doi: 10.13413/j.cnki.jdxblxb.2024257

SDN 中基于 φ-熵与 IDBO-RF 的 DDoS 攻击联合检测模型

高新成[1], 王启龙[2], 王莉利[2]
(1. 东北石油大学 现代教育技术中心, 黑龙江 大庆 163318;
2. 东北石油大学 计算机与信息技术学院, 黑龙江 大庆 163318)

摘要: 为减少软件定义网络中分布式拒绝服务攻击检测中的资源消耗, 提高检测精度, 提出一种基于 φ-熵与 IDBO-RF 的二级联合检测模型. 首先, 通过计算目的 IP 地址 φ-熵筛选异常流量完成一级触发检测; 其次, 利用改进蜣螂优化算法优化随机森林的超参数, 构建 IDBO-RF 模型, 将异常流量通过最优特征子集映射到 IDBO-RF 模型进行分布式拒绝服务攻击二级确认检测. 经公开数据集和仿真实验验证, 该模型有效缩短了检测时间, 减少了软件定义网络的控制器资源消耗, 在分布式拒绝服务攻击二分类和多分类检测中准确率均达 99% 以上, 平均检测时间仅 1.21 s, 对控制器 CPU 占用率仅 33.45%, 具有良好的泛化性能.

关键词: 软件定义网络; 分布式拒绝服务攻击; φ-熵; 随机森林; 蜣螂优化算法
中图分类号: TP393 **文献标志码:** A **文章编号:** 1671-5489(2025)05-1454-08

DDoS Attack Joint Detection Model Based on φ-Entropy and IDBO-RF in SDN

GAO Xincheng[1], WANG Qilong[2], WANG Lili[2]
(1. *Modern Education Technique Center, Northeast Petroleum University, Daqing* 163318, *Heilongjiang Province, China*; 2. *School of Computer and Information Technology, Northeast Petroleum University, Daqing* 163318, *Heilongjiang Province, China*)

Abstract: In order to reduce the resource consumption in distributed denial of service (DDos) attack detection in software defined networks and improve the detection accuracy, we proposed a two-level joint detection model based on φ-entropy and IDBO-RF. Firstly, abnormal traffic was filtered to complete the first level trigger detection by calculating the φ-entropy of the destination IP address. Secondly, the hyperparameters of the random forest were optimized by using the improved dung beetle optimization algorithm to construct the IDBO-RF model. Abnormal traffic was mapped through the optimal feature subset to the IDBO-RF model for secondary confirmation detection of DDoS attacks. Through public datasets and simulation experiments, the proposed model effectively shortens the detection time, reduces controller resource consumption of the software defined

收稿日期: 2024-06-24.

第一作者简介: 高新成(1979—), 男, 汉族, 博士, 教授, 从事网络安全、网络管理和大数据应用的研究, E-mail: gxc@nepu.edu.cn. **通信作者简介:** 王启龙(1999—), 男, 汉族, 硕士研究生, 从事网络安全、软件定义网络和攻击检测的研究, E-mail: wangqilong@stu.nepu.edu.cn.

基金项目: 国家自然科学基金(批准号: 61702093)、中国高校产学研创新基金(批准号: 2021ITA02011)和黑龙江省教育科学"十四五"规划重点项目(批准号: GJB1425352).

networks, and achieves an accuracy of over 99% in both binary and multi-classification detection of DDoS attacks, the average detection time is only 1.21 s, and the CPU occupancy rate for controller is only 33.45%, demonstrating good generalization performance.

Keywords: software defined network; distributed denial of service attack; φ-entropy; random forest; dung beetle optimization algorithm

软件定义网络(software defined networks, SDN)[1-2]作为一种主流的网络架构，广泛应用于各领域，然而其中心化控制和分布式结构也带来了更多的安全挑战. 随着 SDN 的发展，分布式拒绝服务(distributed denial of fervice, DDoS)攻击对 SDN 造成的危害越来越严重，SDN 中的 DDoS 攻击检测已成为网络安全研究的一个重要课题.

