一种基于小波分析的网络流量异常检测方法

杜 臻 马立鹏 孙国梓
(南京邮电大学计算机学院 南京 210023)

摘 要 对大量网络流量数据进行高质量特征提取与异常识别是做好网络取证的重要基础。文中重点研究并实现了网络取证中的数据处理并建立了模型库。对一种基于小波分析的网络流量异常检测方法进行了研究,用于检测包含两种不同注入攻击的pcap文件。文中的研究在Windows系统上进行,采用Python语言完成功能代码编写。首先从大量数据中提取需要的训练数据,然后使用小波分析提取特征,最后使用支持向量机进行分类器训练,从而可以利用该分类器识别出包含正常流量和异常流量的混合流量中的异常。定性和定量实验结果表明该方法对两种类型的异常流量实现了较高的分类精度,以期从特征提取和分类分析两个角度为网络取证的完善提供一种途径。

关键词 网络取证,异常检测,特征提取,小波分析,分类分析
中图法分类号 TP391 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.08.029

Network Traffic Anomaly Detection Based on Wavelet Analysis

DU Zhen MA Li-peng SUN Guo-zi
(School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract High-quality feature extraction and anomaly detection of large-scale network traffic data is an important basis for network forensics. The key research and implementation of this paper is the data processing and modeling library in network forensics. A method of network traffic anomaly detection based on wavelet analysis was studied to detect pcap files containing two different injection attacks. The study was implemented on the Windows system, and Python language was used to complete the function code. First, the required training data from a large amount of data are extracted, then the features are extracted from trainning data by using wavelet analysis. Finally, the support vector machine is used for classifier training. Thus, two types of anomaly traffic are identified from the mixed traffic containing normal traffic and abnormal traffic. Qualitative and quantitative experimental results show that the method achieves good classification results, and can provide a way for the improvement of network forensics from the two perspectives of feature extraction and classification analysis.

Keywords Network forensics, Anomaly detection, Feature extraction, Wavelet analysis, Classification analysis

1 引言

网络取证主要对抓取并记录的网络数据流、主机系统日志等进行分析,从而发现网络异常行为,自动记录犯罪证据,阻止其对网络系统的进一步入侵[1]。在网络取证发展的同时,反取证技术也逐步发展,使计算机取证变得更加困难。因此,如何有效地检测异常流量并进行入侵行为分析成为网络取证中不可或缺的一个环节[2-3]。本文主要讨论面向网络安全的取证,也即异常流量检测和入侵行为的分析。

目前对异常流量的检测一般基于人工经验,如使用预先建立的规则库进行规则匹配、阈值匹配等[4-6]。但是,这些方法都是基于人们的知识,可能受到人们主观错误和知识更新缓慢的影响。对此,一些研究人员提出了基于数据挖掘技术的网络流量异常检测模型,提出从网络流量数据中发现行为异常[7],即当存在异常流量时,通过寻找与正常模式的偏差来发现入侵。但是,一方面网络流量呈现出高度非线性、耗散性和不平衡性;另一方面,并非所有入侵都表现为网络异常流量,且系统的轨迹难以计算和更新。因此现有模式与历史模式之间的匹配程度较低。数据挖掘技术在网络流量异常检测中的局限性在于它只能检测已知模式的网络异常。

目前,小波分析已广泛应用于信号处理[8-9]、语音识别[10]、图像压缩、模式识别[11]和其他一些领域[12]。有学者通过实验发现大规模网络流量具有宏观信号的所有特征[13],可以将网络流量视为信号,并且利用小波分析可以有效地检测短期和长期网络流量异常。将正常网络流量的时变信号与异常网络流量的时变信号进行比较可以发现,其频带范围或频率特性不同。小波分析能够表征信号的局部特征,并能有效地从信号中提取信息。利用小波分析可以同时分析时域和频域的异常流量信号,提高检测效率,降低误检率和漏检率。

