基于 ANN 与 KPCA 的 LDoS 攻击检测方法

吴志军，刘亮，岳猛
（中国民航大学电子信息与自动化学院，天津 300300）

摘 要：低速率拒绝服务（LDoS, low-rate denial of service）攻击是一种新的面向 TCP 协议的攻击方式，它具有攻击速率低、隐蔽性强的特点，很难被传统 DoS 攻击检测措施发现。针对其特点，采用网络大数据分析技术，从路由器队列中挖掘一种 LDoS 攻击特征，将核主成分分析（KPCA, kernel principal component analysis）方法与神经网络结合，提出一种新的检测 LDoS 攻击的方法。该方法将路由器队列特征采用 KPCA 降维，作为神经网络输入，再利用 BP 神经网络自学习能力生成 LDoS 分类器，达到检测 LDoS 攻击的目的。实验结果表明该方法有较好的检测有效性和较低的计算复杂度，对设计防御 LDoS 攻击的路由器有一些借鉴意义。

关键词：低速率拒绝服务攻击；队列特征；核的主成分分析；神经网络
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018073

Detection method of LDoS attacks based on combination of ANN & KPCA

WU Zhijun, LIU Liang, YUE Meng
School of Electronics Information & Automation, Civil Aviation University of China, Tianjin 300300, China

Abstract: Low-rate denial-of-service (LDoS) attack is a new type of attack mode for TCP protocol. Characteristics of low average rate and strong concealment make it difficult for detection by traditional DoS detecting methods. According to characteristics of LDoS attacks, a new LDoS queue future was proposed from the router queue, the kernel principal component analysis (KPCA) method was combined with neural network, and a new method was present to detect LDoS attacks. The method reduced the dimensionality of queue feature via KPCA algorithm and made the reduced dimension data as the inputs of neural network. For the good sell-learning ability, BP neural network could generate a great LDoS attack classifier and this classifier was used to detect the attack. Experiment results show that the proposed approach has the characteristics of effectiveness and low algorithm complexity, which helps the design of high performance router.

Key words: low-rate denial of service, queue feature, kernel principal component analysis, neural network

1 引言

低速率拒绝服务（LDoS, low-rate denial of service）攻击是一种新型的 DoS 形式[1]。它利用网络系统自适应机制中存在的漏洞，产生较低速率的攻击流量。在 LDoS 攻击期间，具有固定周期高速率的短脉冲攻击分组以很短的间隔被发送到受害端。这种攻击方式虽然无法使网络链路完全瘫痪，但是其低能耗会造成网络的虚假拥塞，对客户端及服务器的链接质量造成严重破坏，使服务端无法正常为用户提供服务，导致 TCP 连接质量大幅度下降。据统计，网络中 80%以上的流量是 TCP 流量。因此，

收稿日期：2017-04-20；**修回日期**：2018-02-06
基金项目：国家自然基金委员会与中国民航局联合基金资助项目（No.U1533107）；天津市自然科学基金资助项目（No.17JCZDJC30900）
Foundation Items: The Joint Foundation of National Natural Science Foundation and Civil Aviation Administration of China (No.U1533107), The Natural Science Foundation of Tianjin (No.17JCZDJC30900)

LDoS攻击具有巨大的潜在威胁[1]。LDoS攻击的平均速率低，并且完全混合在网络数据流中，不易与正常数据流量区分[2]。因此，传统的网络恶意流量检测方法难以见效。

在对LDoS攻击的检测处理上，目前，普遍采用信号处理与网络流量数据处理相结合的方法[3]，即将信号处理算法用于提取出的网络特征中，这种方法对提高检测准确度有很大帮助。然而，信号处理方法由于其自身处理数据量小的问题显然无法应对当前网络大数据的环境以及DDoS攻击的广泛性。因此，根据已有的特征与检测算法相结合的经验，提出一种应用队列特征的基于核的主成分分析与神经网络相结合的方法实现LDoS攻击检测。数据挖掘算法可以增大数据处理量，对加快运算速度及实时处理数据也有很大帮助。

2 相关工作

由于LDoS攻击能隐藏在正常网络流量中，很难将遭受LDoS攻击后的网络流量划分为攻击与正常流量，因此，其检测和防御一直是网络安全领域中研究的热点和难点。许多专家学者在攻击流量、TCP特征等多个方面进行了深入的研究，并根据不同的特征提出了多种检测算法[1,3]。其中，最为普遍的是基于信号处理的LDoS攻击检测方法，这种方法是将LDoS攻击流量进行抽样，在时/频域对抽样序列统计分析，进而对得到异于正常流量的特征加以区分[4]。文献[5]首先提出频域检测LDoS攻击的方法，将采样序列自相关后经离散傅里叶变换后得到功率谱密度，再将归一化功率谱密度作为检测特征进行检测。文献[6]依据LDoS攻击周期性脉冲突发特点，设计实现了一种基于小波特征提取的LDoS攻击检测系统，将分组数目作为检测对象，利用小波变换和神经网络的泛化能力提取多个特征并形成分类器，进行综合诊断。这类基于信号处理的方法检测率高，但是有一些缺陷。首先，信号处理技术一般是粗粒度的检测，只能在一段时间后抽样检测LDoS攻击，不能区分每个脉冲；其次，这些方法只能分析未到的或发生过的流量，目前，已有学者研究出可以通过隐藏已知的流量特征来躲避已有的检测方法的攻击模型；第三，这类方法虽然根据流量进行特征检测，但仍然不能区分正常与攻击流量，只能根据特征判断异常与正常的状态，并且信号处理的方法要求数据采样速率与分组传输速率相匹配，才能得到良好的检测效果，这使该技术在高速率低延时的网络环境下难以保证实时性。信号处理技术并不能检测所有的LDoS攻击模型，文献[7]提出了一种基于随机游走算法建模的LDoS攻击，该攻击可以很好地绕过频域检测阶段。因此基于信号处理技术的检测算法对于真实环境下检测及过滤LDoS攻击不够完善，要实现硬件检测LDoS攻击，需要在攻击进入路由器阶段进行检测。文献[8]研究了基于缓存区队列平均长度（ASPQ, average size of packet queue）的LDoS攻击检测方法，利用平均队列分组长度分析攻击分组在队列的占有比例和攻击大小与攻击效果的关系提出了*ASPQ*值，并以此为依据在路由器端检测出LDoS攻击。文献[9~13]都提出了基于AQM机制的LDoS攻击防御方法，其核心思想都是通过改进AQM算法过滤LDoS攻击分组或对带宽进行重新分配来保护TCP资源。基于路由器特征的检测和防御方法一般具有计算量小、实时性好、容易实现的优点。

在路由器方面，使用最多的主动队列管理（AQM, active queue management）算法有随机早期检测（RED, random early detection）、自适应随机早期检测（ARED, adaptive random early detection）、平稳随机早期检测（SRED, stabilized random early detection）和BLUE算法[3]。虽然这些算法能有效控制路由器丢失分组，但是大多数没有网络攻击的顽健性。文献[14~16]指出，RED算法将路由器平均队列长度作为决定启动拥塞控制机制的随机函数的参数，增加了在队列长度变得太大之前平滑瞬时拥塞的可能性，减少了多个流同时受分组丢弃影响的可能性，是目前最普遍的路由器主动队列管理算法。同时，RED及其衍生算法对于LDoS攻击非常脆弱[12]。本文基于RED队列算法提出了一种队列特征，即利用平均队列和瞬时队列来表征LDoS攻击和正常状态，并以此为依据检测LDoS攻击。研究发现，应用于非线性的KPCA算法可较好地处理瞬时和平均队列，并从中提取出特征向量，再利用神经网络实现高性能的检测（KPCA网络）。文献[17]运用KPCA-SVM方法来检测网络攻击，其中，检测率达到97.2%，但是其无法检测隐藏在流量中的低速率攻击。文献[18]提出使用自适应的KPCA方法检测LDoS攻击的流量，检测率达到99%[18]，说明KPCA算法在检测LDoS攻击时有很高的检测率，但是其是针对流量特征的自适应算法，不适用

