计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(4):216−221 [doi: 10.15888/j.cnki.csa.007649]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于深度学习的 DDoS 攻击检测模型①

奚玉龙

(安徽省第二人民医院, 合肥 230041)
通讯作者: 奚玉龙, E-mail: laraech@aliyun.com

摘　要: 构建了基于粒子群优化卷积神经网络 (PSO-CNN) 的分布式拒绝服务攻击 (DDoS) 攻击检测模型. 利用卷积神经网络的权值共享和最大池化自动挖掘网络数据流特征, 引入粒子群对卷积核进行优化, 在提升模型训练效率的同时, 增强了模型的全局寻优能力. 实验结果表明, 该模型能够有效检测 DDoS 攻击, 具有较高的检测准确率.

关键词: 分布式拒绝服务攻击; 卷积神经网络; 粒子群; 准确率

引用格式: 奚玉龙.基于深度学习的 DDoS 攻击检测模型.计算机系统应用,2021,30(4):216–221. http://www.c-s-a.org.cn/1003-3254/7649.html

DDoS Attack Detection Model Based on Deep Learning

XI Yu-Long

(Anhui No.2 Provincial People's Hospital, Hefei 230041, China)

Abstract: This study constructs a Distributed Denial-of-Service (DDoS) attack detection model based on Particle Swarm Optimization-Convolutional Neural Network (PSO-CNN). First, it uses the weight sharing and maximum pooling of CNN to automatically mine the features of data streams. Then, it applies PSO to the convolution kernel, thus increasing the training efficiency and enhancing the global optimization. In conclusion, the model proposed in this study has high detection accuracy for DDoS attacks.

Key words: DDoS attack; Convolutional Neural Network (CNN); particle swarm; accuracy

计算机网络技术的飞速发展给社会生活和经济发展带来了新机遇, 但网络攻击给网络安全带来了巨大的风险[1,2]. 分布式拒绝服务攻击 (DDoS) 在攻击过程使用常见的协议和服务, 准确检测的难度很高. 因此, 对 DDoS 攻击的高性能检测对维护网络安全具有重要意义[3].

针对 DDoS 攻击检测问题, 研究人员提出了很多方法[4,5]. 例如, 文献 [6] 构建了基于 BP 神经网络的 DDoS 攻击检测模型, 采用数据包长度、数据包发送时间等特征检测 DDoS 攻击, 取得了很好的检测效果. 文献 [7] 针对软件定义网络攻击, 提出了基于支持向量机和 K 均值聚类的攻击检测算法, 提高了检测效率. 文献 [8] 提出了基于组合相关度随机森林的 DDoS 攻击检测方法, 具有较低的误报率和漏报率. 这些方法均存在特征主观依赖性较强, 检测模型泛化能力差的问题. 文献 [9] 将深度神经网络应用于 DDoS 攻击检测, 模型泛化能力较强, 但训练效率较低.

本文首先基于卷积神经网络 (CNN) 构建了 DDoS 攻击检测模型, 实现了 DDoS 攻击的高准确率检测. 然后, 引入粒子群算法 (PSO), 对卷积神经网络的卷积核进行优化, 提高模型训练效率, 并与梯度下降方法相结合, 增加模型全局寻优能力.

1　卷积神经网络

CNN 是一种具有深度结构的前馈神经网络, 广泛应用于计算机视觉及自然语言处理等领域[10]. CNN 的

① 收稿时间: 2020-03-19; 修改时间: 2020-04-21; 采用时间: 2020-04-28; csa 在线出版时间: 2021-03-30

主体架构包括卷积层、池化层、全连接层、输入层和输出层, 其中卷积层与池化层是 CNN 的核心.

1.1 卷积层

卷积层输入通常为多维数组, 卷积运算可以看作以卷积核为中心, 不断在输入数据上进行滑动卷积操作的过程, 具体实现过程如下. 首先, 将卷积层中的卷积核与输入数组对应位置的元素进行相乘后计算和值, 然后不断滑动卷积核直到所有输入数据均完成上述操作. 假设 CNN 的输入数据为二维数组x_{ij}, $1 \le i \le N_1$, $1 \le j \le N_2$, 令f_{uv}表示卷积层中的二维卷积核, $1 \le u \le n_1$, $1 \le v \le n_2$. 通常情况下, 卷积核长度小于输入数组长度, 即$n_1 \le N_1$, $n_2 \le N_2$. 此时, 卷积层的输出可以表示为:

$$(x*f)_{ij} = \sum_{u=1}^{n_1}\sum_{v=1}^{n_2} f_{uv}x_{i-u+1,j-v+1} \tag{1}$$

上述二维数据卷积操作的过程如图 1 所示.

