

基于混合深度学习的多类型低速率 DDoS 攻击检测方法

李丽娟, 李曼, 毕红军, 周华春

(北京交通大学, 北京 100044)

摘要: 低速率分布式拒绝服务攻击针对网络协议自适应机制中的漏洞实施攻击, 对网络服务质量造成了巨大威胁, 具有隐蔽性强、攻击速率低和周期性的特点。现有检测方法存在检测类型单一和识别精度低的问题, 因此提出了一种基于混合深度学习的多类型低速率 DDoS 攻击检测方法。模拟不同类型的低速率 DDoS 攻击和 5G 环境下不同场景的正常流量, 在网络入口处收集流量并提取其特征信息, 得到多类型低速率 DDoS 攻击数据集; 从统计阈值和特征工程的角度, 分别分析了不同类型低速率 DDoS 攻击的特征, 得到了 40 维的低速率 DDoS 攻击有效特征集; 基于该有效特征集采用 CNN-RF 混合深度学习算法进行离线训练, 并对比该算法与 LSTM-LightGBM 和 LSTM-RF 算法的性能; 在网关处部署 CNN-RF 检测模型, 实现了多类型低速率 DDoS 攻击的在线检测, 并使用新定义的错误拦截率和恶意流量检测率指标进行了性能评估。结果显示, 在 120 s 的时间窗口下, 所提方法能够在线检测出 4 种类型的低速率 DDoS 攻击, 包括 Slow Headers 攻击、Slow Body 攻击、Slow Read 攻击和 Shrew 攻击, 错误拦截率达到 11.03%, 恶意流量检测率达到 96.22%。结果表明, 所提方法能够显著降低网络入口处的低速率 DDoS 攻击流量强度, 并在实际环境中部署和应用。

关键词: 多类型; 低速率 DDoS 攻击; 混合深度学习; 特征分析; 攻击检测

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022001

Multi-type low-rate DDoS attack detection method based on hybrid deep learning

LI Lijuan, LI Man, BI Hongjun, ZHOU Huachun

Beijing Jiaotong University, Beijing 100044, China

Abstract: Low-Rate distributed denial of service (DDoS) attack attacks the vulnerabilities in the adaptive mechanism of network protocols, posing a huge threat to the quality of network services. Low-Rate DDoS attack was characterized by high secrecy, low attack rate, and periodicity. Existing detection methods have the problems of single detection type and low identification accuracy. In order to solve them, a multi-type low-rate DDoS attack detection method based on hybrid deep learning was proposed. Different types of low-rate DDoS attacks and normal

收稿日期: 2021-07-20; 修回日期: 2021-10-22

通信作者: 李丽娟, 19120069@bjtu.edu.cn

基金项目: 国家重点研发计划 (2018YFA0701604)

Foundation Item: The National Key R&D Program of China (2018YFA0701604)

引用格式: 李丽娟, 李曼, 毕红军, 等. 基于混合深度学习的多类型低速率 DDoS 攻击检测方法[J]. 网络与信息安全学报, 2022, 8(1): 73-85.

Citation Format: LI L J, LI M, BI H J, et al. Multi-type low-rate DDoS attack detection method based on hybrid deep learning[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 73-85.

traffic in different scenarios under 5G environment were simulated. Traffic was collected at the network entrance and its traffic characteristic information was extracted to obtain multiple types of low-rate DDoS attack data sets. From the perspective of statistical threshold and feature engineering, the characteristics of different types of low-rate DDoS attacks were analyzed respectively, and the effective feature set of 40-dimension low-rate DDoS attacks was obtained. CNN-RF hybrid deep learning algorithm was used for offline training based on the effective feature set, and the performance of this algorithm was compared with LSTM-Light GBM and LSTM-RF algorithms. The CNN-RF detection model was deployed on the gateway to realize the online detection of multiple types of low-rate DDoS attacks, and the performance was evaluated by using the newly defined error interception rate and malicious traffic detection rate indexes. The results show that the proposed method can detect four types of low-rate DDoS attacks online, including Slow Headers attack, Slow Body attack, Slow Read attack and Shrew attack, and the error interception rate reaches 11.03% in 120 s time window. The detection rate of malicious traffic reaches 96.22%. It can be judged by the results that the proposed method can significantly reduce the intensity of low-rate DDoS attack traffic at the network entrance, and can be deployed and applied in the actual environment.

Keywords: multi-type, low-rate DDoS attack, hybrid deep learning, feature analysis, attack detection

0 引言

分布式拒绝服务 (DDoS, distributed denial of service) 攻击是一种大范围分布式且具有极强危害性的网络攻击方式, 能够对服务的可用性产生严重影响, 逐渐成为互联网面临的重大安全威胁之一。随着攻击技术的不断演变和更新, 衍生出一种新的攻击变种, 即低速率 DDoS 攻击。该攻击利用网络协议自适应机制中存在的漏洞, 发送较低速率的攻击数据包, 达到降低受害端服务质量的目, 具有隐蔽性强和攻击速率低的特征。网络环境中存在着多种协议的低速率 DDoS 攻击, 同时, 存在着周期性和非周期性的攻击模式^[1]。因此, 如何准确地检测出多种类型的低速率 DDoS 攻击流量是亟待解决的问题。

本文主要针对 5G 环境下的网络提出了一种基于混合深度学习的多类型低速率 DDoS 攻击检测方法。首先, 模拟不同类型低速率攻击和正常通信行为得到了实验数据集; 之后, 分析了不同类型低速率 DDoS 攻击的特征信息, 根据该特征信息进行特征选择; 然后, 结合混合深度学习算法实现检测模型的离线训练和优化; 最后, 将检测模型部署至网络入口处, 实现多类型低速率 DDoS 攻击的在线检测。

本文主要贡献有以下几点。

1) 模拟了多种类型低速率 DDoS 攻击和 5G 环境下不同场景的正常通信, 获取指定时间段内

网络流量的特征信息, 得到已进行标签标记的低速率 DDoS 攻击数据集。

2) 提出了多类型低速率 DDoS 攻击特征集, 从统计阈值和特征工程的角度, 分析不同类型低速率 DDoS 攻击和正常流量的特征信息, 得到低速率 DDoS 攻击的 40 种有效特征。

3) 提出了多类型低速率 DDoS 攻击检测方法。基于低速率 DDoS 攻击特征集实现混合深度学习模型的离线训练、在线部署及检测。检测结果显示, 通过选择最优时间窗口, 本文提出的方法能够有效地检测 Slow Headers 攻击、Slow Body 攻击、Slow Read 攻击和 Shrew 攻击共 4 种类型的低速率 DDoS 攻击。

1 研究现状

一直以来, 对于低速率 DDoS 攻击的研究受到国内外学者的广泛关注。21 世纪初, Kuzmanovic^[2]提出了 Shrew 攻击的定义, 采集了低速率 DDoS 攻击的相关数据并进行了相关分析和研究。对于低速率 DDoS 攻击检测防御的研究主要包括以下两类方法。