于队列特征。文献[19]提出基于拥塞参与度的LDDoS攻击检测及过滤方法，并通过数据证明在路由器方面计算拥塞参与度可以高效地检测及过滤LDDoS攻击。同理，利用路由器队列检测 LDoS 攻击也应该达到较好的效果。因此，本文利用 KPCA 算法提取队列特征，采用人工神经网络进行检测，这种方法既利用了KPCA对复杂特征优化处理的能力，又能结合 ANN 的准确性与实时性对攻击进行检测，提高了算法的处理能力与效率。

3　基于 ANN 与 KPCA 的攻击检测方法

在开展LDoS攻击对RED队列造成影响的研究中发现，瞬时队列在 LDoS 攻击期间波动很大，并且其平均队列也会剧烈变化，特别是以瞬时队列作为测量尺度表示平均队列时，这种变化更为明显。这种在LDoS攻击期间RED队列的变化是检测LDoS攻击的基础。因此，通过抽样提取队列变化特征，利用KPCA算法对队列特征降维，采用实时性较强的机器学习算法进行检测。检测方法如图 1 所示。

在图 1 中，首先，对 LDoS 攻击进行建模，利用 LDoS 攻击工具产生攻击流量，攻击正常网络；然后，对瞬时队列与平均队列分别进行采样，将样本作为 KPCA 的输入数据进行特征分析，输出特征向量作为 BP 神经网络的训练数据与测试数据，形成分类器；最后，实时检测 LDoS 攻击，并对检测性能进行评估。

3.1　LDoS 攻击下的路由器队列特征

RED 算法对 LDoS 攻击的防范能力非常脆弱，在采用 RED 算法的路由器遭受 LDoS 攻击时，其瞬时路由器队列会在攻击期间表现出巨大的波动，平均队列随着瞬时队列的波动产生衍生变化[8]。因此，本文基于 RED 队列进行实验并采集所需特征。RED 算法的思想是根据平均队列长度来进行拥塞控制避免拥塞，平均队列的计算方法为指数加权（EWMA，exponentially weighted moving average）[20]，即

$$Q(n)=(1-W)Q(n-1)+Wq(n) \tag{1}$$

其中，$Q(n)$为平均队列大小；q 为瞬时队列大小；W 为权值。正常情况下，RED 监视平均队列的长度，当拥塞发生时随机丢失分组。

在实际情况中，RED 只有当新的数据分组到达时才会重新计算平均队列。当拥塞发生时如果平均队列长度很大，由于拥塞控制没有新的数据分组到达，此时，瞬时队列是空的[21]。拥塞发生后，当新的数据分组到达时，如果仍然按照式(1)计算平均队列大小，则平均队列的下降率是缓慢的，将导致短期的分组高丢失率。因此，式(1)就不再适合这种情况。理想条件下，当数据分组进入队列时，瞬时队列是空的。当数据分组已到达队列大小为 0 的路由器时，RED 通过式(2)计算平均队列大小，即

$$\begin{cases} m=\dfrac{t-q\_e}{t_a} \\ Q(n)=(1-W)^m Q(n-1) \end{cases} \tag{2}$$

其中，t 为当前统计时间；q_e 为队列空闲的开始时间；t_a 为小分组特定的传输时间。由于瞬时队列是空的，式(2)使平均队列剧烈下降。

LDoS 攻击的目的是使队列拥塞，迫使 TCP 降低拥塞窗口，事实上，LDoS 攻击可以看作反馈控制的过程，如图 2 所示。

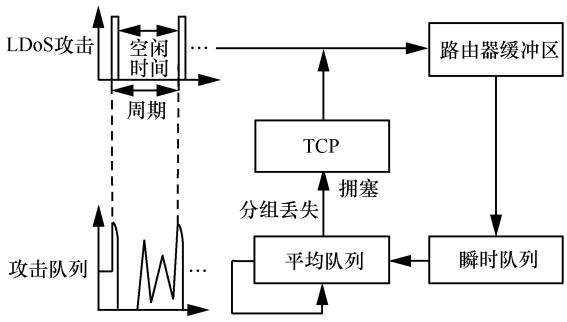


图 2　反馈控制机制

在图 2 中，高速率的 LDoS 脉冲流攻击路由器，使其平均队列长度迅速增加，造成大量合法 TCP 丢

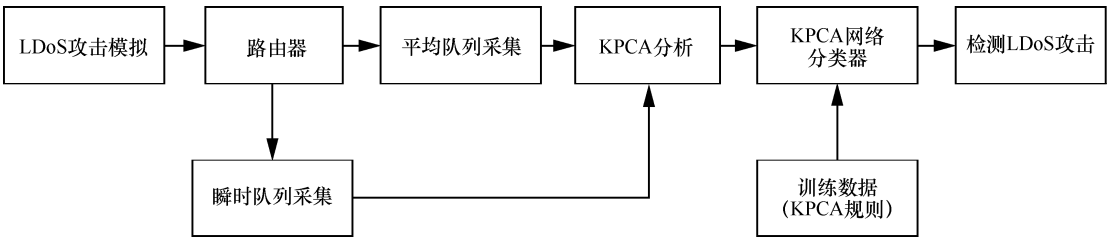


图 1　ANN 与 KPCA 结合的 LDoS 攻击检测方法

失分组。因此，RED 算法通过反馈机制向合法的 TCP 发送者传递拥塞信号。TCP 发送者随即减小拥塞窗口（CWNDS, congestion windows）降低发送速率，甚至在 2 个攻击脉冲之间的空闲时间进入超时重传状态[16]。在这种情况下，路由器的瞬时队列的大小迅速降低甚至变为空，导致路由器的平均队列减少[21]。因此，RED 机制逐渐降低分组丢失率，同时，TCP 端超时重发数据分组状态逐渐恢复。TCP 发送端的拥塞窗口会经历慢启动和加性增加乘性减少（AIMD, additive increase multiplicative decrease）的过程导致路由器队列的增加[20]。一旦路由器缓冲区被塞满，下一个攻击脉冲将会导致出现如上所述的拥塞过程。而网络中随机突发的流量变化由于其时间参数与 LDoS 攻击参数不同，不会对队列产生上述影响。

在 LDoS 攻击期间，平均和瞬时队列长度表现出异常特征，瞬时队列的波动导致平均队列的剧烈波动。因此，提取平均队列与瞬时队列相结合的特征作为样本进行 LDoS 攻击的检测，同时提出了一种降维处理与神经网络相结合的方式，即 KPCA 聚类方法与神经网络相结合（KPCA 网络），可以更好地检测非线性数据，对于队列特征的检测率较高。