为了准确分析并区分两种注入攻击的流量异常,本文提

到稿日期:2018-07-21 返修日期:2018-12-11

杜 臻(1994-),女,硕士生,主要研究方向为数据挖掘,E-mail:sun@njupt.edu.cn;**马立鹏**(1997-),男,主要研究方向为信息安全与数据挖掘;**孙国梓**(1972-),男,教授,硕士生导师,主要研究方向为计算机取证与区块链,E-mail:sun@njupt.edu.cn(通信作者)。

出了一种基于小波分析的异常分类模型。首先，使用小波分析[14]将 pcap 文件中数据包的长度数值序列划分为较小尺度的分量，并提取不同尺度的能量特征。然后，提取时域中的均值和标准差，并将时域特征和频域特征融合为最终特征，并送入支持向量机（Support Vector Machine，SVM）中进行学习。仿真结果表明，该模型对两种不同注入攻击的流量异常具有良好的分类效果。

本文第 1 节简要介绍了网络取证、流量异常检测的重要性以及当前的一些技术难点；第 2 节介绍了与本文内容相关的工作；第 3 节详细介绍了本文提出的模型；第 4 节描述了模拟实验并分析实验结果；最后总结全文。

2　相关工作

从特征提取的角度讲，为了寻找数字证据，需要发现信息行为的关键特征，去除无意义的、无用的特征或噪声。在本文的应用场景中，采用小波分析来挖掘流量特征。

小波分析是应用数学的一个分支，在工程应用中发挥了重要作用，特别是在信号分析中[15]。小波分析具有多分辨率的优点（多尺度），它可以很好地表征时域和频域信号的局部特征。由于小波分析技术可以将信号在不同频级分成不同分量，因此小波分析技术最近被广泛用于网络流量异常检测，典型示例参见文献[16-18]。这些研究的重点是使用小波分析直接提取网络流量信号的特征，并进行一些后续分析以发现异常。

从分类分析的角度讲，网络取证中的分类分析就是通过分析采集到的数据，为每个类别做出准确的描述，或建立分析模型或挖掘出分类规则，然后用这个分类规则对其他数据进行分类。本文采用 SVM 对小波分析所得到的特征进行分类。

本文工作与上述研究之间主要有两点不同：首先，尽管本文也使用小波分析，但输入信号不同；其次，本文工作不仅是发现异常，更注重区分不同类型的异常。换句话说，本文的重点是利用 pcap 文件的外部参数作为小波分析的输入信号，并从中提取特征，即小波分析的输入信号是包长度序列，然后使用分类算法来区分不同类型的异常。

3　模型介绍

网络取证的总体流程如图 1 所示。

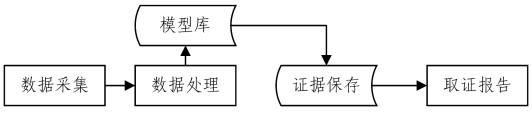

图 1　网络取证工作的流程模型

Fig. 1　Flow model of network forensics work

本文重点研究并实现了网络取证工作中的数据处理，并建立了模型库，具体实现如下文所述。

本文建立模型库的初始数据即原始训练样本使用的网络流量是从服务器捕获的基于 HTTP 协议的 web 攻击数据，其形式为 pcap 文件，包含 XSS 攻击和 SQL 注入攻击。利用所建立的模型库可识别待检测的 web 攻击数据中的 XSS 攻击和 SQL 注入攻击。

告警日志是一些触发告警事件的 pcap 文件的记录，告警日志的数据结构如表 1 所列。

表 1　数据结构说明表

Table 1　Rescription of data structure

参数名称	说明
sip	源 IP 地址
dip	目的 IP 地址
time node	数据包发生时间
anomaly type	触发告警日志的事件 ID
URI	统一资源标识符

