文章编号:1671-4598(2023)07-0028-07 DOI:10.16526/j.cnki.11—4762/tp.2023.07.005 中图分类号:TP393.08 文献标识码:A

边缘计算环境下基于深度学习的 DDos 检测

田 婷[1],虞延坤[2],牛新征[3]
(1.四川省公安科研中心,成都 610000;2.西南石油大学 计算机科学学院,成都 610500;
3.电子科技大学 计算机科学与工程学院,成都 611731)

摘要:边缘计算作为一种用于降低中心节点计算压力,更靠近终端设备和数据源头的新计算范式,满足了计算业务下沉的需求,也带来了安全问题;其中,对边缘计算安全威胁最大、造成过巨大经济损失和安全事故的当属分布式拒绝服务攻击(DDos);边缘计算环境下由于算力受限、存储空间有限等原因,传统的防御手段难以应用;因此,提出了一种适用于边缘计算环境下的基于深度学习的轻量级 DDos 检测框架;采用 CIC-DDos-2019 数据集来模拟边缘计算环境下的遭受 DDos 攻击的网络流量,针对数据集进行了适应性强的预处理技术和相似性标签融合,运用 SMOTE 算法解决了数据集类别不平衡问题,采用一维卷积技术和 BiLSTM 技术搭建了模型并进行了模型剪枝,构建了一个轻量级模型;结果表明,其针对 DDos 攻击类别的八分类实验准确率达到了 96.8%,二分类实验准确率达到了 99.8%。

关键词:边缘计算;分布式拒绝服务攻击;深度学习;入侵检测;一维卷积;BiLSTM

DDoS Detection Based on Deep Learning in Edge Computing Environment

TIAN Ting[1], YU Yankun[2], NIU Xinzheng[3]
(1. Sichuan Provincial Public Security Research Center, Chengdu 610000, China;
2. Southwest Petroleum University, Chengdu 610500, China;
3. University of Electronic Science and technology, Chengdu 611731, China)

Abstract: Edge computing is taken as a new computing paradigm with close terminal devices and data sources, it reduces the pressure of central nodes, meets the needs of calculating subsidence, and also brings security questions. Among them, a distributed denial of service (DDos) is the most threaten security of edge computing, and causes enormous economic losses and security accidents. In edge computing environment, traditional defense methods are difficult to apply due to the causes of limited computing power and lack storage space. Therefore, a lightweight DDoS detection framework based on deep learning for the edge computing environment is proposed. CIC-DDos-2019 data set is used to simulate the network traffic attacked by DDoS in the edge computing environment. The adaptive preprocessing technology and similarity label fusion are carried out for the data set. The SMOTE algorithm is used to solve the problem of the data set category imbalance, and the one-dimensional convolution technology, BiLSTM technology are used to construct the lightweight model and and prune the model, which builds a lightwight model. The results show that it achieves the experimental accuracy of 96.8% in 8-class and that of 99.8% in 2-class for the DDos attack categories.

Keywords: edge computing; distributed denial of service attack; deep learning; IDS; One dimensional convolution; BiLSTM

0 引言

随着物联网技术和云端理念愈发成熟,以往的云计算和雾计算不能满足日益增长的计算业务下沉需求,为了减小中心节点的计算压力并且更多地利用边缘节点的算力和存储资源,边缘计算架构应孕而生。边缘计算无限接近终端设备,能够实时地接收来自数据源头的信息,是一种解决计算、存储卸载问题的计算范式。它作为云计算的扩展,弥补了中心化后产生的一系列缺点,实现了高连续性和低时延性,更适合部署实时性高的智能化任务。随着边缘计算的应用部署,随之衍生出了与之相关的网络安全领域课题,其中针对边缘节点的攻击防御问题备受关注。分布式拒绝服务攻击(DDos)是一种隐蔽性高的大型分布式网络攻击,攻击者可以组建分布式僵尸网络向边缘节点发起洪水般的拒绝服务攻击。通常情况下,攻击者会伪造源 IP,这使得攻击源头极具隐蔽性,检测攻击来源地址也变得极其困难。边缘计算环境下的物联网设备结构简单脆弱,往往难以防御 DDos 攻击,列举近期的一些典型 DDos 攻击案例,比如 Mirai 僵尸网络对 KrebsOnSecurity 的攻击[1]和 Dyn 攻击[2],大都产生了巨大的经济损失和安全威胁。由于物联网设施的连通性和开放性增加,整个物联网的受攻击

收稿日期:2022-09-22; **修回日期**:2022-12-05。
基金项目:四川省科技计划项目(2021YFS0391)。
作者简介:田 婷(1986-),女,四川成都人,大学本科,工程师,主要从事大数据智能应用、通信工程方向的研究。
牛新征(1978-),男,河南唐河人,博士,教授级高工,CCF 高级会员,主要从事移动社交网络和智能视频分析,分布式计算方向的研究。
引用格式:田 婷,虞延坤,牛新征.边缘计算环境下基于深度学习的 DDos 检测[J].计算机测量与控制,2023,31(7):28-34,168.