一类是基于统计分析的检测方法。Wu 等^[3]提出了基于 Pearson 相关性的低速率 DoS 攻击检测方法, 使用网络流量的 Hilbert 谱的 Pearson 相关系数表征网络流量信息, 将该信息与阈值进行比较实现检测针对 TCP 的低速率攻击。Wu 等^[4]从序列匹配的角度分析受害端低速率 DDoS 攻击

脉冲之间的序列相似性,使用 Smith-Waterman 算法并设计双阈值规则,实现对基于 TCP 的低速率攻击的检测。Kaur 等^[5]提出基于网络自相似的方法,分析低速率攻击对流量自相似特性的影响,使用 H-指数结合阈值识别攻击和合法流量。以上几种检测低速率攻击的方法,均仅对基于 TCP 的低速率攻击实施检测,且依赖于阈值的设定,极易受到网络环境的随机性影响,无法达到优异的检测效果。

另一类是基于机器学习的检测方法,该方法通过提取流量特征并结合机器学习算法实现检测低速率 DDoS 攻击。Zhang 等^[6]提出了基于主成分分析和支持向量机的方法,用于检测基于 TCP 的低速率攻击,主成分分析算法过滤环境中的噪声,实现有效采样网络流量中的特征。Liu 等^[7]提出了边缘环境下针对 TCP 的低速率 DDoS 攻击检测方法,利用局部敏感特征提取和深度卷积神经网络自动学习原始数据的最佳特征分布,并采用深度强化学习 Q 网络作为决策者,提高攻击检测的决策精准度。Wu 等^[8]提出基于分解机的低速率 DDoS 攻击检测方法,引入特征组合机制,建立特征样本之间的相关性,实现对基于 HTTP 低速率攻击的检测。文献[9]提出使用机器学习算法检测 SDN 环境下的低速率 DDoS 攻击,包括 J48、随机树、REP 树、随机森林、多层感知器和支持向量机共 6 种模型,检测基于 HTTP 的低速率 DDoS 攻击,但该方法的误报率较高。

混合深度学习算法能够充分利用机器学习和深度学习算法的优点, Malik 等^[10]提出了基于长短期记忆 (LSTM, long short-term memory) 网络和卷积神经网络 (CNN, convolutional neural network) 的混合深度学习框架,用于检测 CICIDS2017 数据集集中的 Bot、Post Scan 和 XSS 攻击,经验证该检测系统具有优异的检测能力。Garg 等^[11]提出了基于深度学习的混合异常检测系统,将受限玻尔兹曼机和支持向量机算法相结合,减小数据的特征维度,但实验使用的数据集是 KDD99,未对 DoS 攻击进行细粒度分类检测。Guo 等^[12]提出了基于长短期记忆网络和 LightGBM 的混合时间序列预测模型,将其用于股票预测,具有优异的预测性能。Hu 等^[13]提出

基于长短期记忆网络和随机森林 (RF, random forest) 的混合深度学习模型,与单一的机器学习方法相比,其具有更加优异的预测效果。

上述低速率 DDoS 攻击检测方法仅针对单类型的低速率 DDoS 攻击实施检测,存在检测类型单一和检测精度低的问题。因此,本文针对以上问题,提出了基于 CNN-RF 混合深度学习的低速率 DDoS 攻击检测方法,该方法能够学习不同类型攻击流量的特征,提高多类型低速率 DDoS 攻击在线检测的准确率。

2 低速率 DDoS 攻击特征分析

本文将低速率 DDoS 攻击分为两类:一类是基于 HTTP 的低速率 DDoS 攻击;另一类是基于 TCP 的低速率 DDoS 攻击^[1]。

基于 HTTP 的低速率 DDoS 攻击包括 Slow Headers 攻击、Slow Body 攻击和 Slow Read 攻击^[14]。该类攻击利用现有 HTTPKeep-Alive 机制的漏洞,长时间保持连接并持续占用服务器资源,导致 Web 服务器产生拒绝服务。其中,Slow Headers 攻击实施者发送以字符 ‘\r\n’ 为结尾的不完整 HTTP 请求,导致服务器认为请求未发送完毕并继续等待,最终连接数达到服务器上限,无法处理新的请求而产生拒绝服务攻击。Slow Body 攻击实施者向服务器发送内容长度值较大的 POST 请求,但服务器每次只发送含少量字节数的数据包,请求数目足够多时耗尽服务器资源。Slow Read 攻击实施者向服务器发送读取大数据文件的合法请求,但将 TCP 滑动窗口设置为较小值,服务器与攻击者之间需长时间建立通信连接,当连接数目足够多时将无法提供服务。

基于 TCP 的低速率 DDoS 攻击有许多种,本文主要分析 Shrew 攻击,该攻击利用 TCP 超时重传机制的漏洞^[2],周期性地发送高速突发脉冲数据包,降低受害端的服务质量和性能。本文主要通过攻击工具和 Python 脚本模拟 Slow Headers 攻击、Slow Body 攻击、Slow Read 攻击、Shrew 攻击 4 种类型的低速率 DDoS 攻击。

低速率 DDoS 攻击的特征分析主要基于原始低速率 DDoS 攻击的特征信息。CICFlowMeter 流特征提取工具能够自动按照时间窗口提取双向流

的详细参数,双向流表示包括正向和反向数据流的特征。除标签值外,该工具共生成 83 种特征信息,包括流 ID、五元组信息、流级特征和包级特征。流 ID 由五元组{源 IP 地址,目的 IP 地址,源端口,目的端口,协议}表示,用于唯一标记流。流级特征包括流处于活跃时间的统计特征、流持续时间和每秒的流字节数等。包级特征包括每秒的前/反向数据包数目、数据包长度的统计特征、SYN/FIN/RST 标志位计数等。

3 低速率 DDoS 攻击检测框架

本节首先介绍检测框架组成,然后介绍数据集生成模块的原理和实现,最后详细介绍混合深度学习模型的离线训练模块和在线检测模块的具体实现和关键技术。

检测框架主要由数据集生成模块、特征分析及选择模块、离线训练模块和在线检测模块组成。低速率 DDoS 攻击检测框架如图 1 所示,该框架分为数据处理部分和混合深度学习部分。

数据处理部分负责对获取到的网络流量进行初步处理,分为数据集生成模块和特征分析及选择模块。数据集生成模块用于获取指定时间段内的网络流量,提取流特征信息并进行数据清洗,得到包含 4 种类型低速率 DDoS 攻击和正常流量的低速率 DDoS 攻击数据集。特征分析及选择模块从统计阈值和特征工程的角度分别分析不同类型低速率 DDoS 攻击的特征信息,总结得到多类型低速率 DDoS 攻击的有效特征。