目前，SDN 中的 DDoS 攻击检测方案主要有基于统计分析和基于机器学习两类. 文献[3]通过相关系数法进行特征选择，通过机器学习算法进行 DDoS 攻击分类，但其未考虑非线性变量对分类的影响. Tsobdjou 等[4]基于动态阈值在线检测 DDoS 攻击，提高了检测的准确性和适应性. Nadeem 等[5]通过递归特征消除和随机森林(RF)算法对 SDN 中的 DDoS 进行检测，准确率达 99.97%. Han 等[6]通过创新特征选择方法提升在 5G 网络中入侵检测的速度和准确性. 王智等[7]设计了结合联合熵与半监督算法的二级检测模型，提高了检测性能. 杨亚红等[8]结合 Renyi 熵和双向门控循环神经网络(BiGRU)进行 DDoS 攻击检测，有较好的检测能力，但选择的特征元组缺少泛化性. Najar 等[9]提出了一种结合平衡随机采样和卷积神经网络的 DDoS 检测模型，实现二分类准确率 99.99%和多分类准确率 98.64%. Yoon 等[10]提出了基于分支注意力机制的深度学习 DDoS 攻击检测模型，但其忽略了资源开销对 SDN 网络的影响. 傅友等[11]通过条件熵判断网络状态，并基于决策树(DT)算法对 SDN 中的 DDoS 攻击进行检测，检测时间仅 6.83 s.

上述研究结果表明：基于熵值的检测方法受阈值的影响，检测误报率较高，多用于筛选异常流量；基于机器学习的检测方法忽略了模型超参数对检测性能的影响. 本文针对上述问题，提出一种 DDoS 攻击二级联合检测模型. 通过设置动态阈值的 φ-熵触发模块触发基于改进蜣螂优化-随机森林(IDBO-RF)的检测模块，在保证检测准确率的同时，提高模型检测效率，降低对 SDN 控制器的资源消耗.

1　基于 φ-熵与 IDBO-RF 的二级联合检测模型

1.1　二级联合检测模型框架

本文设计的 DDoS 攻击二级联合检测模型，主要包括基于 φ-熵的检测触发模块和基于 IDBO-RF 的检测确认模块，如图 1 所示. 检测模型在执行过程中基于滑动窗口机制通过控制器获取 Packet-in 流表信息，提取目的 IP 地址后，通过检测触发模块计算目的 IP 地址 φ-熵值. 若 φ-熵小于阈值，则认为存在异常流量，将异常流量转发到检测确认模块，通过 IDBO-RF 模型进行更准确的 DDoS 攻击确认检测. 如果检测结果为 DDoS 攻击，则发出警报.

1.2　基于 φ-熵的检测触发模块

1.2.1　φ-熵

信息熵[12]用于度量变量间的离散程度，熵值越大，变量分布越离散. φ-熵[13]是一种对数据更敏感、算法收敛速度更快、能增大不同离散数据之间信息距离的信息熵，φ-熵定义如下：

$$H'_{\alpha}(X)=-\frac{1}{\sinh(\alpha)}\left(\sum_{i=1}^{n}p_i\sinh(\alpha lb\,p_i)\right), \tag{1}$$

其中 p_i 表示事件 X 发生的概率，$\alpha\in(0,1)$表示调节度量事物频率发生的敏感度参数.

1.2.2　基于动态阈值的 φ-熵一级触发模块

正常网络流量中目的 IP 地址是较分散的，而 DDoS 攻击会导致目的 IP 地址相对集中. 用熵可表示为 DDoS 攻击发生时，目的 IP 地址熵值会突然变小. 为快速检测 DDoS，本文使用 φ-熵描述目的 IP 地址的变化，通过动态阈值的方法满足流量变化. 在稳定的正常流量环境中，收集 50 个窗口大小的

Packet-in 消息，计算每个窗口的 φ-熵值，并根据 3Sigma 原则计算初始阈值和动态阈值. 动态阈值的更新方式：计算当前窗口的 φ-熵，若连续 5 个窗口 φ-熵大于阈值，则更新阈值. 初始阈值表达式为

$$T_{\mathrm{init}}=\mu-3\sigma, \tag{2}$$

其中 u 表示 φ-熵均值，σ 表示 φ-熵标准差. 一级触发模块如图 2 所示.

