doi:10.11959/j.issn.1000-436x.2017075

基于联合特征的 LDoS 攻击检测方法

吴志军，张景安，岳猛，张才峰
（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）攻击是一种降质服务（RoQ, reduction of quality）攻击，具有平均速率低和隐蔽性强的特点，它是云计算平台和大数据中心面临的最大安全威胁之一。提取了 LDoS 攻击流量的 3 个内在特征，建立基于 BP 神经网络的 LDoS 攻击分类器，提出了基于联合特征的 LDoS 攻击检测方法。该方法将 LDoS 攻击的 3 个内在特征组成联合特征作为 BP 神经网络的输入，通过预先设定的决策指标，达到检测 LDoS 攻击的目的。采用 LDoS 攻击流量专用产生工具，在 NS2 仿真平台和 test-bed 网络环境中对检测算法进行了测试与验证，实验结果表明通过假设检验得出检测率为 96.68%。与现有研究成果比较说明基于联合特征的 LDoS 攻击检测性优于单个特征，并具有较高的计算效率。

关键词：低速率拒绝服务攻击；联合特征；BP 神经网络；异常检测
中图分类号：TP393.08 **文献标识码**：A

Approach of detecting low-rate DoS attack based on combined features

WU Zhi-jun, ZHANG Jing-an, YUE Meng, ZHANG Cai-feng
(College of Electronics Information and Automation, Civil Aviation University of China, Tianjin 300300, China)

Abstract: LDoS (low-rate denial of service) attack is a kind of RoQ (reduction of quality) attack which has the characteristics of low average rate and strong concealment. These characteristics pose great threats to the security of cloud computing platform and big data center. Based on network traffic analysis, three intrinsic characteristics of LDoS attack flow were extracted to be a set of input to BP neural network, which is a classifier for LDoS attack detection. Hence, an approach of detecting LDoS attacks was proposed based on novel combined feature value. The proposed approach can speedily and accurately model the LDoS attack flows by the efficient self-organizing learning process of BP neural network, in which a proper decision-making indicator is set to detect LDoS attack in accuracy at the end of output. The proposed detection approach was tested in NS2 platform and verified in test-bed network environment by using the Linux TCP-kernel source code, which is a widely accepted LDoS attack generation tool. The detection probability derived from hypothesis testing is 96.68%. Compared with available researches, analysis results show that the performance of combined features detection is better than that of single feature, and has high computational efficiency.

Key words: low-rate denial of service attack, united features, BP neural network, anomaly detection

1 引言

低速率拒绝服务（LDoS, low-rate denial of service）攻击利用网络自适应机制中存在的漏洞，使服务端无法正常为合法用户提供服务，导致 TCP 连接的质量下降[1]。LDoS 攻击不需一直维持很高的

收稿日期：2016-07-28；修回日期：2017-02-17
基金项目：国家自然科学基金资助项目（No.U1533107, No.U1433105）；中央高校基本科研业务基金资助项目（No.3122016D003）；中国民航大学研究生课程案例开发基金资助项目；天津市自然科学重点基金资助项目（No.17JCZDJC30900）
Foundation Items: The National Natural Science Foundation of China (No.U1533107, No.U1433105), Fundamental Scientific Research Foundation of the Central University (No.3122016D003), Case Development Project of Graduate Program in Civil Aviation University of China, Key Project of Tianjin Natural Science Foundation (No.17JCZDJC30900)

攻击速率，只是在攻击发起时发送高速率的短时脉冲数据流。因此，LDoS 攻击的外在表现形式为一串连续的脉冲信号，可以用一个三元组（τ，T，R）表示，其中，τ 为攻击脉冲的宽度；T 为攻击脉冲的周期（分为固定周期和变周期 2 种，又称为同步和异步）；R 为攻击脉冲的幅度（最高传输速率）[2]。LDoS 攻击信号的构成特点造就了其在突发脉冲持续时间内具有较低的平均分组发送（攻击）速率，即其平均流量很低，并且混合在巨大的正常网络流量（背景流量）中。因此，LDoS 攻击具有极强的隐蔽性，很难被常用的分布式拒绝服务（DDoS, distributed DoS）攻击检测工具发现，使受害端长期被攻击而没有察觉[3]。目前，LDoS 攻击已经成为云计算平台和大数据中心的主要安全威胁之一[4]。

由于 LDoS 攻击流量混合在正常的网络流量中，掩盖了其外在特征（周期 T、脉宽 τ 和脉冲幅度 R）。因此，很难从信号的表现形式上区分 LDoS 攻击流量和正常流量。解决的方法就是从流量的内含特性入手，挖掘 LDoS 攻击流量的内在特征，作为检测 LDoS 攻击的依据。本文通过分析 LDoS 攻击流量的特征，提取了 3 个 LDoS 攻击流量的内在特征，将其联合起来作为 BP 神经网络的输入，并通过大量数据的训练，得到用于判别 LDoS 攻击的 BP 神经网络分类器，完成 LDoS 攻击的检测。

2 相关工作

针对 LDoS 攻击的研究，利用从 Internet II 骨干网上采集到的 LDoS 攻击流量数据，首先开展了对 LDoS 攻击的研究[5]，他们的研究成果[6]被广泛采用到 LDoS 攻击的检测和防御研究中。文献[7]研究了利用小波分析检测 LDoS 攻击的方法，并提出了防御措施。文献[8]研究了低速率 DoS 攻击下基于反馈控制的互联网服务脆弱性建模。文献[9]研究低速率 DoS 攻击与进展，给出了现有研究方法的比较分析，并对今后的研究方向给出了建议。文献[10]研究了一种新的针对网络路由策略的分布式 LDoS 攻击方式。Yang 等研究了新型的面向 TCP 的低速率 DoS 攻击[11]和低速率 DDoS 攻击的数学模型[12]。文献[13]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。文献[14]研究了一种稳健的随机早期检测（RED，random early detection）算法抵御低速率 DoS 攻击。文献[15]研究了低速率 DoS 攻击对拥塞控制协议的影响，并进行了仿真和分析。文献[16]研究了基于路由器协议的低速率攻击与防御方法。文献[17]研究了基于秩相关的检测分布式反射 DoS 攻击的方法。

目前，用于分析 LDoS 攻击流量的原始采样数据有 2 种：网络流量数据和路由器间的队列数据。本文提取的 LDoS 攻击的 3 个特征源自于网络流量数据和路由器间的队列数据。下面从这 2 个方面展开分析。

在网络流量分析的基础上，针对 LDoS 攻击流量检测的研究取得了很多成果。文献[18]通过研究攻击数据流与合法数据流的网络流量，将其分别变换到频域，发现 LDoS 攻击的功率谱密度主要集中在低频频带，而合法数据流的功率谱则均匀分布在整个频带范围内。通过对功率谱密度做累加，并进行归一化后得到归一化的累计功率谱密度（NCPSD, normalized cumulative power spectrum density）。将 20 Hz 作为检测点，并将此处的归一化累计功率谱密度 NCPSD 值作为检测阈值。由假设检验得到检测值，与检测阈值比较，如果检测值高于阈值则判定网络遭到了 LDoS 攻击。Tang 等[19]提出了运用自适应的加权指数移动平均（AEWMA, adaptive exponential weighted moving average）算法来检测 LDoS 攻击。该方法采用改进的加权指数移动平均算法 EWMA 计算 TCP 流量，得到了网络环境中正常和异常流量的不同的形态分布，以此来检测 LDoS 攻击。文献[20]通过研究网络流量的多重分形特性，根据 LDoS 攻击发生时网络流量的多重分形特征，使用 Holder 指数来表示其多重分形的变化，并由 t 检验得到判决阈值，进而检测 LDoS 攻击。文献[21]通过对比分析基于峰度系数和基于移动极差序列的 2 种 LDoS 攻击检测方法，揭示了当网络流量突变时，2 种方法可以互补，由此提出了一种协同的 LDoS 攻击检测方法。

