# NMF-NAD：基于 NMF 的全网络流量异常检测方法

魏祥麟，陈鸣，张国敏，黄建军
(解放军理工大学 指挥自动化学院，江苏 南京 210007)

**摘 要**：提出了一种基于非负矩阵分解 (NMF, non-negative matrix factorization) 的多元异常检测算法 (NMF-NAD, NMF based network-wide traffic anomalies detection)，该算法首先采用非负子空间方法对流量矩阵进行重构，然后基于重构误差利用 Shewhart 控制图进行异常检测。模拟实验与因特网实测数据的分析表明，NMF-NAD 算法有较高的检测精度和较低的处理复杂度。

**关键词**：网络流量；异常检测；非负矩阵分解；连续异常
**中图分类号**：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)04-0054-08

# NMF-NAD: detecting network-wide traffic anomaly based on NMF

WEI Xiang-lin, CHEN Ming, ZHANG Guo-min, HUANG Jian-jun
(Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China)

**Abstract:** A non-negative matrix factorization (NMF) based network wide traffic anomalies detection (NMF-NAD) method was proposed. NMF-NAD firstly reconstructed the traffic matrix in the non-negative sub-space, and then detected the anomalies through Shewhart control chart based on the reconstruction error. Experimental results on both simulation and Abilene data show that NMF-NAD can achieve high detection accuracy with low complexity.

**Key words:** network traffic; anomaly detection; non-negative matrix factorization; continuous anomalies

## 1 引言

因特网已经成为人类生活的重要基础设施，而因网络设备误配置、网络故障、网络安全事件（如分布式拒绝服务攻击、蠕虫传播等）以及不寻常的用户行为等导致的网络异常事件时有发生，严重地干扰了网络的正常运行。然而，在高速且持续变化的链路上准确地检测出网络流量异常，进而维护网络的平稳运行，是因特网服务提供者(ISP)面临的难题，也是网络研究的热点问题之一。

网络流量异常是指网络流量不寻常地和显著地变化，并且可能涵盖多条链路或者路径[1]。检测流量异常面临的主要难点在于：第一，因特网流量的高波动和长相关性会使异常流量淹没于正常的流量之中；第二，流量异常模式非常分散并且经常出现新型异常流量；第三，网络流量巨大，分布式收集和处理很困难；第四，异常检测的实用化要求做到早期检测，对时效性要求较高。

很多异常行为(如 DDoS 攻击以及蠕虫传播等等)的全局特性使得传统的单链路方法[2~4]失效，为此，Lakhina 等人[1,5]首次采用基于主成分分析(PCA, principal component analysis)的子空间方法进行全网络(network-wide)异常检测，并取得了较好的效果。流量矩阵经过 PCA 投影后，得到由一组正交基组成的正常子空间，可以看作是流量的某种固有变化模式，而每条链路或者路径的流量则是这组基

**收稿日期**：2011-06-22；**修回日期**：2011-12-09
**基金项目**：国家自然科学基金资助项目（61070173, 61103225）；江苏省自然科学基金资助项目（BK2009058, BK2010133）
**Foundation Items:** The National Natural Science Foundation of China (61070173, 61103225); The Natural Science Foundatior of Jiangsu Province (BK2009058, BK2010133)

向量按照某个系数向量的叠加，这形成了 PCA 异常检测的基础。然而，PCA 存在以下问题。第一，系数向量中时常出现负值，而网络流量不可能为负，使得这个分解过程的含义难以解释。第二，PCA 追求全局误差最小的特性使其容易将连续异常学习为正常流量模式并投影到正常子空间，从而无法有效检测连续突发异常的情况[6,7]。第三，PCA 处理复杂度较高。为此，提出了基于非负矩阵分解(NMF, non-negative matrix factorization)的全网络流量异常检测方法 NMF-NAD (NMF based network wide traffic anomalies detection method)。NMF-NAD 首先采用非负子空间方法提取流量矩阵中的主要时变模式，并用这些时变模式构成流量正常子空间，并以非负的系数向量对原始流量矩阵进行重构，得到重构矩阵和残余矩阵，然后应用 Shewhart 控制图基于残余矩阵进行异常点检测。本文首次将 NMF 应用于全网络流量异常检测领域，并取得了良好的检测效果。

本文的内容安排如下：第 2 节综述相关工作；第 3 节研究 NMF-NAD 算法；第 4 节通过实验验证了 NMF-NAD 算法的有效性；第 5 节是结束语。

## 2　相关工作

在全网络异常检测方面，主要采用多元统计分析的方法，这类方法可以检测覆盖多条链路的流量异常，成为近年来网络研究的热点。当前基于多元统计分析的方法主要包括基于 PCA 的方法和核密度估计的方法。Lakhina 等人证实了流量矩阵具有的低维特性以及不同流之间的空间相关性，首次提出了基于 PCA 的异常检测算法[1,5]，将流量矩阵形成的原始空间分离为正常和异常子空间，并使用 Q 统计量计算阈值以检测网络异常；而且，实测数据分析表明该方法对于较大的流量异常具有较好的检测性能。