面也因此扩展，使得 DDos 攻击的危害性也随之上升。边缘节点计算能力和存储空间受限且缺乏有效的安全保护，从而非常容易受到 DDos 攻击。

传统的防御和检测技术难以运用在边缘节点上，虽然边缘节点能够隔绝大部分来自于网络边缘的数据且能在第一时间检测到并拦截最近的 DDos 攻击，但是部署现有的集中式 DDos 检验方式或框架难以满足边缘节点的需求，这种解决方案通常没有考虑到边缘节点算力受限、存储空间小、网络波动大等特点。所以有必要设计一种基于边缘计算环境下的轻量级 DDos 攻击检测方案[3]，以此来克服检测准确率低、误报率高、时延长、算力和存储能力不足等问题。

最近，网络安全领域也开始采用在图像、语言领域大放异彩的深度学习来解决一些棘手的安全问题，深度学习为解决 DDos 攻击的威胁提供了新思路。He 等人[4]基于机器学习技术提出了云端服务器的 DDos 检测方法，He 等人采用的方法分别有线性回归、支持向量机、决策树、朴素贝叶斯、随机森林、无监督 K 均值和高斯期望最大化等方法，每种方法都在一组自主生成的包含 4 种攻击的数据上进行测试并比较这些方法之间的得分，得分最高的是随机森林法，这些机器学习算法能大致满足 DDos 的检测要求，但是检测结果的指标得分并不高，存在较大的提高空间。R. C. Staudemeyer 等人[5]尝试将网络流量异常检测领域和 LSTM 算法结合起来，实验结果表明 LSTM 具备良好的检测异常流量能力，证明了循环神经网络在流量分析领域具有极大的可研价值，但本文使用的数据集发布时间较早，缺少一些现代的 DDos 攻击类型，使得实验结果缺少说服力。Elyased 等人[6]针对 CIC-DDos-2019[7]数据集实现了一种基于深度学习的 DDos 检测方法，该方法由循环神经网络和自动编码器组成，经过一个数据预处理阶段后，在训练阶段得到一个二分类模型，以此判断网络流量是恶意攻击还是良性的。Can 等人[8]增强了 CIC-DDos-2019 的不平衡数据集，使用了自动特征选择来解决数据集存在的不均衡问题。Ferrag 等人[9]针对 CIC-DDos-2019 数据集使用深度学习的经典网络进行训练，但未针对性地做出结构优化。Chartuni A 等人[10]针对 CIC-DDos-2019 数据集进行了预处理和标签处理，并基于 DNN 网络训练了一个 DDos 多分类器，为 DDos 的检测提供了一个可参考的范式。

1　模型设计

1.1　边缘计算环境下的 DDos 检测模型

本文结合一维卷积和 BiLSTM 等深度学习理论，设计了一种适合边缘计算环境下的轻量级 DDos 检测模型，通过剪枝操作得到最佳的模型结构。将网络流量数据送入三层一维卷积构成的卷积层以提取空间特征，随后展平送入 BiLSTM 层以提取时间特征，最后通过全连接层和 Softmax 层输出。本文提出的这种模型不仅可以有效提取和学习网络流量数据的空间特征和时间特征，且通过剪枝操作调整参数量从而对模型进行了轻量化处理。实验证明，本模型能够更好地在边缘计算环境中算力受限、存储空间受限情况下完成防御和检测 DDos 攻击的任务。该网络结构模型如图 1 所示。