在网络遭受 LDoS 攻击时，链路带宽利用率降低，平均队列长度较大，分组丢失率较高。由于路由器队列在一定程度上反映了链路的拥塞程度，因此，基于路由器队列的 LDoS 攻击检测方法应运而生。文献[22]通过研究 LDoS 攻击对路由器队列产生的影响，在现有的队列管理算法中加入了一种数据流检测机制，称为加权窒息中断异常法（HAWK,

halting anomaly with weighted choking)。这种数据流管理机制通过检测固定时间间隔的数据流和突发性数据流的峰值速率，设定一个门限值，由此判别 LDoS 攻击的出现。张等[23]通过研究 LDoS 攻击数据分组的大小对于攻击效果的影响，得出了较小数据分组的数据分组攻击效果更好这一结论。而后进一步研究发现了路由器在攻击前后的平均队列长度的异常，提出了队列平均报文变化程度，并据此设置了检测门限。吴娜等[24]研究了基于数据流势能特征的分布式拒绝服务 DDoS 攻击隐蔽流量检测方法，采用基于支持向量机（SVM, support vector machine)的方法对网络数据流量的特征参数向量进行分类和训练，获得网络数据流量势能集，以此形成对 DDoS 攻击流量特性的描述。

上述检测方法存在的主要问题是依据 LDoS 攻击流量的单个异常特征进行攻击检测，可能导致检测性能不稳定、漏警率和虚警率较高。因此，采用多特征联合检测的方法，可以保证 LDoS 攻击检测的准确率。在采用联合特征检测攻击方面，已有研究者使用多特征的方式检测 DDoS 攻击，提出了基于多特征相似度的 DDoS 检测方法[25]。该方法选择流量、分组尺寸和协议类型的分布作为检测的多个特征，用于判别 DDoS 攻击。虽然 LDoS 与 DDoS 攻击在流量的表现形式和内涵特性方面差别很大，但是基于多特征联合的检测方法对于检测 LDoS 攻击的研究具有一定的借鉴意义。

3　网络流量分析及 LDoS 攻击流量特征提取

针对 LDoS 攻击利用 TCP 超时重传机制漏洞，以固定的周期发送高速率的短脉冲攻击流的情况，本文从网络流量的角度研究 TCP 发送方不断进入超时重传的状态，对 LDoS 攻击造成链路虚假拥塞的性能进行分析，提取 LDoS 攻击流量内在的特征，用于联合特征的检测。

3.1　网络流量分析

由于 LDoS 攻击采用 UDP 协议，并且网络流量中 TCP 流量约占 80%以上[18]。因此，本文研究的正常流量采用 TCP 协议生成，作为背景流量。这种设计思想源于文献[5,6]的研究成果。他们在 2003 年首先开展了 LDoS 攻击的研究，从 Internet II 骨干网上采集到的 LDoS 攻击流量数据，并开发了 LDoS 攻击的开源工具，被很多研究者广泛采用到 LDoS 攻击的检测研究中。

在以下的网络流量分析中，网络环境仿照美国莱斯大学提出的 LDoS 攻击模型，模拟多个正常用户采用 TCP 协议进行数据通信，TCP 流量数据由 Linux TCP 核源码产生；模拟 LDoS 攻击者采用 UDP 协议攻击，LDoS 攻击流量由软件工具产生。实验网络带宽为百兆带宽。

针对产生的网络流量，以 1 s 为采样间隔分别对网络链路中的正常流量数据、攻击流量数据和混合流量数据进行采集，其采集结果如图 1~图 3 所示。

图 1 是网络链路中的正常流量数据，可以看出正常流量经过慢启动阶段之后，在整个时间轴上逐步趋于平稳，传输速率比较稳定，并且 TCP 流量呈现出以往返时间（RTT, round-trip time）为周期的特性。

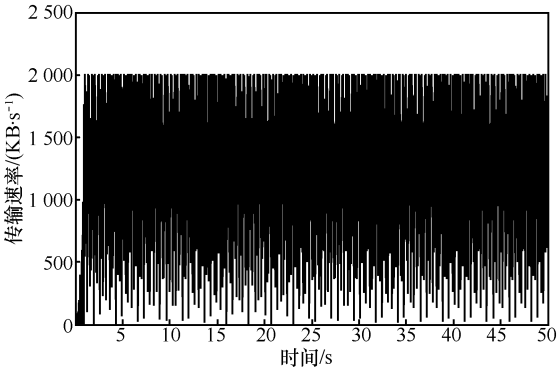


图 1　正常流量数据

图 2 是网络链路中的 LDoS 攻击数据流，可以看出 LDoS 攻击数据流是一个周期性的短时脉冲数据流，且攻击速率恒定。由于 LDoS 攻击的主要数据分组均集中在脉冲期间，因此，其平均攻击速率低于正常数据流平均速率。

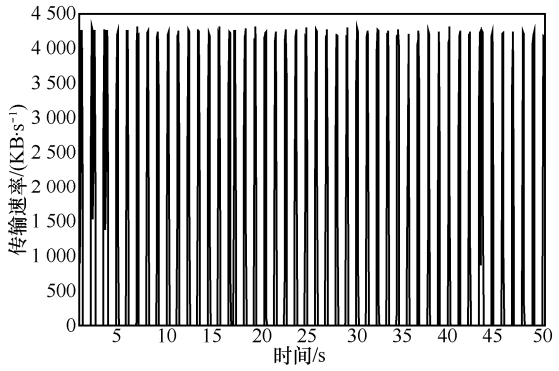


图 2　LDoS 攻击流量数据

在实际网络环境下，LDoS 攻击数据流往往隐

藏于正常 TCP 数据流之中，形成混合数据流，很难分辨。采集到的混合流量数据如图 3 所示。

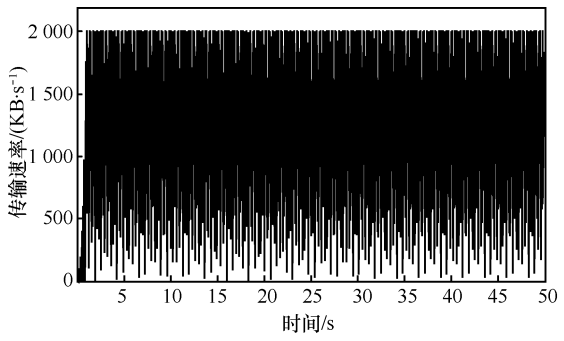


图 3 混合流量数据

对比观察图 3 中的混合数据流和图 1 中的正常数据流，可以发现两者的差异很小，在流量统计方面，很难从中检测出 LDoS 攻击数据流。

3.2 LDoS 攻击流量特征提取

在对网络流量分析的基础上，针对正常 TCP 流量和 LDoS 攻击流量呈现出的特点，提取 LDoS 攻击流量的 3 个内在的突变特征，作为检测 LDoS 攻击的依据。

3.2.1 可用带宽百分比

可用带宽百分比定义为单位时间内的实际流量带宽与链路总带宽的比值，即实际网络带宽占用率，记为 A。正常情况下，网络流量较平稳，带宽占有率较低；而在网络遭受到 LDoS 攻击时，造成网络链路部分拥塞[1,11,12]，导致网络带宽占有率较高。因此，在遭受 LDoS 攻击时链路的可用带宽百分比是一个判定攻击存在的依据。

