文章编号:1671-4598(2023)12-0028-06 DOI:10.16526/j.cnki.11-4762/tp.2023.12.005 中图分类号:TP391 文献标识码:A

基于人工蜂群算法的计算机网络 DDoS 攻击检测方法

田小芳
(北京市地铁运营有限公司 信息中心,北京 100088)

摘要:计算机网络在 DDoS 入侵下容易出现停止服务、网络崩溃,为了提高网络安全性,提出基于人工蜂群算法的计算机网络 DDoS 攻击检测方法;基于特征样本之间的相关性,获取 DDos 攻击的同态样本分布时间序列输出,并且得到对网络入侵数据集的输出阵列模型,构建计算机网络 DDoS 攻击的自适应的入侵检测信息分析模型,根据网络数据流与潜在空间之间的映射关系,结合测试样本和学习样本之间特征差异性进行 DDoS 攻击数据特征提取,在基站上设置入侵检测数据处理终端,采用人工蜂群算法实现对计算机网络攻击检测的个体最优值和全局最优值寻优,获取在相对维度较高的网络入侵检测数据集中的入侵特征分布模型,计算特征选择的信息增益,得到快速相关性过滤输出,通过蜂群算法,分别选择不同的特征子集得到 DOS 攻击检测的离散信息,实现对组合网络流量数据间的攻击信息特征提取和聚类分析,解决计算机网络 DDoS 攻击检测过程中的连续多变量优化问题;仿真测试结果表明,采用该方法进行计算机网络 DDoS 攻击检测的寻优能力较好,精度和效率高于传统方法。

关键词:人工蜂群算法;计算机网络;DDoS 攻击;检测;组合优化

Computer Network DDoS Attack Detection Method Based on Artificial Bee Colony Algorithm

TIAN Xiaofang
(Information Center, Beijing Subway Operation Co., Ltd., Beijing 100088, China)

Abstract: The computer network is prone to stop service and network crash under the intrusion of DDoS. In order to improve the network security, a DDoS attack detection method of computer network based on artificial bee colony algorithm is proposed. Based on the correlation between feature samples, the output of homomorphic sample distribution time series of DDos attacks is obtained, and the output array model of network intrusion data set is obtained. Then, the adaptive intrusion detection information analysis model of computer network DDoS attacks is constructed. The feature extraction of DDoS attack data is carried out based on the feature differences between test samples and learning samples. The intrusion detection data processing terminal is set up on the base station, and the artificial swarm algorithm is used to optimize the individual and global optimal values of computer network attack detection, so as to obtain the intrusion feature distribution model in the network intrusion detection data set with higher relative dimensions. The information gain of feature selection is calculated, and the output of fast correlation filtering is obtained. The discrete information of DOS attack detection is obtained by selecting different feature subsets through the hive algorithm, which realizes the feature extraction and cluster analysis of attack information among the combined network traffic data, and solves the continuous multivariate optimization problem in the process of DDoS attack detection on computer networks. The simulation test results show that this method has better optimization ability, higher accuracy and efficiency than the traditional method.

Keywords: artificial bee colony algorithm; computer network; DDoS attack; detection; combinatorial optimization

0 引言

计算机网络分布式拒绝服务攻击(DDoS, distributed denial of service)是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击,或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击,其是通过植入加载 ECA 规则脚本和打包的病毒,实现对计算机网络在执行运行程序过程中的编译、打包和污点数据部署,达到攻击网络的目的,从而导致整个网络的崩溃和瘫痪[1-2]。因此,为了提高计算机网络的安全性,需要构建优化的计算机网络 DDoS 攻击检测模型,通过 SQL 注入攻击的模型化参数构造,在程序执行引擎及源码情况下实时跟踪污点数据的静态参数分布集[3-4],在现有的基于污点分析的 DDoS 注入攻击检测模型参数下,结合攻击性能特征参数和攻击过程参数模拟分析,并且提取和分析 DDoS 攻击的

收稿日期:2023-06-29; **修回日期**:2023-07-17。
作者简介:田小芳(1982-),女,硕士,高级工程师。
引用格式:田小芳.基于人工蜂群算法的计算机网络 DDoS 攻击检测方法[J].计算机测量与控制,2023,31(12):28-33,41.