但是，近年来的研究[8,9]，以及实际的实验表明，PCA 方法还存在 2 个主要的问题。第一，PCA 方法的检测效果对于其选择的主成分数量以及检测阈值非常敏感。一些基于 PCA 的方法需要人工设定选择的主成分数量才可以取得较好的检测效果，而不同的主成分选择会导致检测精度差别达到 3 倍或者更多。检测阈值更是直接决定了检测率的大小，小的阈值可以达到较高的检测率，但同时也会带来较高的误报率；而大的阈值则会在降低误报率的同时降低检测精度。第二，大的或者连续的异常可以毒害 PCA 的正常子空间。足够大的异常可以显著地污染 PCA 的正常子空间，使得正常子空间的定义出现偏差，导致增加误报率；连续的异常则可以使得 PCA 将其归入正常子空间中，将其当作流量的正常模式，从而降低检测率，这 2 个因素也是用来毒害 PCA 以降低其检测精度的重要方法[10,11]。

钱叶魁等从时空特性出发，提出了基于多尺度 PCA(MSPCA, multiscale PCA)[12]的方法。该方法在进行 PCA 方法之前加入了小波去噪的过程，意在去除数据中的噪声（由于测量数据的错误或不准确导致）并使得数据平滑，然后使用 PCA 方法分离正常和异常子空间，最后使用 Q 统计量计算阈值或者指数滑动平均控制图来检测网络异常。可以看出 MSPCA 方法与 PCA 方法的最主要区别在于其加入了小波去噪过程，而这会减轻大的异常对于正常子空间的影响，从而有可能提高检测精度；第二，MSPCA 方法考虑了采用指数滑动平均控制图来设定检测阈值。

文献[13]提出了基于统计用户行为距离的异常检测方法。为了减小 PCA 算法检测的复杂性，文献[14]提出了分布式实现 PCA 检测的方法。Tarem 等人在文献[7]指出 PCA 方法在检测连续异常时性能较差，并提出了基于核密度估计的检测方法，但这种方法的参数较多，实际检测时需要大量的人工干预。本文方法与已有方法的最大不同在于：在检测连续突发异常时拥有更好的性能，并且分解过程具有更好的可解释性。

## 3　流量矩阵建模及 NMF-NAD 算法

本节首先定义了流量矩阵模型；然后介绍了 NMF 的基本思想，并分析了其与 PCA 的主要区别；最后提出了基于 NMF 的全网络异常检测算法 NMF-NAD，并分析了该算法的复杂度。

### 3.1　流量矩阵和非负矩阵分解

全网络异常检测是基于在多个网络位置经多个测量周期统计得到的流量特征数据进行的[8]。这里的网络位置可以是链路、路由器以及汇聚点等等。流量特征则可以是分组数、流数、字节数以及源 IP 地址熵等各种流量统计信息。为了便于研究，定义流量矩阵 $\boldsymbol{X}$ 为一个 $d \times p$ 的矩阵，其中，$d$ 是测量周期的数量，而 $p$ 是网络位置的数量[8]。$X_{ij}$ 表示在第 $i$ 个测量周期时第 $j$ 个网络位置流量特征数据的测量值。

对于流量矩阵 $\boldsymbol{X}=[X_1,X_2,\cdots,X_p]$，其中，$X_i$ 是第 $i$ 个网络位置的测量值列向量，$X_i\in\boldsymbol{R}^d$，$d$ 是测量周期的数量。NMF 的目标是将 $\boldsymbol{X}$ 分解为 2 个矩阵 $\boldsymbol{U}\in\boldsymbol{R}^{d\times r}$ 和 $\boldsymbol{V}\in\boldsymbol{R}^{r\times p}$，$\boldsymbol{X}\approx\boldsymbol{UV}$，并满足如下目标函数：

$$\min_{\boldsymbol{U}\in\boldsymbol{R}_+^{d\times r},\boldsymbol{V}\in\boldsymbol{R}_+^{r\times p}} \boldsymbol{D}(\boldsymbol{X},\boldsymbol{UV}) \tag{1}$$

其中，$\boldsymbol{R}_+^{d\times r}$ 以及 $\boldsymbol{R}_+^{r\times p}$ 分别表示维度为 $d\times r$ 和 $r\times p$ 的非负矩阵集合。$\boldsymbol{D}(\boldsymbol{X},\boldsymbol{U},\boldsymbol{V})$ 是用于衡量 $\boldsymbol{X}$ 与 $\boldsymbol{UV}$ 的逼近程度的代价函数。本文取如下代价函数[15]：

$$D(\boldsymbol{X},\boldsymbol{UV})=\left\|\boldsymbol{X}-\boldsymbol{UV}\right\|_{\mathrm{F}}^2 \tag{2}$$

其中，$\left\|\cdot\right\|_{\mathrm{F}}^2$ 表示矩阵的 2 范数。

定义了代价函数之后，那么式(2)可以重写为如下带有约束的非线性最优化问题：

$$\begin{aligned} D(\boldsymbol{X},\boldsymbol{UV})&=tr((\boldsymbol{X}-\boldsymbol{UV})(\boldsymbol{X}-\boldsymbol{UV})^{\mathrm{T}})\\ &=tr(\boldsymbol{XX}^{\mathrm{T}})-2tr(\boldsymbol{XV}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}})+tr(\boldsymbol{UVV}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}) \end{aligned} \tag{3}$$

式(3)是一个带约束的非线性规划问题，而约束条件就是 $\boldsymbol{V}$ 非负，可以使用 Lagrange multiplier 方法求解。令 $\boldsymbol{U}=[u_{ij}]$，$\boldsymbol{V}=[v_{ij}]$。令 $\alpha_{ij}$，$\beta_{ij}$ 分别是对应限制条件 $u_{ij}\geqslant 0$ 和 $v_{ij}\geqslant 0$ 的 Lagrange 乘子，并令矩阵 $\boldsymbol{\alpha}=[\alpha_{ij}]$，$\boldsymbol{\beta}=[\beta_{ij}]$。那么拉格朗日函数 $L$ 就如式(4)所示：

$$L=D(\boldsymbol{X},\boldsymbol{UV})+tr(\boldsymbol{\alpha U}^{\mathrm{T}})+tr(\boldsymbol{\beta V}^{\mathrm{T}}) \tag{4}$$