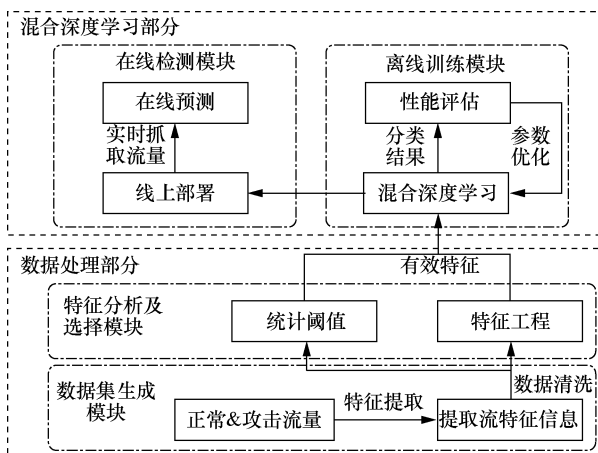


图 1 低速率 DDoS 攻击检测框架

Figure 1 Low-Rate DDoS attack detection framework

混合深度学习部分负责检测不同类型的低速率 DDoS 攻击,分为离线训练模块和在线检测模块。离线训练模块基于有效特征对数据集进行特征选择,采用混合深度学习算法进行训练和测试,根据分类结果进行性能评估及相关参数优化,选择最优的攻击检测模型。在线检测模块将已训练好的混合深度学习检测模型部署至网络入口处,通过实时抓取流量实现对多类型低速率 DDoS 攻击的在线检测,模型的输出信息用于指示待检测流量的低速率 DDoS 攻击具体类型。

3.1 数据处理部分

3.1.1 数据集生成模块

数据集生成模块用于获取一定时间段内的网络流量,通过流特征提取工具 CICFlowMeter 提取流特征信息,得到低速率 DDoS 攻击数据集。该数据集包含多类型低速率 DDoS 攻击和 5G 场景下的正常通信流量,能够反映真实环境下的流量规律。

文献[15]根据第三代合作计划(3GPP)^[16]和电气和电子工程师协会(IEEE)^[17]对不同 5G 应用场景下设备的真实流量规律,建模并生成了海量正常通信模拟请求。该规律通过真实场景下收集的流量数据得到,其结果包含各种环境因素的影响,能够反映真实场景下的请求情况。本文对该方法加以改进,生成了正常通信流量,并结合利用攻击工具和脚本所生成的 4 种低速率 DDoS 攻击流量,得到一个新的低速率 DDoS 攻击数据集。

本文通过攻击工具发送流量实现攻击,基于网络环境安全问题考虑,低速率网络流量的捕获基于 VMware vSphere 虚拟化实验平台实现,实验环境基本接近真实环境,反映实际环境下的流量统计情况。之后,部署安装流量采集工具 Tcpdump 抓取网络中的数据包,数据集采集点在网络入口的接入网关处,可完整捕获网络中的通信流量。最后,使用 CICFlowMeter 提取网络流量的特征信息。同时,根据表 1 中的攻击计划对提取出的特征信息进行标签标记,将标记的数据集用于检测模型的训练和验证。

本文研究的 Slow Headers 攻击、Slow Body 攻击和 Slow Read 攻击 3 种类型的低速率 DDoS

攻击方式通过修改 SlowHttpTest 慢速 Http 攻击工具的参数发送攻击流量^[1], Shrew 攻击则通过编写 Python 脚本实现发送攻击流量。正常通信请求则基于 5G 环境下不同场景的统计规律, 使用 Python 脚本模拟发送海量连接正常请求流量。

基于以上实现方式, 本文在低速率 DDoS 攻击和正常通信行为下收集流量并自动提取流特征信息。捕获期从 2021 年 5 月 19 日的 08:00 开始, 至 5 月 24 日的 17:00 结束。在此期间, 发起不同类型的攻击, 包括低速率 DDoS 攻击、网络层 DDoS 攻击、应用层 DDoS 攻击和分布式反射性放大攻击等, 其中, 低速率 DDoS 发起攻击计划如表 1 所示。

表 1 低速率 DDoS 攻击计划
Table 1 Low-Rate DDoS attack plan

攻击时间	源 IP	目的 IP	流量类型
2021.5.23 15:35-16:15	23.1.0.2	23.1.1.2	Slow Headers
	23.1.0.10	23.1.1.2	Slow Body
	23.1.0.11	23.1.1.2	Slow Read
	23.1.0.12	23.1.1.2	Shrew
	23.1.0.20-23.1.0.29	23.1.1.7	正常流量

基于上述攻击计划获取的网络流量 pcap 文件, 使用流特征提取工具 CICFlowMeter 提取流量的特征信息, 得到多类型低速率 DDoS 攻击数据集。数据集中各流量类型数据样本数及与正常流量样本数的比例情况如表 2 所示。可见, 正常流量的数据样本数远大于每种低速率 DDoS 攻击的数据样本数, 体现了低速率 DDoS 攻击速率低的特性。

表 2 各流量类型数据样本数及比例
Table 2 Number and proportion of data samples of each flow type

流量类型	数据样本数	攻击流量占正常流量的比例
Slow Headers	100 793	1:4.5
Slow Body	110 044	1:4.2
Slow Read	68 074	1:6.7
Shrew	45 389	1:10
正常流量	460 619	—

3.1.2 特征分析及选择模块

为实现对低速率 DDoS 攻击的有效检测, 基

于原始网络流量提取的特征信息, 本文从统计阈值和特征工程的角度, 分别对 4 种类型的低速率 DDoS 攻击进行特征分析和选择, 利用攻击特征描述不同的攻击特性, 降低低速率 DDoS 攻击数据集的特征维度, 减小检测系统的时间复杂度, 提高检测模型的泛化能力。

在统计阈值方面, 分别查看低速率 DDoS 攻击流量和正常流量的各个特征值分布直方图, 选取直方图分布存在明显差异的特征; 分别从攻击原理、攻击源码、特征值生成源码和攻击时序图角度, 结合发起攻击时 Wireshark 等工具的抓包情况, 分析特征阈值分布及产生该分布的原因, 总结各个特征的阈值情况及阈值分布原理。

在特征工程方面, 本文选择使用斯皮尔曼相关系数法、递归特征消除法、XGBoost、基于 Gini 系数的随机森林和基于信息熵的随机森林共 5 种方法^[18], 分别对每种类型的低速率 DDoS 攻击进行特征选择, 依据特征重要性排序选取特征。最终选择至少 3 种方法含有的特征, 作为每种类型低速率 DDoS 攻击特征分析的结论。

根据上述特征选择和分析步骤, 对于 4 种类型的低速率 DDoS 攻击, 分别确定可表征每种类型低速率 DDoS 攻击特性的特征信息, 汇总得到多类型低速率 DDoS 攻击的 40 种有效特征。低速率 DDoS 攻击的有效特征如图 2 所示。例如, 对于 Slow Read 攻击而言, Flow Duration 反映该攻击长期保持连接的特性; Active Max 反映该攻击发包间隔时间长和周期性的特性; ACK Flag Cnt 反映发起攻击时频繁建立和关闭 HTTP 连接时的交互情况; Flow Byts/s 反映攻击发包数目少且攻击速率低的特性。

为验证特征分析的有效性, 基于本文得到的多类型低速率 DDoS 攻击数据集和设计的检测模型, 使用模型的训练时间、测试时间和准确率 3 个指标比较特征选择前后同一检测模型的相关性能, 如表 3 所示。从表 3 可知, 使用有效特征不仅将训练时间降低约 5.2%, 测试时间降低约 12.5%, 而且将准确率提高了约 1%。因此, 使用图 2 中的特征信息可描述多类型低速率 DDoS 攻击实施时的相关特性, 有利于降低模型的时间复杂度。