特征和攻击病毒数据的动态特征[5]，实现计算机网络 DDoS 攻击检测。另外，研究计算机网络 DDoS 攻击检测优化方法，分析对攻击数据的文本向量化和机器学习参数，采用源码分析技术，实现计算机网络的 DDoS 攻击检测优化设计[6]。计算机网络 DDoS（分布式拒绝服务）攻击是一种恶意行为，旨在通过超过目标系统处理能力的流量和请求来使其崩溃或瘫痪。为了构建优化的计算机网络 DDoS 攻击检测模型，相关学者考虑以下方面构建。首先，针对 SQL 注入攻击，进一步研究和构造模型化参数来识别和防止此类攻击。通过分析和理解 SQL 注入攻击的特征和模式，可以构建相应规则和算法检测和阻止这种类型的攻击。其次，除了静态参数分布集外，还可以实时跟踪污点数据的动态参数分布集。通过监控和分析运行时的污点数据，准确地检测和识别 DDoS 攻击行为，并及时采取相应的防御措施。此外，结合攻击性能特征参数分析和攻击过程参数模拟分析，以更好地理解和预测 DDoS 攻击的行为和模式。通过分析攻击数据和攻击病毒数据的动态特征，可以发现新的攻击特征和模式，并及时更新和优化检测模型。然后，在优化计算机网络 DDoS 攻击检测的过程中，可以采用文本向量化和机器学习参数分析的方法。通过将攻击数据转化为可处理的向量表示，并应用机器学习算法进行分析和分类，提高检测模型的准确性和效率。最后，源码分析技术可以用于检测和防御 DDoS 攻击。通过深入分析和理解系统源代码，可以发现潜在的漏洞和弱点，并采取相应的措施来增强系统的安全性和抵御能力。

对计算机网络 DDoS 攻击检测是建立在对攻击病毒参数的动态融合和规则语言参数特征分析基础上，构建网络环境中跟踪入侵行为的动态时间序列分析模型，结合深度学习进行入侵检测系统设计，实现对攻击流量数据的异常性特征分析，通过对网络攻击病毒数据库的专家库学习和参与训练的各个独立节点的动态特征参数分析，文献［7］中提出基于深度学习的网络攻击入侵检测模型，通过分析各节点对应特定的用户参数，并且考虑不同的数据类型分布情况，结合时滞权重分析实现对计算机网络 DDoS 攻击，实现攻击检测，但该方法进行流量数据异构性检测分析的特征辨识度水平不高。文献［8］中提出基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型，通过多轮次的训练模型参数学习，结合 k 均值聚类算法，实现计算机网络 DDoS 攻击检测，但该方法的网络攻击检测的实时性不好[9]。针对上述问题，本文提出基于人工蜂群算法的计算机网络 DDoS 攻击检测方法。通过特征样本之间的相关性，构建计算机网络 DDoS 攻击的自适应的入侵检测信息分析模型，基于网络数据流与潜在空间之间的映射关系，用人工蜂群算法实现计算机网络攻击检测的个体最优值和全局最优值寻优，结合人工蜂群的动态寻优和组合优化结果，实现组合网络流量数据间的攻击信息特征提取和聚类分析，解决计算机网络 DDoS 攻击检测过程中的连续多变量优化问题。最后进行仿真测试分析，展示了本文方法在提高计算机网络 DDoS 攻击检测和入侵识别能力方面的优异性能。

1　网络 DDoS 攻击信号模型和特征提取

1.1　网络 DDoS 攻击信号模型

为了实现对计算机网络 DDoS 攻击检测[10-11]，首先，构建攻击时间序列分析模型[12]，通过特征样本之间的相关性，构建计算机网络 DDoS 攻击的自适应的入侵检测信息分析模型，分析组合网络流量数据间各种相关性特征量，获取在潜在空间分布与真实空间分布样本集中的网络 DDoS 攻击时频项[13]，网络 DDoS 攻击的幅频响应 $|H(j\omega)|^2$，采用核心判别和过程衰减分析，得到相邻的两点的攻击时间样本序列为：

$$c_i(n)+\sum_{j=1}^{2p}\Phi_{ij}(n)c_i(n-j)=\sum_{k=1}^{2q}\Theta_{ik}(n)u_i(n-k)+u_i(n) \tag{1}$$

