DOI：10.7652/xjtuxb202001006

利用残差分析的网络异常流量检测方法

孟永伟[1]，秦涛[1,2]，赵亮[1]，马文强[3]，王换招[1]
（1.西安交通大学智能网络与网络安全教育部重点实验室，710049，西安；2.西安交通大学深圳科学技术研究院，518057，广东深圳；3.西安空间无线电技术研究所，710100，西安）

摘要：针对网络异常流量检测中大数据小异常造成的难题，提出了一种新的基于残差分析的网络异常流量检测方法。从多个角度提取网络流量的特征属性，以准确刻画正常行为和异常行为之间的差异性。利用提取的特征属性构建属性矩阵，采用流之间的相似性构建邻接矩阵。使用属性矩阵和邻接矩阵构建网络异常检测模型，采用*CUR*矩阵分解方法重构属性矩阵得到主模式，对属性矩阵和重构的属性矩阵进行残差计算进而获得残差矩阵。对残差矩阵中的每一个流计算其残差，根据每个流的残差和预设阈值进行异常判定。采集了西安交通大学校园网流量数据进行实验，实验结果表明：所提方法在不需要任何先验知识的情况下能够使异常检测率达到90%以上；与其他异常检测方法相比，所提方法不仅具有较高的检测率，而且能够实现异常源定位。

关键词：异常检测；网络流量；矩阵分解；残差分析
中图分类号：TP393.0 **文献标志码**：A **文章编号**：0253-987X(2020)01-0042-07

Network Anomaly Detection Method Based on Residual Analysis

MENG Yongwei[1], QIN Tao[1,2], ZHAO Liang[1], MA Wenqiang[3], WANG Huanzhao[1]
(1. MOE Key Laboratory for Intelligent and Network Security, Xi'an Jiaotong University, Xi'an 710049, China;
2. Shenzhen Institute of Science and Technology, Xi'an Jiaotong University, Shenzhen, Guangdong 518057, China;
3. Xi'an Institute of Space Radio Technology, Xi'an 710100, China)

Abstract: Focusing on the challenges caused by the increasing traffic volumes and the cunning abnormal attacks, a new algorithm for network anomaly detection by residual analysis is developed. The network behavior attributes from different aspects are described to characterize the differences between the normal and abnormal behavior. The attributes are extracted to construct an attribute matrix, and the similarity of the flows is considered to construct an adjacency matrix, the model of network anomaly detection is then established by the two matrices. *CUR* matrix decomposition is realized to reconstruct attribute matrix to obtain the primary pattern. The residual matrix is obtained by analyzing the difference between the attribute matrix and reconstructed attribute matrix. The anomalies can be distinguished according to the residual value of each flow. Experimental results based on the traces collected from the campus network of Xi'an Jiaotong University show that the proposed algorithm holds a detection accuracy higher than 90% without any prior knowledge. Compared with the other anomaly detection algorithms, the proposed one can determine the goal of anomaly location with higher

收稿日期：2019-06-03。 作者简介：孟永伟(1983—)，男，博士生；秦涛(通信作者)，男，副教授。 基金项目：国家自然科学基金资助项目(61772411)；深圳市基础研究计划资助项目(JCYJ20170816100819428)；陕西省自然科学基金资助项目(2018JM6109)。
网络出版时间：2019-08-08 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20190808.1349.002.html

detection accuracy.

Keywords：anomaly detection；network traffic；matrix decomposition；residual analysis

随着计算机网络的日益发展，互联网已经成为人们生活中不可或缺的一部分。与此同时，各种网络攻击的发生增加了网络管理的难度。异常检测作为网络管理的一种有效手段，能够帮助管理员有效控制网络攻击带来的危害，在网络管理中起着非常重要的作用。异常行为可以引起网络流量的某些特征发生显著的变化，如 DoS 攻击、扫描攻击等可以引起 IP 地址数、端口数、数据包数及网络流数据量等发生显著变化，所以网络流量是网络异常检测的重要数据源之一[1-2]。一些专家学者依据网络流量特征的变化提出了网络流量异常的检测方法[3-6]，这些方法能够通过网络流量特征的变化进行异常检测，但是随着网络带宽的增加，用户所产生的海量流量给异常检测带来了很大的挑战。因此，一些学者使用抽样方法来减少流的数量[7-10]，这些方法虽然理论分析效果较好，然而在实际使用过程中可能会丢失重要的流数据。文献[11]提出了一种概要数据结构来处理大规模流式数据，通过维度减少的方法来重构输入数据，使用较少的存储资源对海量数据进行分析处理，该方法常用于异常检测[12-14]。虽然概要数据结构可以使用较小内存消耗对海量数据流进行快速处理，然而由于冲突的存在会直接影响到异常检测的准确性，并且异常行为越来越隐蔽，从海量的流量数据中识别出微小的异常愈加困难。

针对上述问题，本文从矩阵分解的角度出发，提出了一种利用残差分析进行网络异常流量检测方法。在分析了常见网络攻击的基础上，从多个角度提取流量的特征属性以全面刻画正常行为和异常行为的差异性，特征属性具体包括源 IP 地址的出连接度、入连接度、不同目的 IP 地址流数、不同目的端口流数、流的平均包数、流的平均数据量、流的平均生存时间。使用这些特征属性构建属性矩阵，根据流的相似性构建邻接矩阵，通过 *CUR* 矩阵分解选取有代表性的行和列重构属性矩阵。由于在选取时尽可能地接近原始属性矩阵，所以该重构矩阵代表了原始属性矩阵的主模式。使用原始属性矩阵和重构属性矩阵做残差计算，获得残差矩阵。计算残差矩阵中每一个流的残差，进而判断出异常流。