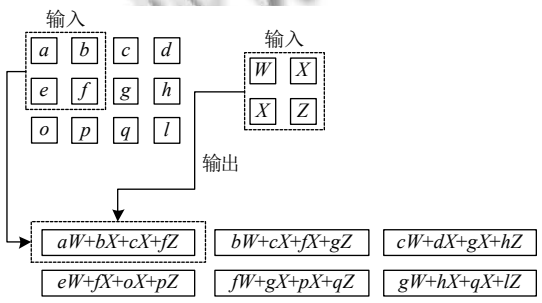

图 1 卷积操作过程

传统人工神经网络的输入层、输出层与神经元层之间的连接通常都是由矩阵乘法构建的全连接结构, 结构十分复杂. CNN 中, 每个输出并不是与各个输入均连接, 而是只连接部分输入, 有效地减少了网络参数, 降低了网络训练的复杂度. CNN 的局部连接使得网络底层只对局部信息进行感知, 在高层将底层信息进行综合, 有效地提高了网络的局部特征提取能力. 并且, CNN 的卷积层中, 权值是可以共享的. CNN 的局部连接和权值共享使其在训练效率和存储需求上均优于传统神经网络, 具有较低的时间和空间复杂性.

1.2 池化层

池化层位于卷积层之后, 通过池化来降低卷积层输出的特征向量, 同时改善训练结果, 避免网络出现过拟合现象. 池化过程是选取某一个位置的总体特征作为该位置的输出, 在保留总体信息的同时, 降低特征参数的维度和网络参数数量. CNN 中的常用池化方法有平均池化法和最大池化法, 平均池化是指提取相邻区域特征值的平均值, 最大池化则提取相邻区域内的特征值的最大值, 图 2 给出了最大池化特征提取过程.

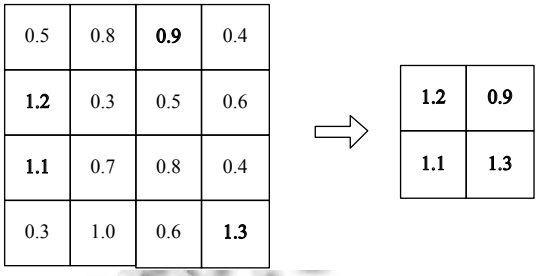

图 2 最大池化过程 (2×2)

如果网络输入为100×100的矩阵, 经过一层池化后, 转化为50×50的矩阵, 显著降低了特征维数, 提高了网络训练效率.

2 PSO 优化 CNN 检测模型

2.1 粒子群优化

PSO 是一种源于鸟群捕食过程的启发式优化算法, 实现疑难问题的优化. PSO 结构简单、计算量小、收敛速度快, 且全局寻优能力强, 在函数优化、系统控制等复杂问题优化领域有着十分广泛的应用[11].

卷积核优化是 CNN 的核心问题, 直接影响了 CNN 的性能. 考虑到 PSO 优化算法的优良寻优性能和快速收敛能力, 将其由于优化 CNN 的卷积核. PSO 优化过程可以总结为各个微粒i的位置与速度、全局极值P_g和个体极值P_i不断更新, 优化的核心是微粒速度与位置的更新. 假设$v_i(t)$表示 t 时刻粒子速度, $X_i(t)$表示 t 时刻粒子位置, 则速度更新过程为:

$$v_i(t+1) = \omega v_i(t) + c_1 r_1 [P_i(t) - X_i(t)] + c_2 r_2 \left[P_g(t) - X_i(t)\right] \tag{2}$$

位置更新过程为:

$$X_i(t+1) = X_i(t) + v_i(t+1) \tag{3}$$

式中, ω代表粒子更新过程的惯性权重, 惯性权重能够有效平衡 PSO 优化的全局搜索能力和局部搜索能力, c_1和c_2表示学习因子, r_1和r_2是位于 0 和 1 之间的随机数.