3.2 基于队列特征的 KPCA 分析

PCA 主要是利用较少的综合指标代替原来较多的指标，即将给定的数据矩阵 $\boldsymbol{x}_{m\times n}$ 由归于中心的样本 $\{\boldsymbol{e}_i\}$ 构成。其中，$\boldsymbol{e}_i \in R$，PCA 通过式(3)将输入数据矢量 $\boldsymbol{e}_i$ 转换为新的矢量，即

$$\boldsymbol{s}_i = \boldsymbol{U}^{\mathrm{T}}\boldsymbol{e}_i \tag{3}$$

其中，$\boldsymbol{U}$ 为正交阵，其第 i 列 $\boldsymbol{U}_i$ 是协方差矩阵 $\boldsymbol{C}$ 的第 i 个特征矢量，进行如式(4)所示的变换。

$$\boldsymbol{C}=\frac{1}{n}\sum_{i=1}^{n}\boldsymbol{e}_i\boldsymbol{e}_i^{\mathrm{T}},\ \boldsymbol{L}_i\boldsymbol{u}_i=\boldsymbol{C}\boldsymbol{u}_i,\ i=1,\cdots,n \tag{4}$$

其中，$\boldsymbol{L}_i$ 是 $\boldsymbol{C}$ 的一个特征值，$\boldsymbol{u}_i$ 是相应的特征矢量。当仅利用前面的 p 个特征矢量 $\boldsymbol{U}$，得到正交矩阵 $\boldsymbol{S}=\boldsymbol{U}^{\mathrm{T}}\boldsymbol{X}$。新的分量 $\boldsymbol{S}$ 称为主分量。当只使用前面的几个特征矢量时，$\boldsymbol{S}$ 中主分量的个数将减少，因此，PCA 处理高阶问题的效果不明显。PCA 为线性映射方法，该方法的局限性比较大，它忽视了数据之间高于 2 阶的相互关系，对于非线性及多维的数据无法完成较优的分类[22]。基于队列特征的异常检测本身表现出较强的非线性，线性特征提取方法得不到好的分类效果[17]，而且分析所用的数据由平均队列与瞬时队列联合表示，属于非线性的二维空间数据。因此，引入核主成分分析法，把输入空间映射到高维空间进行数据处理[22]，此方法能较好地提取非线性特征。设平均队列为 x_i，瞬时队列为 y_i，数据空间到特征空间的映射函数为 φ，则内积变换为

$$(x_i, y_i) \to K(x_i, y_i) = \varphi(x_i)\varphi(y_i) \tag{5}$$

式(5)中增加了非线性映射，因此强化了非线性处理能力，这是传统 PCA 方法无法达到的，核方法完成了瞬时队列与平均队列多维度之间的非线性变换。

选用对非线性空间有较高处理效果的高斯径向基函数作为核函数。KPCA 提取特征的中心思想是利用核函数将输入空间映射到特征空间，在特征空间完成 PCA[17]。

基于以上分析，把平均队列与瞬时队列看成一个联合样本，并根据此样本得到对应的 KPCA 队列特征，实现 KPCA 算法步骤如下。

1) 确定输入数据。输入数据由瞬时队列 y_i 和平均队列 x_i 组成，所以将输入定义为 $n\times 2$ 维矩阵，即

$$\boldsymbol{A}=\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \\ \vdots & \vdots \\ x_n & y_n \end{bmatrix} \tag{6}$$

2) 生成核矩阵。通过高斯径向函数计算核矩阵 $\boldsymbol{K}$。

3) 将瞬时队列 y_i 与平均队列 x_i 转化为确定的特征向量得到 $\{\boldsymbol{v}_1,\cdots,\boldsymbol{v}_n\}$。

4) 对得到的特征向量按特征值的降序排列得到 $\{\boldsymbol{v}_1',\cdots,\boldsymbol{v}_n'\}$。

5) 得到正交向量。利用施密特正交化得到正交向量 $\{\boldsymbol{a}_1,\cdots,\boldsymbol{a}_n\}$。

6) 提取主分量。如果累积贡献率 $B_t \geqslant$ 提取效率 p，则提取 t 个主分量 $\boldsymbol{a}_1,\cdots,\boldsymbol{a}_t$。

7) 计算特征向量的投影。核矩阵 $\boldsymbol{K}$ 在提取出的特征向量上的投影为 $\boldsymbol{Y}=\boldsymbol{K}\boldsymbol{a}$，其中，$\boldsymbol{a}=\{\boldsymbol{a}_1,\cdots,\boldsymbol{a}_t\}$。

投影矩阵 $\boldsymbol{Y}$ 即平均队列与瞬时队列经过 KPCA 处理后得到的新特征序列。由于所得数据在各个类别有明显特征，为了可以同时区分出多个特征，因此，选用有强分辨力的神经网络分类器来判别这一特征。

3.3 基于 KPCA 特征的 BP 神经网络检测方法

BP 神经网络是一种按误差逆传播的多层前馈神经网络，它是一个非线性模型，由输入层、隐含

层和输出层组成，其中隐含层可以有多层[23]。由于 BP 神经网络的非线性映射特性及良好的自学习能力，其作为综合分类器已在多个领域广泛使用。KPCA 特征根据网络的状态（正常、突发和遭受 LDoS 攻击）分为 3 种：正常状态即客户端在无攻击也无其他用户干扰的情况下正常的下载状态；突发状态为客户端在下载时随机加入其他非攻击参数配置的情况；遭受 LDoS 攻击为在客户端下载时由攻击者发送 LDoS 攻击数据分组进行攻击。

由 3.1 节分析可知，在正常的网络状态下，如果出现与 LDoS 攻击参数不匹配的 TCP 突发，则不会对检测结果造成影响。因此，将 BP 神经网络分为 2 种：未遭受 LDoS 攻击和遭受到 LDoS 攻击。分别采集正常网络与遭受 LDoS 攻击的队列数据，再将经 KPCA 分析后的特征作为训练集对分类器进行训练，最后实时采集正常状态、随机突发状态以及遭受 LDoS 攻击状态进行检测。以正常状态为例，神经网络分类器结构如图 3 所示。

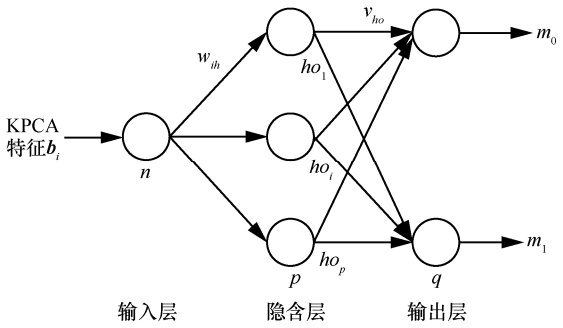


图 3　3 层 BP 神经网络结构

在图 3 中，输入层、隐含层和输出层神经元个数分别为 n、p、q。由于所提 KPCA 特征为线性一维特征，因此，设此神经网络训练集的输入向量 $\boldsymbol{b}_i=(b_1,b_2,\cdots,b_n)$，即 KPCA 算法得出的特征，隐含层输入变量 $\boldsymbol{h}_i=(h_{i1},h_{i2},\cdots,h_{ip})$，隐含层输出变量 $\boldsymbol{h}_o=(ho_1,ho_2,\cdots,ho_p)$，输入层与隐含层的连接权值为 w_{ih}，隐含层与输出层的连接权值为 v_{ho}，隐含层各神经元阈值为 r_h，输出层各神经元阈值为 s_o，使用 logsig 作为传输函数[23]。将 n 个训练样本全部训练完毕后，计算全局误差。当全局误差达到训练目标或最大训练次数时，结束学习算法，BP 神经网络训练完毕。对于训练良好的 BP 神经网络，拥有较为优秀的泛化能力，当向网络输入的样本数据为测试数据时，依然能给出合适的输出[24]，这为使用 BP 神经网络作为判别 LDoS 攻击的分类器提供了可行性。根据文献[6]中对神经网络决策指标的定义，设置本系统的最终决策指标为