解析的 pcap 文件存储在数据库中的 6 个字段中，与告警日志的结构相同。

对应于图 1 中的数据处理和模型库的建立，本文提出的数据处理方法及模型库建立的流程如图 2 所示。在整个过程中，提取包长度是基础工作。

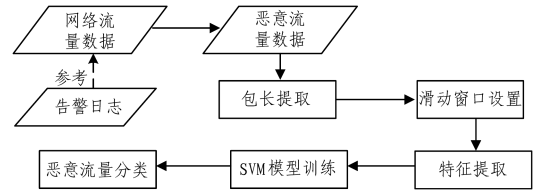

图 2　核心实现流程图

Fig. 2　Flowchart of core implementation

包长度提取步骤如下：

1）解析 pcap 文件；

2）用内容标记每个告警日志记录；

3）将 source ip，destination ip，time node 和 URI 作为匹配条件；

4）将告警日志中的每条记录映射到已解析的 pcap 数据库的文件中，获取相应的数据；

5）提取数据包长度。

如图 2 所示，首先从异常流量所产生的告警日志中将针对不同数据库的两类注入攻击的包长提取出来，并按照发生的时间顺序对包长从 1 开始编号，形成（序号，包长）形式的数值序列。为了提取到足够多的特征，设置滑动窗口大小和步长大小，对每个窗口内的数值序列提取特征，从而可以对一个完整的包长序列提取多组特征向量。然后将特征向量送入 SVM 模型中进行分类器学习，并用学习到的分类器实现分类。

图 2 中最关键的部分为特征提取和分类器学习，它们是网络取证中的重要环节。在特征提取部分，本文将时域特征和小波频域特征相融合；在分类器学习部分，采用 SVM 判别式分类器。图 2 中，模型训练及其之前的工作都属于训练阶段，最后的恶意流量分类就是对实际数据进行检测，检测阶段的数据处理步骤与训练阶段相同，此处不再赘述。然后将得到的特征向量送入训练好的模型中进行分类识别即可。

3.1　小波特征提取方法

3.1.1　小波函数和小波变换

小波分析的基本思想是用小波函数来表示或逼近某一信号或函数，因此选择合适的小波函数是进行小波分析的前提。在实际应用研究中，对于同一信号或时间序列，若选择不同的基小波函数，所得结果往往会有差异，有时甚至差异很大。常

见的基小波函数有多种，本文所采用的是 Daubechies 1 小波函数，即 Haar 小波函数。

Haar 函数是小波分析中最早用到的一个具有紧支撑的正交小波函数，它是支撑域在 $t\in[0,1]$ 范围内的单个矩形波。利用 Haar 小波函数对信号进行小波分解，从数字滤波器的角度看，可以用图 3 所示的结构来实现，其中 H,G 为双尺度方程所决定的滤波器系数。

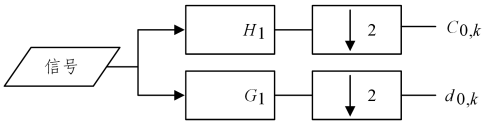

图 3 小波分解示意图

Fig. 3 Diagram of wavelet decomposition

若将信号的输入序列看作一离散序列，则图 2 所示为一输入离散序列进行双通道滤波的过程，可以称 H,G 为双通道滤波器组。进行一次小波分解可以得到信号的低频概况 $C_{0,k}$ 和高频细节 $d_{0,k}$。对信号进行分解，也就是不断对信号实施小波分解运算，从而将采集到的信号分解为不同频段的信号数据，以便在不同频段内对信号进行分析与处理。分解的低频分量包含信号特征，高频成分反映细节或信号的差异。因此在本文中，为了分析流量异常的整体特征，需要提取低频特征；为了区分两种不同的流量异常，需要提取高频特征。下面将分别讨论提取低频信号和高频信号的能量，并分别计算它们的能量比作为特征。

3.1.2 小波特征提取

为了在长序列包中获得足够数量的特征组长度，需要在其中提取具有一定长度的子序列。通过设置滑动窗口，可以满足此要求。对于长度为 m 的数值序列 T 和目标阈值 w，长度为 w 的滑动窗口通过 T 获得 $(m\times w)+1$ 个子序列。

针对两种不同数据库的延时注入进行分析，两种数据库分别为 Postgresql 和 sql server。首先对异常日志和触发相应异常的流量包进行统计，得到包长的数值序列，如表 2 所列。为便于说明，选择整个数值序列的前 5 个值进行展示。序号指序列中的位置编号。