2.2 算法框架

利用 CNN 实现网络攻击检测具有一定的可行性, 但是存在两个问题, 一是网络容易陷入局部最优值, 二

是网络的卷积核难以初始化, 限制了网络性能. 为此, 本文将 PSO 优化算法引入 CNN, 构建了基于优化 CNN 的攻击检测模型, 模型结构如图 3 所示, 具体步骤介绍如下.

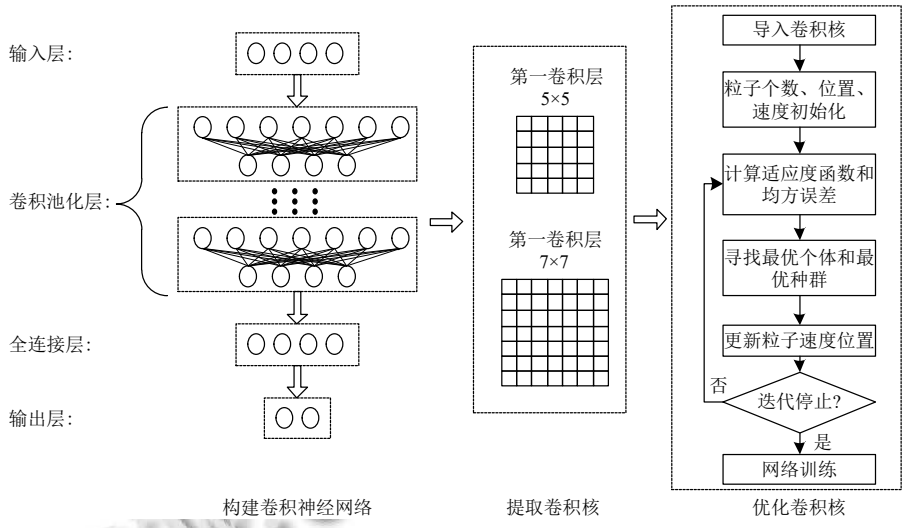

图 3 PSO 优化 CNN 攻击检测模型

步骤 1. 构建 CNN 模型. 将 DDoS 攻击数据输入, 采用随机方式初始化 CNN 的各层卷积核, 卷积层与池化层交替布置, 池化层特征数量与其前一个卷积层相同, 网络最后为全连接层, 导出一维向量给输出层, 实现网络攻击的检测.

步骤 2. PSO 优化卷积核. 从 CNN 的各个卷积层中提取出卷积核作为 PSO 的初始种群, PSO 适应度函数为网络输入与网络输出之间的均方误差. 假设输入输出数据共有 n 组, 适应度函数可以表示为:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(T_i - P_i)^2 \tag{4}$$

其中, P_i和T_i分别表示第 i 组输入和输出的数据. 利用 PSO 寻优不断更新粒子速度和位置进行寻优, 通过训练修正权值, 给出最优的权值参数.

步骤 3. 梯度下降网络训练. 将步骤 2 得出的最优卷积核导入到 CNN 进行训练, 基于梯度下降法实现网络权值寻优, 实现 PSO 全局最优能力和梯度下降局部最优相结合, 最终实现网络攻击检测.

2.3 关键技术

(1) PSO 初始化卷积核

从分布式拒绝服务数据训练集中随机选取出部分数据以及对应的分类标签构建测试集合. 根据 CNN 理论, 网络特征图的数量是由滤波器数量决定的, 而 CNN 的主要权值就是卷积层中的卷积核, 因此由网络各层的卷积核构建 PSO 的初始种群. PSO 优化的位置信息为整个网络权值空间, 且设置最大粒子速度区间, 位置参数和速度参数上均采用随机初始化方法, PSO 种群规模与 CNN 卷积核个数保持一致.

随机选取部分网络攻击数据和对应标签作为 CNN 的输入, 以网络输出和输入的均方误差作为 PSO 的适应度函数. 以各个粒子坐标作为粒子位置, 计算个体的适应度函数值, 通过 PSO 进化不断更新粒子速度和位置, 对比各个粒子的适应度函数值, 当满足迭代终止条件时, PSO 寻优结束, 算法具体步骤如图 4 所示.