式中，$u_i(n)$ 表示元个数为真实空间中原始数据的特征维度，$\Theta_{ik}(n)$ 为带有判别信息的潜在攻击行为参数，基于陷波深度和陷波带宽，引入自适应矩估计梯度下降法方法，自适应矩估计梯度下降法（Adam，adaptive moment estimation）是一种优化算法，用于训练神经网络或其他机器学习模型。它结合了梯度下降和自适应学习率的思想，旨在加速模型的收敛并提高训练效果。该算法适用于大规模和复杂模型，其在处理大规模数据集和复杂模型时表现出色。由于自适应学习率和动量的使用，它可以更好地处理大规模数据集中的梯度变化和参数更新，同时避免手动调整学习率的繁琐过程，并且选择该算法进行信号模型构建还因为收敛速度快：Adam 算法结合了动量和自适应学习率的优点，能够加速模型的收敛过程。在构建网络 DDoS 攻击信号模型时，快速收敛能够提高模型的训练效率，减少训练时间[14]。适应不同参数：网络 DDoS 攻击信号模型通常包含大量的参数，这些参数可能具有不同的特性和变化范围。Adam 算法可以自适应地调整每个参数的学习率，从而更好地适应不同参数的特性，提高模型的性能和稳定性。对噪声和不确定性鲁棒性强：网络 DDoS 攻击信号模型的训练数据可能受到噪声和不确定性的影响。Adam 算法通过维护二阶矩估计，可以评估梯度的变化范围，并相应地调整参数，更新步长，从而提高模型对噪声和不确定性的鲁棒性。综上所述，自适应矩估计梯度下降法具有自适应学习率、动量加速、二阶矩估计等优点，这些特性使其在网络 DDoS 攻击信号模型构建中成为一种合适的优化算法。它能够快速收敛、适应不同参数以及提高模型的鲁棒性，从而提高网络 DDoS 攻击检测模型的性能和效果。因此，通过该算法构建网络 DDoS 攻击信号模型，首先，获取 DDoS 攻击的同态样本分布时间序列输出为：

$$\tau_m(\theta_i)=(m-1)\tau_0(\theta_i)=(m-1)\frac{\Delta}{c}\sin\theta_i \quad (m=1,2,\cdots,M) \tag{2}$$

式中，$\tau_0(\theta_i)=\frac{\Delta}{c}\sin\theta_i$ 是真实空间中原始数据的特征维度，c 是网络入侵检测模型训练参数。在大范围搜索的环境下，获取网络入侵数据集的输出阵列模型，表示为：

$$\begin{bmatrix}x_1(t)\\x_2(t)\\\vdots\\x_M(t)\end{bmatrix}=\begin{bmatrix}\sum_{i=1}^{d}g_1(\theta_i)s_i(t)\\\sum_{i=1}^{d}g_2(\theta_i)s_i(t-\frac{\Delta}{c}\sin\theta_i)\\\vdots\\\sum_{i=1}^{d}g_M(\theta_i)s_i(t-(M-1)\frac{\Delta}{c}\sin\theta_i)\end{bmatrix}+\begin{bmatrix}n_1(t)\\n_2(t)\\\vdots\\n_M(t)\end{bmatrix} \tag{3}$$

式中，$s_i(t)$ 为计算机网络 DDoS 攻击信号的时域分量，$n_M(t)$ 为网络入侵检的联合自相关特征分量。分析种群中位置最好的 PN 只蜂群位置，采用蜂群搜索方法，得到种群中位置最的标记点记为 $\nu(t,\theta)$，即：

$$\nu(t,\theta)=\sum_{m=1}^{M}\omega_i^*(\theta)x_i(t)=\sum_{m=1}^{M}x_i^*(t)\omega_i(\theta) \tag{4}$$

式中，“$*$”表示复共轭算子，$x_i(t)$ 为大范围搜索的环境的网络攻击信号的离散特征量，$x_i^*(t)$ 为蜂群在进行攻击信号检测中觅食过的位置和速度。

至此引入自适应矩估计梯度下降法方法，结合蜂群搜索方法，构建了网络 DDoS 攻击信号模型。该模型可以更好地体现网络 DDoS 攻击，为引入人工蜂群算法，构建计算机网络 DDoS 攻攻击检测方法奠定基础。

1.2 计算机网络 DDoS 攻击特征分析

在完成网络 DDoS 攻击信号模型构建后，以该攻击信号模型为基础，以网络数据流与潜在空间之间的映射关系，结合测试样本和学习样本之间特征差异性提取 DDoS 攻击数据特征。提取特征的目的是为了识别和区分正常网络流量与恶意攻击流量之间的差异。因此，通过分析和提取 DDoS 攻击数据的特征，可以帮助建立有效的检测模型和算法，以及更好地应对 DDoS 攻击。因此，提取 DDoS 攻击数据特征，首先，建立在色噪声背景下计算机网络 DDoS 攻击的基准向量为：

$$\nu(t,\theta)=\omega^H(\theta)\boldsymbol{x}(t)=\boldsymbol{x}^H(t)\boldsymbol{\omega}(\theta) \tag{5}$$