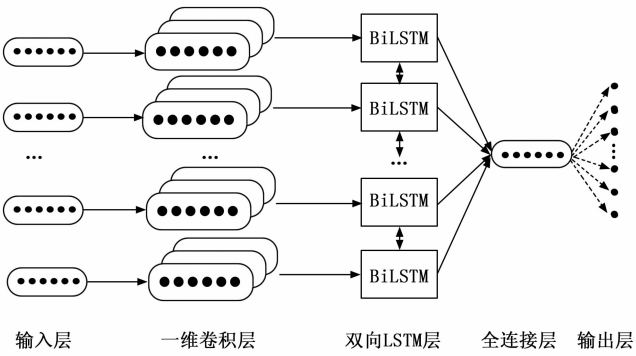

图 1　网络结构模型

1.2　一维卷积层

卷积层是深度学习中用于提取局部特征的有效方法，一维卷积常用于处理序列数据[13]。网络流量数据的属性通常是序列化的数值串。对比常用的二维卷积，使用一维卷积进行特征提取后，实验准确率提到了有效提升，故本文没有采用常见的二维卷积法来提取特征。提取此类数据的局部特征图。一维卷积层效果更佳，将提取后的特征图作为下一层网络的输入，随着卷积层深度的增加，神经网络将学习到不同维度的特征。一维卷积运算公式如式（1）所示：

$$y^j = f\left(\sum_i k^{ij} * x^j\right) \tag{1}$$

式（1）中，x^j 为第 j 个输入特征图，i 为一维卷积的层数，k^{ij} 为所使用的卷积核，$*$ 代表卷积运算且采用“same”填充方式，f（）为激活函数，本文采用 ReLU 来进行非线性化处理，卷积层不填加偏置。

每个卷积激活层后接一个 BN（batch normalization）层[16]，通过 BN 层的处理，可以使该层的特征值符合标准正态分布，减小了训练过程中发生梯度相关问题（消失或爆炸）的可能性，加快了模型收敛的速度。BN 层的运算公式如式（2）所示：

$$\mathrm{BN}(y^j) = \boldsymbol{\gamma} \odot \frac{y^j - \hat{\boldsymbol{\mu}}_B}{\hat{\boldsymbol{\sigma}}_B} + \boldsymbol{\beta} \tag{2}$$

式（2）中，y^j 为非线性化后输入 BN 层的特征图，$\hat{\boldsymbol{\mu}}_B$ 为 y^j 的平均值，$\hat{\boldsymbol{\sigma}}_B$ 为 y^j 的方差值，$\boldsymbol{\gamma}$ 为标准化后再次进行缩放的参数，$\boldsymbol{\beta}$ 为标准化后进行平移的参数。

1.3　*BiLSTM* 层

通过卷积层提取到网络流量数据的各维度特征图后，变换形状以适应性输入 BiLSTM 层。BiLSTM 层[17]（双向长短时记忆层）是一种特殊的循环神经网络结构，相比一般的 RNN，它能够兼顾在前向和后向两个方向输入的网络流量数据信息，此种双向信息收集的性质极大地加强了全局性，使它能对数据的时间特征进行有效的提取。BiLSTM 模型的网络体系结构如图 2 所示。

BiLSTM 单元设置有输入门 i、遗忘门 f 和输出门 o，

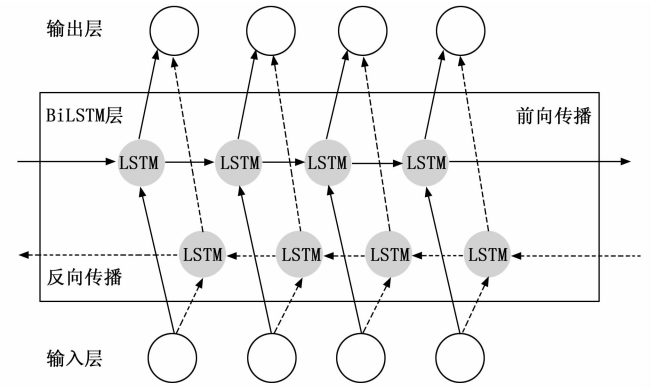

图 2 BiLSTM 网络体系结构

当前时刻数据 x_t 进入时，结合内部存储单元 c_{t-1} 和输出 h_{t-1} 进行计算得出当前输出 h_t，然后及时更新内部存储单元 c_t[18]。遗忘门的运算公式如式（3）所示：