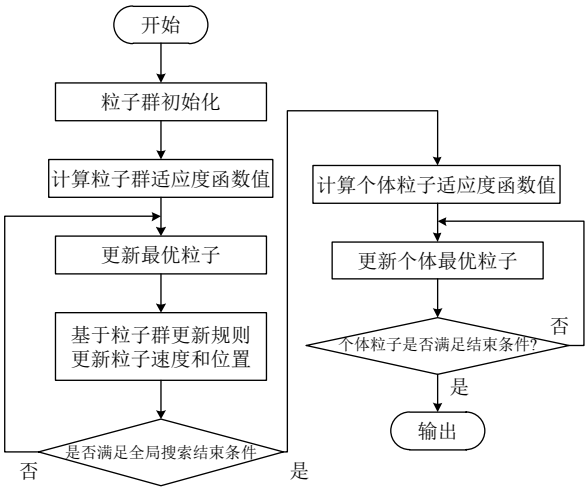

图 4 PSO 优化卷积核流程

(2) PSO 结合梯度下降

基于 PSO 的优良全局最优能力, 不断更新迭代粒子位置和速度, 得出一组最优粒子, 用最优粒子初始化 CNN 卷积核, 对新 CNN 进行重新训练. 经过卷积和池化后, 特征值输入到全连接层转化为一维特征向量, 最后利用输出层实现网络攻击检测. 输出值与样本标签之间的误差作为反向传播依据, 基于梯度下降法进行网络权值修正. 上述训练过程将 PSO 全局最优能力与 CNN 局部搜索能力相结合, 能够有效避免 CNN 陷入局部最优, 具体流程如图 5 所示.

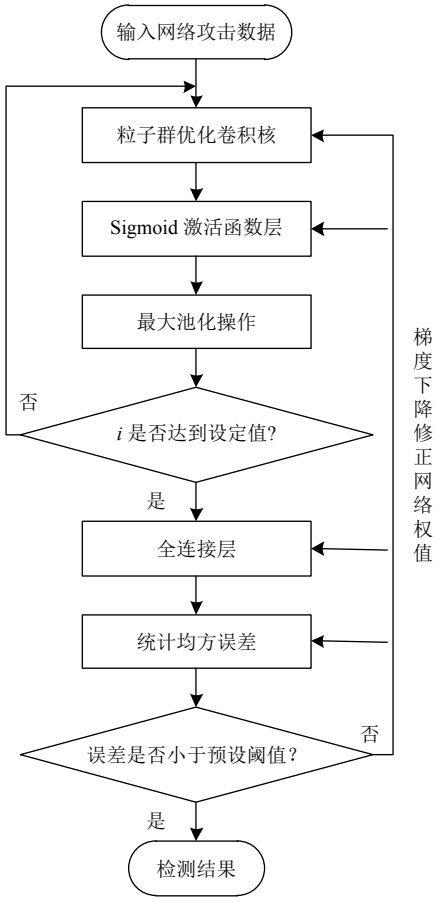

图 5 PSO 结合梯度下降

3 实验与分析

3.1 实验条件

实验基于 Tensorflow 框架构建 CNN 模型, 采用 Python 语言实现 PSO 优化程序, 硬件环境为戴尔 T640 类型的 GPU 运算服务器, 软件环境为 Windows 10 操作系统.

实验数据分为网络正常数据 (正常流) 和 DDoS 攻击数据 (攻击流), 正常流数据为自动获取, 而攻击流数据为自动获取与人工构建相结合. 数据集总量为 10 万条, 按照正常流与攻击流比例随机将数据分为训练集和测试集, 其中训练集 8 万条数据, 测试集 2 万条数据, 具体如表 1 所示.

表 1 实验数据集 (单位: 条)

数据集	正常流数据	攻击流数据
训练集	30000	50000
测试集	8000	12000

3.2 评估指标

利用准确率、召回率、精确率、$F1$ 值和混淆矩阵对模型的 DDoS 攻击检测进行性能评价. 准确率定义为检测模型检测正确的数据数量占总数据量的比例, 计算方法为:

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \tag{5}$$

其中, TP 表示攻击流样本数据被模型正确检测为攻击流数据的样本数量, TN 表示正常流样本数据被模型检测为正常流数据的样本数量, FP 表示正常流样本数据被模型检测为攻击流数据的样本数量, FN 表示攻击流数据被模型检测为正常流的样本数量.

召回率定义为检测模型判定为攻击流数据占所有攻击流数据的比例, 计算方法为:

$$R = \frac{TP}{TP+FN} \tag{6}$$

精确率定义为检测模型判定为攻击流数据中, 确实为攻击流数据的比例, 计算方法为:

$$P = \frac{TP}{TP+FP} \tag{7}$$

$F1$ 值定义为精确率和召回率之间的调和平均值, 能够较好低评估 DDoS 攻击检测模型的性能, 计算方法为:

$$F1 = \frac{2PR}{P+R} \tag{8}$$

混淆矩阵是评价检测模型的常用指标, 能够有效描述检测模型检测结果与样本标签之间的匹配程度, 有利于校验模型的检测能力.