$$m=\sqrt{\frac{m_1^2+(1-m_0)^2}{2}} \tag{7}$$

其中，输出层输出变量为 m_0 与 m_1，输出节点趋近 0、1 时，表示正常；趋近 1、0 时，表示有 LDoS 攻击发生。具体实验步骤如图 4 所示。

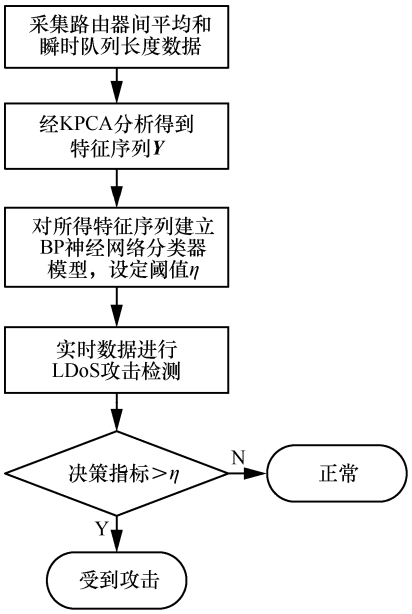


图 4　ANN 与 KPCA 结合的 LDoS 攻击检测总体流程

在图 4 中，首先采集到路由器之间的队列信息，再将采集到的队列利用 KPCA 算法进行特征提取，特征向量作为神经网络的训练组，形成分类器。将需要检测的数据作为输入组，完成神经网络的训练后，由决策指标 m 作为 LDoS 攻击的判决依据。在未受 LDoS 攻击的 m 和受 LDoS 攻击的 m 之间选定阈值，如果 m 大于阈值就说明网络环境遭受到 LDoS 攻击。

4　实验结果及分析

为了验证本文方法对 LDoS 攻击的检测效果，在网络平台中采用真实的网络设备搭建了测试平台——test-bed 实验平台，其拓扑结构如图 5 所示。

该 test-bed 实验平台是根据美国莱斯大学在 Network Simulator version 2（NS-2）仿真平台中搭建的实验环境[1]设计的。其中，包含交换机及路由器各一台，客户端（client）主机 5 台，LDoS 攻击者（attacker）主机一台以及 FTP 服务器（FTP server）一台。

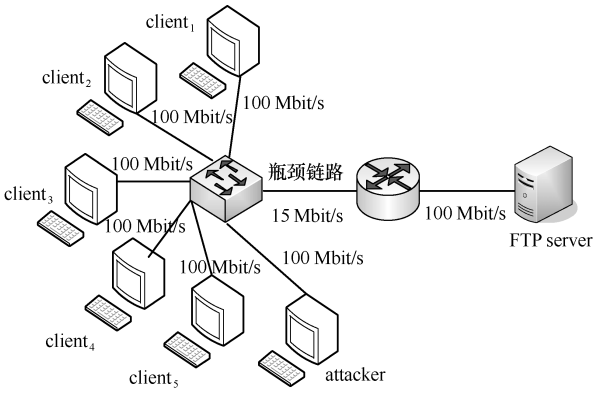


图 5 实验环境

client$_1$~client$_5$ 的 IP 地址分别为 10.1.20.1~10.1.20.5，攻击者的 IP 地址为 10.1.30.1，服务器的 IP 地址为 10.1.10.1。RTO 设置为 1 s，连接的单向传播时延在 50~70 ms 随机生成，所以平均往返时间（RTT）设置为 120 ms。数据分组的平均大小是 1 000 B，瓶颈链路的缓冲区大小由 $C\times\overline{RTT}$ 确定，C 为链路容量，$\overline{RTT}$ 为平均 RTT。RED 队列的最大和最小阈值分别为 50 和 150，权值为 0.000 1。

实验中，主机均采用 Redhat 9.0 操作系统，利用 ShrewAttack 攻击软件发送 LDoS 攻击分组，使用 RED 队列管理机制，攻击者（attacker）运用 CBR 机制发送攻击分组。受害端为 FTP 服务器，瓶颈链路为 15 Mbit/s，其他链路为 100 Mbit/s。

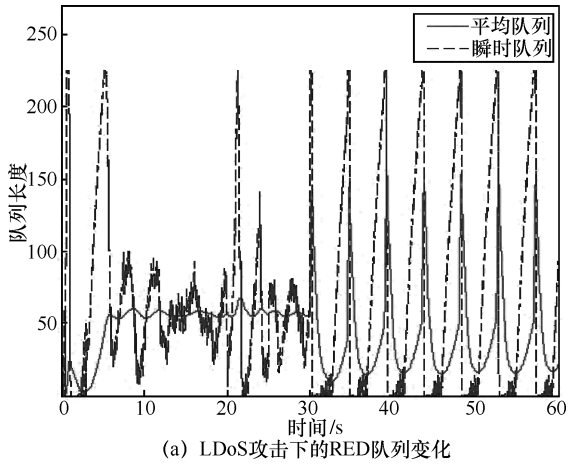
由于网络应用层协议是基于 TCP/IP 协议的，同时，普遍的 TCP 版本是基于 RED 队列管理算法的，因此，不同的协议不会对实验产生影响，但为保证实验的普适性，加入了林肯实验室的 DARPA 数据集中 2000 年某一周美国政府网站的正常数据作为背景流量。

首先，利用 iproute 和 tcpdump 采集路由器信息，提取出平均与瞬时队列信息。对平均队列与瞬时队列进行 KPCA 算法的处理，将分析后的结果作为神经网络分类器的输入进行 LDoS 攻击的检测，并对检测性能进行分析。本文实验的攻击工具 ShrewAttack 和真实网络拓扑环境是研究 LDoS 公认的实验平台，因此，所采集到的队列特征不会对训练数据造成较大影响，同时也不会影响分类器的泛化能力。

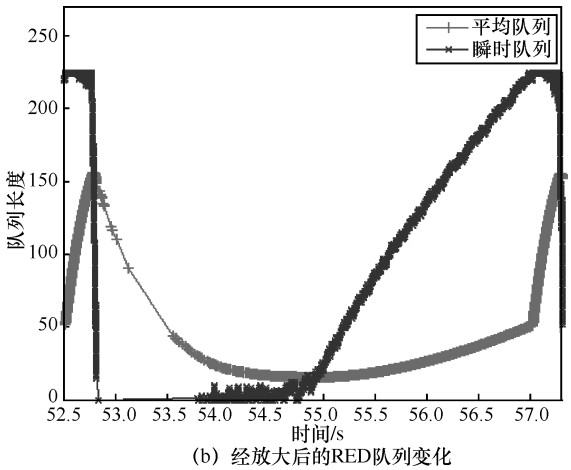
4.1 LDoS 攻击特征提取

在 test-bed 平台中测试时，攻击开始于第 30 s，设置攻击周期为 4.5 s，脉冲长度为 0.3 s。

对图 5 中路由器的队列进行采样，同时采集平均队列与瞬时队列的数据，采样时间长度为 60 s。实验证明，当攻击速率为瓶颈链路大小时攻击效果最明显[1,2]，因此攻击速率为 15 Mbit/s，并且随机在 20~30 s 启动突发（这种突发并没有配置 LDoS 攻击参数）。根据 3.1 节的分析可知，平均队列需要上一个瞬时队列与平均队列的联合计算生成，当路由器队列中无分组到达时，平均队列不会更新，在采样长度内会出现平均队列少于瞬时队列的情况，为了使平均队列和瞬时队列在时间和状态上相互对应，设定平均队列和瞬时队列的采样间隔均为 10 ms。图 6 为 LDoS 攻击对 RED 队列随时间变化的影响，该队列的基本特征如图 6(a)所示，图 6(b)是在 LDoS 起作用时进行局部放大的效果。