为了验证所提方法的有效性，收集了西安交通大学校园网凌晨、上午、晚上 3 个不同时间段的 NetFlow 数据进行实验，该数据集共包括 276 149 条流记录。同时，通过在不同时间段的原始样本中插入攻击数据构建测试数据集。基于该数据集的测试结果显示，本文所提方法在不需要任何先验知识的情况下能够使得异常检测率达到 90％以上，与其他异常检测方法相比，本文方法不仅具有较高的检测率，而且能够实现异常源定位。

1　网络异常流量检测描述

1.1　问题提出

在固定时间窗口 Δt 内，将每一个特定源 IP 地址抽象成一个聚合流，用集合 $V=\{e_1,e_2,\cdots,e_n\}$ 表示 n 个源 IP 地址，其中每个源 IP 地址都有一个 d 维的统计特征属性 $F=\{f_1,f_2,\cdots,f_d\}$，使用源 IP 地址的统计特征属性构建一个属性矩阵 $\boldsymbol{X}\in\boldsymbol{\Omega}^{d\times n}$，其中 $\boldsymbol{X}(:,i)\in\boldsymbol{\Omega}^d$ 表示第 i 个源 IP 地址的特征属性。由于 IP 地址之间的相似性与流量之间存在一定的关系，因此根据 IP 地址的相似性构建邻接矩阵 $\boldsymbol{A}\in\boldsymbol{\Omega}^{n\times n}$，如果邻接矩阵中的某个元素 $A(i,j)=1$，则表示 e_i 与 e_j 相似，否则不相似。为了得到属性矩阵的主模式，从属性矩阵中提取代表性的行与列组成新的属性矩阵 $\hat{\boldsymbol{X}}\in\boldsymbol{\Omega}^{d\times n}$，该矩阵代表属性矩阵 $\boldsymbol{X}$ 的主模式，可以通过 $\boldsymbol{X}$ 与 $\hat{\boldsymbol{X}}$ 之间的差异进行网络异常流量的检测。可以看出，网络异常流量检测可以描述为从大量 IP 地址中找出一个异常 IP 地址集合，该集合中的 IP 地址的流量特征与其他绝大多数 IP 地址的流量特征具有显著的差异性。

1.2　检测框架设计

针对网络异常流量检测中的问题，给出了网络异常流量检测过程，如图 1 所示。可以看出，整个过程可以分为 4 个部分，具体描述如下。

(1)特征提取。为了能够准确刻画正常行为和异常行为之间的差异性，在分析了常见网络攻击特性的基础上，从原始网络流中提取出 7 个典型的特征属性，包括源 IP 地址的出连接度、入连接度、不同目的 IP 地址流数、不同目的端口流数、流的平均包数、流的平均数据量、流的平均生存时间。

(2)矩阵分解。根据统计的源 IP 地址的特征属性构建一个属性矩阵，同时根据源 IP 地址的相似性构建一个邻接矩阵，使用属性矩阵和邻接矩阵构建网络异常检测模型，采用 *CUR* 矩阵分解方法从构建的属性矩阵中选择若干有代表性的源 IP 地址和