求 $L$ 对于 $\boldsymbol{U}$ 和 $\boldsymbol{V}$ 的偏导如式(5)所示：

$$\begin{cases} \dfrac{\partial L}{\partial \boldsymbol{U}}=-\boldsymbol{XV}^{\mathrm{T}}+\boldsymbol{UVV}^{\mathrm{T}}+\boldsymbol{\alpha}\\ \dfrac{\partial L}{\partial \boldsymbol{V}}=-\boldsymbol{X}^{\mathrm{T}}\boldsymbol{U}+\boldsymbol{V}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}+\boldsymbol{\beta} \end{cases} \tag{5}$$

利用 Kuhn-Tucker 条件 $\alpha_{ij}u_{ij}=0$，$\beta_{ij}v_{ij}=0$，得到式(6)：

$$\begin{cases} (\boldsymbol{XV}^{\mathrm{T}})_{ij}u_{ij}-(\boldsymbol{UVV}^{\mathrm{T}})_{ij}u_{ij}=0\\ (\boldsymbol{X}^{\mathrm{T}}\boldsymbol{U})_{ij}v_{ij}-(\boldsymbol{V}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U})_{ij}v_{ij}=0 \end{cases} \tag{6}$$

从而得到式(7)所示的更新方程：

$$\begin{cases} u_{ij}\leftarrow u_{ij}\dfrac{(\boldsymbol{XV}^{\mathrm{T}})_{ij}}{(\boldsymbol{UVV}^{\mathrm{T}})_{ij}}\\ v_{ij}\leftarrow v_{ij}\dfrac{(\boldsymbol{X}^{\mathrm{T}}\boldsymbol{U})_{ij}}{(\boldsymbol{V}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U})_{ij}} \end{cases} \tag{7}$$

### 3.2 基于 NMF 的全网络流量异常检测

基于 NMF 的全网络流量异常检测主要分为 3 步：构建正常子空间、获取残余矩阵以及异常凸显与检测。

#### 3.2.1 构建正常子空间

对于原始流量矩阵 $\boldsymbol{X}$，第 $i$ 个网络位置的测量值向量可以看作位于 $d$ 维实空间的一个点。由于具有低维特性，因此流量矩阵可以用一个 $r$（$r\ll d$）维子空间表示，而这个 $r$ 维子空间则可以通过 NMF 构建。更具体地说，对 $\boldsymbol{X}$ 进行 NMF 之后，得到的 $\boldsymbol{U}=[U_1,U_2,\cdots,U_r]$ 的每一列都构成了 $r$ 维子空间的一个基向量，其中每一维基向量都捕获了流量随时间变化的一种时变模式。而 $\boldsymbol{V}=[V_1,V_2,\cdots,V_p]$ 则是矩阵 $\boldsymbol{X}$ 中每一列在这个 $r$ 维子空间的系数向量。类似于文献[15]中的概念，称该 $r$ 维子空间为正常子空间。

基于 NMF 的正常子空间构建过程与基于 PCA 的基向量提取过程[15,16]有 2 点不同。第一，由于 NMF 是带约束条件的最优化问题且目标函数是非凸函数，因此采用梯度下降的优化方法只能得到局部最优解，与 PCA 追求的全局误差最小化相比，局部最优的结果使得连续突发异常现象能够较好地凸显出来；第二，NMF 抽取的基向量和系数具有非负的特点，这使得各个基向量之间的内积均大于零，因此基向量之间不完全正交，这与“网络流量的变化是多种流量变化模式的加性组合”这一事实相吻合。而 PCA 的系数向量中存在负值，这使得网络流量可能是多个时变模式的负的叠加，可解释性较差。

#### 3.2.2 获取残余矩阵

构建了 $r$ 维子空间以后，就可以利用这 $r$ 个基向量对流量矩阵进行重构，得到矩阵 $\hat{\boldsymbol{X}}=[U_1,U_2,\cdots,U_r][V_1,V_2,\cdots,V_p]$，并且将 $\tilde{\boldsymbol{X}}=\boldsymbol{X}-\hat{\boldsymbol{X}}$ 看作是流量矩阵中的噪声和异常部分，称为残余矩阵。每个测量周期在残余矩阵中对应的行是异常时刻凸显的基础，称为这个测量周期对应的残余流量。

#### 3.2.3 凸显与检测异常

对于第 $i$ 个测量周期的测量值 $X^i=(X_{i1},X_{i2},\cdots,X_{ip})$，经过 NMF 之后，可以记作 $X^i\approx\hat{X}^i+\tilde{X}^i$。其中，$\hat{X}^i$ 与 $\tilde{X}^i$ 分别表示矩阵 $\hat{\boldsymbol{X}}$ 与 $\tilde{\boldsymbol{X}}$ 的第 $i$ 行，并且 $\hat{X}^i$ 与 $\tilde{X}^i$ 分别是 $X^i$ 中的正常和异常(残余)流量的成分。如果在第 $i$ 个测量周期发生了网络异常，则 $X^i$ 将有更多的流量落入 $\tilde{X}^i$ 中，使得其在 $\tilde{\boldsymbol{X}}$ 中的值大于那些未发生网络异常的测量周期的值，使发生网络异常的测量周期和正常测量周期在 $\tilde{\boldsymbol{X}}$ 中对应的向量的值存在较大的差别。