(a) LDoS攻击下的RED队列变化



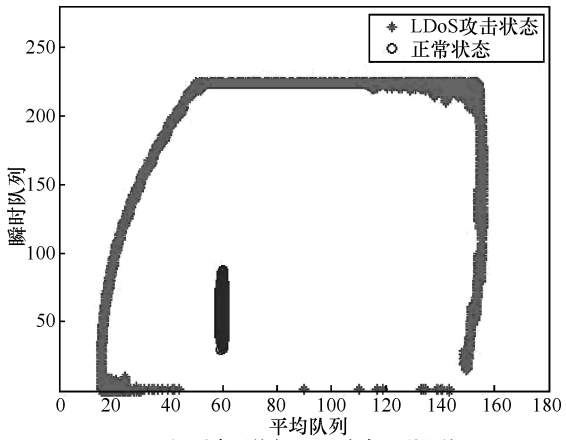
(b) 经放大后的RED队列变化

图 6 LDoS 攻击对 RED 队列的影响

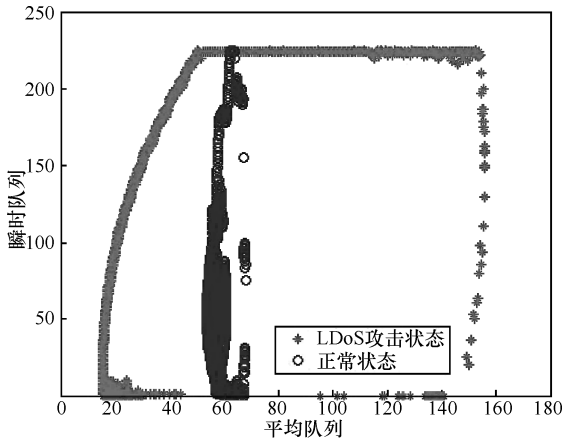
在图 6(a)中，一段时间后队列趋于平稳，然而在 t=30 s 时，队列波动剧烈。在图 6(b)中，放大来看，攻击脉冲在 t=52.5 s 和 t=57 s 造成瞬时队列剧烈波动，同时存在一段未记录平均队列的中断时间（接近最小 RTO），此时，平均队列将保存最后一个值。在中断时间后，平均队列快速降到最小值之下。图 6(a)也显

示在正常流量的随机突发不会呈现分布的特征，因为它的实现没有攻击参数配置。因此，突发不影响检测率，除非它恰巧与 LDoS 攻击具有相同的参数配置。当横坐标为平均队列长度，纵坐标为瞬时队列长度时，攻击状态与正常状态之间的关系显示得比较明显，其平均队列随瞬时队列的变化如图 7 所示。

图 7(a)中，横坐标为平均队列，纵坐标为瞬时队列。将攻击数据与正常数据进行比较，横坐标为 57~60，纵坐标为 20~100 时的区域代表正常网络区域分布，其他的点是存在攻击时的特征。



(a) 正常网络与LDoS攻击队列比较



(b) 有突发正常网络与LDoS攻击队列比较

图 7　平均队列与瞬时队列的联合特征

图 7(a)中正常流量队列存在于某一区域内，平均队列随瞬时队列的变化平稳，而存在攻击的队列波动很大。图 7(b)包含正常突发，通过分析，平均队列没有很大的变化，其与图 7(a)正常队列在同一区域内，可以认为突发不会被错认为攻击脉冲。而通过 KPCA 分析，可以将这种二维的特征转换为抽样点数与特征值表示的一维特征，从而直观地表现出二者之间的关系。

4.2　KPCA 特征分析

对 LDoS 攻击的队列、正常平稳的队列和正常的但是有突发的队列进行采集，分别提取出实验所需的数据特征，对于趋势明显的队列特征，以 3 为周期进行抽样，再将特征向量利用 KPCA 算法选用高斯径向函数对其降维和聚类，得出特征曲线，如图 8 所示。其中，每一点是由瞬时队列与平均队列联合分析出的特征向量。

图 8(a)与图 8(b)均为正常网络状态，它们之间的区别在于图 8(a)无突发，而图 8(b)存在突发。二者在开始处有些差异，但由于算法的自适应性，在随后的各点表现出相似的特征。

图 8(c)表示存在 LDoS 攻击，与正常队列趋势差距很大。由图 8(d)可以看出，正常平稳队列与有突发队列曲线趋势基本一致，但是由于时延等原因，放在一起不能定量化分析。相同地，这 2 组曲线虽然与攻击曲线趋势有区别，但是也无法直接区分，因此，需要运用更准确的方法进行分类。由于正常队列与 LDoS 攻击队列的特征曲线的不一致性，符合神经网络分类器的输入特征，因此，运用 BP 神经网络进行分类处理，以完成更准确的检测。

4.3　检测结果

在采用 BP 神经网络进行分类检测中，将 KPCA 特征曲线分别作为训练和检测数据，对其进行分类和检测。将所得特征分为 3 组，分别为正常网络、正常网络加随机突发与有 LDoS 攻击网络，测试集每组 10 个样本集，训练集每组 20 个样本集，每个样本集中包含一个采样周期内所有样本（即总的样本数目为 20×6 000 =120 000 个），输入数据中无训练数据中的样本。隐藏层个数的确定通过隐含层个数与最小均方误差的关系确定，如图 9 所示。

考虑到 BP 神经网络的复杂度及其学习规则，并不是隐含层节点数越多，算法性能越好。图 9 中，当隐藏节点个数在 20 时，均方误差达到最低点即 0.03 左右，且处理当前数据量的任务时算法时间在 1 s 左右，与路由器平均队列的统计时间基本相同，因此，选用隐含层节点数为 20。

迭代次数和决策指标阈值 η 为影响神经网络性能的关键因素。在测试中，当学习率为 0.01，学习目标取 0.05 时，考虑到分类器迭代时间过长及过拟合问题，设置迭代次数为 500、1 000、1 500、2 000，分别运行 500 次，得到反映分类器性能的 ROC 曲线，如图 10 所示。