在实验中测试得到的网络链路可用带宽百分比如图 4 所示。其中，前 50 s 网络为正常情况，从 50 s 开始网络遭受到 LDoS 攻击。

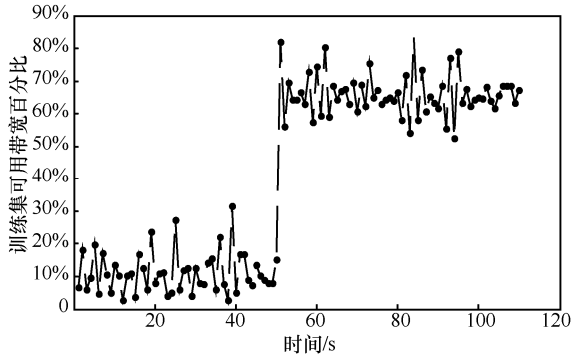


图 4 可用带宽百分比

图 4 表明在网络未遭受 LDoS 攻击的 0~50 s 内链路带宽比较均匀，可用带宽百分比较小；在遭受到 LDoS 攻击后，链路的虚假拥塞使链路的可用带宽百分比较大。

3.2.2 小分组比例

小分组比例定义为单位时间内的小分组（分组尺寸小于 200 B）个数与链路中的所有分组个数的比值，记为 R。

研究成果[1,9]表明：在保持攻击速率一定的情况下，LDoS 攻击的分组越小，攻击效果越好；攻击分组在 200 B 以下时，攻击效果最为明显。因此，为了达到较好的攻击效果，LDoS 攻击采用的数据分组一般较小。攻击分组为 50 B 时链路的小分组比例曲线如图 5 所示。其中，前 50 s 网络为正常情况，从 50 s 开始网络遭受到 LDoS 攻击。

图 5 表明在网络未遭受 LDoS 攻击的 0~50 s 内链路中传输的数据主要以 TCP 分组为主，而 TCP 分组的大小不会太小，因此小分组比例较小；50 s 开始网络遭受到 LDoS 攻击，短脉冲式的 LDoS 攻击使链路中的小分组个数增多，小分组比例随之增大。

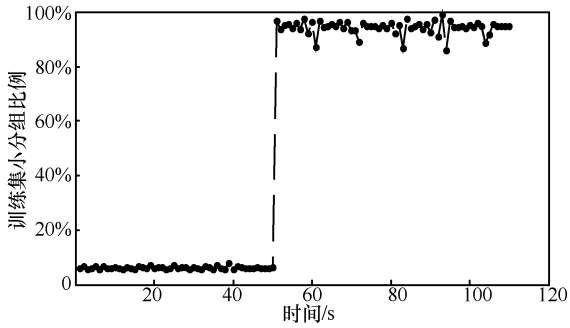


图 5 小分组比例

3.2.3 分组丢失率

分组丢失率定义为单位时间内未收到的数据分组数与发送的数据分组数的比值，即为一个时间范围内的分组丢失比率，记为 L。路由器的队列管理算法的基本思想是通过监控队列的平均长度来探测拥塞。在网络遭受到 LDoS 攻击时，链路中的分组个数瞬间增大，远远超出了路由器的最大队列长度，队列管理算法就会通知源端启动控制拥塞，丢弃一定数量的数据分组。图 6 是分组丢失率曲线，其中，前 50 s 网络为正常情况，从 50 s 开始网络遭受到 LDoS 攻击。

图 6 显示在网络未遭受 LDoS 攻击的 0~50 s 内链路数据交互良好，路由器的分组丢失率较小；在

遭受到 LDoS 攻击后，大量的数据分组进入链路，队列瞬时增大使链路拥塞，链路中数据分组依据队列管理算法进行丢弃，导致遭受攻击时的分组丢失率增大。

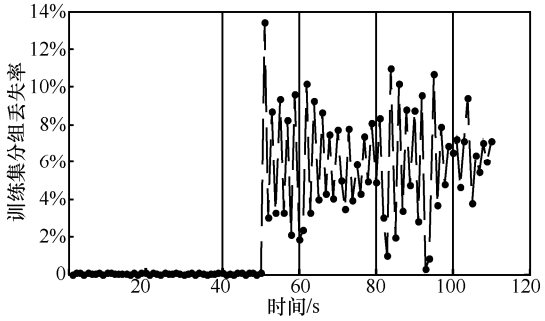


图 6　分组丢失率

由上述分析可知，在遭受 LDoS 攻击时，网络中的流量和可用带宽百分比 A、小分组比例 R 以及分组丢失率 L 都具有明显的变化。因此，以三元组(A, R, L)作为检测 LDoS 攻击的特征。但是，随着 LDoS 攻击参数的改变或网络系统的变化，这 3 个特征的表现也不尽相同，仅依靠其中单个特征去判别 LDoS 攻击是非常困难的。所以，必须采用检测分类器将 3 个特征综合起来，根据分类器的判决结果断定是否存在 LDoS 攻击。因此，本文采用 BP 神经网络作为攻击检测的分类器。

4　基于 BP 神经网络的攻击检测分类器

网络系统的状态有 2 种：正常状态（未遭受 LDoS 攻击）和异常状态（遭受 LDoS 攻击）。当网络遭受 LDoS 攻击时，把提取的 LDoS 攻击的 3 个内在特征作为输入，采用 BP 神经网络对网络数据流量的特征参数向量进行分类和训练，获得网络数据流量状态变化的信息，形成对 LDoS 攻击流量特性的描述。

采用 BP 神经网络作为 LDoS 攻击检测分类器的主要原因是基于 BP 神经网络的几个能力[26]。

1) 非线性映射能力：BP 神经网络的非线性映射能力表现在实现了从输入到输出的映射。对于 LDoS 攻击检测而言，待检测的数据是多维、多组的，经过 LDoS 攻击检测分类器后，每组数据的输出即为检测结果，而复杂的检测过程可以在 BP 神经网络分类器内部实现。

2) 自学习能力：遭受到 LDoS 攻击的网络数据通过攻击检测分类器，期望的输出结果为“有攻击”；而正常的网络数据通过攻击检测分类器，期望的输出结果为“无攻击”。建立输出数据与期望输出之间的“合理规则”对于正确检测 LDoS 攻击十分重要。BP 神经网络具有优秀的自学习能力，通过学习训练集数据，能够自动提取合适的规则来对待测数据进行分类。

3) 泛化能力：在对 LDoS 攻击检测分类器进行训练时，使用的训练集数据是有限数据集，并且在不同的网络环境下采集的数据也存在较大区别。因此，要求分类器具有对未知的待检测数据进行正确分类的能力，而 BP 神经网络分类器就是最佳选择之一。

在网络遭受 LDoS 攻击情况下，提取的网络流量和带宽的 3 个特征(A，R，L)具有区分度较高和不可伪造的特性。使用大量的数据对 BP 神经网络进行训练，即可得到适用于判别 LDoS 攻击的 BP 神经网络，将 BP 神经网络作为特征联合的工具，把带宽的 3 个特征联合作为 BP 神经网络的输入，构建 3 层 BP 神经网络，如图 7 所示[28]。

