$ 对应的小波函数系数矩阵,$\boldsymbol{H}_L$ 表示最粗尺度对应的尺度函数系数矩阵.

由于流量矩阵 $\boldsymbol{X}$ 的每列应用同样的标准正交小波变换 $\boldsymbol{W}$,所以,$\boldsymbol{WX}$ 不同列之间的关系与 $\boldsymbol{X}$ 不同列之间的关系完全相同,即 $\boldsymbol{X}$ 在小波变换前后不同列之间的互相关性没有发生变化.所以,我们可以通过对 $\boldsymbol{WX}$ 中不同尺度的小波系数矩阵进行主成分分析来实现对 $\boldsymbol{X}$ 在不同时间尺度下空间相关性的分析[3].

图 16 显示了表 1 中 $B,P,F$ 这 3 个数据集中每个主轴对应的方差贡献率.可以看出,如果选取累计方差贡献率阈值为 0.85,则这 3 个数据集的固有维度都不超过 5<<121.因此,这 3 个数据集的所有小波系数矩阵均具有低维度特性.这是因为不同的 OD 流量可能来自某些共同的用户群体,而且这些用户群体的行为呈现不同的时间尺度,所以相应地,这些 OD 流量在各个时间尺度下均存在空间相关性.




(a) 数据集 $B$ (b) 数据集 $P$ (c) 数据集 $F$

Fig.16 Variance contribution ratio of principal axes

图 16 主轴的方差贡献率


**钱叶魁**(1980－),男,安徽安庆人,博士,讲师,CCF 学生会员,主要研究领域为网络测量,网络安全.

**陈鸣**(1956－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络测量,网络体系结构,网络管理.

**叶立新**(1966－),男,副教授,主要研究领域为系统工程.

**刘凤荣**(1961－),男,教授,主要研究领域为网络安全.

**朱少卫**(1976－),男,讲师,主要研究领域为武器系统与运用工程.

**张晗**(1980－),女,讲师,主要研究领域为网络安全.