$$f_t = \text{sigmoid}(W_{xf}x_t + W_{hf}h_{t-1} + b_f) \tag{3}$$

i 为 $\widetilde{C}_t$ 中的每个单元生成区间在［0，1］的对应值，用以控制添加新信息的量，输入门的运算公式可以表示为式（4）～（6）：

$$C_t = \text{sigmoid}(f_t \cdot C_{t-1} + i_t \cdot \widetilde{C}_t) \tag{4}$$

$$i_t = \text{sigmoid}(W_{xi}x_t + W_{hi}h_{t-1} + b_t) \tag{5}$$

$$\widetilde{C}_t = \tan h(W_c x_t + W_c h_{t-1} + b_c) \tag{6}$$

i 用于筛选当前单元状态的数量，可以表示为式（7）：

$$o_t = \text{sigmoid}(W_{xo}x_t + W_{ho}h_{t-1} + b_o) \tag{7}$$

对于时刻 t 处的 BiLSTM 模型，输出 h_t、$\overleftarrow{h}_t$ 和 $\vec{h}_t$ 可以表示为式（8）～（10）：

$$h_t = \overleftarrow{h}_t + \vec{h}_t \tag{8}$$

$$\vec{h}_t = \tan h(W_{x\vec{h}}x_t + W_{\vec{h}\vec{h}}\vec{h}_{t-1} + b_{\vec{h}}) \tag{9}$$

$$\overleftarrow{h}_t = \tan h(W_{x\overleftarrow{h}}x_t + W_{\overleftarrow{h}\overleftarrow{h}}\overleftarrow{h}_{t-1} + b_{\overleftarrow{h}}) \tag{10}$$

x 代表输入，W 代表单元之间的连接权重，b 是偏置向量，“·”代表点积运算。

1.4 Softmax 层

数据经过 BiLSTM 后，进入全连接层和 Softmax 层。该层是一种多分类器，表达式如式（11）所示：

$$\text{Softmax}(x) = \frac{e^{x_i}}{\sum_t e^{x_t}} \tag{11}$$

该层能转化实数范围内的分类结果数值，然后通过交叉熵损失函数来评测本文模型的检测结果。

2 实验结果与分析

2.1 数据集的选择

为了更真实地模拟边缘计算场景下遭受 DDos 攻击下的网络流量数据，本文调研了多个不同场景下的数据集，最后筛选出 3 个数据集来源：NSL-KDD 数据集[12]，由加拿大网络安全研究所（CIC）公开提供的 CIC-IDS-2017 数据集[11]和 CIC-DDos-2019 数据集[7]。

3 个数据集的内容都是针对被攻击情况下捕获的完整的网络流量信息，数据量充足，适合进行深度学习模型训练。但是 NSL-KDD 数据集缺乏 NTP、TFTP 和 NetBIOS 等现代 DDos 攻击方式，且训练集和测试集的攻击种类不相等。CIC-IDS-2017 数据集加入了以往数据集缺乏现代攻击方式，其中包含 DDos 攻击，但是并没有针对 DDos 攻击进行细粒度划分，该数据集主要包含漏洞 Web 攻击，且存在类别不均衡的问题。基于对所研究数据集的评估和分析，本文决定使用 CIC-DDos-2019 数据集对所用模型进行训练和验证。

CIC-DDos-2019 数据集的内容是由 CIC 机构在两天内不同时间段采用不同的 DDos 攻击方式进行攻击测试，数据集中的部分时段加入了网络受限和网络波动等干扰因素，能够更贴近边缘计算环境下的网络流量数据，记录整理得出的具体分类如图 3 所示[7]。该数据集针对性地克服了过往数据集的缺点，提出了一种新的 DDoS 攻击分类法[7]，主要分为两个主类：基于反射的 DDos 攻击和基于漏洞利用的 DDos 攻击。

1）基于反射的 DDos，指的是那些利用合法的第三方组件且执行过程中隐藏攻击者身份的攻击。攻击者伪装 IP 地址，使用反射服务器发送响应数据包，使被攻击者发生过载。在该数据集中根据使用协议，进一步细分为了基于 TCP 的攻击包括 MSSQL、SSDP，基于 UDP 的攻击包括 CharGen、NTP、TFTP，以及使用 TCP 或 UDP 的攻击包括 DNS、LDAP、NETBIOS 和 SNMP。

2）基于漏洞利用的 DDos 攻击，与基于反射的 DDos 攻击相似，不同点在于这些攻击可以通过使用传输层协议的应用层协议进行。具体可细分为基于 TCP 的攻击 SYN Flood，基于 UDP 的攻击包括 UDP Flood 和 UDP Lag。