3.3 结果分析

不同深度 CNN 的检测能力不同, 目前缺乏设置 CNN 架构的理论结论. 大量测试结果表明, CNN 的架

构对于 DDoS 攻击检测具有较大影响, 实验中选取了 4 种典型的 CNN 结构进行对比分析.

考虑到模型训练效率, 采用小批量训练, batch 大小设置为 50, 共构建了 4 型 CNN, 分别为 C3P2F2、C3P3F3、C2P2F2、C2P2F4, 其中 C3P3F3 表示该 CNN 有 3 个卷积层、3 个最大池化层和 3 个全连接层, 其它网络定义相同, 网络激活函数均采用 Sigmoid 函数. 采用表 1 中数据集分别对 4 型 CNN 进行对比测试, 4 型 CNN 的准确率、召回率、精确率、*F*1 值统计结果如表 2 所示.

表 2　不同类型 CNN 检测结果 (%)

模型结构	*ACC*	*R*	*P*	*F*1
C3P2F2	97.35	98.09	97.92	98.00
C3P3F3	97.39	97.93	97.83	97.87
C2P2F2	95.43	96.53	96.90	96.71
C2P2F4	94.34	96.47	96.20	96.33

结果表明, 3 层 CNN(C3P2F2、C3P3F3) 对 DDoS 网络攻击的检测性能显著优于 2 层 CNN(C2P2F2、C2P2F4). 3 层 CNN 中, C3P2F2 的精确度、召回率以及 F1 值指标性能优于 C3P3F3, 但检测准确率不如 C3P3F3. 为进一步比较 4 型 CNN 对 DDoS 的检测性能, 图 6 给出了 4 型 CNN 的混淆矩阵.

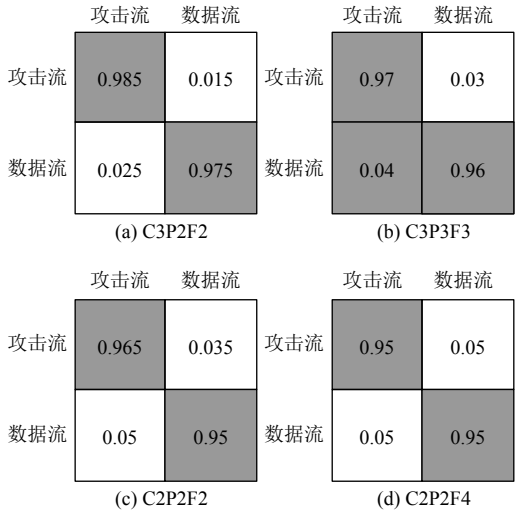

图 6　不同 CNN 检测混淆矩阵

图 6 表明, 2 层 CNN 对于正常流数据和攻击流数据的判型能力上均弱于 3 层 CNN, 这与表 2 指标结果保持一致. 对比 C3P2F2 和 C3P3F3 混淆矩阵可知, C3P2F2 对于攻击流数据的检测能力优于 C3P3F3. 在网络运行过程中, 一旦出现 DDoS 攻击机会对整个计算机网络系统的正常运行带来很大的隐患, 因此网络攻击检测模型必须要对攻击流数据敏感, 因此 C3P2F2 更适合于符合实际对 DDoS 攻击进行检测的需求.

C3P2F2 模型检测精度较高, 由于模型层数较深、数据规模大, 因此训练过程中收敛速度慢, 难以满足实际需求, 且易陷入局部最优. 为了提高 CNN 训练效率以及避免 CNN 陷入局部最优, 本文构建了基于 PSO 优化 CNN 的 DDoS 攻击检测模型, 下面通过实验测试其性能. 图 7 给出了原始 C3P2F2 模型和经过 PSO 优化后 C3P2F2 模型检测准确率与训练次数之间的关系.