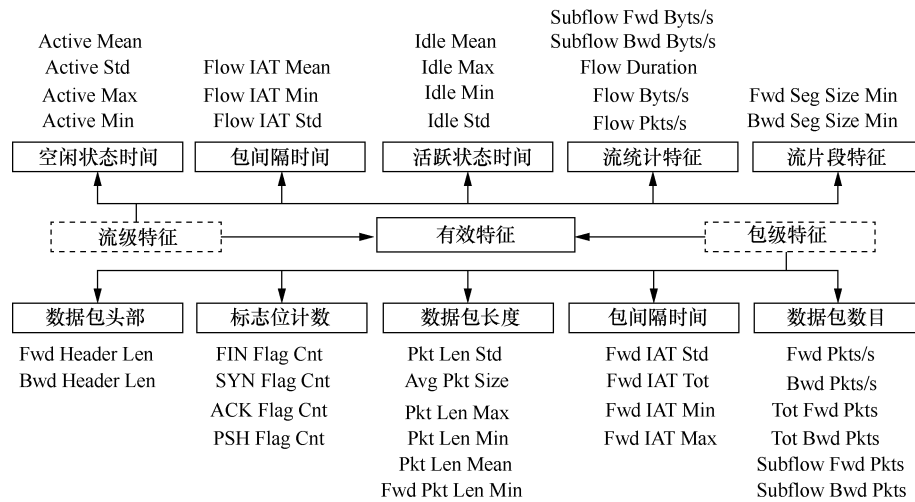


图 2 低速率 DDoS 攻击的有效特征
Figure 2 Low-Rate DDoS attack effective characteristics

表 3 特征选择前后的检测性能对比
Table 3 Comparison of detection performance before and after feature selection

特征数目	训练时间/s	测试时间/s	准确率
83	281.631 2	5.490 0	0.980 1
40	266.966 9	4.798 6	0.990 5

3.2 混合深度学习部分

基于混合深度学习的低速率 DDoS 检测方法主要用于区分 4 种不同类型的低速率攻击流量和正常流量。本文将模拟的 4 种低速率 DDoS 攻击均标识为攻击流量, 进行统一的检测和防御。本文使用的检测方法流程如图 3 所示, 使用混合深度学习算法构建攻击检测模型, 利用生成的数据集实现模型的离线训练, 并将其部署至虚拟环境中实施在线检测。

3.2.1 混合深度学习模型

本文提出使用混合深度学习算法实现多类型

低速率 DDoS 攻击的在线检测。所构建的攻击检测模型利用深度学习算法学习低速率 DDoS 攻击数据集的隐藏特征, 将机器学习算法作为分类器实现多类型低速率 DDoS 攻击的在线检测, 最终准确地检测出多种类型的低速率 DDoS 攻击。

卷积神经网络引入权值共享、池化层和局部感受野^[19], 改善了传统神经网络存在的缺陷。权值共享特性保证卷积平面中的所有卷积单元共享同一个卷积核值; 池化层则减小了数据的尺寸, 改善过拟合问题; 局部感受野使得每个神经元映射到局部特征, 减少训练的权值参数。随机森林则采用 CART 决策树作为弱分类器, 通过 Bagging 的集成学习方法, 将形成的许多决策树结合起来形成森林, 通过投票得到最终分类结果^[19]。该算法能够有效处理高维度数据和不平衡数据, 检测不同特征之间的相关性关系。因此, 本文提出使用随机森林代替卷积神经网络原有的输出层作分

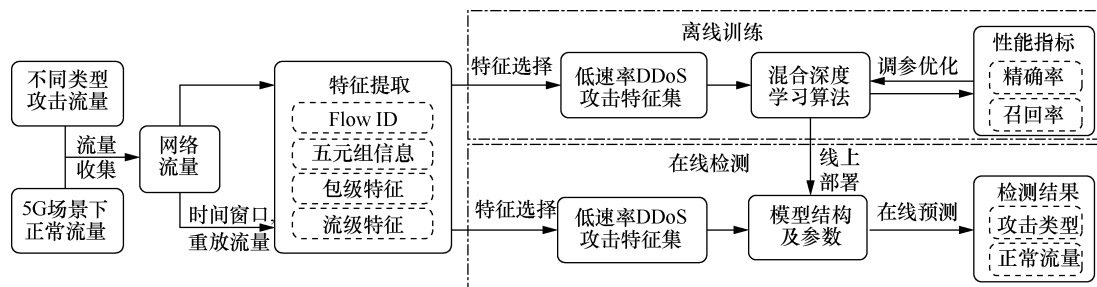


图 3 基于混合深度学习的低速率 DDoS 检测方法流程
Figure 3 Process of low-rate DDoS detection method based on hybrid deep learning

类, 克服 CNN 训练时间过长的问题, 提高模型的检测准确率。

本文提出的 CNN-RF 混合深度学习模型, 能够充分发挥卷积神经网络在特征提取方面的优势和随机森林速度快且不易过拟合的优点。该模型使用卷积层和池化层提取输入数据集特征间的隐藏特性, 之后将其输入 RF 分类器中得到分类结果。

3.2.2 离线训练模块

模型的离线训练阶段, 构建包含卷积层、池化层、全连接层和随机森林算法的 CNN-RF 混合深度学习模型。其中, 卷积层通过权值共享和稀疏连接保证单层卷积具有较小的训练参数; 池化层用于保留输入数据集的显著特征; 全连接层则作为卷积层和池化层之间的连接层, 输出 CNN 提取的隐藏特征。基于特征分析结论, 使用经特征选择的低速率 DDoS 特征集进行混合深度学习算法的训练和测试, 并根据精确率和召回率等性能指标表现对模型进行调参优化, 最后选择分类性能最优的检测模型。

本文提出的 CNN-RF 混合深度学习模型结构如图 4 所示, 包含 3 个卷积层, 3 个最大池化层, 两个零值填充层, 一个 AlphaDropout 层及两个全连接层, 最后一个全连接层的输出作为随机森林分类器的输入, 分类器的输出则作为检测结果。输入的流特征向量经过第一个卷积层以提取抽象的高维度特征, 然后对这些特征进行最大池化处理, 实现特征降维和数据压缩。之后, 经过第二个卷积层和第二个最大池化层, 提取更深层次的特征。同时, 使用零值填充层, 用于保持数据的

边界信息。经过第 3 个卷积层、最大池化层和第二个零值填充层, 得到更高维度的特征向量。之后, 经过 AlphaDropout 层按照一定的概率将神经网络训练单元从网络中移除, 增加各个特征之间的正交性。最后, 将这些高维特征向量输入全连接层, 经过该层的非线性变化提取特征之间的关联。最终, 在输出端使用随机森林分类器, 并通过超参数搜索进行参数调优, 选择性能最优的模型作为最后的随机森林分类器。

本文通过小批量分批的方式标准化处理输入数据的特征。该方式对输入数据进行规范化处理, 通过缩放和平移使得丢弃后仍能保证数据的自规范性, 防止在提取特征时, 模型出现收敛较慢或特征无效等现象。