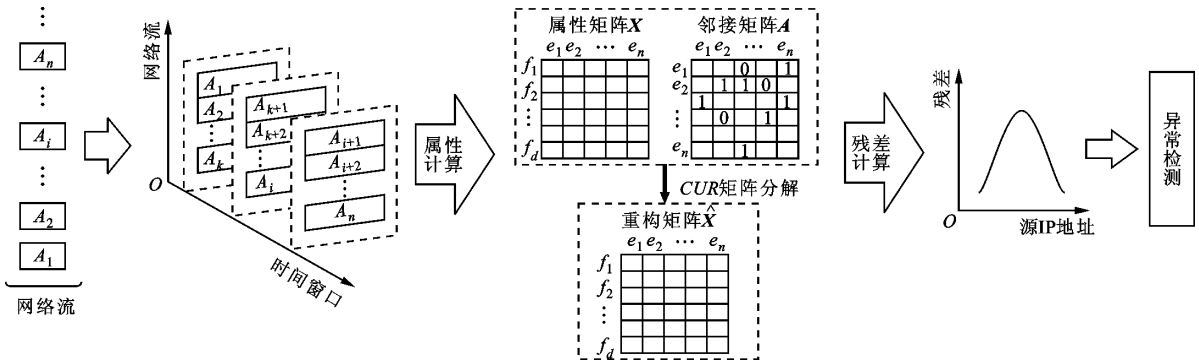

图 1 基于残差分析的网络异常流量检测方法框架

属性重构一个属性矩阵。

(3)残差计算。对构建的属性矩阵与重构的属性矩阵做残差计算,可以得到两个矩阵的差,即残差矩阵。

(4)异常检测。使用残差矩阵计算出每个源 IP 地址的残差,残差超过预先设置的阈值的源 IP 地址为异常。

2 网络流量特征属性构建

2.1 特征属性定义

通过对网络攻击和用户行为进行分析,从网络流量中提取出 7 个特征属性以全面刻画异常行为和正常行为之间的差别。7 个特征属性的具体定义如下。

特征属性 1 为源 IP 地址出连接度,定义为在固定时间窗口 Δt 内,某特定源 IP 地址产生的流的总数,具体描述为

$$O_i = |\ f_{\text{sip}}^i\ |,\ 1 \leqslant i \leqslant n \tag{1}$$

式中:f_{sip}^i 为第 i 个源 IP 地址产生的所有流的集合;i 为源 IP 地址的索引号;$|\cdot|$ 为求解集合中的元素数。

特征属性 2 为源 IP 地址入连接度,定义为在固定时间窗口 Δt 内,某特定源 IP 地址作为目的 IP 地址产生的流的总数,具体描述为

$$I_i = |\ f_{\text{dip}}^i\ |,\ 1 \leqslant i \leqslant n \tag{2}$$

式中 f_{dip}^i 为第 i 个源 IP 地址作为目的 IP 地址产生的所有流的集合。

特征属性 3 为源 IP 地址流中不同目的 IP 地址流数,定义为在固定时间窗口 Δt 内,某特定源 IP 地址产生的流中不同目的 IP 地址的流的数目,具体描述为

$$D_i = |\ d_j\ |d_k \neq d_j, 1 \leqslant k, j \leqslant n\ |,\ 1 \leqslant i \leqslant n \tag{3}$$

式中 d_k 和 d_j 为不同目的 IP 地址。

特征属性 4 为源 IP 流中不同目的端口流数,定义为在固定时间窗口 Δt 内,源 IP 地址端口产生的流中不同目的端口的流的数目,具体描述为

$$P_i = |\ p_j\ |p_k \neq p_j, 1 \leqslant k, j \leqslant n\ |,\ 1 \leqslant i \leqslant n \tag{4}$$

式中 p_k 和 p_j 为不同目的端口。

特征属性 5 为源 IP 地址流中的平均包数,定义为在固定时间窗口 Δt 内,某特定源 IP 地址产生的流中数据包的平均值,具体描述为

$$S_i = \frac{1}{m}\sum_{j=1}^{m} p(i,j) \tag{5}$$

式中:$p(i,j)$ 为第 i 个源 IP 地址的第 j 条流的包数;m 为源 IP 地址产生的流的总数。

特征属性 6 为源 IP 地址的平均流数据量,定义为在固定时间窗口 Δt 内,某特定源 IP 地址产生的流的数据量的平均值,具体描述为

$$B_i = \frac{1}{m}\sum_{j=1}^{m} b(i,j) \tag{6}$$

式中 $b(i,j)$ 为第 i 个源 IP 地址的第 j 条流的数据量。

特征属性 7 为源 IP 地址的流平均生存时间,定义为在固定时间窗口 Δt 内,某特定源 IP 地址产生的流生存时间的平均值,具体描述为

$$L_i = \frac{1}{m}\sum_{j=1}^{m} l(i,j) \tag{7}$$

式中 $l(i,j)$ 为第 i 个源 IP 地址的第 j 条流的生存时间。

2.2 属性矩阵构建

在固定的时间窗口 Δt 内,统计出每个源 IP 地址的 7 个特征属性,将每个源 IP 地址作为列、特征属性作为行,构建属性矩阵 $\boldsymbol{X}$,再从该矩阵中选择若干有代表性的行和列重构属性矩阵得到 $\hat{\boldsymbol{X}}$。$\hat{\boldsymbol{X}}$ 代表了属性矩阵 $\boldsymbol{X}$ 的主模式,需确保矩阵 $\hat{\boldsymbol{X}}$ 尽可能地接近属性矩阵 $\boldsymbol{X}$。将属性矩阵与重构的属性矩阵做残

差计算,可以得到残差矩阵 $\widetilde{\boldsymbol{R}}=\boldsymbol{X}-\hat{\boldsymbol{X}}$。$\widetilde{\boldsymbol{R}}$ 反映了流量特征变化的程度,能够很好地反映异常情况。在数学上,以上过程可表示为

$$\min_{\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\hat{\boldsymbol{X}}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,0} \tag{8}$$

重构矩阵的过程可以看作矩阵分解问题,CUR 矩阵分解不仅可以选择源 IP 地址,而且可以选择特征属性,因此该方法可以重构属性矩阵[15],具体描述为

$$\min_{\boldsymbol{C},\boldsymbol{U},\boldsymbol{R},\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\boldsymbol{C}\boldsymbol{U}\boldsymbol{R}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,0} \tag{9}$$

式中:$\boldsymbol{C}\in\boldsymbol{\Omega}^{d\times h}$ 表示从属性矩阵 $\boldsymbol{X}$ 中选择 h 个有代表性的源 IP 地址;$\boldsymbol{R}\in\boldsymbol{\Omega}^{r\times n}$ 表示从属性矩阵 $\boldsymbol{X}$ 中选择 r 个具有代表性的属性;$\boldsymbol{U}\in\boldsymbol{\Omega}^{h\times r}$ 表示 h 行 r 列的矩阵,并且它的秩尽应可能小。从式(9)可以看出,生成矩阵 $\boldsymbol{C}$ 和 $\boldsymbol{R}$ 的过程就是从属性矩阵 $\boldsymbol{X}$ 中选择 h 个源 IP 地址和 r 个特征属性的过程。

2.3　邻接矩阵构建

Kohler 等对 IP 地址的网络地址号进行数据包聚合,发现具有相同前缀的网络用户会表现出相似的网络流量特征[16],也就是说,如果两个用户的网络流量特征具有相似性,那么他们的 IP 地址也具有相似性。因此,可以使用 IP 地址的相似度表示用户之间的关系。