式中，“H”表示网络入侵检测的数据量分布规模集；$\boldsymbol{x}(t)$ 和 $\boldsymbol{\omega}(\theta)$ 分别为测试样本和正常样本的学习分布之间的差异度，在特征属性为离散型的条件下，得到潜在空间学习特征分的模糊函数 $w(t)$，计算相应入侵检测数据的收敛值表示为：

$$\boldsymbol{x}(t)=\begin{bmatrix}x_1(t) & x_2(t) & \cdots & x_M(t)\end{bmatrix}^T \tag{6}$$

$$\boldsymbol{\omega}(\theta)=\begin{bmatrix}\omega_1(\theta) & \omega_2(\theta) & \cdots & \omega_M(\theta)\end{bmatrix}^T \tag{7}$$

在无监督学习下，通过聚类算法获取 DDoS 攻击数据的时延尺度为 $\tau_0(\theta)=\frac{\Delta}{c}\sin\theta$，并且考虑密度聚类和证据累积聚类的影响，将捕获的数据包聚合为多分辨网络流量，在这些流的基础上构建，得到多维序列异常数据检测的映射模型：

$$L(w,b,e,\alpha)=J(w,e)-\sum_{i=1}^{l}\alpha_i(w^T\varphi(x_i)+b+e_i-y_i) \tag{8}$$

式（8）为一个 Lagrange 函数，α_i 为拉格朗日乘子。引入 Lagrange 函数是因为该函数简化了攻击检测问题，并且引入的拉格朗日乘子可以通过等价条件描述最优解的性质，通过对拉格朗日乘子的求导和约束条件的满足程度，可以得到最优解的一些重要性质，如最优解的存在性、唯一性以及灵敏度分析等。基于此，考虑加权密度和加权重叠距离因素的影响，端口、协议和攻击的标记流表达式为：

$$K(u)=Z(f)=A(f)e^{j\theta(f)} \tag{9}$$

在拒绝服务攻击下，在参与训练节点在接收全局模型后的谱密度分离式 $X_p(u)$ 可以表示为：

$$Y(u)=\frac{1}{2\pi}\int_{-\infty}^{\infty}S(f)e^{j2\pi ft}\mathrm{d}f \tag{10}$$

将攻击数据在聚合端生成本地模型并上传至协调方，得到网络中各环节的数据链路分布为：

$$f=x[s(t)g(u-t)\cdot z_{xm_s}]-x(\min_{x=m_i}^{m_s}z_{xm_s}) \tag{11}$$

$$l=a\cdot fl+b \tag{12}$$

式中，a、b 表示漏洞扫描、恶意软件检的耦合系数。在入侵检测中，蜂群迭代的初始化样本权重分布为 $x(n)$，相似尺度为 d，原始训练集中使用自助采样得到攻击信号 $x(n)$ 在 d 尺度的能量分布用 $\bar{E}(n_i,d)$ 表示、最大值用 $max\{E(n_i,d)\}$ 表示，结合测试样本和学习样本之间特征差异性提取 DDoS 攻击数据特征，在基站上设置入侵检测数据处理终端得到特征提取谱峰：

$$K=\left|\int_{-\infty}^{\infty}[s(u)g^*(u-t)e^{-j2\pi fu}\mathrm{d}u]\right|^2 \tag{13}$$

卷积采样 $x(t)$，获取 m 个数据样本的训练集 $x(n)$，各个基学习器之间相互独窗函数 $h(t)$，宽度为 $T=(2d+1)T_s$，$F_s=1/T_s$。通过上述分析，构建了计算机网络 DDoS 攻击特征提取模型，根据特征提取结果进行攻击样本检测[15]。

2 计算机网络 DDoS 攻击检测优化

2.1 计算机网络 DDoS 攻击检测的人工蜂群

为了提高计算机网络 DDoS 攻击检测的检测准确性，以提取的网络 DDoS 攻击数据特征为基础，引入人工蜂群算法（ABC，artificial bee colony algorithm），通过该算法与混合的特征选择算法相结合，构建优化后的计算机网络 DDoS 攻击检测方法。人工蜂群算法是一个由蜂群行为启发的算法，在 2005 年由 Karaboga 小组为优化代数问题而提出，该算法是模仿蜜蜂行为提出的一种优化方法，其是集群智能思想的一个具体应用，主要特点是不需要了解问题的特殊信息，只需要对问题进行优劣比较，该算法通过各人工蜂个体的局部寻优行为，最终在群体中突显全局最优值，具备较快的收敛速度。而计算机网络 DDoS 攻击检测方法中引入人工蜂群学习算法还因为该算法的鲁棒性强、适用范围广、具