为了进一步提升模型的泛化性、克服模型的过拟合问题, 本文使用了 AlphaDropout 技术。在 CNN 传递特征向量数据的过程中, AlphaDropout 层将其中 50% 的隐藏神经元输出设置为 0, 即丢弃对后续分类没有贡献的神经元, 使神经网络模型变得稀疏。因此, 该方式能够使 CNN 模型学习更多输入流特征数据本身的特性, 提高 RF 分类器的分类精度。

为验证本文提出的 CNN-RF 混合深度学习算法的性能, 将与同文献[12]提出的 LSTM-LightGBM 算法和文献[13]提出的 LSTM-RF 算法进行对比, 分别在精确率、召回率和 F1 值等方面衡量模型的分类性能。

3.2.3 在线检测模块

在线测试环境中, 重放不同类型的低速率 DDoS 攻击流量和 5G 环境中不同场景下的正常

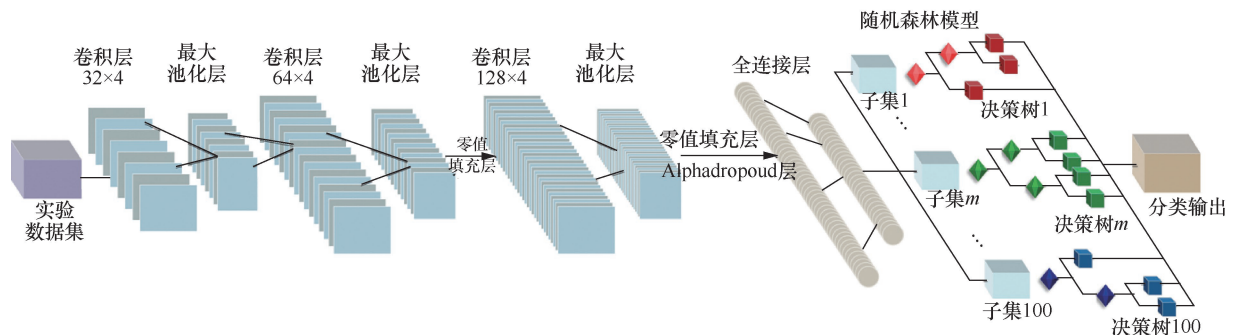


图 4 CNN-RF 混合深度学习模型结构
Figure 4 CNN-RF hybrid deep learning model structure

通信流量, 基于训练好的 CNN-RF 混合深度学习模型在线检测多类型低速率 DDoS 攻击。输出正常流量和不同类型低速率 DDoS 攻击的检测分类结果, 并基于统计的方法分析模型的恶意流量检测率和准确率等性能。

在采用 CNN-RF 混合深度学习模型实现多类型低速率 DDoS 攻击在线检测时, 引入检测时间窗口的概念。本文通过自定义改变检测时间窗口, 实现对网络环境中不同类型低速率 DDoS 攻击的检测。由于较长的检测时间窗口能够存储更多的低速率 DDoS 攻击流量, 并且可以更完整地反映低速率 DDoS 攻击活动。因而引入检测时间窗口, 对于多类型低速率 DDoS 攻击行为的检测具有一定的说服力。

基于多类型低速率 DDoS 攻击特征集中 Flow Duration 的分析, 得到低速率 DDoS 攻击的基准检测时间窗口。通过绘制其核密度估计图, 能够直观地看到特征值的分布特征。以 Slow Body 攻击为例, 该攻击 Flow Duration 特征值的核密度估计如图 5 所示, 可见该攻击特征值分布在 0.6×10^{-8} 的概率最大, 特征值计数单位为毫秒, 则表示分布在 60 s 的概率最大, 其他 3 种类型的低速率攻击表现相同。因此, 多类型低速率 DDoS 攻击的基准检测时间窗口为 60 s。

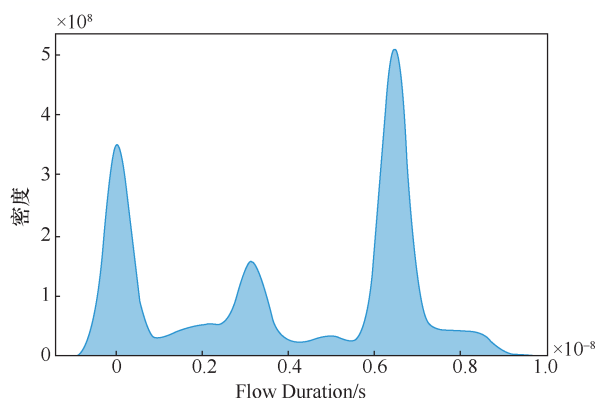


图 5 Flow Duration 的核密度估计图
Figure 5 A kernel density estimate for Flow Duration

按照选定的检测时间窗口获取网络流量并提取流特征信息, 依据特征分析结论进行特征选择, 得到低速率 DDoS 攻击特征集。在线读取已训练好的多类型低速率 DDoS 攻击检测模型结构及参数, 依次将缓存区的低速率 DDoS 攻击数据集输

入攻击检测模型。该模型输出信息包含预测标签和真实标签, 基于统计的方法计算恶意流量检测率和准确率等指标, 分析模型在线检测的性能。

4 实验与结果分析

本文实验模拟 5G 环境下多种类型的低速率 DDoS 攻击和正常通信请求, 分别进行了不同混合深度学习检测模型的性能评估及不同检测时间窗口下的在线检测性能测试。

4.1 实验环境

为验证本文方法对于多类型低速率 DDoS 攻击的检测效果, 在网络平台采用真实的网络设备搭建了相关测试平台, 其拓扑结构如图 6 所示。

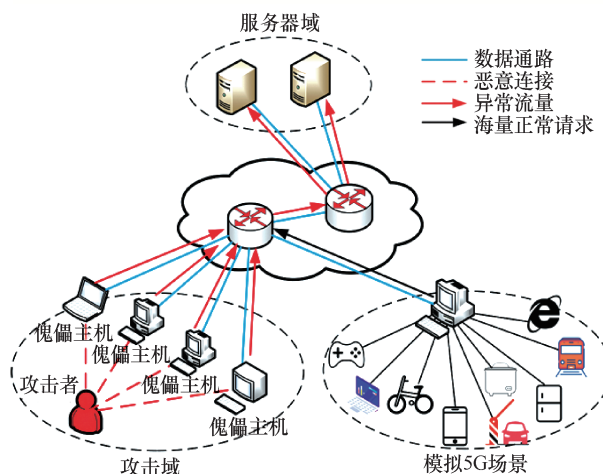


图 6 低速率 DDoS 攻击实验拓扑结构
Figure 6 Low-Rate DDoS attack experimental topology

本文实验搭建了基于 VMware vSphere 的虚拟平台作为实验环境。实验一共使用 9 台主机, 其中包含两台路由器、一台客户端主机、4 台傀儡主机和两台 Web 服务器。本文实验基于 TensorFlow 框架构建混合深度学习模型, 编程语言采用 Python3.8, 并使用 TensorFlow2.1、Keras2.2.4 的机器学习库进行模型搭建, 软件环境为 Ubuntu18.04 Server 操作系统, 虚拟核数为 8, 内存为 8 GB。图 6 中将 4 台主机作为傀儡主机, 两台搭建 Web 服务器的虚拟机作为被攻击服务器, 在网络入口路由器处实施检测, 并提供数据的采集和数据清洗功能。