如果在每个测量周期采取均值、标准差或者极

差作为统计信息，则发生网络异常的测量周期与正常的测量周期在 $\tilde{\boldsymbol{X}}$ 中对应的向量的值之间的差别就表现为二者统计信息之间的差别。该差别可用 Shewhart 控制图[17]很好地捕捉到。为了描述清晰，将每个测量周期称为一个采样点，将发生异常的测量周期称作异常采样点，而将未发生异常的测量周期称为正常采样点。

Shewhart 控制图的理论依据是中心极限定理[17]，它假定研究对象服从正态分布，利用样本数据检验总体的均值 $\mu$ 和标准差 $\sigma$ 是否发生显著变化来设定控制限，并以控制限为标准来判断某个采样点是否发生异常或超出控制。本文选择的是均值-极差控制图($\bar{x}$-$R$ 控制图)。

假定 $d$ 个样本 $\tilde{X}^i, i=1,2,\cdots,d$，独立服从正态分布 $N(\mu,\sigma^2)$，并且每个采样点有 $p$ 个采样值。在第 $i$ 个采样点，其极差为 $R_i$，而 $\bar{R}$ 是 $d$ 个采样点极差的均值，$\bar{R}=\sum R_i/d$。

当 $\mu$ 和 $\sigma$ 都已知时，$\bar{x}$ 以概率 $1-\alpha$ 落在区间 $\left[\mu-u_{1-\alpha/2}\frac{\sigma}{\sqrt{p}},\mu+u_{1-\alpha/2}\frac{\sigma}{\sqrt{p}}\right]$ 中。在实际应用中，$\mu_{1-\alpha/2}$ 通常取为 3，也就是生产中的 $3\sigma$ 控制线。根据中心极限定理，即使样本偏离正态假设，Shewhart 控制图的结果仍然近似可用。对于均值和方差，采用样本进行估计，则控制图的控制界限可以写作式(8)~式(10)：

$$CL=\mathrm{E}(R)=\bar{R} \tag{8}$$

$$\begin{aligned}UCL&=\mathrm{E}(R)+\mu_{1-\alpha/2}\sqrt{D(R)}\\&=\left(1+\mu_{1-\alpha/2}\frac{d_3}{d_2}\right)\bar{R}\end{aligned} \tag{9}$$

$$\begin{aligned}LCL&=\mathrm{E}(R)-\mu_{1-\alpha/2}\sqrt{D(R)}\\&=\left(1-\mu_{1-\alpha/2}\frac{d_3}{d_2}\right)\bar{R}\end{aligned} \tag{10}$$

其中，$d_3\bar{R}/d_2$ 是极差标准差的无偏估计，而 $d_2$ 与 $d_3$ 可以通过一定的计算规则得到[17]。得到 $UCL$ 以及 $LCL$ 后，如果某个测量点的值超过了 $UCL$ 或者低于 $LCL$，那么这个采样点就被判断为异常采样点，与其对应的测量周期就被认为发生了异常。

### 3.3 NMF-NAD 算法描述

#### 3.3.1 NMF-NAD 算法

基于上述讨论，提出一种基于 NMF 的全网络异常检测算法 NMF-NAD。该算法包含以下基本步骤：1) 对原始流量矩阵 $\boldsymbol{X}$ 进行非负矩阵分解，得到重构矩阵 $\hat{\boldsymbol{X}}$，如算法 1 中的第 1 到第 2 步所示；2) 计算得到误差矩阵 $\tilde{\boldsymbol{X}}=\boldsymbol{X}-\hat{\boldsymbol{X}}$，如算法 1 中的第 3 步所示；3) 使用 Shewhart 控制图检测发生异常的测量周期，如算法 1 中的第 4 到第 9 步所示。

**算法 1**　NMF-NAD

输入：$\boldsymbol{X}$　　//原始流量矩阵

输出：ATS(anomalies time period set)　//发生异常的测量周期的集合

1) $[\boldsymbol{U}\ \boldsymbol{V}] \leftarrow NMF(\boldsymbol{X}, r, k)$　//$\boldsymbol{U}$ 是分解后的基矩阵，$\boldsymbol{V}$ 是系数矩阵，$r$ 是基向量的个数，$k$ 是迭代的轮数

2) $\hat{\boldsymbol{X}}=\boldsymbol{UV}$

3) $\tilde{\boldsymbol{X}}=\boldsymbol{X}-\hat{\boldsymbol{X}}$

4) [residual, $UCL$, $LCL$] = Shewhart ( $\tilde{\boldsymbol{X}}$ )//计算控制限

5) for $i$ = 1; $i$ < $d$; $i$++

6) if $R(i) > UCL$ or $R(i) < LCL$ then //$R(i)$是第 $i$ 行的极差

7) add $i$ to ATS

8) end if

9) end for

#### 3.3.2 复杂性分析

NMF-NAD 算法的时间复杂性主要包括 2 个部分：NMF 分解和根据阈值进行的异常检测。NMF 分解的复杂性为 $O(pdkr)$，其中，$k$ 是迭代的轮数，$r$ 是子空间的维数，$d$ 是测量周期的数量，$p$ 是网络位置的数量。而基于阈值的判断部分复杂度为 $O(d)$，因此 NMF-NAD 算法的时间复杂性为 $O(pdkr)$。相比之下，PCA 方法的复杂度为 $O(dp^2)$[15]。$k$ 与 $r$ 在实际计算中取值均较小，因此一般地，NMF-NAD 的实际处理复杂度低于 PCA 方法的处理复杂度。