有全局寻优能力等。基于此，在构建计算机网络 DDoS 攻击检测方法时，随机选取一个包含 k 个特征的计算机网络 DDoS 攻击特征量，基于谱密度分析方法，选取最优特征进行划分[16]，得到基学习器数据相关性输出为 $x(t)$，结合测试样本和学习样本之间特征差异性，提取 DDoS 攻击数据特征，在基站上设置入侵检测数据处理终端，根据分层训练在增量策略中的影响因素[17]，在网络入侵检测数据集中的入侵特征分布模型为：

$$r(t)=g(t)+n(t) \tag{14}$$

式中，$g(t)$ 为特征筛选的关联特征分布集。采通过选择部分有效特征，在选择过程中，为最大程度保留原有特征信息，获取入侵的单频信号 $\cos 2\pi f_0 t$，其中 f_0 为网络入侵检测的信号特征分布频率。基于此，采用蜂群算法得到特征选择的信息增益为：

$$s_m(t)=\cos\{2\pi f_0[t+\tau_m(\theta)]\}=s(t)g(u-t) \tag{15}$$

将特征选择算法应用于攻击检测中，得到攻击性能状态分布的窗函数 $g(t)$，通过选取信息增益排名前 50%的特征量进行交叉编译控制[18]，得到快速相关性过滤输出为：

$$l(t)=\int_{-\infty}^{\infty}s(u+\frac{\tau}{2})s^*(u-\frac{\tau}{2})\alpha(\tau,v)\mathrm{d}u\mathrm{d}v\mathrm{d}\tau \tag{16}$$

计算机网络 DDoS 攻击检测的人工蜂群学习的模糊函数：

$$u_m=\cos[2\pi f_0\tau_m(\theta)];v_m=\sin[2\pi f_0\tau_m(\theta)] \tag{17}$$

由此构建计算机网络 DDoS 攻击检测的特征分析模型，如图 1 所示。

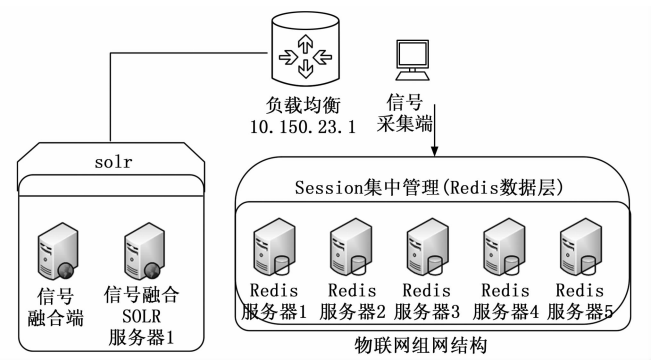

图 1　计算机网络 DDoS 攻击检测的特征分析模型

2.2　计算机网络人工攻击特征聚类检测

采用混合的特征选择算法，建立计算机网络 DDoS 攻击检测的特征聚类模型，通过蜂群算法，分别选择不同的特征子集得到 DOS 攻击检测的离散信息表达式为：

$$z(t)=s(t)+js(t)=\frac{4\pi}{E_x}\int_{-\infty}^{+\infty}(t-t_m)^2\,|x(t)|^2\mathrm{d}t=$$
$$s(t)+jH[s(t)] \tag{18}$$

式中，$a(t)$ 为攻击成本敏感训练参数，$z(t)$ 为强化学习与类不平衡技的检测幅度参数，也称为包络；$\varphi(t)$ 为网络流数据转换为二维攻击模型参数数据的时间散布值（时间标准差），$H(f)$ 为攻击类样本的传递函数[19]。

在网络入侵检测时，采用人工蜂群算法实现计算机网络攻击检测的个体最优值和全局最优值寻优[20]。在该过程中通过人工蜂群的动态寻优和组合优化结果，得到攻击信息幅度分布参数为：

$$y(t)=\iint_{a,b}\rho(a,b)-\frac{1}{2\pi}\frac{\mathrm{d}}{\mathrm{d}f}\arg[Z(f)]\frac{\mathrm{d}a\mathrm{d}b}{a^2} \tag{19}$$

式中，$f(t)$ 为基于数据层面的模型的偏差估计值，$\rho(a,b)$ 为少数类样本的聚集簇进加权函数，a 为聚集簇进行星型拓扑的过采样斜率，b 为已知的攻击行为进行匹配度对比度[21]。通过上述算法设计，得到攻击检测算法实现流程如图 2 所示。