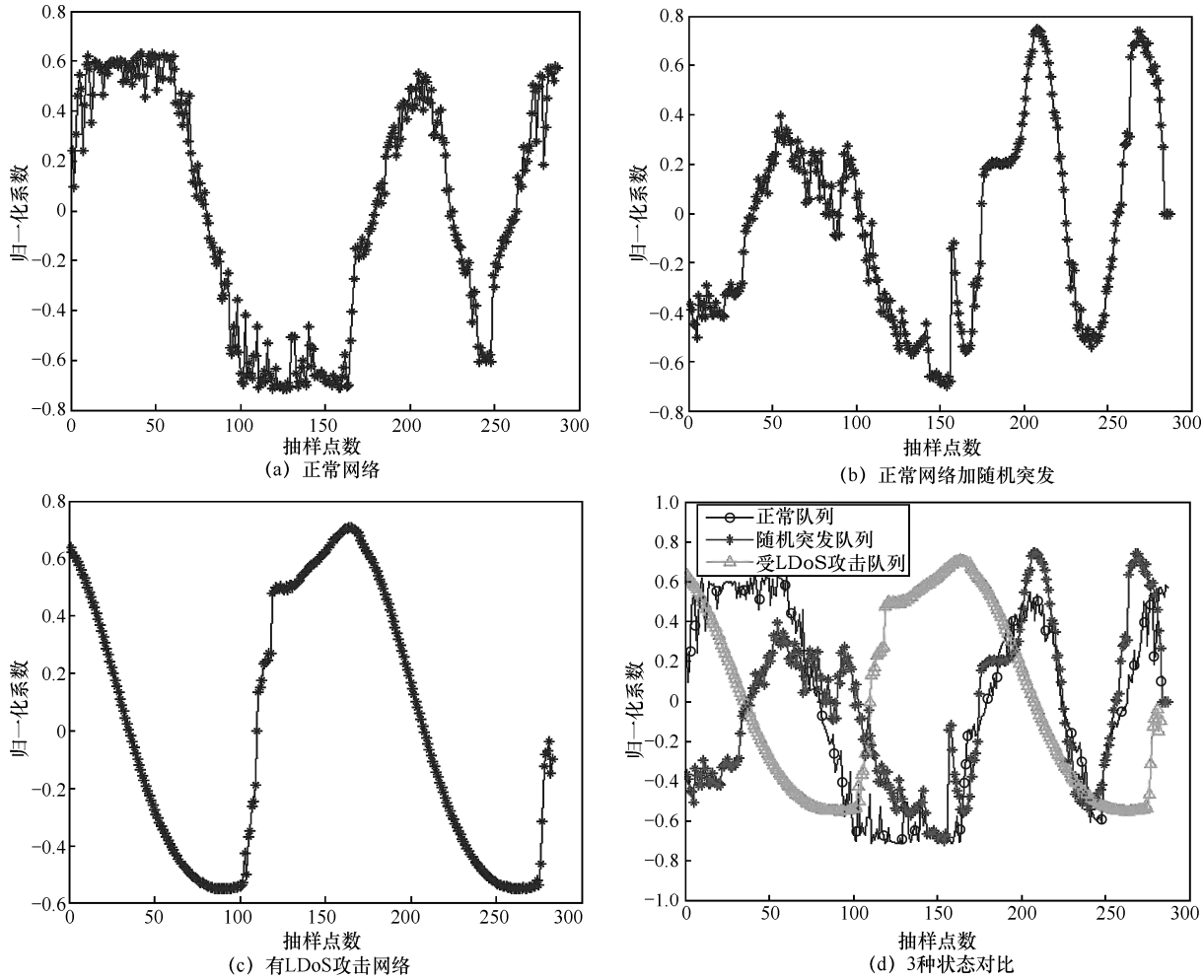


图 8 KPCA 特征

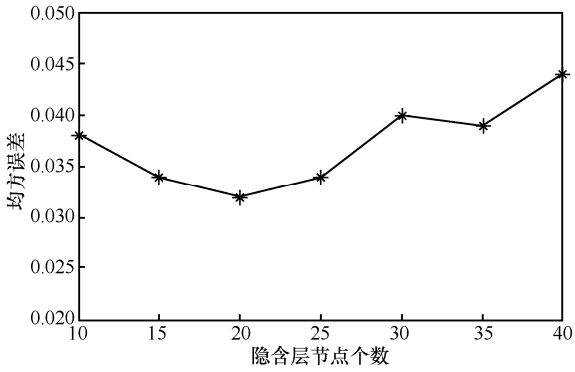


图 9 神经网络节点数与最小均方误差比较

在图 10 中，除 2 000 次迭代外，其他迭代次数的分类器性能都不高。这是由于迭代次数少的分类器对于所选特征很难达到最终训练目标，而迭代次数为 2 000 的曲线更靠近左上角点，同时包含面积最大，明显好于其他迭代次数的分类器，测试结果的达成率达到 95%以上，运行时间与最短时间相差不超过 2 s，虽然运行时间略有延长，但是与其他迭代次数相比较是可以接受的，且对于采样周期 60 s 来说，是可以容忍的误差。

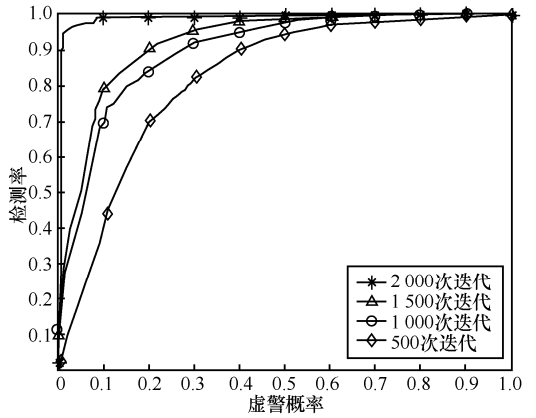


图 10 不同迭代次数分类器性能对比

根据文献[6]，一般神经网络决策指标的阈值在 0.5 左右。从图 10 的实验数据可以得出：神经网络决策指标的阈值低于 0.45 时，误警率较高；高于

0.65 时，检测率较低，都会在很大程度上影响检测性能。因此，根据实验结果，当阈值取 $\eta \in (0.45,0.65)$ 时，可以获得较好的检测效果。提取 2 000 次迭代次数 ROC 曲线中阈值 $\eta \in (0.45,0.65)$ 内的检测率和虚警概率，结果如表 1 所示。

表 1　不同决策指标阈值 η 下工作性能

阈值 η	检测率	虚警概率
0.45	97.21%	8.22%
0.47	96.52%	7.36%
0.49	96.24%	5.71%
0.51	95.62%	3.70%
0.53	95.21%	1.33%
0.55	94.54%	1.15%
0.57	93.25%	1.13%
0.59	92.12%	1.10%
0.61	90.35%	0.91%
0.63	88.21%	0.87%
0.65	85.42%	0.82%

在表 1 中，不同 η 对应的检测性能差别较大，当阈值 η 为 0.53 时，最靠近 ROC 曲线的左上角(0,1)点，且有最合适的检测率和虚警概率，因此，选择此点为最终的决策指标阈值 η，通过以上参数的设置，训练完成最终的 LDoS 攻击分类器。

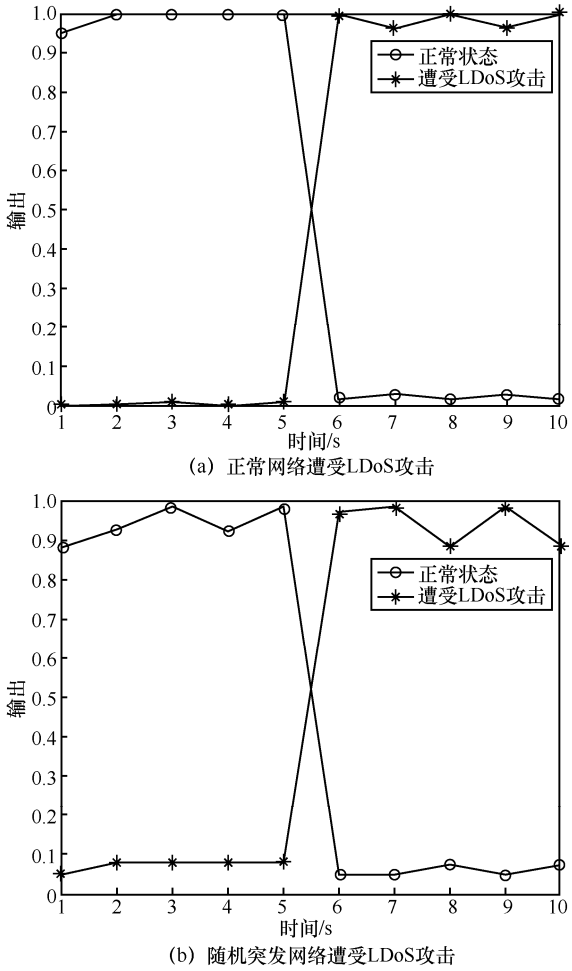
形成分类器后，在真实网络下实时采集队列信息，转换为 KPCA 特征后作为输入送入分类器中进行检测，各分类器输入数据如下。