表 2 包长序列示意

Table 2 Diagram of packet length sequence

序号	1	2	3	4	5
包长	695	687	692	692	701

对两种延时注入的包长序列分别进行如下操作：

1)对包长序列进行初步分析，得出其大致的周期。

2)为了得到足够量的特征向量组，需要通过滑动窗口进行操作。即一个窗口内提取一组特征向量，将窗口大小设置为周期大小，滑动步长设为 1。通过分析包长数值序列发现其周期约为 600，然后滑动滑动窗口 600 次以获得 600 组特征向量。

在模式识别中有两个重要环节：特征提取和分类器的设计。特征提取是高效、准确完成识别的前提。对于模式特征(参数)的选取，应遵循以下原则：

1)特征具有显著的类别差异，且互不冗余，使分类器具有较好的分类性能和效率；

2)维数尽可能低，尽可能少的辨识信息将降低分类器的复杂性，利于软硬件实现。

小波变换是一种时-频窗面积固定、形状可自适应调整的信号分析工具，在时、频局部化方面具有独特优势，非常适用于信号的异常检测[15]。本文将二进离散小波变换应用于包过程的处理。首先将包过程 $\{X(t)\}$ 进行 J 层分解：

$$X(t)=\sum_{j=1}^{J}\sum_{k}d_{j,k}\psi_{j,k}(t)+\sum a_{j,k}\varphi_{J,k}(t) \tag{1}$$

其中，$d_{j,k}$ 为小波系数，表示尺度 j 上的细节信息；$a_{j,k}$ 为近似系数，表示尺度 j 上的逼近信息。

信号的分解在理论上可以无限制地进行，但实际上，当高频分量仅包含单个样本时分解可以停止。因此，在实际应用中，通常根据信号或适当标准的特性选择适当数量的分解层。本文发现将高频分量按照图 4 所示进行 1 层分解后已经充分展示了细节，对其进行进一步的分解后其波形没有变化，因此无需对该高频分量进行多层分解；我们不断分解低频成分，并且发现当分解到 5 层后该低频分量的波形没有了变化，故对低频分量使用 5 层分解即可。

在提取特征这一步骤中，对每个窗口内的包长序列使用小波变换，将序列进行 5 尺度分解，具体如图 4 所示。

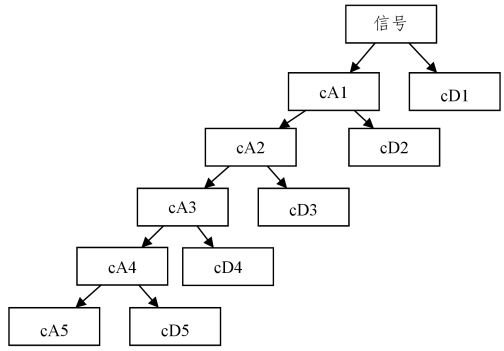

图 4 5 尺度分解示意图

Fig. 4 Diagram of 5-scale decompsition

本文选择 Daubechies1 小波的分解结果进行进一步分析。选择以下 8 个特征参数 ERa_5，ERd_1，ERd_2，ERd_3，ERd_4，ERd_5，μ，σ，它们构成一个 8 维的特征向量 $[ERa_5,ERd_1,ERd_2,ERd_3,ERd_4,ERd_5,\mu,\sigma]$。

1)平均值(Mean Value)。信号的均值表示信号序列的算术平均值或数学期望值，反映了信号相对于均值的波动情况，在模式识别中代表信号的能量或功率，由式(2)计算：

$$\mu=\frac{1}{N}\sum_{1}^{N}X_i \tag{2}$$

其中，X_i 代表信号在 i 点的取值，N 为信号的长度。

2)标准差(Standard Deviation)。标准差能反映一个数据集的离散程度，由下式计算：

$$\sigma=\sqrt{\frac{1}{N}\sum_{1}^{N}(X_i-\mu)^2} \tag{3}$$

3)能量占比(Energy Ratio，ER)。能量占比是低频信号 a_5 能量和各高频信号 $d_1,d_2,\cdots,d_5$ 的能量与总能量的比值。其中，低频能量如式(4)所示，高频能量如式(5)所示，能量占比如式(6)、式(7)所示。