当计算两个 IP 地址相似度时,首先将 IP 地址转化为二进制表示形式,然后从左到右依次进行异或运算,当出现第一个不同的位时停止运算,将该位及后面的位全部设置为 0,前面的位设置为 1。此时,可以得到两个用户的子网掩码 M,1 的个数即为两个 IP 地址的距离 D,除以 IP 地址总位数 32,可以得到它们的相似度 S。如果两个 IP 地址相似度大于某个阈值,将它们设置为 1,否则设置为 0,这样可以构建 IP 地址的邻接矩阵。

同样地,如果两个 IP 地址在邻接矩阵中是相似的,那么它们进行重构之后,在残差矩阵 $\widetilde{\boldsymbol{R}}$ 中的属性模式也应该是相似的。因此,邻接矩阵和 IP 地址属性之间的关系为

$$\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}(\widetilde{\boldsymbol{R}}^{\mathrm{T}}(i,:)-\widetilde{\boldsymbol{R}}^{\mathrm{T}}(j,:))^{2}\boldsymbol{A}(i,j)=\mathrm{tr}(\widetilde{\boldsymbol{R}}\boldsymbol{L}\widetilde{\boldsymbol{R}}^{\mathrm{T}}) \tag{10}$$

式中 $\boldsymbol{L}$ 为由邻接矩阵 $\boldsymbol{A}$ 产生的拉普拉斯矩阵。

3　网络异常流量检测模型构建

3.1　异常流量检测建模

从 2.3 节可以发现,源 IP 地址的属性信息和地址之间的关系对残差矩阵有非常显著的影响。因此,在构建异常流量检测模型时需要同时考虑源 IP 地址的属性信息以及地址之间的关系,构建的模型为

$$\min_{\boldsymbol{C},\boldsymbol{U},\boldsymbol{R},\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\boldsymbol{C}\boldsymbol{U}\boldsymbol{R}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,0}+\varphi\mathrm{tr}(\widetilde{\boldsymbol{R}}\boldsymbol{L}\widetilde{\boldsymbol{R}}^{\mathrm{T}}) \tag{11}$$

选择源 IP 地址和特征属性的过程可描述为

$$\min_{\boldsymbol{W},\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\alpha \| \boldsymbol{W} \|_{2,0}+\beta \| \boldsymbol{W}^{\mathrm{T}} \|_{2,0}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,0}+\varphi\mathrm{tr}(\widetilde{\boldsymbol{R}}\boldsymbol{L}\widetilde{\boldsymbol{R}}^{\mathrm{T}}) \tag{12}$$

式中:$\boldsymbol{W}=\mathrm{diag}(\boldsymbol{v})\hat{\boldsymbol{U}}\mathrm{diag}(\boldsymbol{p})\in\boldsymbol{\Omega}^{n\times d}$;向量 $\boldsymbol{v}=[v_1,\cdots,v_n]^{\mathrm{T}}\in\{0,1\}^{n}$;$\boldsymbol{p}=[p_1,\cdots,p_n]^{\mathrm{T}}\in\{0,1\}^{d}$;$\mathrm{diag}(\boldsymbol{v})$为生成对角元素为 $\boldsymbol{v}$ 的对角矩阵;$\mathrm{diag}(\boldsymbol{p})$为生成对角元素为 $\boldsymbol{p}$ 的对角矩阵。如果向量 $\boldsymbol{v}$ 中具有 h 个元素是 1,则 $\boldsymbol{X}\mathrm{diag}(\boldsymbol{v})$表示属性矩阵 $\boldsymbol{X}$ 中 h 列不变,剩余 $n-h$ 列设置为零向量。同样的道理,如果将 $\boldsymbol{W}\boldsymbol{X}$ 看作系数矩阵,当第 i 行不是零向量时,$\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}$ 表示第 i 个源 IP 地址被选择。$\| \boldsymbol{W} \|_{2,0}$能够确保选择部分源 IP 地址。可以用同样的方法分析属性的选择。由于 $\zeta_{2,0}$ 范式是一个 NP-hard 问题,可以使用 $\zeta_{2,1}$ 范式近似代替 $\zeta_{2,0}$ 范式,最后的约束函数为

$$\min_{\boldsymbol{W},\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\alpha \| \boldsymbol{W} \|_{2,1}+\beta \| \boldsymbol{W}^{\mathrm{T}} \|_{2,1}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,1}+\varphi\mathrm{tr}(\widetilde{\boldsymbol{R}}\boldsymbol{L}\widetilde{\boldsymbol{R}}^{\mathrm{T}}) \tag{13}$$

3.2　方法优化

$\boldsymbol{W}$ 和 $\widetilde{\boldsymbol{R}}$ 同时存在使得式(13)不一定为凸函数,因此很难找到最优解。为了解决此问题,采用交替更新的方法进行优化。

(1)固定 $\boldsymbol{W}$ 更新 $\widetilde{\boldsymbol{R}}$。当 $\boldsymbol{W}$ 固定的时候,式(13)对于 $\widetilde{\boldsymbol{R}}$ 就是凸函数,可以表示为

$$\min_{\widetilde{\boldsymbol{R}}} \| \boldsymbol{X}-\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\gamma \| \widetilde{\boldsymbol{R}}^{\mathrm{T}} \|_{2,1}+\varphi\mathrm{tr}(\widetilde{\boldsymbol{R}}\boldsymbol{L}\widetilde{\boldsymbol{R}}^{\mathrm{T}}) \tag{14}$$