1) 无突发队列数据和有 LDoS 攻击数据。

2) 有突发队列数据和有 LDoS 攻击数据。

对于每一种方案，都存在正常与存在 LDoS 攻击的数据，且根据理论分析，有突发的正常流不会对 LDoS 攻击的检测造成影响。

根据神经网络的原理，如果输出接近于(1,0)则认为是正常网络，如果输出接近于(0,1)则认为是 LDoS 攻击。本文实验结果如图 11 所示，检测窗口为 1 s，图 11(a)中前 5 s 为正常网络，从第 5 s 开始有 LDoS 攻击，可见此时开始检测到攻击；图 11(b)与图 11(a)相同，说明网络正常突发不会影响 LDoS 攻击的检测，而且期望输出可以达到较理想的分类检测效果。由于 2 种情况都是当 LDoS 攻击出现在第一个检测窗口（5~6 s）时就会立即被检测，因此，也证明了所选神经网络的实时性。实验证明，ANN 与 KPCA 结合的 LDoS 攻击检测的平均检测率为 94.7%，漏警概率为 5.3%，虚警概率为 1.7%。



(a) 正常网络遭受LDoS攻击

(b) 随机突发网络遭受LDoS攻击

图 11　神经网络输出结果

4.4　比较分析

KPCA 网络算法属于不同机器学习算法的结合，利于处理大规模复杂数据及挖掘潜在特征，在评价其算法性能时，需要考虑算法的复杂度与检测性能。本文将实验数据分别用于归一化互功率谱密度[5]（NCPSD, normalized cross-power spectral density）、隐马尔可夫模型[4]（HMM, hidden Markov model）以及 Adaptive-KPCA[18]检测 LDoS 攻击的方法中，从算法时间复杂度 $T(n)$、空间复杂度 $S(n)$以及检测率等指标定量分析，并根据结果做出综合评价。通常，$T(n)$值越低，$S(n)$值越低，则检测率越高，综合评价就越高。

1) 时间复杂度评估

信号处理算法的时间复杂度一般为 $O(n^2)$，因此，NCPSD 与 HMM 时间复杂度均为 $O(n^2)$[25]。

KPCA 算法是一种聚类算法，计算量较大，时间复杂度为 $O(n^3)$[26]，Adaptive-KPCA[18]同样符合该规则。

KPCA 网络将数据降维，利用新的特征作为神经网络的输出，所以应考虑 2 个方面的时间复杂度问题。一般地，KPCA 算法复杂度较高，但本文方案根据路由器队列的连续性和平稳性，在 KPCA 分析之前进行预处理，按特征规律进行抽样，将其分解成一个 $\frac{n}{r}\times\frac{n}{r}$ 的矩阵，大大降低了算法复杂度，其计算复杂度为 $T_1(n)=O\left(\left(\frac{n}{r}\right)^3\right)$[26]。对于前馈神经网络，算法复杂度分为测试部分与训练部分，训练部分 $T_2(n)=O(m\times n_2)$；测试部分为 $T_3(n)=O(n_1+n_2+n_3)=O(n_2)$。其中，$n_1$ 与 n_3 为输入与输出节点数；n_2 为隐含层节点数；m 为输入数据量。一般 n_2 远大于输入与输出节点数总和，而且经测试，KPCA 网络的时延主要来自预处理及 KPCA 变化方面，神经网络的检测时延很少，所以总时间复杂度为 $T_0=T_1+T_2+T_3$。经实验验证，当输入数据为 n 时，各个算法的平均时间频度及时间复杂度如表 2 所示。

表 2 算法时间复杂度

算法	时间复杂度	时间频度/s
NCPSD	$O(n^2)$	24.1
HMM	$O(n^2)$	20.6
Adaptive-KPCA	$O(n^3)$	32.5
KPCA 网络	$T_0(n)$	5.1

2) 空间复杂度评估

当输入数据量为 n 时，KPCA 网络经抽样与降维，可将总数据量降到 $\frac{n}{6}$。其他算法由于没有预处理能力，输入数据量仍为 n。KPCA 网络较大幅度地降低了固定存储空间开销。

由于各算法循环次数和排序方式不同，执行过程各变量所占辅助空间也不同，对于数字信号处理算法，如 NCPSD 与 HMM 算法的空间复杂度为 $O(n)$[25]，KPCA 算法在特征空间中是线性相关的，其空间复杂度也为 $O(n)$[26]，各算法的空间复杂度如表 3 所示。

3) 检测性能分析

从检测率、漏警概率和虚警概率这 3 个方面分析 4 种算法的检测性能。检测 LDoS 攻击时，各算法性能如表 4 所示。

表 3 算法空间复杂度

算法	输入数据量	空间复杂度
NCPSD	n	$O(n)$
HMM	n	$O(n)$
Adaptive-KPCA	n	$O(n)$
KPCA 网络	$\frac{n}{6}$	$O(n)$

表 4 不同检测算法性能比较

算法	检测率	漏警概率	虚警概率
NCPSD	88.0%	12.0%	16.7%
HMM	99.9%	0.04%	1.11%
Adaptive-KPCA	99.2%	0.8%	2.0%
KPCA 网络（正常）	95.2%	4.8%	1.3%
KPCA 网络（突发）	94.2%	5.8%	2.0%

表 2 表示各算法的时间复杂度，表 3 为空间复杂度，表 4 代表各算法对 LDoS 攻击的检测性能。从表 2~表 4 可以看出，KPCA 网络由于其良好的预处理能力，在时间频度上更有优势。空间上，基于流量特征的检测算法的采样率需要与分组速率保持一致，数据量远大于路由器队列算法，所以本文算法处理数据能力高于其他算法。

在检测性能和实时性方面，KPCA 网络所耗费的时间都来自于 KPCA 处理，在神经网络检测方面耗时很少；在检测性能方面，KPCA 网络明显好于 NCPSD，虚警概率优于 Adaptive-KPCA，在实时性方面好于 HMM，能满足检测 LDoS 攻击的要求；且 KPCA 网络检测的特征为路由器队列，队列比网络流量要复杂得多，更难提取，考虑到已经存在的能躲避频域检测的 LDoS 攻击模型，队列特征在检测 LDoS 攻击方面更有意义。因此，KPCA 网络检测 LDoS 攻击的综合性能更好，且为实时防御 LDoS 攻击提供了一种新思路。

5 结束语

本文在对 LDoS 攻击队列分析的基础上，提出了基于 KPCA 及神经网络的 LDoS 队列特征的检测方法，将平均及瞬时队列遭受 LDoS 攻击时的剧烈变化作为依据，经 KPCA 提取特征后，利用 BP 神经网络进行检测。实验证明，该算法不仅可以分辨正常与 LDoS 攻击状态，还可以区分出正常网络

中存在突发的情况与遭受 LDoS 的状态，相比于其他方法有算法复杂度低、实时性强等优点，能有效检测 LDoS 攻击。KPCA 网络基于队列特征的检测方法对实际的网络管理、防御 LDoS 攻击以及设计高性能路由器有一定的借鉴意义。本文算法也存在一些局限性，例如，需要训练数据进行支撑，对大数据预处理时间过长等，因此，该算法还有待进一步改进。在混合流中细粒度筛选出攻击流并进行过滤是未来需要关注的问题，也是努力的方向。本文提出的队列分布特征已经考虑了攻击脉冲的参数，提取了每一个攻击周期的特征，而不是以一个较长的时间采样提取特征。因此，已经向细粒度检测方向改进，今后将结合网络测量、IP 地址统计等方法继续提高检测技术。

参考文献：

[1] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks -the shrew vs. the mice and elephants[C]// ACM SIGCOMM. 2003: 25-29.