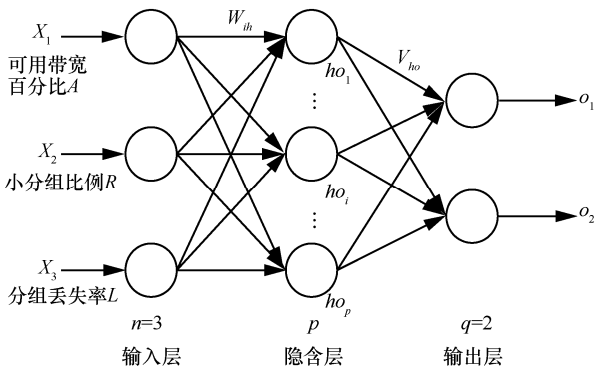


图 7　3 层 BP 神经网络结构

图 7 中，输入层由 3 个神经元组成，定义输入向量 $\boldsymbol{x}_i=(x_1,x_2,x_3)$，依次对应 LDoS 攻击的 3 个特征($A$，$R$，$L$)；隐含层神经元个数的选择在实验中根据 BP 神经网络的网络均方误差性能选择；输出层由 2 个神经元组成，输出层输出变量 $o_y=(o_1,o_2)$，期望输出变量 $d_y=(d_1,d_2)$。为了使 BP 神经网络更易区别正常数据与 LDoS 攻击数据，定义期望输出 (d_1,d_2) 为（0,1）时代表 BP 神经网络输入为正常数据的特征；期望输出 (d_1,d_2) 为（1,0）时代表 BP 神经网络输入为 LDoS 攻击数据的特征。

用于判别 LDoS 攻击的 BP 神经网络使用误差逆传播算法学习，学习过程主要包括前向传播过程及后向传播过程 2 部分。前向传播过程在给定 BP 神经网络输入的情况下，完成经输入层、隐含层和输出层逐层处理并计算得到实际输出值；后向传播

过程完成了实际输出与期望输出间误差的计算，并以此调整各层的权值阈值使网络的输出不断接近期望输出[26,27]。

定义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 w_{ho}；隐含层各神经元阈值为 r_h；输出层各神经元阈值为 s_i；激活函数为 $f(\cdot)$；训练集样本个数 $k=1,2,\cdots,m$，对于第 k 个输入样本 $x(k)=(x_1(k),x_2(k),x_3(k))$ 及对应期望输出 $d_y(k)=(d_1(k),d_2(k))$。

隐含层的各神经元的输入和输出[26,27]分别为

$$hi_h(k)=\sum_{i=1}^{3}w_{ih}x_i(k)-r_h,\quad h=1,2,\cdots,p \tag{1}$$

$$ho_h(k)=f(hi_h(k)),\quad h=1,2,\cdots,p \tag{2}$$

输出层各神经元的输入由隐含层神经元的输出进一步进行加权求和得到。则输出层各神经元的输入和输出[26,27]分别为

$$o_i(k)=\sum_{h=1}^{p}w_{ho}ho_h(k)-s_i,\quad i=1,2 \tag{3}$$

$$o_y(k)=f(o_i(k)),\quad i=1,2 \tag{4}$$

由式(4)可得 BP 神经网络模型的最终输出。此时 BP 神经网络学习过程中的前向传播过程完成。

计算第 k 个输入样本的误差函数[26,27]为

$$e_k=\frac{1}{2}\sum_{y=1}^{2}(d_y(k)-o_y(k))^2 \tag{5}$$

依据误差函数对各层的权值阈值求偏导数，并利用梯度下降法修正权值。将 k 个训练集样本全部训练完毕后，计算 m 个训练样本的全局误差[26,27]为

$$E=\frac{1}{2m}\sum_{k=1}^{m}\sum_{y=1}^{2}(d_y(k)-y_y(k))^2 \tag{6}$$

当全局误差达到训练目标或最大训练次数时，BP 神经网络学习过程中的后向传播过程完成，结束学习算法。因而，BP 神经网络训练结束。

对于训练良好的 BP 神经网络，其泛化能力也较为优秀。当向网络输入的样本数据不是训练集数据时，BP 神经网络依然能给出合适的输出，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。

BP 神经网络的输出结果为二元向量，为了得到一个单一的判决指标，并结合 BP 神经网络期望的输出特点，定义决策指标 $D=\dfrac{o_1^2+(o_2-1)^2}{2}$。

基于联合特征的 LDoS 攻击检测方法总体流程如图 8 所示[27]。

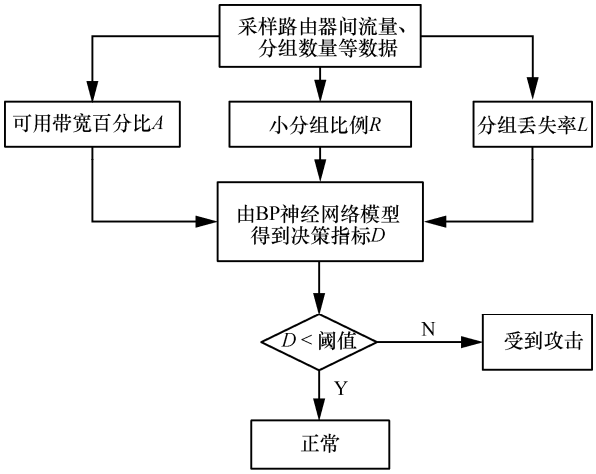


图 8 基于联合特征的 LDoS 攻击检测方法总体流程

按照图 8 所示检测流程，首先采样路由器间的流量、分组数量等数据，从中提取可用带宽百分比、小分组比例和分组丢失率 3 个典型的 LDoS 攻击特征，将其共同作为 BP 神经网络的输入。完成 BP 神经网络训练后，最后由 BP 神经网路输出得到的决策指标 D 作为 LDoS 攻击的判决依据。在网络未遭受 LDoS 攻击的 D 值和遭受 LDoS 攻击的 D 值之间选择一个阈值。如果 D 值超过阈值，说明网络环境遭受了 LDoS 攻击。

5 实验及结果分析

本文提出的方法在 NS2 仿真环境和 test-bed 网络环境中进行了实验验证和测试。

5.1 建 NS2 仿真实验及其结果分析

根据文献[5,6]设计的 LDoS 攻击实验环境，在 NS2 网络仿真平台中搭建了攻击检测实验环境，它是一个哑铃型拓扑结构的网络，如图 9 所示[5,6]。

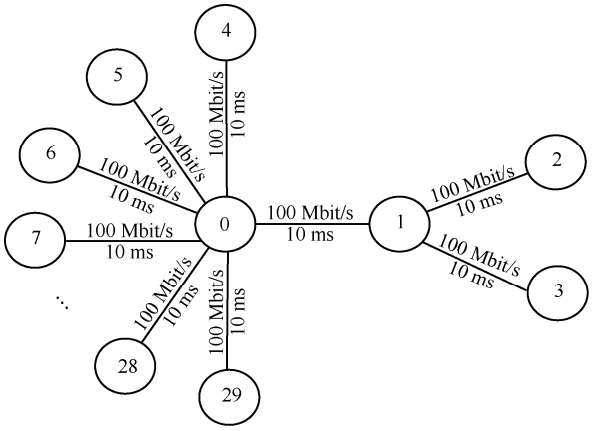


图 9 网络拓扑结构

图 9 中，节点 0 和节点 1 分别代表 2 个路由器，它们中间是一条 100 Mbit/s 的瓶颈链路，路由器缓冲队列管理算法采用 RED 算法；节点 2 代表 FTP 服务器；节点 3 代表 UDP 服务器；节点 4~28 代表 25 个合法用户；节点 29 代表 LDoS 攻击方。合法用户和 LDoS 攻击方与路由器之间、2 个路由器之间以及路由器与服务器之间的链路带宽均为 100 Mbit/s 带宽，单向延时 10 ms。

实验开始于 0 s，结束于 100 s。3 个正常流量在 0 s 开始，100 s 结束；攻击流量在 50 s 开始，100 s 结束。LDoS 攻击的攻击速率为 90 Mbit/s，攻击周期为 1 150 ms，攻击脉宽为 150 ms。