将式(14)对 $\widetilde{\boldsymbol{R}}$ 求导并让其为 0,变换后可得

$$\widetilde{\boldsymbol{R}}=(\boldsymbol{X}-\boldsymbol{X}\boldsymbol{W}\boldsymbol{X})(\boldsymbol{I}+\gamma\boldsymbol{D}_{R}+\varphi\boldsymbol{L})^{-1} \tag{15}$$

式中:$\boldsymbol{D}_R$ 是一个对角阵,对角元素为 $\boldsymbol{D}_R(i,i)=1/2\| \widetilde{\boldsymbol{R}}^{\mathrm{T}}(i,:) \|_{2}$;矩阵 $\varphi\boldsymbol{L}$、$\boldsymbol{I}$ 和 $\gamma\boldsymbol{D}_R$ 都是半正定矩阵。

(2)固定 $\widetilde{\boldsymbol{R}}$ 更新 $\boldsymbol{W}$。当 $\widetilde{\boldsymbol{R}}$ 固定的时候,式(13)对于 $\boldsymbol{W}$ 就是凸函数,此时式(13)可转换为

$$\min_{\boldsymbol{W}} \| \boldsymbol{X}-\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}-\widetilde{\boldsymbol{R}} \|_{\mathrm{F}}^{2}+\alpha \| \boldsymbol{W} \|_{2,1}+\beta \| \boldsymbol{W}^{\mathrm{T}} \|_{2,1} \tag{16}$$

同样地,将式(16)对 $\boldsymbol{W}$ 求导并让其为 0,可得

$$\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{W}\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}+\alpha\boldsymbol{D}'_{W}\boldsymbol{W}+\beta\boldsymbol{W}\boldsymbol{D}''_{W}=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}-\boldsymbol{X}^{\mathrm{T}}\widetilde{\boldsymbol{R}}\boldsymbol{X}^{\mathrm{T}} \tag{17}$$

式中 $\boldsymbol{D}'_W$ 与 $\boldsymbol{D}''_W$ 是对角阵,其对角元素分别为

$\boldsymbol{D}'_W(i,i)=1/2\ \|\ \boldsymbol{W}(i,:)\ \|_2$，$\boldsymbol{D}''_W(i,i)=1/2\|\boldsymbol{W}^{\mathrm{T}}(i,:)\|_2$。

为了求解 $\boldsymbol{W}$，引入以下两个引理。

引理 1 对任意矩阵 $\boldsymbol{B}\in\boldsymbol{\Omega}^{m\times n}$ 右面乘以一个对角阵 $\boldsymbol{D}\in\boldsymbol{\Omega}^{n\times n}$，表达式 $\boldsymbol{BD}$ 可以被记做 $\boldsymbol{D}^*\odot\boldsymbol{B}$，其中⊙表示 Hadamard 积，$\boldsymbol{D}^*\in\boldsymbol{\Omega}^{m\times n}$ 被定义为 $\boldsymbol{D}^*(i,j)=\boldsymbol{D}(j,j)$，$\forall i=1,2,\cdots,m$，$\forall j=1,2,\cdots,n$。

引理 2 若有关于矩阵 $\boldsymbol{U}$ 的等式

$$\boldsymbol{C}_1\boldsymbol{U}\boldsymbol{C}_2+a'\boldsymbol{D}_1\boldsymbol{U}+b'\boldsymbol{D}_2\odot\boldsymbol{U}=\boldsymbol{V}\tag{18}$$

式中：$\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 是对称半正定矩阵；$\boldsymbol{D}_1$ 和 $\boldsymbol{D}_2$ 为对角矩阵；a' 和 b' 是系数。式(18)可以被重写为

$$\boldsymbol{\Theta}_1\boldsymbol{K}\boldsymbol{\Theta}_2+a\boldsymbol{P}^{\mathrm{T}}\boldsymbol{D}_1\boldsymbol{P}\boldsymbol{K}+b\boldsymbol{D}_2\odot\boldsymbol{K}=\boldsymbol{P}^{\mathrm{T}}\boldsymbol{V}\boldsymbol{Q}\tag{19}$$

式中：$\boldsymbol{C}_1=\boldsymbol{P}\boldsymbol{\Theta}_1\boldsymbol{P}^{\mathrm{T}}$；$\boldsymbol{C}_2=\boldsymbol{Q}\boldsymbol{\Theta}_2\boldsymbol{Q}^{\mathrm{T}}$；$\boldsymbol{K}=\boldsymbol{P}^{\mathrm{T}}\boldsymbol{U}\boldsymbol{Q}$；$\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 为正交矩阵；$\boldsymbol{\Theta}_1$ 和 $\boldsymbol{\Theta}_2$ 为特征值组成的对角矩阵。

通过引理 1 和引理 2 推理得知，式(16)中的 $\boldsymbol{W}$ 可以表示为

$$\boldsymbol{W}=\boldsymbol{P}\boldsymbol{Y}\boldsymbol{Q}^{\mathrm{T}}\tag{20}$$

具体推理过程如下。首先，式(17)可以变为

$$\boldsymbol{\Theta}_1\boldsymbol{Y}\boldsymbol{\Theta}_2+\alpha\boldsymbol{Z}\boldsymbol{Y}+\beta\boldsymbol{D}_W^*\odot\boldsymbol{Y}=\boldsymbol{M}\tag{21}$$