## 4 算法评价与分析

NMF-NAD 作为一种新的子空间方法，为了考察其性能，将其与 2 种典型的子空间方法 PCA[16]以及 MSPCA[12]进行了对比。为了对这 3 种方法进行综合的对比并分析 NMF-NAD 方法的敏感性，首先进行了模拟实验，在人工生成的数据注入具有不同参数的异常，然后对 3 种方法的检测结果进行了

对比。为了进一步地验证 NMF-NAD 方法在实际流量数据中的检测效果，又采用最新提出的实验方法基于因特网实测数据进行了实验。为了评价异常检测算法的检测性能，采用了 2 个测度：检测率和误报率。检测率定义为所有异常测量周期中被检测出来的比例；误报率定义为正常流量周期中被判定为异常的比例。

### 4.1 模拟实验及其分析

#### 4.1.1 模拟实验方法

网络流量通常由 3 种成分构成[18]：近似周期性的正常成分、高斯噪声成分和异常成分。产生这 3 种成分并按适当比例人工合成流量矩阵中每条网络流(即 $\boldsymbol{X}$ 的一列)。具体步骤如下：利用多种不同周期的流量(比如周期为 7 天、5 天、3 天、24h、12h、6h、3h 和 1.5h 的周期流)叠加来模拟周期性的网络流量[16]，并构造基准流量矩阵，如图 1(a)所示；在基准流量矩阵上叠加上零均值的高斯噪声，获得不含异常的流量矩阵，如图 1(b)所示；再以一定的规则加入各种典型异常，如图 1(c)所示，其中，虚线圈中是异常注入的采样点。用这种方法生成 121 条网络流并组成流量矩阵 $\boldsymbol{X}$，其中，每条流包含 2 010 个测量周期。

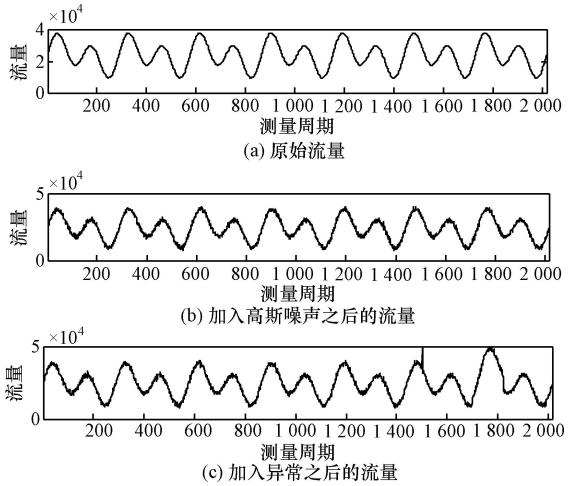



图 1 合成一条异常流的步骤

在此考虑了 4 种典型的流量异常[19]：阿尔法(alpha)异常、(分布式)拒绝服务攻击(DoS, DDoS)、闪拥(flash crowd)和入口/出口移动(ingress/egress shift)异常。阿尔法异常是指点到点之间不寻常的高速字节传输；(分布式)拒绝服务攻击是指单源或多源对单个目的地的洪泛攻击；闪拥是指大量客户同时访问某一站点，比如某个 Web 服务器或视频网站等；入口/出口移动则是 BGP 策略变化引起流量出口点的变化。

一般可以使用 4 个参数来描述这 4 种网络流量异常[19]：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 5～30min，阿尔法和闪拥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 2 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网络流乘上一个乘法因子，二是通过为基准流量矩阵中部分网络流加上一个常数项。源-目的数是指异常所涉及的网络流的数目，拒绝服务攻击或阿尔法事件一般涉及到单个源和单个目的地；入口/出口移动异常则通常涉及到 2 个源点和 2 个目的地；而闪拥则会涉及到多个源和单个目的。形状参数是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，闪拥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，这些行为可以用不同的形状函数(比如斜坡、指数和台阶函数等)及其组合来表征。

在实验中，采样点之间间隔为 5min，异常注入过程如下：从第 300 个采样点到第 800 个采样点期间，每隔 50 个采样点注入一次阿尔法攻击，并且阿尔法攻击持续 30min(持续 6 个采样点)；从第 1 000 个到第 1 500 个采样点里，每隔 50 个采样点注入一次分布式拒绝服务攻击或者闪拥攻击，攻击持续时间为 30min(持续 6 个采样点)；从第 1 700 到第 1 800 个采样点期间，持续注入入口/出口移动的异常(持续 100 个采样点)，将某条网络流的一定比例的流量迁移到另外一个网络流对上。

#### 4.1.2 检测结果

3 种算法异常时刻凸显的结果如图 2 所示，其中，竖轴为各种检测方法得到的每个测量周期对应的残余流量向量中所有元素的平方和 (SSE, square sum of the elements of the residual traffic)。

对于 PCA 方法，采用的是 Q 统计量的方法进行检测。

$$\delta_\alpha^2 = \phi_1 \left[ \frac{c_\alpha \sqrt{2\phi_2 h_0^2}}{\phi_1} + 1 + \frac{\phi_2 h_0 (h_0 - 1)}{\phi_1^2} \right]^{\frac{1}{h_0}} \qquad (11)$$