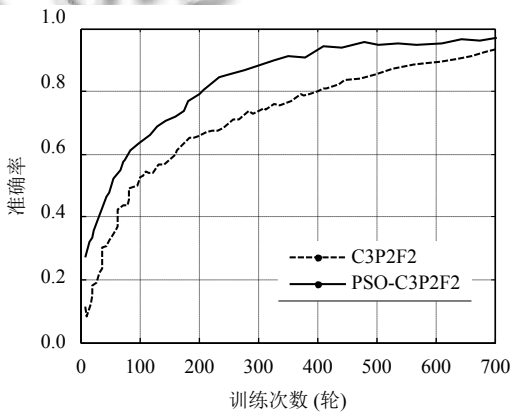

图 7　PSO 优化性能测试

实验结果表明, 经过 PSO 优化后, 显著加快了 CNN 的训练速度. 为了进一步测试本文构建 PSO 优化 CNNDDoS 攻击检测模型 (PSO-C3P2F2) 性能, 将其分别与目前常用 DDoS 攻击检测模型中的支持向量机模型 (SVM)[7]、随机森林 (RF) 模型[8] 进行同等条件下的检测性能对比, 每种模型进行 10 次试验, 统计指标平均值, 结果如表 3 所示.

表 3　不同模型检测性能对比 (%)

检测方法	*ACC*	*R*	*P*	*F*1
SVM	94.57	95.39	94.27	94.82
RF	95.54	96.43	96.15	96.29
C3P2F2	97.35	98.09	97.92	98.00
PSO-C3P2F2	98.13	98.52	98.40	98.46

从表 3 结果可知, C3P2F2 模型在各个指标上的性能均优于 SVM 模型和 RF 模型, 且 PSO-C3P2F2 模型相比 C3P2F2 模型有略微提升. 这是因为, SVM 模型和 RF 模型均需要人为选取特征向量, 不能很好地表征 DDoS 攻击数据特征, 而 C3P2F2 模型能够自适应提

取隐含在数据中的局部特征, 避免受到主观因素影响, 因此检测性能优于传统机器学习方法. PSO-C3P2F2 模型检测性能的提升是由于将 PSO 的全局寻优能力与 CNN 局部最优能力相结合, 能够有效避免 CNN 陷入局部最优.

4 结束语

研究了 DDoS 攻击检测问题, 构建了基于 CNN 的攻击检测模型, 利用权值共享和最大池化实现了 DDoS 攻击的高准确率检测. 针对训练效率偏低的问题, 引入 PSO 对 CNN 的训练过程进行优化, 提高网络训练效率和全局寻优能力.

参考文献

1 于亚芳, 潘耘, 王励成. 命名数据网络中的 DoS/DDoS 攻击研究综述. 信息技术, 2017, (6): 78–82, 87.

2 冯晓荣. 基于人工蜂群算法的双门限 CRN 网络攻击检测算法. 计算机应用与软件, 2019, 36(10): 316–322, 333. [doi: 10.3969/j.issn.1000-386x.2019.10.054]

3 张龙, 王劲松. SDN 中基于信息熵与 DNN 的 DDoS 攻击检测模型. 计算机研究与发展, 2019, 56(5): 909–918. [doi: 10.7544/issn1000-1239.2019.20190017]

4 程杰仁, 罗逸涵, 唐湘滟, 等. 基于 LSTM 流量预测的 DDoS 攻击检测方法. 华中科技大学学报 (自然科学版), 2019, 47(4): 32–36.

5 余学山, 韩德志, 杜振鑫. 基于智能蜂群算法的 DDoS 攻击检测系统. 计算机科学, 2018, 45(12): 123–129.

6 杨可心, 桑永胜. 基于 BP 神经网络的 DDoS 攻击检测研究. 四川大学学报 (自然科学版), 2017, 54(1): 71–75.

7 马乐乐, 束永安. SDN 环境下基于机器学习算法的 DDoS 攻击检测模型. 微电子学与计算机, 2018, 35(5): 15–20.

8 李梦洋, 唐湘滟, 程杰仁, 等. 基于组合相关度的随机森林 DDoS 攻击检测方法. 郑州大学学报 (理学版), 2019, 51(2): 23–28, 39.

9 Priyadarshini R, Barik RK. A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences, 2019, 23(3): 55–63.

10 罗靖遥, 黄征. 基于 CNN 分类器和卷积的目标检测. 信息技术, 2017, (9): 101–104, 108.

11 吴旋, 来兴平, 郭俊兵, 等. 综采面区段煤柱宽度的 PSO-SVM 预测模型. 西安科技大学学报, 2020, 40(1): 64–70.