[2] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks and counter strategies[J]. IEEE/ACM Transactions on Networking, 2006, 14(4):683-696.

[3] 何炎祥, 刘陶, 曹强, 等.低速率拒绝服务攻击研究综述[J].计算机科学与探索, 2008, 2(1): 1-19
HE Y X, LIU T, CAO Q, et al. A survey of low-rate denial-of-service attacks[J]. Journal of Frontiers of Computer Science and Technology, 2008, 2(1): 1-19

[4] 岳猛, 张才峰, 吴志军. 隐马尔科夫模型检测 LDoS 攻击方法的研究[J]. 信号处理, 2015, 31(11):1454-1460.
YUE M, ZHANG C F, WU Z J. The research of detecting LDoS attacks based on hidden Markov model[J]. Journal of Signal Processing, 2015, 31(11):1454-1460.

[5] YU C, KAI H, KWOK Y K. Collaborative defense against periodic shrew DDoS attacks in frequency domain[J]. ACM Transactions on Information and System Security, 2005: 2-27.

[6] 何炎祥, 曹强, 刘陶, 等. 一种基于小波特征提取的低速率 DoS 检测方法[J]. 软件学报, 2009, 20(4):930-941.
HE Y X, CAO Q, LIU T, et al. A low-rate DoS detection method based on feature extraction using wavelet transform[J]. Journal of Software, 2009, 20(4):930-941.

[7] LIU X, ZHANG M, XU G. Construction of distributed LDoS attack based on one-dimensional random walk algorithm[C]//International Conference on Cloud Computing and Intelligence Systems. 2012:685-689.

[8] 张静, 胡华平, 刘波, 等. 基于 ASPQ 的 LDoS 攻击检测方法[J]. 通信学报, 2012, 33(5):79-84.
ZHANG J, HU H P, LIU B, et al. Detecting LDoS attack based on ASPQ [J]. Journal on Communications, 2012, 33(5):79-84.

[9] SUN J, ZUKERMAN M. An adaptive neuron AQM for a stable internet[M]//Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet. Springer Berlin Heidelberg, 2007:844-854.

[10] KUZMANOVIC A. The power of explicit congestion notification[J]. ACM Sigcomm Computer Communication Review, 2005, 35(4):61-72.

[11] SARAT S, TERZIS A. On the effect of router buffer sizes on low-rate denial of service attacks[C]//International Conference on Computer Communications and Networks. 2005:281-286.

[12] MOHAN L, JOHN J K, BIJESH M G. Shrew attack prevention in RED queue with partial flow analysis[J]. International Journal of Computer Applications, 2013, 67(8):9-15.

[13] 张长旺, 殷建平, 蔡志平, 等. 抗 DDoS 攻击的主动队列管理算法[J]. 软件学报, 2011, 22(9):2182-2192.
ZHANG C W, YIN J P, CAI Z P, et al. Active queue management algorithm to counter DDoS attacks[J]. Journal of Software, 2011, 22(9): 2182-2192.

[14] HAMLET M R, MICHEL K, BÉATRICE P P. TCP and network coding: equilibrium and dynamic properties[J]. IEEE/ACM Transactions on Networking, 2016, 24(4): 1935-1947.

[15] ZHAO Y, MA Z G, ZHENG X F, et al. An improved algorithm of nonlinear RED based on membership cloud theory[J]. Chinese Journal of Electronics, 2017, 26(3): 537-543.

[16] GUIRGUIS M. BESTAVROS A, MATTA I. Exploiting the transients of adaptation for RoQ attacks on Internet re-sources[C]//IEEE ICNP. 2004: 184-195.

[17] 高海华, 杨辉华, 王行愚, 等. 基于 PCA 和 KPCA 特征抽取的 SVM 网络入侵检测方法[J]. 华东理工大学学报（自然科学版）, 2006, 32(3): 321-326.
GAO H H, YANG H H, WANG X Y, et al. PCA/KPCA feature extraction approach to SVM for anomaly detection[J]. Journal of East China University of Science and Technology, 2006, 32(3):321-326.

[18] ZHANG X Y, WU Z J, CHEN J S, et al. An adaptive KPCA approach for detecting LDoS attack[J]. International Journal of Communication Systems, 2017, 30(4): 1-8.

[19] ZHANG C W, CAI Z, CHEN W, et al. Flow level detection and filtering of low-rate DDoS[J]. Computer Networks the International Journal of Computer & Telecommunications Networking, 2012, 56(15): 3417-3431.

[20] FENG W C, KANDLUR D D, SAHA D, et al. Stochastic fair blue: a queue management algorithm for enforcing fairness[C]//The 20th Joint Conference of the IEEE Computer & Communications Societies. 2001:1520-1529.

[21] MOHAN L, BIJESH M G, JOHN J K. Survey of low rate denial of

service (LDoS) attack on RED and its counter strategies[C]//IEEE International Conference on Computational Intelligence & Computing Research. 2012:1-7.

[22] 苏治, 傅晓媛. 核主成分遗传算法与 SVR 选股模型改进[J]. 统计研究, 2013, 30(5):54-62.
SU Z, FU X Y. Kernel principal component genetic algorithm and improved SVR stock selection model[J]. Statistical Research, 2013, 30(5):54-62.

[23] LI J, YU L. Using BP neural networks for the simulation of energy consumption[C]//IEEE International Conference on Systems, Man and Cybernetics. 2014:3542-3547.

[24] 刘陶, 何炎祥, 熊琦. 一种基于 Q 学习的 LDoS 攻击实时防御机制及其 CPN 实现[J].计算机研究与发展, 2011, 48(3):432-439.
LIU T, HE Y X, XIONG Q. A Q-learning based real-time mitigating mechanism against LDoS attack and its modeling and simulation with CPN[J]. Journal of Computer Research and Development, 2011, 48(3): 432-439.

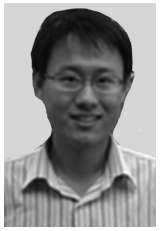
[25] WU Z J, ZHANG L Y, YUE M. Low-rate DoS attacks detection based on network multifractal[J]. IEEE Transactions on Dependable & Secure Computing, 2016, 13(5):559-567.

[26] 赵峰, 张军英. 一种 KPCA 的快速算法[J]. 控制与决策, 2007, 22(9):1044-1048.
ZHAO F, ZHANG J Y. Fast algorithm about KPCA[J]. Control and Decision, 2007, 22(9):1044-1048.

[作者简介]

吴志军（1965-），男，河南固始人，博士，中国民航大学教授、博士生导师，主要研究方向为网络空间安全。

刘亮（1991-），男，天津人，中国民航大学硕士生，主要研究方向为网络信息安全、低速率拒绝服务攻击的检测。



岳猛（1984-），男，河北沧州人，博士，中国民航大学讲师，主要研究方向为信息安全、云计算、低速率拒绝服务攻击的检测。