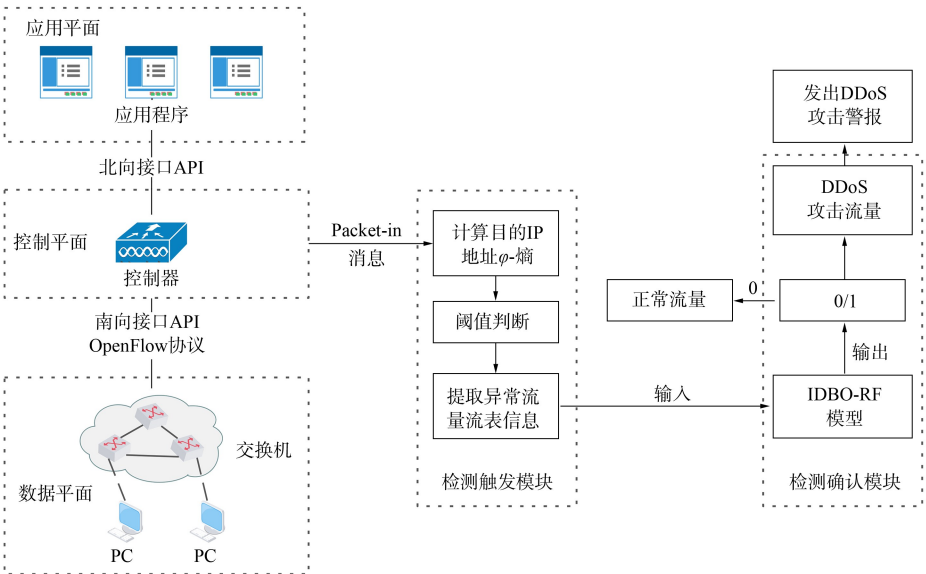


图 1 二级联合检测模型

Fig. 1 Two-level joint detection model

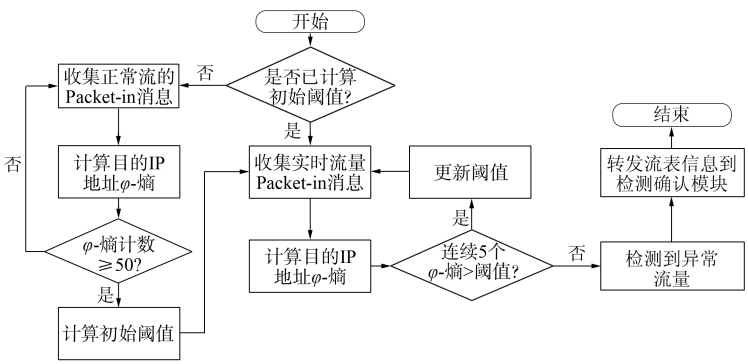


图 2 一级触发模块

Fig. 2 First level trigger module

1.3 多策略融合改进的蜣螂优化算法

蜣螂优化算法(dung beetle optimizer，DBO)[14]具有求解精度高、寻优速度快、稳定性强等优点. 但 DBO 全局探索和局部开发的平衡能力存在一定的局限性，为解决上述问题，本文对 DBO 算法提出一种多策略融合改进的方法.

1.3.1 基于 Bernoulli 映射与反向学习策略的种群初始化

Bernoulli 映射具有高度随机性和不可预测性[15]，能生成均匀分布的随机数序列，可使初始化种群个体分布更均匀. Tizhoosh[16]指出反向学习机制得出的反向解比当前解逼近最优解的概率高 50%. 因此，本文采用 Bernoulli 映射初始化种群，对其进行反向学习后，将初始种群与反向种群合并，选择出其中适应度最优的 N 个个体作为初始化种群，以增加种群的多样性和种群质量. Bernoulli 映射公式为

$$z_{n+1}=\begin{cases}\dfrac{z_n}{1-\beta}, & 0\leqslant z_n\leqslant 1-\beta,\\[2ex] \dfrac{z_n-(1-\beta)}{1-\beta}, & 1-\beta<z_n\leqslant 1,\end{cases} \tag{3}$$

其中：z_n 表示产生的第 n 代混沌序列的当前值；β 为映射参数，$\beta\in(0,1)$. 反向学习公式为

$$X_{\mathrm{OBL}}=\boldsymbol{k}\times(U_b+L_b)-X, \tag{4}$$

其中 $\boldsymbol{k}$ 表示 d 维服从正态分布的随机向量，U_b 和 L_b 分别表示种群边界的上界和下界，X 表示初始种群.