设置采样间隔为 1 s，对路由器间的可用带宽百分比、小分组比例和分组丢失率数据分别进行采样，各得到 50 组正常数据和 50 组 LDoS 攻击数据（每个特征共采样得到 100 组数据）。将该 3×100 的矩阵作为 BP 神经网络的输入，BP 神经网络初始学习速率为 0.01，训练目标为 0.001，最大训练次数为 500，训练函数为 traingdx。正常数据的期望输出为向量（0,1），LDoS 攻击数据的期望输出为向量（1,0）。

为了保证 BP 神经网络对 LDoS 攻击特征的准确分类，必须保障 BP 神经网络具有较高的性能。由于隐含层神经元个数对 BP 神经网络性能具有较大的影响。因此，这里比较了神经元个数为 6、8、10、12、14、16 的网络均方误差(MSE, mean squared error)性能，如图 10 所示。

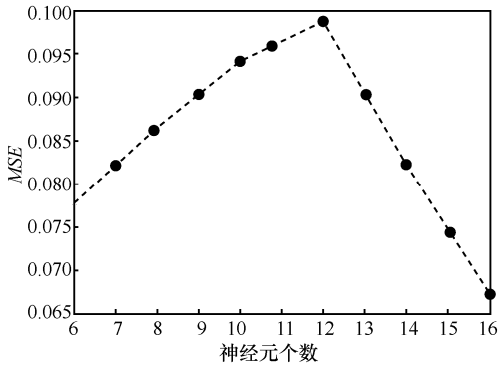


图 10　不同隐含层神经元个数的均方误差曲线

从图 10 可以看出，当隐含层神经元个数为 16 时，均方误差最小。因此，本文方法选取隐含层神经元个数为 16 的 BP 神经网络进行训练。在训练结束后，将该 BP 神经网络作为分类器判别 LDoS 攻击。

为了检验 BP 网络分类器的检测性能，将 LDoS 的攻击速率从 90 Mbit/s 调整为 55 Mbit/s，其余参数不变。同样，以 1 s 间隔进行采样，采集得到 100 组正常数据和 100 组 LDoS 攻击数据作为测试集数据。

训练集（攻击速率 90 Mbit/s）和测试集（攻击速率 55 Mbit/s）数据中包含的 3 个特征如图 11 所示。

由图 11 可以看出，当攻击速率降为 55 Mbit/s 后，3 个特征均发生了变化：1) 可用带宽百分比变小，出现了个别的突变点；2) 小分组比例变小；3) 分组丢失率变小。当攻击参数发生明显的改变时，独立的单个特征变化也不尽相同。

采用训练好的 BP 神经网络分类器判别调整 LDoS 攻击参数后的网络，其判别结果如图 12 所示。决策指标 D 的判决结果如图 13 所示。

由图 12 中 BP 神经网络的输出不难发现，虽然测试集数据的 3 个特征均出现了变化，但是，未遭受攻击的网络，大多数测试数据的输出结果更接近向量(0,1)；而遭受攻击后的网络，输出结果更接近向量(1,0)。

由图 13 可得，不同的决策指标对于判决结果的影响也不同。

针对上述实验中的 BP 神经网络分类器，可以得到不同阈值时的检测性能，如表 1 所示。

从表 1 可以看出，检测性能对阈值的取值敏感度不高，虽然测试集的 3 个特征与训练集比较均发生了改变，但作为联合特征输入到 BP 神经网络依然可以检测 LDoS 攻击，且检测性能较好。

设置 LDoS 攻击速率为 90 Mbit/s，其余攻击参数不变。重新采样 50 组正常数据和 50 组 LDoS 攻击数据，从中提取 3 个特征(A, R, L)，将每个特征的 100 组数据分别作为 BP 网络的训练集，再把 3 个特征两两组合作为 BP 网络的训练集，即 BP 神经网络的输入分别为 1×100 的矩阵和 2×100 的矩阵，对 BP 神经网络进行训练，总共训练 6 个 BP 神经网络模型，直到每个 BP 神经网络均可作为分类器判别 LDoS 攻击。

将 LDoS 攻击的攻击速率调整为 55 Mbit/s 后，再采样 50 组正常数据和 50 组 LDoS 攻击数据作为测试集数据，测试数据根据不同训练数据的输入而随之变化，决策指标阈值取 $D > 0.6$，得到的检测性能如表 2 所示。