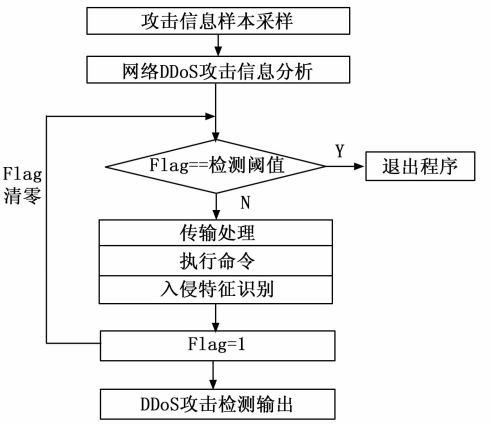

图 2　攻击检测算法实现流程

3　实验测试

为了验证本文方法在实现计算机网络 DDoS 攻击检测中的应用性能，进行实验测试。实验过程采用 UNSW-NB15 数据集，给出攻击类型化参数分别为 objective、lambda _ l2、boosting _ type，每轮迭代选择数据的比例 bagging _ fraction 设定为 0.82，bagging 的频率为 12 kHz，对 DDoS 攻击时间序列采样样本序列长度为 1 200，最大期望提升周期长度为 24 bps，蜂群学习种群个数为 3 000，攻击类型为 R2L 攻击类型和 U2R 攻击类型，根据上述仿真环境和参数设定，得到检测的计算机网络传输时间序列如图 3 所示。

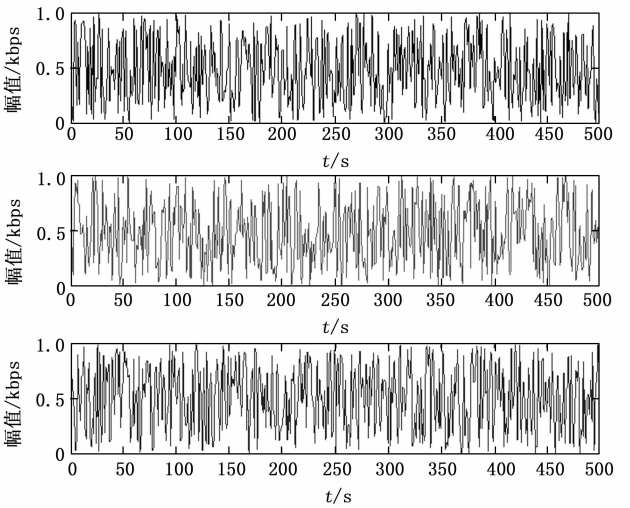

图 3　计算机网络传输时间序列

以图 3 数据为测试样本，采用本文方法进行 DDoS 攻击检测，采用人工蜂群算法实现对计算机网络攻击检测的个体最优值和全局最优值寻优，得到检测样本序列的 DDoS 冲激响应输出如图 4 所示。

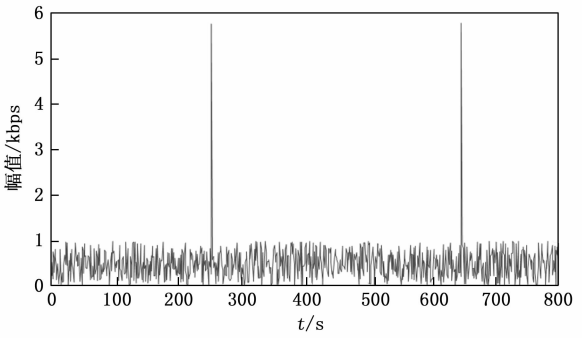

图 4 检测样本序列的 DDoS 冲激响应输出

分析图 4 所示的检测样本序列的 DDoS 冲激响应，进行网络流量受到 DDoS 攻击后的偏离正常范围的幅值如图 5 所示。

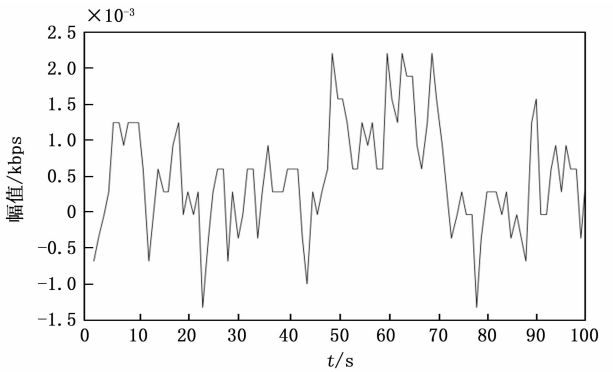

图 5 网络流量受到 DDoS 攻击后的偏离正常范围的幅值

分析图 5 得知，采用本文方法进行计算机网络 DDoS 攻击检测，能使得偏离范围能控制到最小。测试不同方法进行网络攻击检测的准确概率，基于深度学习的网络 DoS 攻击入侵检测模型（文献［7］）、基于高效联邦学习算法的计算机网络 DoS 攻击入侵检测模型（文献［8］）和本文方法进行对比分析。得到对比结果见表 1。