式中：$\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}=\boldsymbol{P}\boldsymbol{\Theta}_1\boldsymbol{P}^{\mathrm{T}}$，$\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}=\boldsymbol{Q}\boldsymbol{\Theta}_2\boldsymbol{Q}^{\mathrm{T}}$；$\boldsymbol{Y}=\boldsymbol{P}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{Q}$；$\boldsymbol{Z}=\boldsymbol{P}^{\mathrm{T}}\boldsymbol{D}'_W\boldsymbol{P}$；$\boldsymbol{M}=\boldsymbol{P}^{\mathrm{T}}(\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}-\boldsymbol{X}^{\mathrm{T}}\widetilde{\boldsymbol{R}}\boldsymbol{X}^{\mathrm{T}})\boldsymbol{Q}$。然后，定义 $\boldsymbol{Y}=[\boldsymbol{y}_1,\boldsymbol{y}_2,\cdots,\boldsymbol{y}_d]\in\boldsymbol{\Omega}^{n\times d}$，$\boldsymbol{M}=[\boldsymbol{m}_1,\boldsymbol{m}_2,\cdots,\boldsymbol{m}_d]\in\boldsymbol{\Omega}^{n\times d}$，$\boldsymbol{Z}=[\boldsymbol{z}_1,\boldsymbol{z}_2,\cdots,\boldsymbol{z}_n]\in\boldsymbol{\Omega}^{n\times n}$，根据此定义和引理 1，可以将式(21)转化为

$$\boldsymbol{\Theta}_2(i,i)\boldsymbol{\Theta}_1\boldsymbol{y}_i+\alpha\boldsymbol{Z}\boldsymbol{y}_i+\beta\boldsymbol{D}_W^*(1,i)\boldsymbol{I}\boldsymbol{y}_i=\boldsymbol{m}_i\tag{22}$$

列向量 $\boldsymbol{y}_i$ 可以表示为

$$\boldsymbol{y}_i=(\boldsymbol{\Theta}_2(i,i)\boldsymbol{\Theta}_1+\alpha\boldsymbol{Z}+\beta\boldsymbol{D}_W^*(1,i)\boldsymbol{I})^{-1}\boldsymbol{m}_i\tag{23}$$

由式(23)可知，计算得到每一个 $\boldsymbol{y}_i$ 后即可得到矩阵 $\boldsymbol{Y}$，再根据 $\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{W}\boldsymbol{Q}^{\mathrm{T}}$，即可得到 $\boldsymbol{W}$。

3.3 方法描述

构建属性矩阵 $\boldsymbol{X}$ 和邻接矩阵 $\boldsymbol{A}$，使用这两个矩阵以及相应的参数作为输入，交替更新矩阵 $\boldsymbol{W}$ 和 $\widetilde{\boldsymbol{R}}$，直到式(13)收敛。此时，可以得到最优的残差矩阵 $\widetilde{\boldsymbol{R}}$，通过 $\widetilde{\boldsymbol{R}}$ 即可判断异常源 IP 地址。网络流量异常检测方法的伪代码如下。

1. 从 $\boldsymbol{A}$ 矩阵构建拉普拉斯矩阵 $\boldsymbol{L}$
2. 初始化 $\boldsymbol{D}_R$、$\boldsymbol{D}'_W$、$\boldsymbol{D}''_W$ 为单位矩阵
3. 初始化残差矩阵 $\widetilde{\boldsymbol{R}}=\boldsymbol{X}(\boldsymbol{I}+\gamma\boldsymbol{D}_R+\varphi\boldsymbol{L})^{-1}$
4. 构建正交矩阵 $\boldsymbol{P}$、$\boldsymbol{Q}$ 以及对角阵 $\boldsymbol{\Theta}_1$ 和 $\boldsymbol{\Theta}_2$
5. While 式(13)不收敛 do
6. 通过式(20)更新 $\boldsymbol{W}$
7. 通过 $\boldsymbol{D}'_W(i,i)=1/2\|\boldsymbol{W}(i,:)\|_2$ 更新 $\boldsymbol{D}'_W$
8. 通过 $\boldsymbol{D}''_W(i,i)=1/2\|\boldsymbol{W}^{\mathrm{T}}(i,:)\|_2$ 更新 $\boldsymbol{D}''_W$
9. 通过式(15)更新 $\widetilde{\boldsymbol{R}}$
10. 通过 $\boldsymbol{D}_R(i,i)=1/2\|\widetilde{\boldsymbol{R}}^{\mathrm{T}}(i,:)\|_2$ 更新 $\boldsymbol{D}_R$
11. 循环结束
12. 计算每一个 IP 地址的残差 $\|\widetilde{\boldsymbol{R}}(:,i)\|_2$
13. 输出超过阈值的源 IP 地址

4 实验结果分析

4.1 实验数据

为了验证本文方法的有效性，2019 年 1 月 11 日在西安交通大学校园网某个路由器收集了 NetFlow 网络流量数据。考虑到不同时间段的网络使用情况不同，为了尽可能全面反映网络用户行为的特征，分别在 3 个不同的时间段进行采集，每个时间段都持续 2 个小时。3 个不同的时间段分别是：凌晨的 1 点到 3 点，代表休息时间；上午 9 点到 11 点，代表上课时间；晚上 21 点到 23 点，代表休息时间。对本文所用到的数据集进行统计分析，发现该数据集共有 276 149 条流记录，3 个时间段的流的数量分别为 104 973、81 116 和 90 060 条。