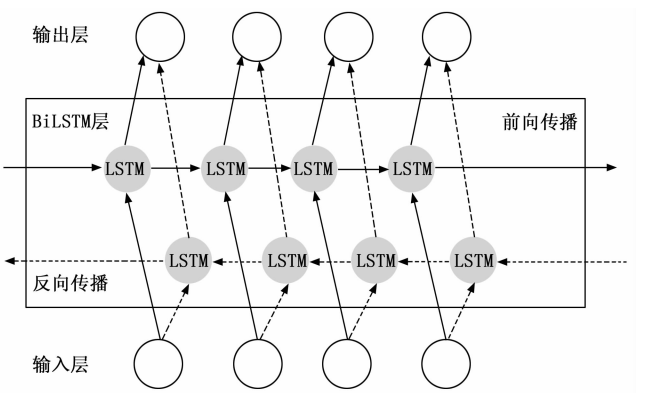

图 3 CIC-DDos-2019 数据集中的 DDos 攻击分类

2.2 数据集的预处理

原始的 CIC-DDos-2019 数据集中存在 NaN 值和 Infinite 值不利于模型的训练，因此在合并了所有 CSV 文件后需要清理脏数据。因为数据量较大，所以本文将包含 NaN 和 Infinite 的数据作为脏数据整行删除。

目前数据集中存在 87 种属性，属性中存在两个名为“Fwd Header Length.1”的冗余属性，一列名为“Unnamed”的匿名属性以及“Source Port”、“Destination Port”、“Source IP”、“Destination IP”、“Flow ID”、“Time-

stamp”、“SimilarHTTP”等不能用于分类的套接字属性都进行舍弃以减少实验数据的特征维数。实际场景中 IP 地址等属性真实性很低，而且，使用套接字信息训练模型，会使模型依赖于使用套接字信息来分类，导致过拟合问题。最后本文保留了 78 种属性。

针对属性值存在分布不均匀、分布区间过大等问题，预处理需要对数据进行归一化处理。针对每一列数据（即每一种特征）进行 L2 范数归一化，L2 归一化的公式如式（13）所示：

$$\| x \|_2 = \sqrt{\sum_{i=1}^{n} | x_i |^2} \tag{12}$$

特征值归一化后，对数据进行分位数映射处理，该方法变换每条数据的属性值，使属性值映射到正态分布。服从正态分布的属性值能有效缩短训练收敛时间。

接下来，分析数据集中攻击类型的分布情况，结果如图 4 所示。结果显示，数据集存在类别不均衡的情况：TFTP 类别在数据集中占比很高而 Portmap、良性和 UDPLag 占比极少。这会导致模型训练出现长尾效应，使分类结果偏向数量多的那些类，训练得到的模型对少数类不敏感，分类能力差。因此，对 TFTP 稠密类进行下采样操作，以均衡其对整体模型的影响力；使用过采样技术 SMOTE[19-20]生成稀疏类的合成数据，以增强稀疏类数据对整体模型的影响力。这一系列操作均有利于数据集实现类平衡。

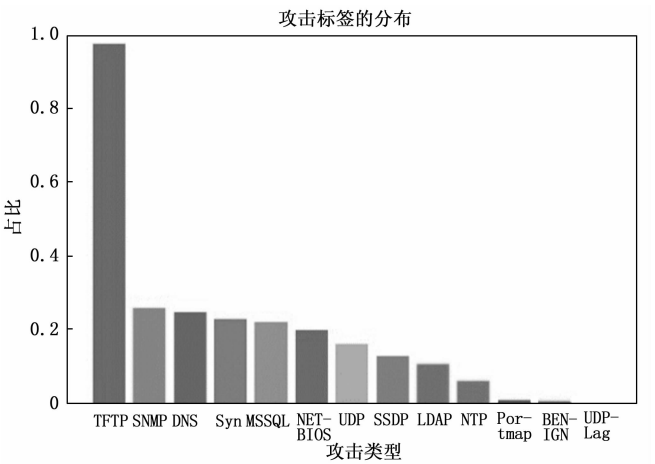

图 4　攻击标签分布图

SMOTE 算法是由 Bowyer 等人[19]提出一种通过生成合成数据来实现类平衡的方法。SMOTE 在特征空间进行采样生成合成数据，所以生成数据的真实性高于传统采样方法。SMOTE 算法的内容为：针对少数类中的每一个样本 s 求到同类样本的欧式距离，得到该少数类的 K 近邻。合成数据 so 是由样本 s 和最近邻 sn 的距离差值，并将差值乘以一个 0 到 1 范围内的随机数 r，最后添加到 s 的向量中生成的。SMOTE 算法公式[19-20]如式（12）所示：

$$S_S = S + r \times (S - S_n) \tag{13}$$

采样操作后，包括所有攻击类型以及良性在内的 13 个类的数据数量达到平衡，平衡的数据集能够有效地避免训练过程产生长尾效应，以此增加模型对于数据数量少的类别的分类准确率。