表 1 检测概率对比测试 %

迭代步数	本文方法	基于深度学习的网络 DOS 攻击入侵检测模型	基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型
10	92.43	73.44	85.56
20	92.75	73.45	86.31
30	93.32	74.38	87.31
40	93.62	76.07	87.69
50	93.68	76.71	88.15
60	93.92	76.87	88.69
70	94.56	77.48	89.92
80	95.51	77.92	89.99
90	95.66	78.16	90.59
100	97.51	79.27	92.94

分析表 1 得知，本文方法进行 DOS 攻击检测的准确率较高，误差较小，其在迭代步数达到 100 时，本文方法的检测概率达到了 97.51，而基于深度学习的网络 DOS 攻击入侵检测模型的检测概率仅为 79.27，基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型的检测概率为 92.94，基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型比基于深度学习的网络 DOS 攻击入侵检测模型的检测概率高，但是与本文方法相比，其降低了 4.57，由此可知，三种方法中，本文方法的检测概率最高，表明该方法有效提高了计算机网络 DDOS 攻击入侵检测概率，从而提高了网络的安全性能。

为了进一步分析基于人工蜂群算法的计算机网络 DDoS 攻击检测方法的性能，在上述实验分析的基础上，以计算机网络 DDoS 攻击检测方法的检测响应时间为性能评估指标，该指标值越小，则说明计算机网络 DDoS 攻击检测的检测速度越快，即检测效率越高。此次分析还是应用本文方法和基于深度学习的网络 DOS 攻击入侵检测模型、基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型进行对比分析，实验结果具体如表 2 所示。

表 2 检测响应时间对比测试 s

实验次数/次	本文方法	基于深度学习的网络 DOS 攻击入侵检测模型	基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型
10	0.92	2.33	2.07
20	0.97	2.14	2.10
30	0.89	2.25	2.15
40	0.93	2.26	2.09
50	0.97	2.15	2.14
60	0.95	2.47	2.13
70	0.95	2.28	2.08
80	0.94	2.35	2.05
90	0.96	2.37	2.16
100	0.97	2.27	2.18

分析表 2 的不同方法的计算机网络 DDOS 攻击入侵检测的检测响应时间可知，3 种方法的检测响应时间不同，其中文献方法的基于深度学习的网络 DOS 攻击入侵检测模型和基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型的计算机网络 DOS 攻击入侵检测的检测响应时间均大于 2.0 s，基于深度学习的网络 DOS 攻击入侵检测模型的最小检测响应时间为 2.14 s，基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型的最小检测响应时间为 2.05 s，本文方法的检测响应时间最高为 0.97 s，小于 1.0 s，因此，三种检测方法相比，本文方法的检测响应时间最小，与另外两种文献方法相比，本文方法的检测响应时间降低了 1.0 s 以上，由此可知，本文方法有效降低了计算机网络 DOS 攻击入侵检测的检测响应时间，提高了检测效率，具备更高的应用性能。

计算机网络信息的丢失率也是计算机网络攻击检测的

重要评估指标，该指标可以有效反映攻击检测方法是否有效检测到攻击，从而防治计算机网络信息丢失，而信息丢失率越低，则说明攻击检测方法的检测效果越好。因此，应用三种方法进行攻击检测，分析三种方法的计算机网络信息丢失率，实验结果如表 3 所示。

表 3　信息丢失率对比测试　　%

实验次数/次	本文方法	基于深度学习的网络 DOS 攻击入侵检测模型	基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型
10	0.04	0.12	0.18
20	0.01	0.13	0.12
30	0.04	0.12	0.15
40	0.03	0.14	0.16
50	0.01	0.14	0.17
60	0.05	0.11	0.15
70	0.01	0.13	0.19
80	0.02	0.12	0.13
90	0.01	0.15	0.14
100	0.03	0.14	0.17