由于原始数据集收集于真实的网络环境，可能包含网络攻击，为了确保数据集在人工插入异常之前不含有异常，采用了多种方法对原始流进行了过滤，具体包括：①分析了常见的网络攻击特征，根据这些特征进行异常过滤；②从安全机构收集了大量的恶意 IP 地址信息，根据这些 IP 地址对数据进行过滤；③采用了一些专家知识对流量进行了预处理。在此基础上，对过滤后的流量进行异常注入，3 个时间段内注入的异常流的数量分别为 19、19 和 17 条。

4.2 性能分析

4.2.1 评价标准 本文使用召回率、精确率以及 F_1-score 共 3 个指标来衡量本文方法的有效性与准确性。召回率的定义为

$$R=a''/g\tag{24}$$

式中：a'' 为检测出的所有异常为真正异常的数量；g 为实验样本中所有异常的数量。精确率的定义为

$$P=a''/b''\tag{25}$$

式中 b'' 为检测出的所有异常的数量。F_1-score 是召回率和精确率的调和平均数，其定义为

$$F_1=2RP/(R+P)\tag{26}$$

4.2.2 结果分析 在实验中，时间窗口设置为 1 min，构建属性矩阵 $\boldsymbol{X}$ 和邻接矩阵 $\boldsymbol{A}$，设置参数 $\alpha=0.015$，$\beta=0.01$，$\gamma=0.009$，$\varphi=0.01$。在本文方法中，设置合理的阈值 θ 至关重要，它直接影响到检测结果的准确性，通过设置不同的阈值可以得到不同的运行结果，具体如表 1～3 所示。对样本 1 和样本

2:当阈值为 0.65 时,虽然能够使得召回率达到 84%以上,但是精确率仅有 50%左右,这说明有很多的误报;当阈值为 0.70 时,召回率和精确率都超过 84%,检测效果较好;当阈值为 0.75 时,召回率下降,精确率增加,说明检测的异常变少了。对于样本 3,随着阈值的增加,召回率虽然没有发生变化,但是精确率在递增,当阈值为 0.80 时,召回率和精确率均在 94%以上,检测效果良好。

表 1　样本 1 的阈值与检测率

θ	a''	b''	R/%	P/%	F_1/%
0.65	16	32	84.21	50.00	62.74
0.70	16	19	84.21	84.21	84.21
0.75	13	14	68.42	92.86	78.79

表 2　样本 2 的阈值与检测率

θ	a''	b''	R/%	P/%	F_1/%
0.65	18	30	94.73	60.00	73.47
0.70	18	20	94.73	90.00	92.30
0.75	17	18	89.47	94.44	91.89

表 3　样本 3 的阈值与检测率

θ	a''	b''	R/%	P/%	F_1/%
0.70	16	27	94.12	59.26	72.73
0.75	16	19	94.12	84.21	88.89
0.80	16	17	94.12	94.12	94.12

实验结果符合校园网用户的习惯:在凌晨和上课时间,使用网络用户较少,上网模式相对比较简单,因此适中的阈值就能有良好的异常检测率;在晚上休闲的时间段,使用网络用户相对较多,用户上网模式相对繁杂,因此需要设置较高的阈值。综合考虑以上因素,0 点到 19 点阈值设置为 0.70,19 点到 24 点阈值设置为 0.80。

(1)灵敏度分析。灵敏度定义为检测出的真正异常流数和总异常流数的比,攻击强度定义为异常流数和总流数的比。按照一定的时间间隔向原始的网络流量中注入不同攻击强度的异常流量,注入异常流量的数据量可以检验所提方法的灵敏度,注入异常数越少,攻击强度越小,模型越不容易检测到异常,如果此时模型依然能够实现异常的准确检测,说明模型的灵敏度越高。每隔 10 min 从样本 1 中抽取时间窗口内的原始流记录,注入不同攻击强度的异常流量对灵敏度进行计算,结果如表 4 所示。可以看出,本文方法在攻击强度达到 1.0%及以上时,能检测出超过 90%以上的异常 IP,并且能够定位这些异常。

表 4　本文方法的灵敏度分级检测结果

攻击强度/%	灵敏度/%	攻击强度/%	灵敏度/%
0.3	45.8	3.0	100
0.5	70.83	5.0	100
1.0	91.67	10.0	100

(2)异常检测方法对比分析。在样本 1 的原始流中插入 12 条异常流,并确保每条异常流仅插入到一个时间窗口中,这样就组成了攻击样本,然后使用不同方法进行异常检测。

为验证本文方法的有效性,选取信息熵、互信息熵、EWMA 共 3 种方法进行对比。文献[17]根据网络流量的多个特征分布的熵对滑动窗口内的流进行异常检测。由于网络攻击会造成网络流数据量分布的变化,采用信息熵量化网络流量数据量分布的变化,并依据变化的程度实现异常检测。由于网络异常的变化具有突发性,正常行为则通常具有惯性,不会在短时间内改变行为特征,据此利用互信息熵量化相邻时间窗口的网络流数据量分布的变化,若存在突变,则表示存在网络异常。文献[18]采用 EWMA 模型对源端口的熵进行异常检测。网络异常也可以体现在单位时间窗口内的数据包总数,DDoS 等网络攻击会产生大量的异常数据包,据此采用 EWMA 模型预测单位时间窗口内的数据包总数,并根据 EWMA 确定置信区间,如果预测值不在置信区间内,则视为异常点。信息熵、互信息熵、EWMA 这 3 种方法的检测结果如表 5 所示,本文方法的检测结果为表 1 中 $\theta=0.70$ 时的数据。