1.3.2　基于适应度-距离平衡策略的偷窃行为

算法中偷窃行为受全局最优解的影响，使种群向全局最优解靠拢. 为平衡种群的多样性和收敛性，本文采用适应度-距离平衡策略(fitness-distance balance，FDB)[17]对偷窃行为进行改进，避免陷入局部最优解. 该策略基于种群适应度和局部最优位置进行更新，用公式可表示为

$$X_i(t+1)=X^{\mathrm{FDB}}+\beta\times\boldsymbol{g}\times(|X_i(t)-X^*|+|X_i(t)-X^{\mathrm{FDB}}|), \tag{5}$$

其中 X^{FDB}表示第 t 次迭代时 FDB 策略选择的第 i 只偷窃蜣螂的候选解，X^* 为当前局部最优位置，β 为一个加权系数，$\boldsymbol{g}$ 为一个 D 维的正态分布随机向量.

1.3.3　基于动态权重的 Cauchy-Gauss 变异扰动

本文基于动态权重的 Cauchy-Gauss 变异扰动[18]对当前全局最优位置进行干扰，使算法在初期以 Cauchy 扰动为主，增强全局搜索能力，在后期以 Gauss 异扰动为主，增强局部开发能力. 位置更新公式如下：

$$X_r^t=X_{\mathrm{best}}\times[1+u_1\times\mathrm{Cauchy}(0,1)+(1-u_1)\times\mathrm{Gauss}(0,1)], \tag{6}$$

其中：X_r^t 表示第 t 次迭代中变异后的位置；Cauchy(0,1)和 Gauss(0,1)分别表示满足 Cauchy 分布和 Gauss 分布的随机变量；u_1 表示动态权重因子，计算公式为

$$u_1=1-\frac{t^2}{T_{\max}^2}. \tag{7}$$

在扰动更新位置后，为选择出最优位置，加入贪婪规则，通过比较扰动前后适应度值的大小，将适应度值更优的位置作为全局最优位置. 贪婪规则如下：

$$X_{\mathrm{best}}=\begin{cases}X_r, & f(X_r)\leqslant f(X_{\mathrm{best}}),\\ X_{\mathrm{best}}, & f(X_r)>f(X_{\mathrm{best}}),\end{cases} \tag{8}$$

其中 $f(X_r)$和 $f(X_{\mathrm{best}})$分别表示扰动后位置和全局最优位置的适应度值.

1.4　基于 IDBO-RF 的检测确认模块

RF 模型的预测效果主要受 RF 的决策树个数 n_estimators、树最大深度 max_depth 和最大特征数 max_features 3 个超参数的影响. 通过网格搜索算法进行参数寻优，易陷入局部最优解. 为提高超参数寻优的效率和精度，本文使用 IDBO 对 RF 的超参数寻优，以提高 RF 模型的分类性能，进而提高 DDoS 攻击检测的准确率和实时性. 检测确认模块中，首先提取检测触发模块转发的异常流量信息，然后在 IDBO-RF 模型上输出 DDoS 攻击检测结果. 检测确认模块如图 3 所示.

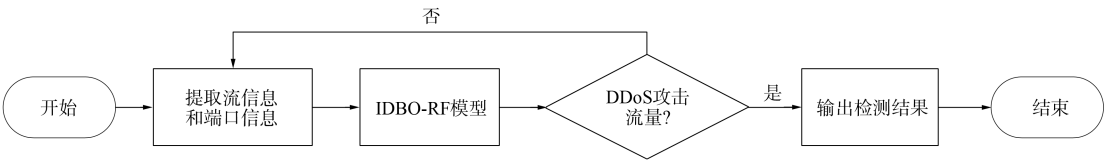


图 3　二级确认模块

Fig. 3　Secondary validation module

2　实验与分析

2.1　基于公开数据集的实验结果分析

为验证本文模型的可靠性，选用在 SDN 环境中采集的数据集 InSDN[19]作为实验数据. 为验证 IDBO-RF 模型的有效性，设置单一的 DT、RF 模型和使用粒子群优化的 PSO-RF 模型作为对照实验组，进行模型性能评估，评估结果列于表 1. 由表 1 可见，经过 IDBO 和 PSO 优化参数的 IDBO-RF 和

PSO-RF 模型在准确率、召回率和 F_1 得分上均优于传统的 DT 和 RF 模型. IDBO-RF 模型比 RF 模型的训练时间缩短了 5.08 s，比 PSO-RF 模型训练时间缩短了 2.35 s.