本文在利用预处理后的数据集进行包括攻击和良性标签的 13 分类任务时，存在个别类混淆严重的情况。

攻击标签对应的数据由于攻击类型和攻击特征的相似性高，导致网络监控软件捕获到的信息总是具有相似性[7]。比如目前比较严重的泛洪攻击，其包括 DNS 泛洪攻击、UDP 泛洪攻击和 Syn 泛洪攻击共 3 种。因此数据集中对应的不同攻击种类的同一种属性的值也具有相似性，所以直接进行 13 分类容易产生标签的混淆，影响到模型的准确率。

统计 12 种攻击类型（不包含良性类）在属性空间中具有强相似性的类别的子集概要情况，结果如表 1 所示。

表 1　强相似性标签的子集概要

子集	ACV	AFR0	ASAH
DNS/LDAP/SNMP	12	24	34
NetBIOS/Portmap	12	31	41
SSDP/UDP	12	25	32
UDPLag/Syn	12	25	30

表 1 中划分了 4 个子集，其他攻击标签保持独立，表中 ACV 是指具有恒定值的属性，AFR0 表示零值高频的属性，ASAH 指的是由于属性值具有很强的同质性而导致偏差的属性。因此将对应具有强相似性的子集进行标签融合操作。

对应的攻击标签融合成“DNS/LDAP/SNMP”、“NetBIOS/Portmap”、“SSDP/UDP”、“UDPLag/Syn”。标签融合后，存在 8 种包括各类 DDos 攻击和良性的类别。故实验过程可简化为进行一个 DDos 攻击下的网络流量八分类任务，此种情况作为实验场景一。

本文也将所有的攻击标签融合成“DDos”标签结合良性标签，进行一个 DDos 攻击下的网络流量二分类任务，此种情况作为实验场景二。

最后，数据集依次进行：数字编码和独热编码，该操作为每一类标签分配一个新列，如果该条记录属于这一类则为 1，否则为 0。

从预处理后的数据中按每种攻击以及良性等比例抽样提取数据，合成共 200 000 条训练数据的总数据集用作模型训练。

对总数据集进行 8：2 的划分得到训练集和测试集，训练集采取四折交叉验证的方式划分验证集，用来验证模型精度和调整模型超参数。

2.3　模型的评价指标

本文采用的模型评估指标为准确率、精确率、召回率和 F1-score，并绘制混淆矩阵来分析每个类别的分类结果，公式如式（14）～（17）所示：

$$\text{准确率} = \frac{t_p + t_n}{\text{样本数}} \tag{14}$$

$$精确率 = \frac{t_p}{t_p + f_p} \tag{15}$$

$$召回率 = \frac{t_p}{t_p + f_n} \tag{16}$$

$$f_1 - score = \frac{精确率 * 召回率}{精确率 + 召回率} \tag{17}$$

2.4 模型的参数

本文基于 TensorFlow 框架实现本文的 DDos 检测模型，将多分类交叉熵作为损失函数，实例化的优化器使用 Adam[21]。

本文对比实验了各种结构，并对实验模型在保证实验准确率基础上针对不必要结构进行了剪枝操作，一是为了减少工作时延，二是为了便于网络移植到计算能力较弱的边缘节点上，将模型优化缩减为本文最终呈现的形式：其中一维卷积中输出滤波器的数量分别为 20、40、60，卷积核的尺寸为 4 * 1，填充方式为“same”；一维卷积后使用 Relu 作为激活函数，并接入 BN 层，构成复合一维卷积层结构。Bilstm 层由一层输出空间的维数为 80 的 BiLSTM 模块接 BN 处理来担任时间特征提取任务。

本文利用粒子群优化算法进行超参数寻优实验，寻找到适合本模型的最佳超参数序列，学习率寻优曲线如图 5 所示。

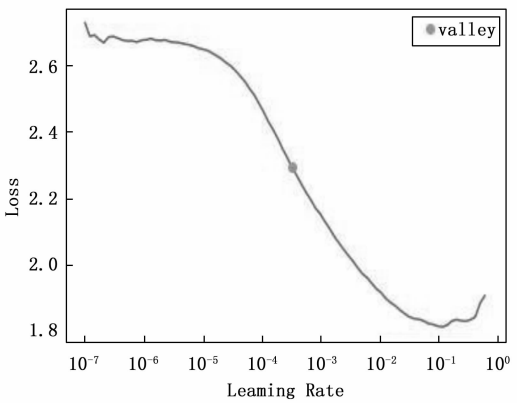

图 5 学习率寻优曲线

当学习率为 2×10^{-4}，批大小为 128，练轮数设置为 100 轮时模型的训练速度有效提升且提升了模型准确率，总结以上操作，列出参数列表如表 2 所示。

表 2 模型的参数列表

参数名	参数值
一维卷积＋ ReLu＋BN	3 层
BiLSTM	1 层
优化器	Adam
批大小	128
学习率	2×10^{-4}
训练轮数	100
损失函数	多分类交叉熵
模型总参数量	1×10^{6}