表 5　不同检测方法的检测率

检测方法	a''	b''	R/%	P/%	F_1/%
信息熵	4	15	33.33	26.67	29.63
互信息熵	11	25	91.67	44.00	59.46
EWMA	3	13	25.00	23.08	24.00

从表 5 可以看出:对于信息熵检测方法,预测异常有 15 个,预测中的真实异常有 4 个,召回率和精确率都比较低,因此传统的香农信息熵方法对异常反应不明显,较难检测异常;对于互信息熵检测方法,在阈值设置为 0.1 的情况下,检测出 25 个异常,其中 11 个异常为真,召回率很高但是精确率较低,说明误报率高;对于 EWMA 检测方法,检测出 13 个异常,其中 3 个为真异常,该方法不仅异常检测率

较低，并且会出现误报。

(3)复杂度分析。由于本文所提出的优化方法涉及到矩阵分解、矩阵求逆等计算操作，因此时间复杂度较高，在下一步的研究中，将探索如何降低时间复杂度。同时，实验结果表明本文方法在进行异常流量检测中准确性较高、检测过程可解释、不需要先验知识并且可以定位异常源，若能克服超大规模矩阵计算复杂度的难题，本文方法将更加具有实用性。

5 结 论

为了解决网络异常流量检测中大数据小异常的难题，从矩阵分解的角度出发，采用 *CUR* 矩阵分解描述异常检测过程，并且通过残差分析判断异常，为网络流量的异常检测提供了一个新的解决方法。在分析常见的网络攻击行为的基础上，从多个角度提取能够引起网络流量异常变化的特征属性。采集真实环境下的实验数据，对能够引起方法准确性的阈值进行分析，结果表明，在不同时间段设置合理的阈值可以使本文方法的异常检测率高达 90% 以上。与其他异常检测方法相比，本文方法不仅具有较高的异常检测率，而且可以准确定位异常。灵敏度分析结果表明，本文方法在攻击强度达到 1.0% 以上能时，能够检测出超过 90% 以上的异常，具有很强的敏感性。在下一步的工作中，将研究如何降低本文方法的计算复杂度。

参考文献：

[1] AGRAWAL S, AGRAWAL J. Survey on anomaly detection using data mining techniques [J]. Procedia Computer Science, 2015, 60: 708-713.

[2] ILIOFOTOU M, PAPPU P, FALOUTSOS M, et al. Network monitoring using traffic dispersion graphs (TDGs) [C]// Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. New York, USA: ACM, 2007: 315-320.

[3] BEHAL S, KUMAR K. Detection of DDoS attacks and flash events using novel information theory metrics [J]. Computer Networks, 2017, 116: 96-110.

[4] AHMED M, NASER MAHMOOD A, HU J K. A survey of network anomaly detection techniques [J]. Journal of Network and Computer Applications, 2016, 60: 19-31.

[5] LAKHINA A, CROVELLA M, DIOT C. Mining anomalies using traffic feature distributions [C]// Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. New York, USA: ACM, 2005: 217-228.

[6] GIORGI G, NARDUZZI C. Detection of anomalous behaviors in networks from traffic measurements [J]. IEEE Transactions on Instrumentation and Measurement, 2008, 57(12): 2782-2791.

[7] 周爱平，程光，郭晓军，等. 高速网络超点检测的并行数据流方法 [J]. 软件学报，2016，27(7)：1841-1860.
ZHOU Aiping, CHENG Guang, GUO Xiaojun, et al. Parallel data streaming method for detection of super points in high-speed networks [J]. Journal of Software, 2016, 27(7): 1841-1860.

[8] ANDROULIDAKIS G, PAPAVASSILIOU S. Two-stage selective sampling for anomaly detection: analysis and evaluation [J]. Security and Communication Networks, 2011, 4(6): 608-621.

[9] 程光，龚俭，丁伟. 基于抽样测量的高速网络实时异常检测模型 [J]. 软件学报，2003，14(3)：594-599.
CHENG Guang, GONG Jian, DING Wei. A real-time anomaly detection model based on sampling measurement in a high-speed network [J]. Journal of Software, 2003, 14(3): 594-599.

[10] PELE L, BUCZKO U, GALOR O, et al. Detecting traffic anomalies with adaptive sampling [C]// Proceedings of the 12th ACM International Conference on Systems and Storage. New York, USA: ACM, 2019: 186.

[11] 罗娜，李爱平，吴泉源，等. 基于概要数据结构可溯源的异常检测方法 [J]. 软件学报，2009，20(10)：2899-2906.
LUO Na, LI Aiping, WU Quanyuan, et al. Sketch-based anomalies detection with IP address traceability [J]. Journal of Software, 2009, 20(10): 2899-2906.

[12] JING X Y, YAN Z, JIANG X Q, et al. Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch [J]. Information Fusion, 2019, 51: 100-113.

[13] YANG T, LIU L T, YAN Y B, et al. SF-sketch: a fast, accurate, and memory efficient data structure to store frequencies of data items [C]// 2017 IEEE 33rd International Conference on Data Engineering (ICDE). Piscataway, NJ, USA: IEEE, 2017: 103-106.

[14] KRISHNAMURTHY B, SEN S, ZHANG Y, et al. Sketch-based change detection [C]// Proceedings of the 2003 ACM SIGCOMM Conference on Internet Measurement. New York, USA: ACM, 2003: 234-247.

(下转第 84 页)