表 1 不同检测模型的性能对比

Table 1 Performance comparison of different detection models

模型	准确率/%	精确度/%	召回率/%	F_1/%	训练时间/s
DT	99.97	99.94	99.89	99.91	0.20
RF	99.98	99.28	99.93	99.60	6.13
PSO-RF	99.99	100	99.99	99.99	3.40
IDBO-RF	99.99	100	99.99	99.99	1.05

2.2 仿真模拟实验结果分析

2.2.1 实验环境

本文通过 Mininet 搭建仿真网络，基于 RYU 控制器和 OpenVSwitch 交换机实现的网络拓扑如图 4 所示.

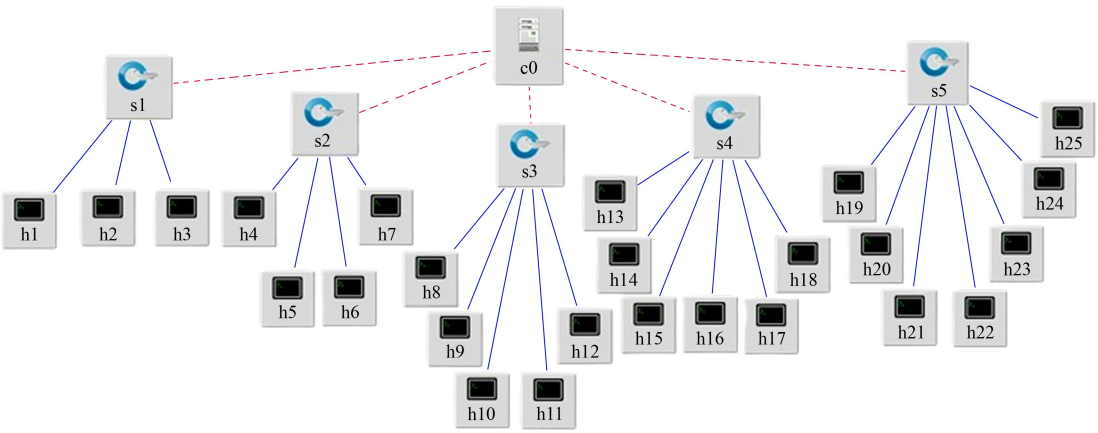


图 4 SDN 网络拓扑

Fig. 4 SDN network topology

2.2.2 数据集的生成与特征选择

为验证模型的泛化性能，对 DDoS 攻击进行多分类检测. 在 SDN 中利用 Hping3 和 Iperf 等工具生成 TCP,UDP,ICMP 的正常流量和 TCP-SYN flood,UDP flood,ICMP flood 泛洪 DDoS 流量，利用 SlowHTTPTest 工具产生 Slowloris,Slowpost 和 Slowread 慢速率 DDoS 流量，并收集流量数据，形成包含 25 个特征的混合 DDoS 攻击数据集. 然后将数据集按 7∶3 划分为训练集和测试集，数据集分布列于表 2. 图 5 为不同特征数量在 RF 模型上的性能度量.

表 2 数据集分布

Table 2 Distribution of dataset

数据集	正常流量	泛洪 DDoS 攻击流量/条			慢速率 DDoS 攻击流量/条		
		ICMP flood	UDP flood	TCP-SYN flood	Slowloris	Slowpost	Slowread
训练集	25 348	30 064	29 107	33 332	33 262	34 324	37 803
测试集	10 863	12 884	12 475	14 286	14 256	14 710	16 201

2.2.3 检测触发模块有效性验证

实验以目的 IP 地址的信息熵和 φ-熵评估检测触发模块的有效性. 在前 80 个窗口内收集正常流量情况下目的 IP 的熵值，其稳定在一定范围内. 然后通过 Scapy 编写的 DDoS 攻击脚本发起攻击，目的 IP 地址的集中程度变高，熵值急剧下降. 到 160 个窗口时，停止 DDoS 攻击，熵值逐渐恢复到正常流量的水平. 目的 IP 地址熵值随窗口数的变化曲线如图 6 所示. 与信息熵相比，φ-熵能有效放大流量的变化情况. 因此，本文选择 φ-熵作为检测触发模块的指标有效.