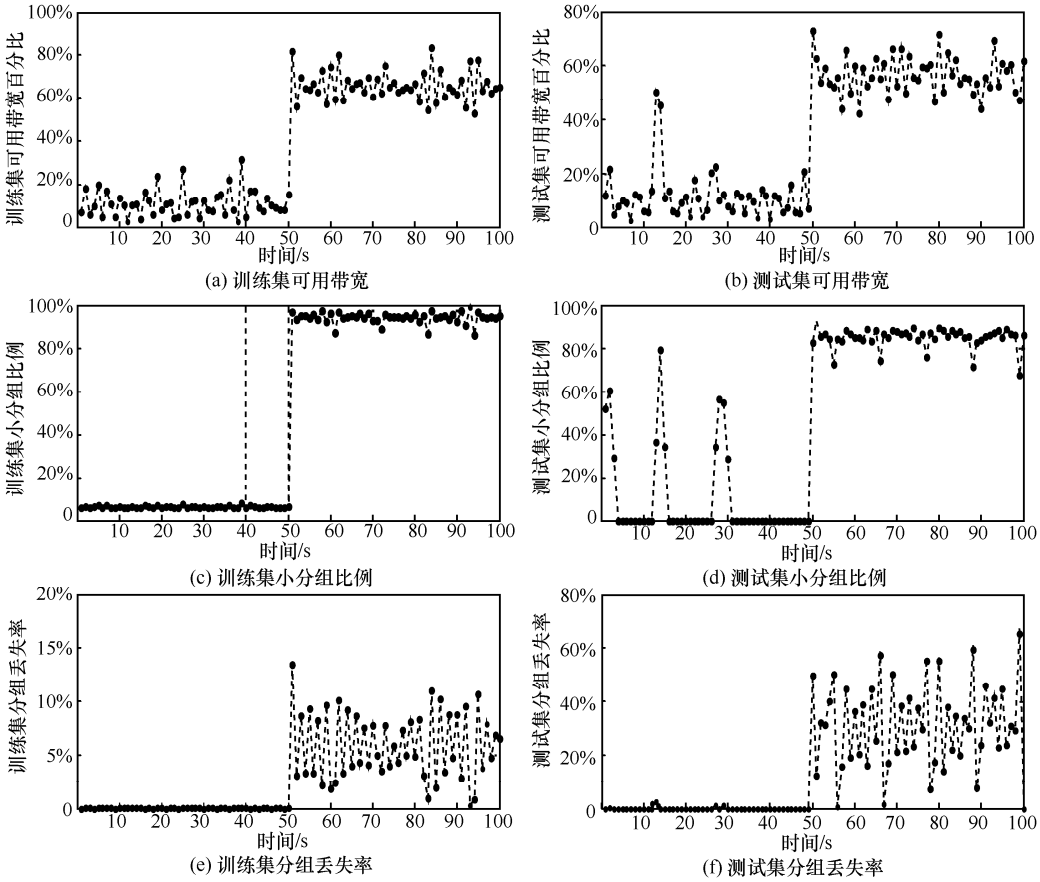


图 11　训练集与测试集 3 个特征的比较

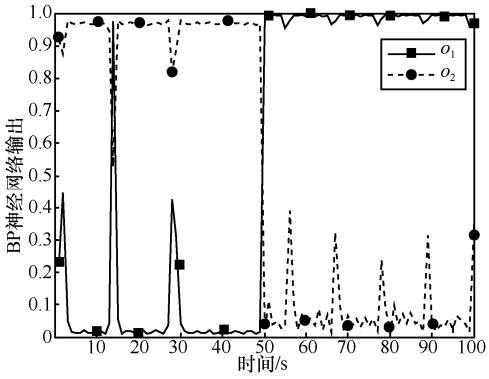


图 12　BP 神经网络的输出

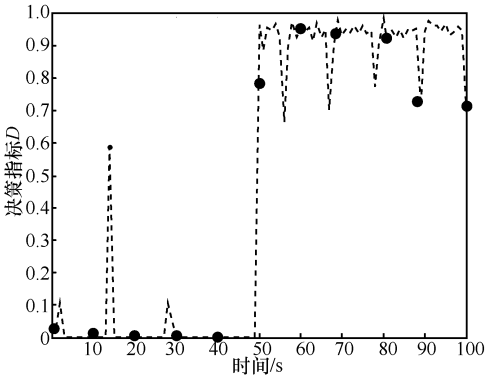


图 13　决策指标 D 判决结果

表 1　不同决策指标阈值的检测性能

D	检测率	漏警率	虚警率
0.1	100%	0%	6%
0.2	100%	0%	2%
0.3	100%	0%	2%
0.4	100%	0%	2%
0.5	100%	0%	2%
0.6	100%	0%	0%
0.7	96%	4%	0%
0.8	90%	10%	0%
0.9	86%	14%	0%

表 2　不同训练特征作为输入的检测性能比较

输入的训练特征	检测率	漏警率	虚警率
可用带宽百分比	90%	10%	2%
小分组比例	86%	14%	10%
分组丢失率	94%	6%	4%
可用带宽百分比+小分组比例	86%	14%	10%
可用带宽百分比+分组丢失率	96%	4%	0%
小分组比例+分组丢失率	88%	12%	6%
联合特征	100%	0%	0%

由表 2 可知，使用单个或 2 个特征训练得到的 BP 神经网络分类器，对每个特征的变化更加敏感，导致 LDoS 攻击的判别效果较差。而使用 3 个特征作为联合特征训练得到的 BP 神经网络分类器，对单个特征的变化敏感度较小，而检测性能较好。

5.2　test-bed 实验及其结果分析

为了更好地验证本文方法，本文在实际的网络环境搭建了 test-bed 实验平台，用来测试和评估本文检测方法在实际网络环境下的检测性能。该平台参照 Aleksandra 等[5,6]设计的 NS2 仿真环境，在实际网络环境中设计搭建的。

Test-bed 实验平台由 2 台合法用户、一台 LDoS 攻击者、一台交换机、一台路由器和一台 FTP 服务器受害机组成，各链路间均为 100 Mbit/s 带宽。实验网络拓扑如图 14 所示。

图 14 中，2 台合法用户同时下载受害机 FTP 服务器上的资源；LDoS 攻击者使用 LDoS 攻击工具发起攻击；数据的采集使用 Tcpstat 抓包工具完成。

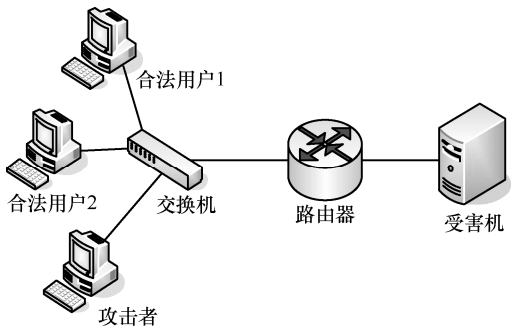
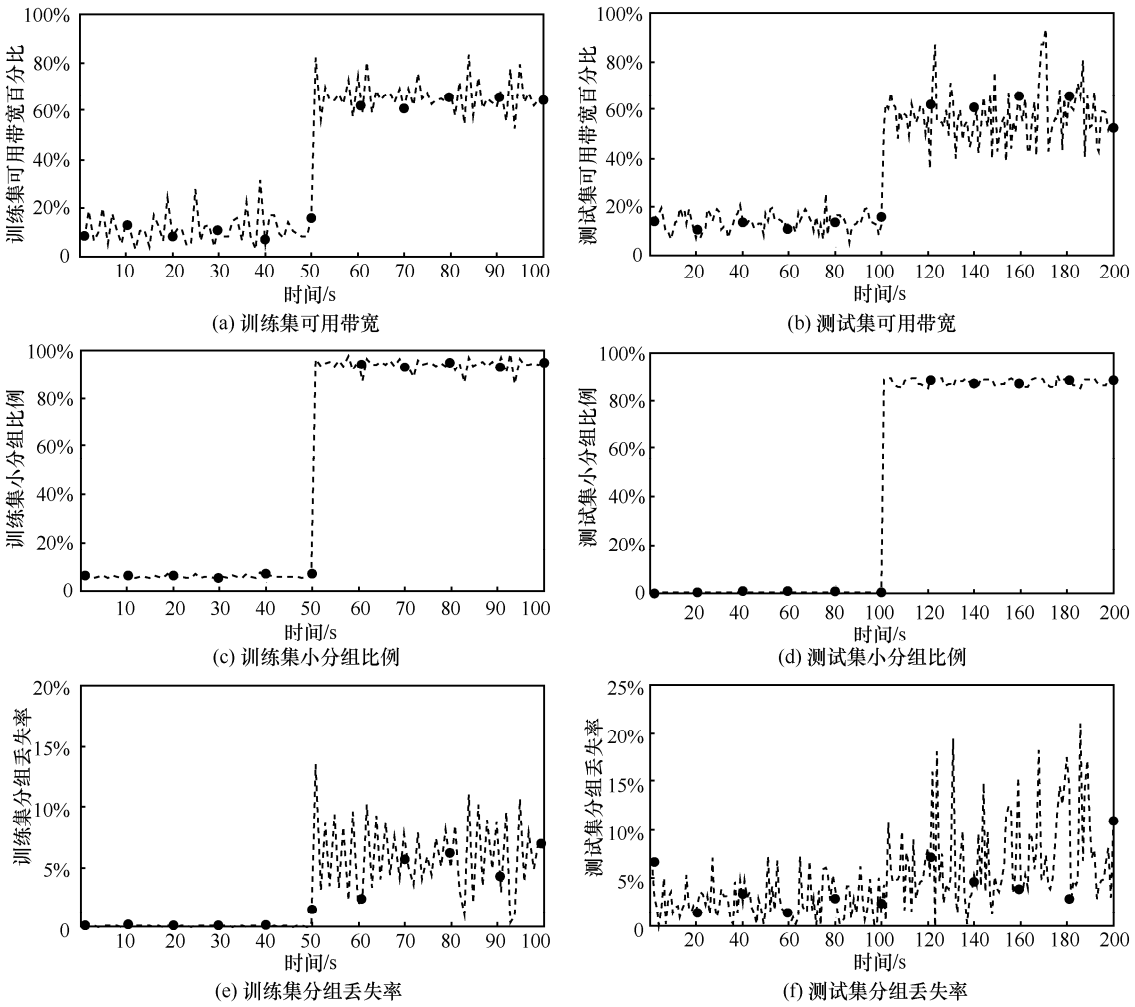


图 14　test-bed 实验网络拓扑

LDoS 攻击在 100 s 时刻发起，攻击参数为（τ，T，R）= (1 150 ms,150 ms,90 Mbit/s)。以 1 s 为采样间隔，分别采样可用带宽百分比、小分组比例以及分组丢失率数据，得到的采样数据如图 15(b)、图 15(d)和图 15(f)所示。