其中，$h_0 = 1 - \frac{2\phi_1\phi_3}{3\phi_2^2}$ 是历史数据的相对权重，$\phi_i = \sum_{j=r+1}^{p} \lambda_j^i, i = 1,2,3$，$\lambda_j$ 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，$c_\alpha$ 是是标准正态分布中的 $1-\alpha$ 分位数，$\alpha$ 通常取 0.001。如图 2(a)中虚线所示，就是 Q 统计量设定的阈值曲线。

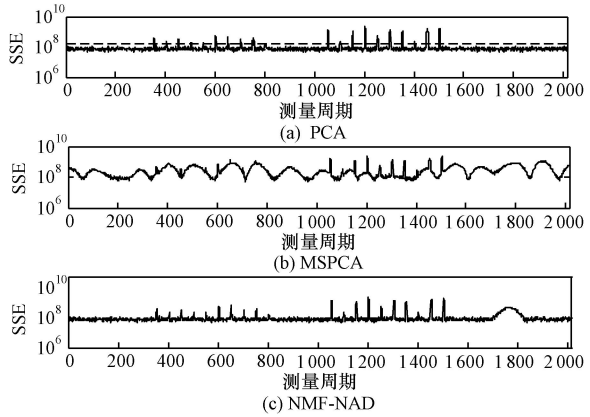



图 2　3 种方法的异常凸显对比

对于 MSPCA 以及 NMF-NAD 方法，采用了 Shewhart 控制图进行异常检测。检测的具体过程如 3.2.3 节所述，是基于误差矩阵进行的。结果分别如图 3 和图 4 所示。

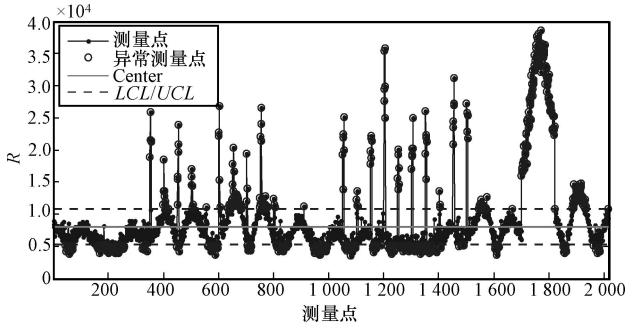



图 3　MSPCA 方法的检测结果

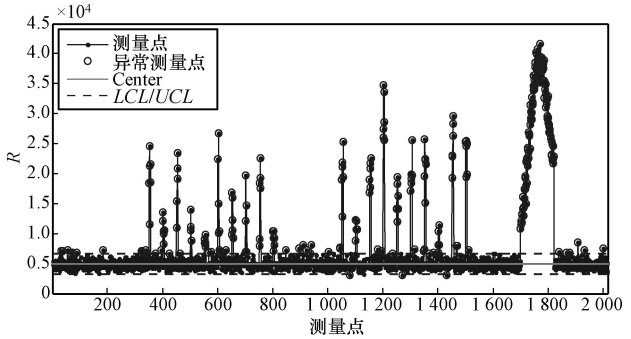



图 4　NMF-NAD 方法的检测结果

由图 3 和图 4 可以看出，MSPCA 和 NMF-NAD 不同程度地检测出了 PCA 无法检测的连续异常点。与 NMF-NAD 方法相比，MSPCA 方法具有更高的误报率，如在它第 200 个采样点周围的异常点都是由于误报形成的。

具体的检测结果如表 1 所示。可见 NMF-NAD 方法在三者中间检测率最高，同时误判率也较低。

**表 1**　　**异常检测结果**

| 方法 | 检测率/% | 误判率/% |
|---|---|---|
| PCA | 34.02 | 0 |
| MSPCA | 91.7 | 24.85 |
| NMF-NAD | 98.34 | 3.04 |

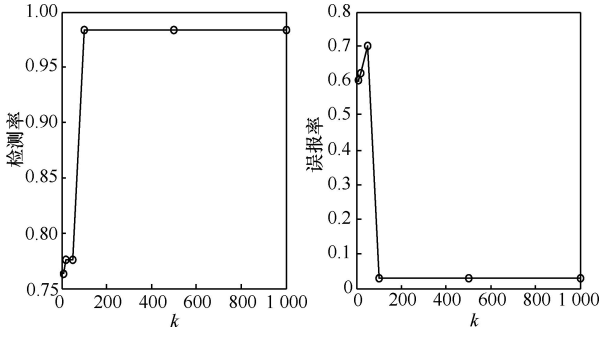
### 4.1.3　参数影响的讨论

在 NMF-NAD 方法中，选取的 $r$ 的数量和迭代周期 $k$ 不仅会影响 NMF-NAD 方法的复杂性，也会影响方法的检测效果。表 2 给出了在 $r$ 取不同值时的检测结果。由表 2 可以看出，$r$ 取值为 2 时检测效果最佳。$r$ 的取值与数据集的特性有关，在不同的数据集上取值会有所不同。

**表 2**　　**$r$ 取值不同时的检测结果**

| $r$ | 检测率/% | 误判率/% |
|---|---|---|
| 1 | 78.84 | 71.15 |
| 2 | 98.34 | 2.93 |
| 3 | 97.93 | 4.06 |
| 4 | 97.10 | 8.00 |
| 5 | 97.93 | 9.35 |
| 6 | 97.93 | 8.28 |
| 7 | 97.10 | 6.59 |
| 8 | 97.10 | 9.30 |

另外，考察了子空间的维数 $r$=2 时，迭代轮数 $k$ 对于检测效果的影响。实验结果如图 5 所示。可见，当 $k$ 取值为 50 时就可以达到稳定的检测效果。