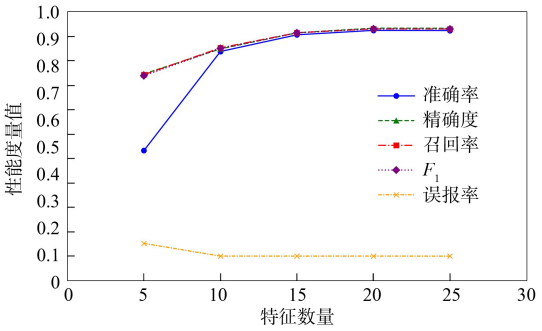


图 5　不同特征数量在 RF 模型上的性能度量

Fig. 5　Performance metrics for different number of features on RF model

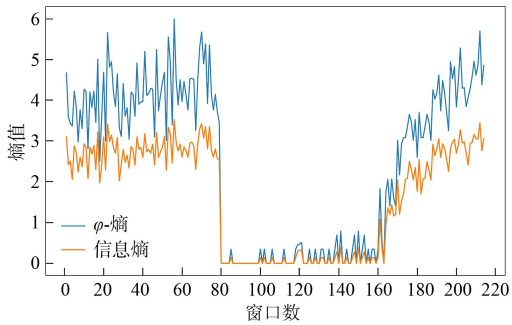


图 6　目的 IP 地址熵值随窗口数的变化曲线

Fig. 6　Variation curves of entropy values of destination IP address with number of windows

2.2.4　二级联合检测模型有效性验证

为验证检测确认模块的有效性，基于 SDN 的混合 DDoS 攻击数据集，本文设置 3 个模型 DT，RF，PSO-RF 作为对照实验组进行多分类检测. 通过传统的 DT 和 RF 模型验证超参数调优的有效性，与 PSO-RF 对比验证 IDBO-RF 的优越性. 多分类实验性能对比结果列于表 3. 由表 3 可见，本文 IDBO-RF 模型对多个 DDoS 攻击类型的检测准确率达 99%以上，且模型训练时间仅 25.97 s，比传统的 RF 模型减少了 10.08 s.

表 3　多分类实验结果

Table 3　Experimental results of multiclassification

模型	准确率/%	精确度/%	召回率/%	F_1/%	训练时间/s
DT	89.38	89.38	89.38	89.39	37.03
RF	92.85	93.29	92.97	92.97	36.05
PSO-RF	96.96	95.88	96.29	96.00	22.18
IDBO-RF	99.16	99.14	99.14	99.14	25.97

各模型针对不同类型 DDoS 攻击的各性能指标如图 7 所示. 与 PSO-RF，DT 和 RF 模型相比，IDBO-RF 模型对 6 种不同 DDoS 攻击检测准确率均达 99%，特别是对 Slowloris，Slowpost 和 Slowread 的检测误报率明显比其他 3 种方法更低，仅为 0.5%，检测效果更优.

为验证本文模型的在线检测效果，设置了 RF、φ-熵＋DT、φ-熵＋RF、φ-熵＋PSO-RF 4 组检测模型作对照实验. 通过 RF 对比验证二级检测模型的优越性，通过 φ-熵＋DT、φ-熵＋RF 和 φ-熵＋PSO-RF 模型对比验证超参数调优的有效性，通过 φ-熵＋PSO-RF 验证本文二级联合检测模型的优越性. 经过 10 次实验后，比较各模型平均训练时间及在线检测时间和 CPU 占用率，实验结果列于表 4.