如图 6 所示, 正常用户使用 Python 脚本在客户端和服务端之间建立连接, 基于此连接模拟了

包含公共服务、智能家居、PC 机上网及 MTC 通信的 4 种场景，生成了海量正常通信数据请求。低速率 DDoS 攻击由攻击者控制 4 台傀儡主机周期性地向 Web 服务器发送基于 HTTP 协议和基于 TCP 协议的低速率 DDoS 攻击。实验的低速率 DDoS 攻击类型选择基于 HTTP 协议的 Slow Headers 攻击、Slow Body 攻击、Slow Read 攻击和基于 TCP 协议的 Shrew 攻击。

4.2 评估指标

低速率 DDoS 攻击检测框架基于混合深度学习算法对多类型低速率 DDoS 攻击数据实现离线训练和在线检测。离线训练主要通过准确率、精确率、召回率、 $F1$ 值、检测时间和混淆矩阵 6 个评估指标来分析模型的分类性能。其中，准确率表示模型分类正确样本数占总样本数的比例；精确率表示模型判断为攻击类型的样本数中，真正为攻击类型样本数所占的比例；召回率表示模型判断为攻击类型的样本数占所有该攻击类型样本数的比例； $F1$ 值综合了查准率和查全率的结果，表示两者的调和平均值，能够更准确地反映模型性能；检测时间反映模型的时间复杂度情况，用于衡量模型的时间效率；混淆矩阵则用于分析模型的分类效果及预测标签与实际标签相匹配的程度，在数值上与召回率相对应。

此外，为分析在线检测的分类情况，新定义评估指标：错误拦截率和恶意流量检测率，将其用于评估正常和恶意流量的在线检测情况。其中，错误拦截率表示将正常流量误判为不同类型低速率 DDoS 攻击的比例，计算如式(1)所示；恶意流量检测率表示检测出的恶意流量占总恶意流量样本数的比例，如式(2)所示。

$$\text{错误拦截率} = \sum_{i=1}^4 F_i / N \quad (1)$$

$$\text{恶意流量检测率} = 1 - \sum_{i=1}^4 T_i / \sum_{i=1}^4 A_i \quad (2)$$

其中， F_i 表示经在线检测后将网络环境中的正常流量误判为其他 4 种类型低速率 DDoS 攻击流量的数据样本数； N 表示网络环境中正常流量的总数据样本数； T_i 则表示经在线检测后网络环境中低速率 DDoS 攻击流量未被检测出的数据样本

数； A_i 表示网络环境中不同类型低速率 DDoS 攻击的总数据样本数。

4.3 离线训练分析

基于 3.1 节数据集生成模块得到的低速率 DDoS 攻击数据集，对其进行数据清洗，包括处理特征值为空及处理特征值为无穷大的特征数据等。根据图 2 所示的 40 种有效特征进行特征选择，并以 7:3 的比例划分为训练集和测试集，数据集如表 4 所示。低速率 DDoS 攻击特征数据集的总数据样本数为 794 919 条，其中包括训练集 556 444 条，测试集 238 475 条。

表 4 低速率 DDoS 攻击数据集
Table 4 Low-Rate DDoS attack dataset

数据集类型	正常流量样本数	攻击流量样本数
训练集	288 544	267 900
测试集	129 632	108 843

在输入相同低速率 DDoS 攻击数据集和特征值的情况下，通过超参数搜索获得最优性能时的 CNN-RF 模型。同时，将本文提出的 CNN-RF 模型同 LSTM-LightGBM 模型和 LSTM-RF 模型作比较，从中选择最优的混合深度学习模型实现多类型低速率 DDoS 攻击的在线检测。本文使用了检测时间、精确率、 $F1$ 值和混淆矩阵 4 个评估指标。图 7 展示了 3 种混合深度学习模型的混淆矩阵表现。由图 7 可知，LSTM-LightGBM 模型对每种流量类型的识别准确率表现差异较大，尤其是对 Slow Body 攻击的识别准确率仅为 0.556 5，对 Slow Headers 攻击产生 0.269 5 的误报率；LSTM-RF 模型对 5 种流量类型的识别准确率均优于 LSTM-LightGBM 模型，尤其对 Slow Read 攻击的识别准确率达到 0.999 2 左右，但在识别 Slow Body 攻击时会产生 0.078 8 的误报率；CNN-RF 模型的准确率表现均优于 LSTM-RF，特别是对 Slow Read 攻击和 Shrew 攻击的识别准确率可达到 0.999 9，同时对于 Slow Headers 攻击流量的识别准确率也可达到 0.956 6。

图 8 展示了 3 种模型在精确率和 $F1$ 值方面的性能表现。由图 8 可知，对于正常良性流量的识别，CNN-RF 模型在精确率和 $F1$ 值上的表现均优于其他两种模型；对于 Slow Headers 攻击流量的检测，CNN-RF 模型的精确率表现最优，LSTM-RF