$$Ea_j=\sum_{1}^{N}a_i^2,j=5 \tag{4}$$

$$Ed_j=\sum_1^N d_i^2, j=1,2,\cdots,5 \tag{5}$$

$$ERa_5=\frac{Ea_5}{Ea_5+\sum_1^5 Ed_j} \tag{6}$$

$$ERd_j=\frac{Ed_j}{Ea_5+\sum_1^5 Ed_j} \tag{7}$$

3.2 SVM 模型

对于非线性的情况，支持向量机的处理方法是选择一个核函数 $k(x_i,x_j)$，首先在低维空间中完成计算，然后通过核函数将输入空间映射到高维特征空间，最终在高维特征空间中构造出最优分离超平面，从而把平面上本身不好分的非线性数据分开。因此，SVM 核函数的选择对于其性能的表现有至关重要的作用，尤其针对那些线性不可分的数据。常用的核函数包括线性核函数、多项式核函数、高斯径向基核函数、sigmoid 核函数。本文采用高斯径向基核函数。

径向基核函数(Radial Basis Function，RBF)的公式如下：

$$k(x,y)=\exp(-\gamma\|x-y\|^2) \tag{8}$$

其中，γ 为核函数宽度，也叫高斯核(Gaussian Kernel)。因为径向基核函数可以看成如式(9)的高斯函数的另一种形式：

$$k(x,y)=\exp(-\frac{\|x-y\|^2}{2\sigma^2}) \tag{9}$$

高斯径向基函数是一种局部性强的核函数，其可以将一个样本映射到一个更高维的空间内，该核函数的应用最广泛，无论对于大样本还是小样本都有比较好的性能，而且其相对于多项式核函数的参数要少，因此在大多数情况下优先使用高斯核函数。

4 仿真实验与结果分析

4.1 仿真实验

在本文中，“标签”对应于表 1 中的触发告警日志的事件 ID，也就是异常类型。将 Postgresql 注入攻击标记为 0，将 sql server 注入攻击标记为 1。“编号”是特征向量组的数量编号，为了便于说明，选择每种异常类型的前 5 个特征向量组进行展示。提取的特征参数如表 3 和表 4 所列。

表 3　Postgresql 注入攻击包长序列的部分特征参数

Table 3　Partial eigenvalues of postgresql injection attack sequence

ERa_5	ERd_1	ERd_2	ERd_3	ERd_4	ERd_5	μ	σ	标签	编号
99.3779662	0.073471	0.173008	0.132587	0.160355	0.082611	649.57	71.526114	0	1
99.3620277	0.257978	0.051503	0.112615	0.098089	0.117785	649.60	71.541462	0	2
99.3638390	0.073421	0.247511	0.104735	0.058947	0.151545	649.63	71.556795	0	3
99.3567760	0.257802	0.057856	0.100963	0.053260	0.173340	649.66	71.572533	0	4
99.3351520	0.073371	0.172770	0.140886	0.072150	0.205667	649.69	71.588255	0	5

表 4　sql server 注入攻击包长序列的部分特征参数

Table 4　Partial eigenvalues of sql server injection attack sequence

ERa_5	ERd_1	ERd_2	ERd_3	ERd_4	ERd_5	μ	σ	标签	编号
99.682658	0	0.105326	0.024766	0.167352	0.019894	671.74666	56.206258 06	1	1
99.643259	0.072056571	0.035781	0.059124	0.158563	0.031213	671.79333	56.226089 23	1	2
99.608822	0	0.038792	0.148362	0.157950	0.046071	671.84000	56.245874 42	1	3
99.579600	0.072053883	0.030973	0.119694	0.128430	0.069246	671.87333	56.259382 12	1	4
99.555120	0	0.105310	0.116289	0.125980	0.097298	671.90666	56.272866 69	1	5

SVM 算法最初是为二值分类问题设计的，在处理多类问题时，就需要构造合适的多类分类器。目前，构造 SVM 多类分类器的方法主要分为直接法和间接法。间接法主要是通过组合多个二分类器来实现多分类器的构造。