2.5 实验结果

本实验的模型训练流程图整体描述如图 6 所示，实验整体流程可简化为：数据样本提取输入、数据预处理、模型搭建与初始化、模型训练、模型剪枝、模型指标评估、模型部署等步骤。

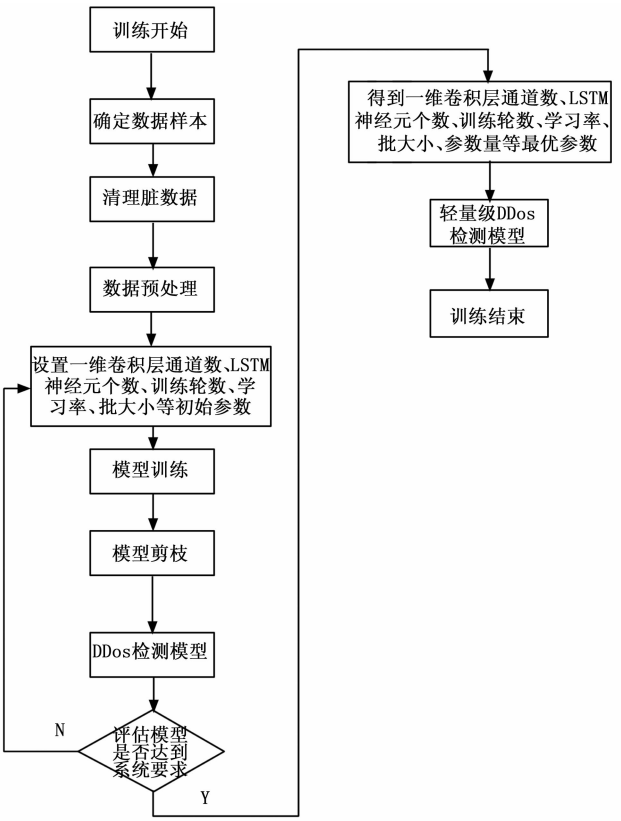

图 6 模型训练流程图

在实验场景一中，通过模型训练得到一个能有效检测 DDos 攻击的模型，可以对包括攻击标签和良性标签的网络流量数据进行八分类，检测出可能正在遭受的 DDos 攻击。训练过程中，以训练轮数为横轴，损失和准确率的变化为纵轴，绘制折线图如图 7 所示，模型分类结果的指标参数如表 3 所示。

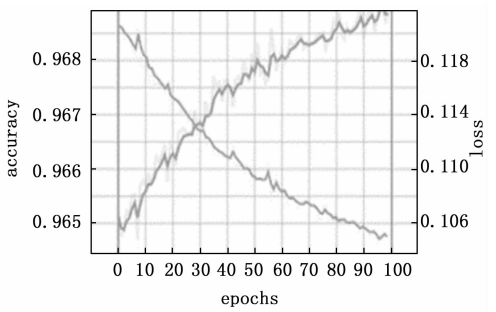

图 7 损失变化曲线和准确率变化曲线

表 3 实验场景一的分类结果

准确率	精确率	召回率	F1-score
0.968	0.96	0.96	0.96

对每一类攻击标签的检测情况进行指标参数统计分析，结果如图 11 所示，模型对于 MSSQL 的检测能力相对较弱，分析可能是因为用于分辨 MSSQL 攻击类的特征属性较少，根据文献［7］显示，影响 MSSQL 检测的强相关属性为端口号，但端口号属性不能用于模型分类任务的训练中而进行了舍弃，故有所影响。