(a) 训练集可用带宽　(b) 测试集可用带宽
(c) 训练集小分组比例　(d) 测试集小分组比例
(e) 训练集分组丢失率　(f) 测试集分组丢失率

图 15　训练集数据与 test-bed 数据对比

采用训练好的 BP 神经网络分类器对 test-bed 实验数据进行判别，得到判决结果如图 16 所示。

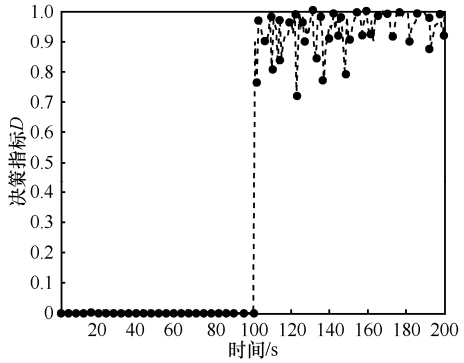


图 16　test-bed 数据判决结果

由于攻击参数的不同、网络模型的差异以及决策指标 D 阈值的取值不同，导致每次测试得到的检测性能也不尽相同。这里，通过对大量实验数据进行采集分析，采用大样本的假设检验方法统计得出本文检测方法的检测性能。

根据中心极限定理，大量随机变量近似服从正态分布，那么对于参数做如下假设[18]。

$$\begin{cases} D_0\text{：没有LDoS攻击} \\ D_1\text{：存在LDoS攻击} \end{cases}$$

假设，没有 LDoS 攻击时的 D_0 值服从均值为 μ_0，方差为 σ_0^2 的正态分布；存在 LDoS 攻击时的 D_1 值服从均值为 μ_1，方差为 σ_1^2 的正态分布。

针对不同的 LDoS 攻击模型和参数、提取可用带宽百分比、小分组比例以及分组丢失率特征，在 test-bed 中采集 2 000 组 LDoS 攻击数据和 2 000 组正常数据，由训练好的 BP 神经网络分类器进行判别，共得到 4 000 个 D 值，通过计算可以得出以下结论。

1) 没有 LDoS 攻击时，$D_0 \sim N(0.1275, 0.0474)$；

2) 存在 LDoS 攻击时，$D_1 \sim N(0.8631, 0.0367)$。

没有 LDoS 攻击和存在 LDoS 攻击时的 D 值正态分布如图 17 所示。

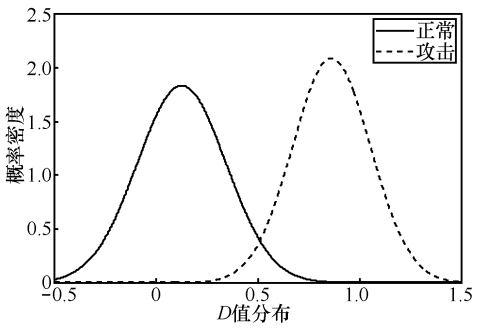


图 17　决策指标 D 值的分布

由图 17 可以看出，没有 LDoS 攻击和存在 LDoS 攻击的分布曲线之间的交集并不大。

选择不同的 D 值，可以计算检测率 P_{D}、漏警率 P_{FN} 和虚警率 P_{FP}。

$$\begin{cases} P_{\mathrm{D}} = P(D_1;D_1) = P_r\{x>D;D_1\} = \int_D^{\infty} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left\{-\frac{(x-\mu_1)^2}{2\sigma_1^2}\right\} \\ P_{\mathrm{FN}} = P(D_0;D_1) = P_r\{x<D;D_1\} = \int_{-\infty}^{D} \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left\{-\frac{(x-\mu_1)^2}{2\sigma_1^2}\right\} \\ P_{\mathrm{FP}} = P(D_1;D_0) = P_r\{x>D;D_0\} = \int_D^{\infty} \frac{1}{\sqrt{2\pi}\sigma_0} \exp\left\{-\frac{(x-\mu_0)^2}{2\sigma_0^2}\right\} \end{cases}$$

经过实验统计，采用不同的 D 值得出检测率 P_{D}、漏警率 P_{FN} 和虚警率 P_{FP} 结果如表 3 所示。

表 3　　不同 D 值的检测性能

D	P_{D}	P_{FN}	P_{FP}
0.400 0	99.22%	0.78%	10.54%
0.511 5	96.68%	3.32%	3.89%
0.550 0	94.89%	5.11%	2.62%
0.600 0	91.52%	8.48%	1.50%
0.650 0	86.70%	13.30%	0.82%

从表 3 中可以看出，不同的 D 值对应的检测性能相差很大。由图 17 可知，2 条正态分布曲线的交点即为 D 的最优取值，此时 D= 0.511 5，检测率为 96.68%，漏警率为 3.32%，虚警率为 3.89%。

5.3　比较分析

将在 NS2 仿真平台中得到的实验结果与在 test-bed 网络环境中得到的实验结果进行比较，可以得出如下结论。

由图 15 可以看出，test-bed 实验平台的数据较之前用于训练 BP 神经网络的训练集数据，可用带宽百分比以及分组丢失率 2 个特征波动较大，小分组比例特征较为稳定。主要原因是：1）NS2 仿真时，各个 TCP 节点的网络流量较为平均，提取的各个特征较为平稳，而实际的网络环境中，各个用户之间存在竞争关系，提取的可用带宽百分比以及分组丢失率特征随之波动较大，且突发较多；2）在实际的网络环境中，FTP 服务器存在一定的防御机制，使 LDoS 攻击效果不如 NS2 仿真环境中的理想。

虽然在 3 个特征中突发值的出现可以导致训练好的 BP 神经网络分类器的判决结果出现一定的偏差。从图 16 中不难看出，基于联合特征的 LDoS

攻击检测方法判决效果依然很好。

比较表 1 和表 3 的结果，在检测性能方面，test-bed 平台实验得到的数据比在 NS2 仿真环境下得到的数据下降了很多。主要原因是实际网络中突发较多，导致提取的特征不及仿真环境中理想。

将本文方法实验得到的结果与典型的相关成果在检测率、漏警率以及虚警率方面进行比较。选取了典型的检测方法，即基于 NCPSD[18]、多重分形[20]和卡尔曼滤波[28]的检测方法，比较结果如表 4 所示。

表 4　　不同检测方法性能比较

方法	检测率	漏警率	虚警率
NCPSD	88.00%	12.00%	16.70%
卡尔曼滤波	89.60%	10.40%	12.60%
多重分形	91.00%	9.00%	10.00%
本文方法	96.68%	3.32%	3.89%

表 4 说明基于联合特征的 LDoS 攻击检测方法相较于基于 NCPSD 和基于多重分形的 LDoS 攻击检测方法在检测率上有了很大的提升，在漏警率和虚警率也有很好的改善，显示了优越的总体检测性能。

6　结束语

LDoS 攻击消耗大量的网络流量，降低了服务质量，已经成为云计算平台和大数据中心的主要威胁之一。本文提出了基于联合特征的 LDoS 攻击检测方法，提取了含有 LDoS 攻击的网络流量的 3 个内在特征，形成联合特征作为 BP 神经网络模型的输入，利用 BP 神经网络设计网络流量异常分类器，通过 BP 神经网络的输出获得决策指标，进而判定是否发生 LDoS 攻击，并利用假设检验对大量实验数据进行统计，得到该方法的检测性能指标。本文的主要创新性的工作体现在：1）提取了 LDoS 攻击流量的 3 个内在特征，作为检测 LDoS 攻击的依据；2）建立基于 BP 神经网络的 LDoS 攻击分类器，用于 LDoS 攻击的判定；3）提出了基于联合特征的 LDoS 攻击检测方法，将 LDoS 攻击的 3 个内在特征组成联合特征作为 BP 神经网络的输入，设置决策指标，达到检测 LDoS 攻击的目的。与现有研究成果比较，本文方法避免了某一攻击特征被伪造导致检测失效的缺陷，具有检测概率高、虚警率和漏警率低的优点。