本文采用间接法构造 SVM 多类分类器，以便日后扩展数据类别时使用。采用不同的 SVM 核函数和参数所得到的训练效果也是不同的。

SVM 模型有两个非常重要的参数，即 *cost* 与 *gamma*。其中 *cost* 是惩罚系数，即对误差的宽容度，*cost* 越大，说明越不能容忍出现误差，对错误例惩罚程度越大，越容易过拟合，*cost* 越小则越容易欠拟合。*cost* 过大或过小都会使泛化能力变差。*gamma* 是 RBF 函数自带的一个参数，它隐含地决定了数据映射到新的特征空间后的分布，*gamma* 越大，支持向量越少，分类界面越“散”，分类效果越好，但有可能过拟合；*gamma* 值越小，支持向量的个数越多，分类界面越连续，从而越影响训练与预测的速度。一般将其默认为类别数目 *n_features* 的倒数，在本文中为 0.5。分别使用不同的 SVM 核以及不同参数，得到如表 5 所列的结果。

表 5　基于 8 维特征 SVM 的分类精度表

Table 5　Classification accuracy of SVM based on 8-dimensional features

SVM 核函数	cost	gamma	训练集精度	测试集精度
linear	—	—	0.75	0.73
poly	—	—	0.75	0.76
sigmoid	—	—	0.51	0.46
RBF	0.1	0.5	0.83	0.81
RBF	1	0.5	0.88	0.86
RBF	10	0.5	0.92	0.90
RBF	100	0.5	0.96	0.93
RBF	1000	0.5	0.99	0.94
RBF	10000	0.5	0.99	0.93

4.2 结果分析

从表 5 可以看出，训练组及测试组中除了 sigmoid 核函数的识别结果明显较差外，线性核函数和多项式核函数的识别准确率相似。径向基核函数的识别准确率明显优于其他核函数。这说明流量曲线分类的问题的本质是非线性的分类问题。两种非线性的核函数识别结果基本一致，这也与 Vapnik，Scholkopf 等所得的结果一致，即非线性的 SVM 会表现

出大致相同的性能。sigmoid 核函数的结果出现异常，甚至比线性 SVM 的识别结果更差，这可能是原始问题中的数据分布导致了 sigmoid 核矩阵的异常，从而引起二次优化问题解的偏差。

送入 SVM 模型的学习数据是基于小波变形提取的能量特征，并利用这些数据对两种注入攻击进行分类。从表 6 可以看出，精度可以达到 90%左右，这表明这种分类方法具有良好的性能。

表 6 平均分类精度

Table 6 Average classification accuracy

SVM 核函数	训练集平均精度	测试集平均精度
RBF	0.92	0.89

在确定 SVM 分类器核函数为 RBF 的前提下，为了更有说服力地解释小波基 Daubechies1 的优越性，我们对 3 种不同的典型小波函数(Daubechies1(Haar)，Coiflets1 和 Discrete Meyer)进行比较，以区分不同类型的异常。从表 7 可以看出，Daubechies1(Haar)的性能比其他两个小波系列的性能稍好。

表 7 不同小波函数下的性能比较表

Table 7 Performance comparison under different wavelet functions

小波函数	训练集平均精度	测试集平均精度
Daubechies1	0.92	0.89
Coiflets1	0.89	0.86
Discrete Meyer	0.91	0.88

从表 7 还可以看出，当使用 RBF 内核进行模型学习时，保持参数 *gamma* 不变并调整参数 *cost* 可以使精度发生显着变化。当 *cost* 按 0.1，1，10，100，1000 的顺序变化时，训练集和测试集的精度都得到了提高，但是当它继续增加到 10000 时，精度开始下降，表明在本文的应用场景中，*cost* 的最优值在 1000 到 10000 之间。

结束语 网络取证技术正朝着精细化、自动化方向发展，将其与其他学科技术结合是网络取证技术突破的重要途径。针对当前网络取证中特征提取和分类分析的局限性，本文融合包长序列时域和频域特征提取，提出了基于小波变换的异常流量识别方法。该方法具有很强的鲁棒性，对小样本有很强的泛化能力。仿真实验结果表明，从包长序列的小波变换域提取特征的计算方法效率高，同时也可以达到较高的分类精度。本文通过构建异常流量包长序列，并结合 SVM 的方法进行基于小波的特征提取，为解决异常流量识别方法探索到新的研究手段。在未来的工作中，我们将致力于研究更加有效的波形特征，并设计新的 SVM 核函数，使分类效果更佳，为网络取证提供更有效的帮助。

参 考 文 献

[1] WANG L，QIAN H L. Computer forensics technology and its development trend[J]. Journal of Software，2003，14(9)：1635-1644. (in Chinese)
王玲，钱华林. 计算机取证技术及其发展趋势[J]. 软件学报，2003，14(9)：1635-1644.