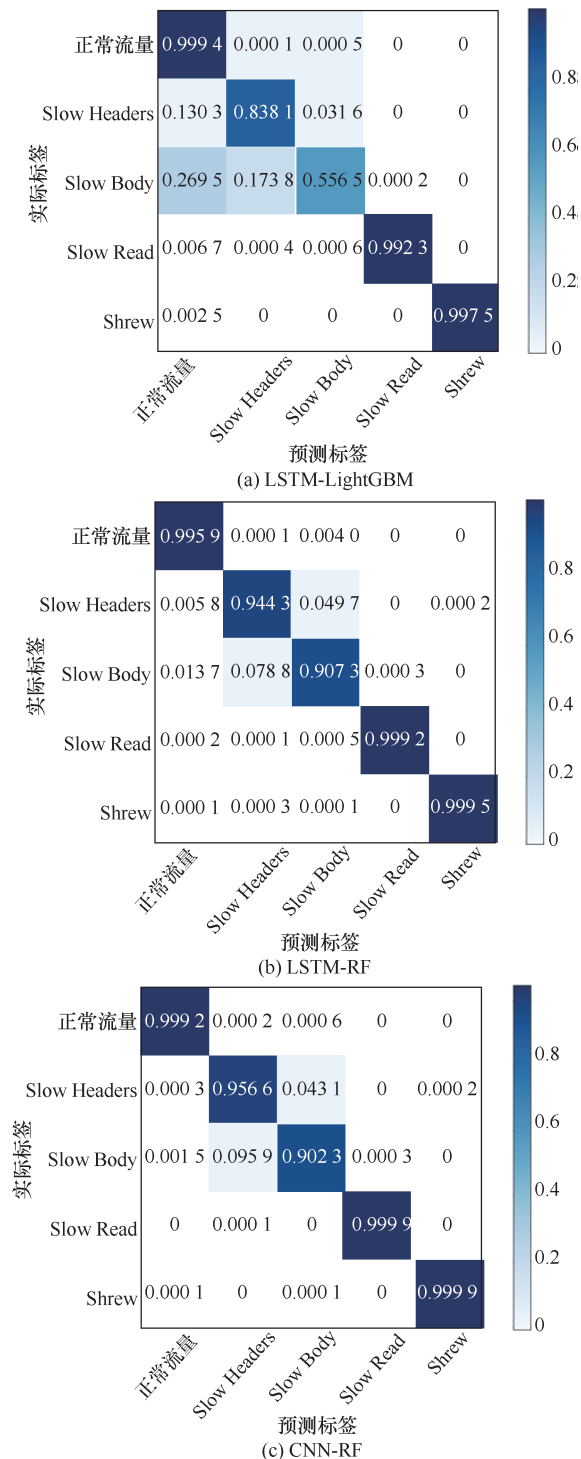
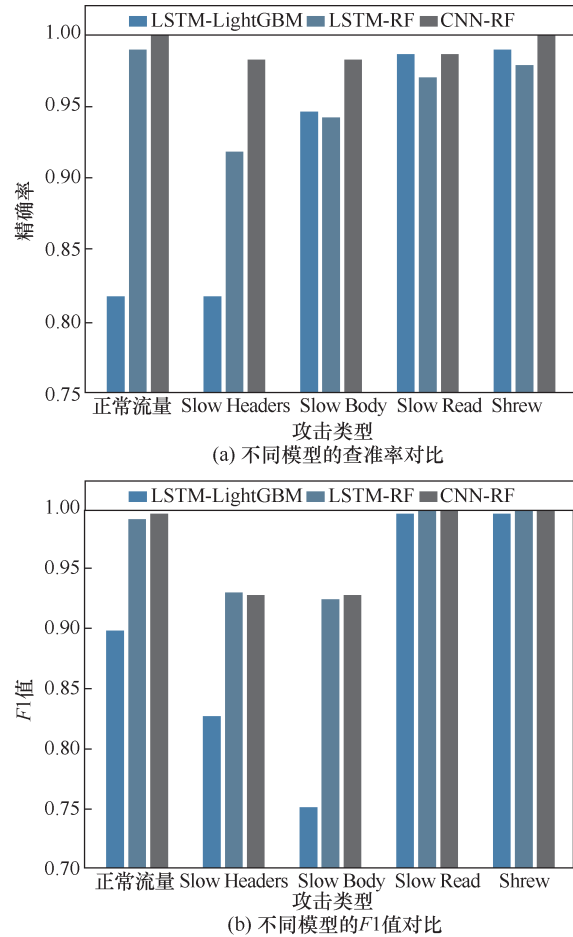


图 7 不同模型的混淆矩阵对比

Figure 7 Comparison of confusion matrix of different models

和 LSTM-LightGBM 模型在 $F1$ 值上表现相似; 对于 Slow Body 和 Slow Read 攻击流量的检测, LSTM-LightGBM 模型在精确率和 $F1$ 分数上的表现都较差, CNN-RF 模型的表现最优; 对于 Shrew

攻击流量的检测, 3 种模型在两种评估指标中均表现良好。

图 8 不同模型的精确率和 $F1$ 分数对比Figure 8 Comparison of precision and $F1$ scores of different models

不同混合深度学习模型的检测时间对比如表 5 所示。由表 5 可知, CNN-RF 模型的检测时间为 268.235 4 s, 比 LSTM-LightGBM 模型检测时间多约 9 s, 相比 LSTM-RF 模型检测时间减少约 40 s。但 LSTM-LightGBM 模型在检测精确率和 $F1$ 分数方面, 均明显低于 CNN-RF 模型。因此, CNN-RF 模型在检测时间较短的同时, 对于各类别低速率 DDoS 攻击和正常流量的精确率和 $F1$ 值均有更为优异的表现。

表 5 不同模型的检测时间对比
Table 5 Comparison of detection time of different models

模型类别	LSTM-LightGBM	LSTM-RF	CNN-RF
检测时间/s	259.894 7	308.493 2	268.235 4

综合上述评价指标可以得出,相较于 LSTM-LightGBM 模型和 LSTM-RF 模型,本文提出的 CNN-RF 模型在正常流量、Slow Headers 攻击、Slow Body 攻击、Slow Read 攻击和 Shrew 攻击流量的检测分类方面均表现出优异的性能,能够准确检测出不同类型的低速率 DDoS 攻击。

4.4 在线检测验证

经 4.3 节离线训练实验及分析表明 CNN-RF 模型具有优异的检测性能。为进一步说明该模型在线检测时性能仍为最优,本节从准确率、错误拦截率和恶意流量检测率方面,对比了 LSTM-LightGBM、LSTM-RF 和 CNN-RF 模型的性能。最终,选择最优时间窗口下性能最优且已训练好的模型,部署实现多类型低速率 DDoS 攻击的细粒度在线检测。首先,在线重放多类型低速率 DDoS 攻击流量文件,使用 Tcpdump 抓取指定检测时间窗口内的网络流量,并通过 CICFlowMeter 提取流特征信息;然后,读取已训练好的检测模型结构及参数并实施在线检测,模型输出检测分类标签、真实标签及恶意流量 IP 地址;最后,基于统计的方法查看模型的检测准确率和恶意流量检测率等指标。

本节依据基准检测时间窗口 60 s,将其与 120 s 和 180 s 的检测时间窗口进行性能对比,并分别比较 LSTM-LightGBM、LSTM-RF 和 CNN-RF 模型的性能表现,选择最优检测模型下的最优检测时间窗口作为最终的在线检测参数。表 6 展示了不同模型在不同时间窗口下的准确率、错误拦截率和恶意流量检测率的性能对比。

表 6 不同模型在不同时间窗口下在线检测性能对比
Table 6 Comparison of online detection performance of different models in different time windows

模型名称	时间窗口/s	准确率	错误拦截率	恶意流量检测率
LSTM-LightGBM	60	0.853 4	0.249 7	0.852 4
	120	0.896 5	0.203 1	0.895 7
	180	0.873 9	0.210 2	0.872 2
LSTM-RF	60	0.908 0	0.201 1	0.898 6
	120	0.924 3	0.174 1	0.919 3
	180	0.897 6	0.192 7	0.892 9
CNN-RF	60	0.953 7	0.170 9	0.951 0
	120	0.965 2	0.110 3	0.962 2
	180	0.958 8	0.251 4	0.958 3

由表 6 可知,在 120 s 的时间窗口下,LSTM-LightGBM、LSTM-RF 和 CNN-RF 模型均表现出相对最优的检测性能。LSTM-RF 模型的准确率达到 0.924 3,恶意流量检测率为 0.919 3。而当检测时间窗口为 180 s 时,LSTM-RF 模型的准确率下降至 0.897 6;同时,错误拦截率提高至 0.192 7,表示将大量的正常良性流量误判为恶意流量。在 120 s 的时间窗口下,LSTM-LightGBM 模型表现最差,准确率仅为 0.896 5,错误拦截率则是 0.203 1。对于 CNN-RF 模型,当在线检测时间窗口为 120 s 时,错误拦截率最低为 0.110 3,即正常流量被误判为恶意流量的比例最低;同时,通过该检测机制检测出的恶意流量数据样本数所占比例达 0.962 2。经分析,120 s 的检测时间窗口下完整地包含不同类型低速率 DDoS 攻击的特征信息,反映了完整的低速率 DDoS 攻击活动,从而有效区分不同类型的低速率 DDoS 攻击和正常流量。