本文方法研究的对象是一种典型的 LDoS 攻击形式，其周期是固定值。而针对攻击周期按照 RTT 指数变化的情况（属于同步攻击方式）以及变速率 LDoS 攻击类型，本文方法并没有进行验证。因此，本文方法在针对不同类型的 LDoS 攻击和建立精确的非线性网络流量模型方面需要改进。今后的研究工作的思路是：1）需要进一步改善非线性网络流量建模的精度，准确刻画网络流量的特点，提高 LDoS 攻击的检测精度；2）不断地采用新的数据，训练 BP 神经网络分类器，使其适用于不同类型的 LDoS 攻击的精确检测；3）随着云计算、云存储和大数据技术的不断发展，针对它们面临 LDoS 攻击威胁的问题，开展针对云端的 LDoS 攻击检测与防范的研究。

参考文献：

[1] 吴志军, 岳猛. 基于信号处理的低速率拒绝服务攻击的检测技术[M]. 北京: 科学出版社, 2015.
WU Z J, YUE M, Detection technology of LDoS attacks based on signal processing[M]. Beijing: Science Press, 2015.

[2] MACIÁ-FERNÁNDEZ G, DÍAZ-VERDEJO J E, GARCÍA- TEODORO P. Mathematical model for low-rate DoS attacks against application servers[J]. IEEE Transactions on Information Forensics and Security, 2009, 4(3): 519-529.

[3] TANG Y J, LUO X P, HUI Q, et al. Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 339-353.

[4] FICCO M, RAK M. Stealthy denial of service strategy in cloud computing[J]. IEEE Transactions on Cloud Computing, 2015,3(1):80-94.

[5] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks- the Shrew vs. the Mice and Elephants [C]//ACM SIGCOMM 2003. Karlsruhe, Germany, 2003: 25-29.

[6] 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.

[7] 何炎祥, 刘陶. 降质服务攻击及其防范方法[M]. 北京: 机械工业出版社, 2011.
HE Y X, LIU T. Reduction of quality attack and the defense methods[M]. Beijing: China Machine Press, 2011.

[8] TANG Y, LUO X, HUI Q, et al. Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks[J].IEEE Transactions on Information Forensics and Security (TIFS), 2014,9(3):339-353.

[9] 文坤, 杨家海, 张宾. 低速率拒绝服务攻击研究与进展综述[J]. 软件学报, 2014, 25(3): 591-605.
WEN K, YANG J H, ZHANG B, Survey on research and progress of low-rate denial of service attacks[J]. Journal of Software, 2014, 25(3): 591-605.

[10] ZHU H L, YANG X, WU Q X, et al. A novel distributed LDoS attack scheme against internet routing[J]. China Communications, 2014, 113: 101-107.

[11] LUO J T, YANG X L. The new shrew attack: a new type of low-rate TCP-targeted DoS attack[C]//International Conference on Communications, Sydney, Australia, 2014: 713-718.

[12] LUO J T, YANG X L, WANG J, et al. On a mathematical model for low-rate shrew DDoS[J]. IEEE Transactions on Information Forensics and Security (TIFS), 2014, 9(7):1069-1083.

[13] 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.

[14] ZHANG C, YIN J, CAI Z, et al. RRED: robust RED algorithm to counter low-rate denial-of-service attacks[J]. IEEE Communication Letter, 2010,415: 489-491.

[15] 马建红, 姬莉霞, 文坤. Shrew 攻击对拥塞控制协议的影响及仿真分析[J]. 河南科技大学学报(自然科学版), 2013,34(4): 51-56.
MA J H, JI L X, WEN K. Shrew attacks' influence of congestion control protocol and simulation analysis[J]. Journal of Henan University of Science & Technology (Natural Science), 2013,34(4): 51-56.

[16] 刘文胜, 周长胜. 基于路由器 BGP 协议的低速率攻击与防御[J]. 北京信息科技大学学报, 2014,29(6): 90-94.
LIU W S, ZHOU C S, Low-rate attack and defense based on BGP protocol router[J]. Journal of Beijing Information Science and Technology University, 2014,29(16): 90-94.

[17] WEI W, CHEN F, XIA Y J, et al. A rank correlation based detection against distributed reflection DoS attacks[J]. IEEE Communications Letters, 2013,17(1):173 – 175.

[18] CHEN Y, HUANG K, KWONG K Y. Collaborative defense against periodic shrew DDoS attacks in frequency domain [C]//ACM Transactions on Information and System Security. ACM: Los Angeles, California, USA, 2005: 2-27.

[19] TANG D, CHEN K, CHEN X S, et al. Adaptive EWMA method based on abnormal network traffic for LDoS attacks[J]. Mathematical Problems in Engineering, 2014(3): 166-183.

[20] WU Z J, ZHANG L Y, YUE M. Low-rate dos attacks detection based on network multifractal[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 315: 559-567.

[21] 刘映. 基于 TCP 流量统计特征的 LDoS 攻击检测方法研究[D]. 华中科技大学, 2015.
LIU Y. Research on LDoS attacks detection method based on the statistical features of TCP traffic[D]. Huazhong University of Science and Technology, 2015.

[22] KWOK Y K, TRIPATHI R, CHEN Y, ET AL. HAWK: halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks[C]//Networking and Mobile Computing, Third International Conference, ICCNMC 2005. 2005: 423-432.

[23] 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.

[24] 吴娜, 穆朝阳, 张良春. 基于数据流势能特征的分布式拒绝服务隐蔽流量检测[J]. 计算机工程, 2015, 42(3): 142-146.
WU N, MU C Y, ZHANG L C. Distributed denial of service covert flow detection based on data stream potential energy feature[J]. Computer Engineering, 2015, 42(3): 142-146.

[25] 李振军, 程杰仁. 基于多特征分布式拒绝服务攻击的检测[J]. 信息网络安全, 2013(5): 25-28.
LI Z J, CHENG J R. Detecting distributed denial of service attack based on multi-feature fusion[J]. Netinfo Security, 2013(5):25-28.

[26] HSIAO K J, XU K S, CALDER J, et al. Multicriteria similarity-based anomaly detection using pareto depth analysis[J]. IEEE Transactions on Neural Networks and Learning Systems, 2016, 27(6):1307 - 1321.

[27] 徐琴珍, 杨绿溪. 一种优化的神经网络树异常入侵检测方法[J]. 信号处理, 2010, 26(11): 1663-1669.
XU Q Z, YANG L X. An optimized neural network tree based anomaly intrusion detection method[J]. Journal of Signal Processing, 2010, 26(11): 1663-1669.

[28] 吴志军, 岳猛. 基于卡尔曼滤波的 LDDoS 攻击检测方法[J].电子学报, 2008,36(8): 1590-1594.
WU Z J, YUE M. Detection of LDDoS attack based on Kalman filtering[J]. Acta Electronica Sinica, 2008, 26(8):1590-1594.

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。

张景安（1989-），男，山东临沂人，中国民航大学硕士生，主要研究方向为信息安全、拒绝服务攻击的入侵检测。

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

张才峰（1991-），男，山东济南人，中国民航大学硕士生，主要研究方向为信息安全、拒绝服务攻击的入侵检测。