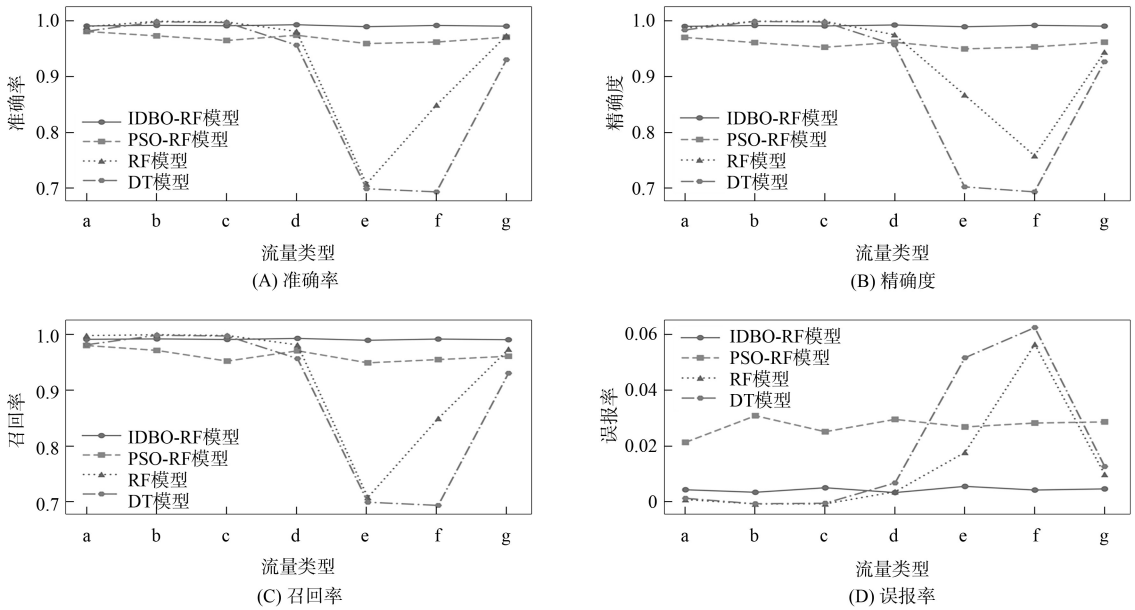
表 4　不同检测模型在线检测实验结果

Table 4　Experimental results of online detection of different detection models

模型	训练时间/s	检测时间/s	CPU 占用率/%
φ-熵＋IDBO-RF	25.97	1.21	33.45
φ-熵＋PSO-RF	22.18	1.84	42.28
φ-熵＋RF	36.05	2.45	62.73
φ-熵＋DT	37.03	2.23	60.56
RF	36.05	5.65	70.12

由表 4 可见，结合 φ-熵与超参数优化的 RF 模型在训练时间、检测时间和 CPU 占用率方面均性能优异. φ-熵＋IDBO-RF 二级联合检测模型的检测时间为 1.21 s，CPU 占用率为 33.45%. 而仅使用 RF 模型的检测时间为 5.65 s，CPU 占用率高达 70.12%. 二级联合检测模型在各方面均优于传统的 RF 和 DT 模型，有效减少了检测时间和资源消耗. 因此，本文模型在保证检测精确率的同时，缩短了检测时间，降低了对 SDN 控制器 CPU 的占用率，能有效进行实时 DDoS 攻击多分类检测.

综上所述，针对 SDN 环境中分布式拒绝服务攻击分类检测精度及资源消耗的问题，本文提出了



a. Benign; b. ICMP flood; c. UDP flood; d. TCP-SYN flood; e. Slowloris; f. Slowpost; g. Slowread.

图 7 检测确认模块性能对比

Fig. 7 Performance comparison of detection and confirmation module

一个基于 φ-熵与 IDBO-RF 的 DDoS 攻击二级联合检测模型. 使用 φ-熵作为一级触发模块标准，增大了异常流量与正常流量的表征距离，降低了检测误报率；二级确认模块中使用多策略融合改进的 DBO 算法优化 RF 的超参数，提高了模型的检测性能. 实验结果表明，二级联合检测模型适用于 SDN 中 DDoS 攻击的实时分类检测，有效减少了检测时间和资源开销.

参 考 文 献

[1] CHAHAL J K, BHANDARI A, BEHAL S. DDoS Attacks & Defense Mechanisms in SDN-Enabled Cloud: Taxonomy, Review and Research Challenges [J]. Computer Science Review, 2024, 53: 100644-1-100644-19.

[2] 高新成，刘威，王启龙，等. 基于 SDN 的混合分段路由概率流调度机制 [J]. 计算机应用研究，2023，40(11)：3382-3387.（GAO X C, LIU W, WANG Q L, et al. SDN-Based Hybrid Segmented Routing Probabilistic Flow Scheduling Mechanism [J]. Application Research of Computers, 2023, 40(11): 3382-3387.）

[3] ZHOU L, ZHU Y, ZONG T R, et al. A Feature Selection-Based Method for DDoS Attack Flow Classification [J]. Future Generation Computer Systems, 2022, 132: 67-79.