(a)$k$ 取不同值时的检测率　　(b)$k$ 取不同值时的误报率

图 5　$k$ 取值不同时的 NMF-NAD 检测效果对比

### 4.2 对因特网实测数据的分析

#### 4.2.1 数据集、实验方法以及测度

为了评价NMF-NAD算法在真实流量数据集上的检测性能，采用了从 Abilene 实测得到的流量矩阵数据集[1,2,6,18]，数据集的具体描述如表 3 所示。Dataset1 与 Dataset2 采自不同的时期且有不同粒度，可以用来考量检测方法的适用性。

**表 3 Abilene 流量矩阵**

| 持续时间 | 间隔时间/min | 测度 | 矩阵形式 | 数据集 |
|---|---|---|---|---|
| 2004.4.7-2004.4.13 | 5 | 字节数 | 2 016× 144 | Dataset1 |
| 2003.12.15-2003.12.21 | 5 | 流数 | 2 010× 121 | Dataset2 |

为了保证对比的公平，采用文献[20]最新提出的实验方法。对于每一种检测方法和每一个的数据集，具体过程如下。

第 1 步：对数据集应用检测方法得到初始异常集合(BAS, base anomaies set)，其数量为|BAS|=$N_{\mathrm{BAS}}$，其中，| |表示集合的势。

第 2 步：向数据集注入 4 种异常，并记为注入异常集合(IAS, injected anomalies set)，其数量为|IAS|=$N_{\mathrm{IAS}}$。

第 3 步：对注入异常后的数据集再次应用检测方法，得到检测异常集合(DAS, detected anomalies set)，并且异常的数量为|DAS|=$N_{\mathrm{DAS}}$，其中，属于 BAS 的异常的数量为 $N_1$，属于 IAS 的数量为 $N_2$。

第 4 步：根据 BAS、IAS 和 DAS 计算检测率和保持率。

其中，检测率(TPR, true positive ratio)以及保持率(KPR, keep positive ratio)定义如式(12)所示：

$$TPR=\frac{N_2}{N_{\mathrm{IAS}}},KPR=\frac{N_1}{N_{\mathrm{BAS}}} \tag{12}$$

另外，在异常注入过程中，需要避免与现有异常的重合。

#### 4.2.2 实验结果

取子空间维数 $r$=2，并且迭代轮数为 50 轮，3 种方法的异常凸显结果如图 6 和图 7 所示。图 6 和图 7 分别给出了针对 Dataset1 和 Dataset2 的异常时刻凸显结果，其中，$y$ 轴是各种方法的残余矩阵的 2 范数值。可以看出，NMF-NAD 方法更好地凸显出了发生异常的那些采样点，MSPCA 方法次之，而 PCA 方法无法较好地凸显出异常的采样点。

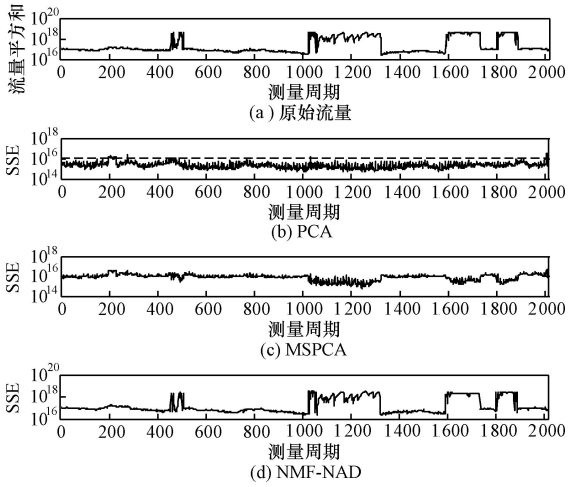



图 6 Dataset1 数据集异常凸显结果

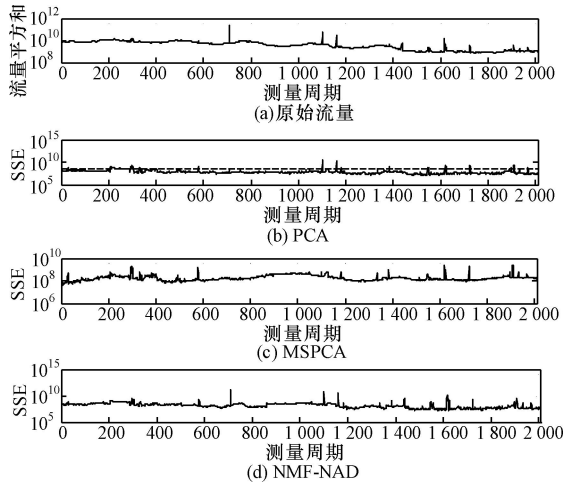



图 7 Dataset2 数据集异常凸显结果

运行 50 次后取均值，最终的检测结果分别如表 4 和表 5 所示。可见 NMF-NAD 方法在实测数据环境下，取得了高于 PCA 和 MSPCA 方法的检测率，并且较好地检测出了原有的异常点。