因此,将检测时间窗口设置为 120 s,部署性能最优的 CNN-RF 模型实现在线检测。通过在线检测得到针对不同类型低速率攻击及正常流量的检测性能,如表 7 所示。由表 7 可得,CNN-RF 混合深度学习模型对于 Slow Headers 攻击、Shrew 攻击和正常流量的精确率均达到 0.95 以上;对于 Slow Read 攻击和 Slow Body 攻击流量的精确率和召回率均为 0.86 以上,两种攻击类型间产生较少的误判。综上,CNN-RF 混合深度学习模型对于每种类型低速率 DDoS 攻击和正常流量的检测准确率达到 0.965 2,能够准确地在线检测出不同类型的低速率 DDoS 攻击。

表 7 120 s 时间窗口下的在线检测性能
Table 7 Online detection performance under 120 s time window

流量类型	精确率	召回率	准确率
Slow Headers	0.954 6	0.866 6	0.965 2
Slow Body	0.995 2	0.863 9	
Slow Read	0.864 2	0.994 8	
Shrew	0.999 8	0.999 4	
正常流量	0.999 9	0.999 5	

通过上述分析可见,本文提出的 CNN-RF 混合深度学习模型在线检测性能优异,能够实现对

4 种类型低速率 DDoS 攻击的在线检测。同时, 每种低速率 DDoS 攻击的精确率均达 0.85 以上, 能够防止该攻击给网络造成更大的破坏; 恶意流量检测率达到 0.962 2, 检测准确率达到 0.965 2, 能够有效地在线检测出网络中的恶意流量, 降低了网络入口处的低速率 DDoS 攻击流量强度。

5 结束语

本文针对 4 种类型的低速率 DDoS 攻击, 获得了低速率 DDoS 攻击数据集, 分析得到了低速率 DDoS 攻击的 40 种有效特征, 提出了一种基于 CNN-RF 混合深度学习的多类型低速率 DDoS 攻击检测方法, 在线部署该模型实现了多类型低速率 DDoS 攻击的在线检测。此外, 提出在线检测时间窗口的概念, 并使用错误拦截率和恶意流量检测率评估了在线检测性能。实验表明基于 CNN-RF 混合深度学习算法的模型能够准确检测出不同类型的低速率 DDoS 攻击。同时, 本文的检测方法有高度的可移植性, 所用的低速率 DDoS 攻击数据集接近真实情况, 可以部署并应用在实际环境中。

混合深度学习模型在针对多类型低速率 DDoS 攻击实现训练和检测时, 不同场景下在线检测精度有所下降, 与攻击流量发送速率和正常流量在检测窗口中的占空比有关系。未来将研究优化模型及时间窗口, 分析时间窗口与数据集和特征选择之间的关系, 使该模型更好地适应环境且具有更高的准确率和检测效率。

参考文献:

- [1] 陈兴蜀, 滑强, 王毅桐, 等. 云环境下 SDN 网络低速率 DDoS 攻击的研究[J]. 通信学报, 2019, 40(6): 210-222.
CHEN X S, HUA Q, WANG Y T, et al. Research on low-rate DDoS attack of SDN network in cloud environment[J]. Journal on Communications, 2019, 40(6): 210-222.
- [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] WU X, TANG D, TANG L, et al. A low-rate DoS attack detection method based on Hilbert spectrum and correlation[C]//Proceedings of 2018 IEEE Smart-World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation. 2018: 1358-1363.
- [4] WU Z, PAN Q, YUE M, et al. Sequence alignment detection of TCP-targeted synchronous low-rate DoS attacks[J]. Computer Networks, 2019, 152: 64-77.
- [5] KAUR G, SAXENA V, GUPTA J P. Detection of TCP targeted high bandwidth attacks using self-similarity[J]. Journal of King Saud University: Computer and Information Sciences, 2020, 32(1): 35-49.
- [6] ZHANG D, TANG D, TANG L, et al. Pca-svm-based approach of detecting low-rate DoS attack[C]//Proceedings of 2019 IEEE 21st International Conference on High Performance Computing and Communications. 2019: 1163-1170.
- [7] LIU Z, YIN X, HU Y. CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-Learning[J]. IEEE Access, 2020, 8: 42120-42130.
- [8] WU Z J, XU Q, WANG J J, et al. Low-rate DDoS attack detection based on factorization machine in software defined network[J]. IEEE Access, 2020, 8: 17404-17418.
- [9] PÉREZ-DÍAZ J A, VALDOVINOS I A, CHOO K K R, et al. A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning[J]. IEEE Access, 2020, 8: 155859-155872.
- [10] MALIK J, AKHUNZADA A, BIBI I, et al. Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN[J]. IEEE Access, 2020, 8: 134695-134706.
- [11] GARG S, KAUR K, KUMAR N, et al. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: a social multimedia perspective[J]. IEEE Transactions on Multimedia, 2019, 21(3): 566-578.
- [12] GUO Y K, LI Y Y, XU Y. Study on the application of LSTM-LightGBM model in stock rise and fall prediction[J]. MATC Web of Conferences, 2021, 336: 05011.
- [13] HU W, SHI Y X. Prediction of online consumers' buying behavior based on LSTM-RF model[C]//Proceedings of 2020 5th International Conference on Communication, Image and Signal Processing (CCISP). 2020: 224-228.
- [14] JAZI H H, GONZALEZ H, STAKHANOVA N, et al. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling[J]. Computer Networks, 2017, 121: 25-36.
- [15] 王子恒. 基于区块链的海量连接管理架构设计与实现[D]. 北京: 北京交通大学, 2021.
WANG Z H. Design and implementation of mass connection management architecture based on blockchain[D]. Beijing: Beijing Jiaotong University, 2021.
- [16] ROSENBROCK K H, ANDERSEN N P S. The third generation partnership project (3GPP)[M]//GSM and UMTS. Chichester, UK: John Wiley & Sons, Ltd., : 221-261.
- [17] PACKET S. Institute of electrical and electronics engineers[J]. IEEE Standard Computer Dictionary a Compilation of IEEE Standard Computer Glossaries, 2009, 3(8): 128.
- [18] GUALBERTO E S, DE SOUSA R T, DE BRITO VIEIRA T P, et al. The answer is in the text: multi-stage methods for phishing detection based on feature engineering[J]. IEEE Access, 2020, 8: 223529-223547.
- [19] SUSILO B, SARI R F. Intrusion detection in IoT networks using deep learning algorithm[J]. Information, 2020, 11(5): 279.

[作者简介]



李丽娟（1997-），女，山东泰安人，北京交通大学硕士生，主要研究方向为人工智能、网络安全。



毕红军（1965-），男，山东潍坊人，北京交通大学副教授，主要研究方向为光通信、网络安全。



李曼（1997-），女，河南洛阳人，北京交通大学博士生，主要研究方向为网络安全、智能通信。



周华春（1965-），男，博士，北京交通大学教授、博士生导师，主要研究方向为智能通信、移动互联网、网络安全与卫星网络。