[2] HOU H H. Application research of data mining in computer dynamic forensics technology[J]. Digital Technology and Application，2017，14(8)：76-77. (in Chinese)
侯欢欢. 数据挖掘在计算机动态取证技术中的应用研究[J]. 数字技术与应用，2017，14(8)：76-77.

[3] HU D H，XIA D R，SHI X L，et al. Network forensics technology research[J]. Computer Science，2015，23(b10)：1-22. (in Chinese)
胡东辉，夏东冉，史昕岭，等. 网络取证技术研究[J]. 计算机科学，2015，23(b10)：1-22.

[4] LAMABA H，GLAZIER T J，SCHMERL B，et al. A model-based approach to anomaly detection in software architectures[C]// Symposium and Bootcamp on the Science of Security，2016：69-71.

[5] ATEFI K，YAHYA S，REZAEI A，et al. Anomaly detection based on profifie signature in network using machine learning technique[C]// Region 10 Symposium. 2016：71-76.

[6] LEITNER M，RINDERLEB M S. Anomaly detection and visualization in generative rbac models[C]// ACM Symposium on Access Control MODELS and Technologies. 2014：41-52.

[7] ZHOU Y J. Network traffic anomaly detection based on data mining in time-series graph[J]. Computer Science，2009，36(1)：46-50.

[8] BARFORD P，KLINE J，PLONKA D. A signal analysis of network traffic anomalies[C]// Proc. ACM SIGCOMM Internet Measurement Workshop. Marseille，France，2002：71-82.

[9] LUAN K. Robust detection method for network attacks based on wavelet scale decomposition [J]. Electronic Technology and Software Engineering，2016，8(4)：9. (in Chinese)
栾凯. 基于小波尺度分解的网络攻击稳健检测方法[J]. 电子技术与软件工程，2016，8(4)：9.

[10] MA X H，Cao J P，DONG S F. Wavelet analysis and application [J]. Microcomputer Development，2003，56(1/2)：231-262.

[11] Al-QAMMAZ A Y，YUSOF Y，AHAMAD F K. An enhanced discrete wavelet packet transform for feature extraction in electroencephalogram signals[C]// International Conference. 2017：88-93.

[12] AHANI S，GHAEMMAGHAMI S Z，WANG Z J. A sparse representation-based wavelet domain speech steganography method[J]. IEEE/ACM Transactions on Audio Speech & Language Processing，2015，23(1)：80-91.

[13] ALI S，HUNG C C. An empirical study on feature extraction for the classification of textural and natural images[C]// International Conference on Research in Adaptive and Convergent Systems. 2016：51-55.

[14] ALNASHASH H A，PAUL J S，THAKOR N V. Wavelet entropy method for EEG analysis：application to global brain injury[C]// International IEEE Embs Conference on Neural Engineering. 2016：348-351.

[15] MA X H，CAO J P，DONG S F. Wavelet analysis and application [J]. Microcomputer Development，2003，56(1/2)：231-262.

[16] WEI L，GNORBANI A A. Network anomaly detection based on wavelet analysis[J]. Eurasip Journal on Advances in Signal Processing，2009，1(2003)：1-16.

[17] CHEN Z，CHAI K Y，BU S L，et al. A novel anomaly detection system using feature-based MSPCA with sketch[C]// Wireless and Optical Communication Conference. IEEE，2017：1-6.

[18] SALAGEAN M. Real network traffic anomaly detection based on analytical discrete wavelet transform[C]// International Conference on Optimization of Electrical and Electronic Equipment. 2010：926-931.