**表 4 3 种检测方法对 Dataset1 的检测结果**

| 方法 | *TPR*/% | *KPR*/% |
|---|---|---|
| PCA | 34.65 | 21.62 |
| MSPCA | 72.28 | 83.97 |
| NMF-NAD | 81.19 | 78.61 |

**表 5 3 种检测方法 Dataset 2 的检测结果**

| 方法 | *TPR*/% | *KPR*/% |
|---|---|---|
| PCA | 33.17 | 29.73 |
| MSPCA | 59.41 | 93.49 |
| NMF-NAD | 70.59 | 82.61 |

## 5　结束语

本文提出了一种基于非负子空间的全网络异常检测方法 NMF-NAD，理论分析表明该算法与 PCA 类方法相比，在检测连续突发的情况下具有更好的性能。模拟实验数据以及因特网实测数据的分析表明，NMF-NAD 算法具有更好的检测性能，优于 PCA 以及 MSPCA 方法。目前提出的 NMF-NAD 方法属于批处理的检测方法，下一步要对其进行改进，提出在线的、存储开销更低的检测方法，并考虑对发生异常的网络流进行定位。

## 参考文献：


[1] LAKHINA A, CROVELLA M, DIOT C. Characterization of network-wide anomalies in traffic flows[A]. IMC[C]. 2004. 201-206.

[2] LOGG C, COTTRELL L, NAVRATIL J. Experiences in traceroute and available bandwidth change analysis[A]. SIGCOMM Workshop[C]. 2004. 247-252.

[3] BRUTLAG J D. Aberrant behavior detection in time series for network monitoring[A]. USENIX[C]. New Orleans, Louisiana, USA, 2000. 139-146.

[4] MA J, PERKINS S. Online novelty detection on temporal sequences[A]. SIGKDD[C]. Washington, DC, USA, 2003.613-618.

[5] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions[A]. SIGCOMM[C]. Philadelphia, Pennsylvania, USA, 2005. 217-228.

[6] AHMED T, COATES M, LAKHINA A. Multivariate online anomaly detection using kernel recursive least squares[A]. INFOCOM[C]. Anchorage, Alaska, USA, 2007. 625-633.

[7] AHMED T. Online anomaly detection using KDE[A]. GlobeCom[C]. Honolulu, Hawaii, USA, 2009. 1-8.

[8] REINGBERG H, SOULE A, REXFORD J, *et al*. Sensitivity of PCA for traffic anomaly detection[A]. ACM Sigmetrics[C]. 2007. 109-120.

[9] BRAUKHOFF D, SALAMATIAN K, MAY M. Applying PCA for traffic anomaly detection: problems and solutions[A]. IEEE INFOCOMM[C]. 2009. 2866-2870.

[10] RUBINSTEIN B I P, NELSON B, HUANG L, *et al*. ANTIDOTE: understanding and defending against poisoning of anomaly detectors[A]. ACM IMC[C]. 2009.1-14.

[11] 钱叶魁, 陈鸣. 面向 PCA 异常检测器的攻击和防御机制[J]. 电子学报, 2011, 39(3):543-548.
QIAN Y K, CHEN M. Poison attack and defense strategies on PCA-based anomaly detector[J]. Acta Electronica Sinica, 2011, 39 (3):543-548.

[12] BAKSHI B. Multiscale PCA with application to multivariate statistical process monitoring[J]. AIChE Journal,1998,44(7): 1596-1610.

[13] SENGAR H, WANG X, WANG H, *et al*. Online detecting of network traffic anomalies using behavioral distance[A]. IWQoS[C]. Charleston, South Carolina, 2009. 1-9.

[14] LIU Y, ZHANG L, GUAN Y. Sketch-based streaming PCA algorithm for network-wide traffic anomaly detection[A]. ICDCS[C]. Genoa, Italy, 2010. 807-816.

[15] XU W, LIU X, GONG Y. Document clustering based on non-negative matrix factorization[A]. ACM SIGIR[C]. Toronto, Canada, 2003. 267-273.

[16] LAKHINA A, CROVELLA M, DIOT C. Diagnosing network-wide traffic anomalies[A]. SIGCOMM[C]. Portland, OR, USA, 2004. 219-230.

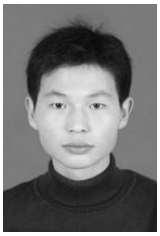
[17] 王兆军, 邹长亮, 李忠华. 统计质量控制图理论与方法[EB/OL]. http://www.202.113.29.3/~zjwang/publications/books/spc.pdf.
WANG Z J, ZOU C L, LI Z H. The theory and methods of statistical quality control charts[EB/OL]. http://www.202.113.29.3/~zjwang/publications/ books/ spc.pdf.

[18] LAKHINA A, PAPAGIANNAKI K, CROVELLA M, *et al*. Structural analysis of network traffic flows[A]. SIGMETRICS[C]. New York, NY, USA, 2004.61-72.

[19] SOULE A, SALAMATIAN K E, TAFT N. Combining filtering and statistical methods for anomaly detection[A]. IMC[C]. Berkeley, CA, USA, 2005. 1-14.

[20] NYALKALKAR K, SINHA S, BAILEY M, *et al*. A comparative study of two network-based anomaly detection methods[A]. INFOCOM[C]. Shanghai, China, 2011. 176-180.


## 作者简介：

**魏祥麟**（1985-），男，安徽砀山人，解放军理工大学博士生，主要研究方向为对等网络、网络测量和网络异常检测。

**陈鸣**（1956-），男，江苏无锡人，博士，解放军理工大学教授、博士生导师，主要研究方向为网络体系结构、网络管理、网络测量和分布式系统。

**张国敏**（1979-），男，山东济南人，博士，解放军理工大学讲师，主要研究方向为网络测量和网络安全。

**黄建军**（1984-），男，福建漳州人，解放军理工大学博士生，主要研究方向为盲源分离和压缩感知。