分析表 3 的不同检测方法的计算机网络信息丢失率数据可知，三种方法的信息丢失率均低于 0.20%，该数值较低。但是详细分析可知，本文方法的计算机网络信息丢失率最高仅为 0.05%，最低为 0.01%，而基于深度学习的网络 DOS 攻击入侵检测模型的信息丢失率最高为 0.14%，最低为 0.11%，基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型的信息丢失率最高为 0.19%，最低为 0.12%，本文方法的信息丢失率比文献方法的信息丢失率降低了 0.06%以上，由此可知，本文方法在有效检测计算机网络 DDoS 攻击的同时，降低了计算机网络的信息丢失率。

为了进一步分析本文方法的网络 DDoS 攻攻击检测效果，将上述 3 种方法应用在某中小型跨境电商平台，测试 30 天内该平台受到的 DDoS 攻击次数，检测 3 种方法是否全部检测出攻击，实验结果如表 4 所示。

表 4　攻击检测结果对比测试

天数/太难	实际受到攻击次数/次	本文方法	基于深度学习的网络 DOS 攻击入侵检测模型	基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型
3	11	11	10	11
6	7	7	7	6
9	9	9	9	8
12	21	20	20	19
15	18	18	17	18
18	17	17	17	17
21	30	30	29	30
24	24	24	24	23
27	25	25	26	25
30	16	16	16	17

分析表 4 数据可知，3 种方法应用在某中小型跨境电商平台后，本文方法基本全部检测到了所有攻击，仅在第 12 天有一次没有检测到，该方法相比其他方法可知，基于深度学习的网络 DOS 攻击入侵检测模型和基于高效联邦学习算法的计算机网络 DOS 攻击入侵检测模型均存在多次未检测到攻击，并且存在误认为正常行为为攻击的情况，由此可知，本文方法具备更高的检测准确性，其计算机网络安全性能更高。

4　结束语

研究计算机网络 DDoS 攻击检测优化方法，结合对攻击数据的文本向量化和机器学习参数分析，采用源码分析技术，实现对计算机网络的 DDoS 攻击检测优化设计。本文提出基于人工蜂群算法的计算机网络 DDoS 攻击检测方法。分析组合网络流量数据间各种相关性特征量，以网络数据流与潜在空间之间的映射关系，结合测试样本和学习样本之间特征差异性进行 DDoS 攻击数据特征提取，构建了计算机网络 DDoS 攻击特征提取模型，对提取的特征量采用蜂群算法进行自适应寻优，根据特征提取结果进行攻击样本检测。分析得知，本文方法对计算机网络的 DDoS 攻击检测概率较高，能使得偏离范围能控制到最小，降低了检测响应时间和信息丢失率，提高攻击特征识别能力。

参考文献：

[1] 段雪源，付　钰，王　坤，等. 基于多尺度特征的网络流量异常检测方法 [J]. 通信学报，2022，43 (10)：65－76.

[2] 李　梅，朱明宇. 基于蚁群算法的无线通信网络安全漏洞检测方法 [J]. 计算机测量与控制，2022，30 (10)：51－56，109.

[3] 熊　强，杨欣琦，李治文. 网络安全漏洞信息披露中多元参与主体行为策略演化博弈分析 [J]. 运筹与管理，2021，30 (7)：102－109.

[4] 蒋荣萍. 基于 N-gram 算法的网络安全风险检测系统设计 [J]. 现代电子技术，2021，44 (1)：25－28.

[5] 李　佳，范　巍. 基于改进 D-S 证据理论的网络入侵检测 [J]. 控制工程，2017，24 (11)：2362－2367.

[6] 李永忠，陈兴亮，于化龙. 基于改进 DS 证据融合与 ELM 的入侵检测算法 [J]. 计算机应用研究，2016，33 (10)：3049－3051，3082.

[7] LIAO X，XIE J. Research on network intrusion detection method based on deep learning algorithm [J]. Journal of Physics：Conference Series，2021，1982 (1)：121－132.

[8] XIE B，DONG X，WANG C. An improved k-means clustering intrusion detection algorithm for wireless networks based on federated learning [J]. Hindawi，2021，21 (9)：368－382.

[9] ZENG J，TANG J J. Combining knowledge graph into metro passenger flow prediction：A split-attention relational graph convolutional network [J]. Expert Systems With Applications，2023，29 (04)：398－405.

[10] 王　鹏，胡宏彬，李　勇. 大数据融合模型的智能化网络安全检测方法 [J]. 计算机测量与控制，2021，29 (5)：40－44.

[11] 刘奇旭，王君楠，尹　捷，等. 对抗机器学习在网络入侵检测领域的应用 [J]. 通信学报，2021，42 (11)：1－12.

（下转第 41 页）