[4] TSOBDJOU L D, PIERRE S, QUINTERO A. An Online Entropy-Based DDoS Flooding Attack Detection System with Dynamic Threshold [J]. IEEE Transactions on Network and Service Management, 2022, 19(2): 1679-1689.

[5] NADEEM M W, GOH H G, PONNUSAMY V, et al. DDoS Detection in SDN Using Machine Learning Techniques [J]. Computers, Materials & Continua, 2022, 71(1): 1-6.

[6] HAN D Q, LI H H, FU X L, et al. Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning [J]. Sensors, 2024, 24(13): 4344-1-4344-22.

[7] 王智，张浩，顾建军. SDN 网络中基于联合熵与多重聚类的 DDoS 攻击检测 [J]. 信息网络安全，2023，23(10)：1-7.（WANG Z, ZHANG H, GU J J. A Hybrid Method of Joint Entropy and Multiple Clustering Based DDoS Detection in SDN [J]. Netinfo Security, 2023, 23(10): 1-7.）

[8] 杨亚红，王海瑞. 基于 Renyi 熵和 BiGRU 算法实现 SDN 环境下的 DDoS 攻击检测方法 [J]. 计算机科学，2022，49(增刊 1)：555-561.（YANG Y H, WANG H R. DDoS Attack Detection Method in SDN Environment Based on Renyi Entropy and BiGRU Algorithm [J]. Computer Science, 2022, 49(Suppl 1): 555-561.）

[9] NAJAR A A, NAIK S M. Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of

DDoS Attacks [J]. Computers & Security, 2024, 139: 103716-1-103716-23.

[10] YOON N, KIM H. Detecting DDoS Based on Attention Mechanism for Software-Defined Networks [J]. Journal of Network and Computer Applications, 2024, 230: 103928-1-103928-15.

[11] 傅友，邹东升. SDN 中基于条件熵和决策树的 DDoS 攻击检测方法 [J]. 重庆大学学报，2023，46(7)：1-8.（FU Y, ZOU D S. A DDoS Attack Detection Method Based on Conditional Entropy and Decision Tree in SDN [J]. Journal of Chongqing University, 2023, 46(7): 1-8.）

[12] SABIROV D S, SHEPELEVICH I S. Information Entropy in Chemistry: An Overview [J]. Entropy, 2021, 23(10): 1240-1249.

[13] BEHAL S, KUMAR K. Detection of DDoS Attacks and Flash Events Using Novel Information Theory Metrics [J]. Computer Networks, 2017, 116: 96-110.

[14] XUE J K, SHEN B. Dung Beetle Optimizer: A New Meta-Heuristic Algorithm for Global Optimization [J]. The Journal of Supercomputing, 2023, 79(7): 7305-7336.

[15] JAMEEL M, ABOUHAWWASH M. Revolutionizing Optimization: An Innovative Nutcracker Optimizer for Single and Multi-objective Problems [J]. Applied Soft Computing, 2024, 164: 112019-1-112019-38..

[16] TIZHOOSH H R. Opposition-Based Learning: A New Scheme for Machine Intelligence [C]//International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06). Piscataway, NJ: IEEE, 2005: 695-701.

[17] KAHRAMAN H T, ARAS S, GEDIKLI E. Fitness-Distance Balance (FDB): A New Selection Method for Meta-Heuristic Search Algorithms [J]. Knowledge-Based Systems, 2020, 190: 105169-1-105169-27.

[18] 吴艳敏，刘家旗，王璐，等. 基于改进哈里斯鹰优化算法的配电网动态重构 [J]. 科学技术与工程，2024，24(8)：3251-3259.（WU Y M, LIU J Q, WANG L, et al. Dynamic Reconfiguration of Distribution Network Based on Improved Harris Hawk Optimization Algorithm [J]. Science Technology and Engineering, 2024, 24(8): 3251-3259.）

[19] ELSAYED M S, LE-KHAC N A, JURCUT A D. InSDN: A Novel SDN Intrusion Dataset [J]. IEEE Access, 2020, 8: 165263-165284.

（责任编辑：韩　啸）