结果绘制混淆矩阵如图 8 所示。

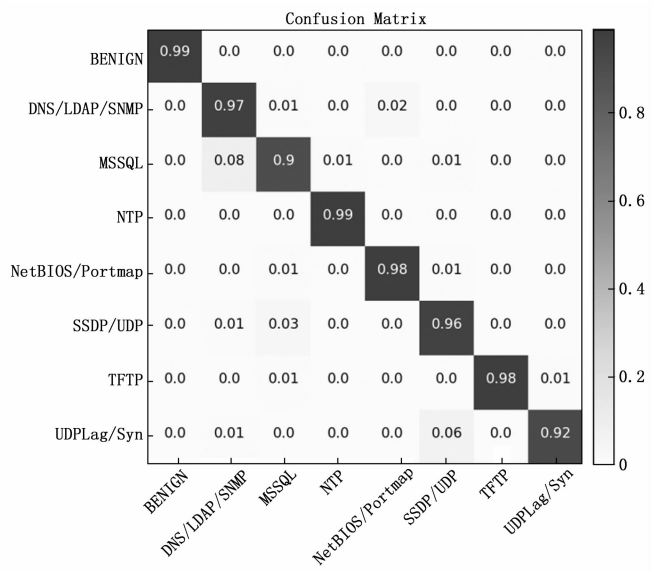

图 8　实验场景一混淆矩阵

混淆矩阵的分类结果显示，模型在分类 MSSQL 和 DNS/LDAP/SNMP 时发生了混淆，在分类 UDPLag/Syn 和 SSDP/UDP 时发生了混淆，针对发生混淆的两类可继续着手进行改进，进一步提高模型检测 DDos 攻击的准确率，其他类均表现良好，由于模型的参数量和计算量较小，对分类 DDos 攻击有良好的性能，故本文的模型适合部署在边缘计算环境下进行 DDos 攻击的检测任务。

在实验场景二中，通过模型训练得到一个能有效检测 DDos 攻击的模型，可以对 DDos 攻击标签和良性标签的网络流量数据进行二分类，检测出可能正在遭受的 DDos 攻击。实验场景二的检测结果的指标参数如表 4 所示。

表 4　实验场景二分类结果

准确率	精确率	召回率	F1-score
0.998	0.99	0.99	0.99

验证训练后模型的检测能力，据结果绘制混淆矩阵如图 9 所示。

混淆矩阵的分类结果显示，模型对于 DDos 类和良性类有极佳的分类能力，本文的模型能够完美解决 DDos 和良性标签的网络流量二分类问题，由于模型的参数量和计算量相对较小且具备极佳的检测 DDos 攻击能力，表明这一模型适合部署在边缘计算环境下进行 DDos 检测任务。

对每一类攻击标签的检测情况进行指标参数统计分析，

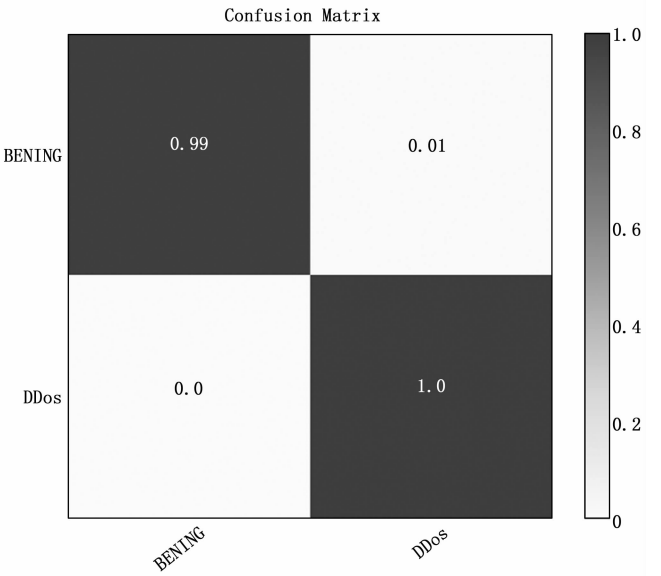

图 9　实验场景二混淆矩阵

结果如图 10 所示，证明模型在实验场景二中具备优秀的检测能力。

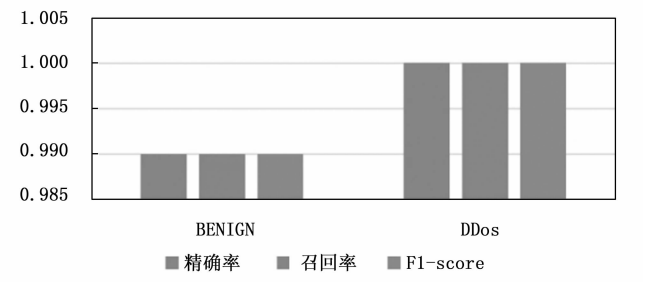

图 10　实验场景二分类情况统计图

将训练好的模型部署到边缘节点中，搜集节点中的网络流量数据，使用 CICFlowMeter-V3 插件来对流量数据进行量化提取，放入预处理阶段进行数据清理后，流量数据删除了脏数据且进行了特征降维，随后送入部署的训练模型进行实时 DDos 预测。

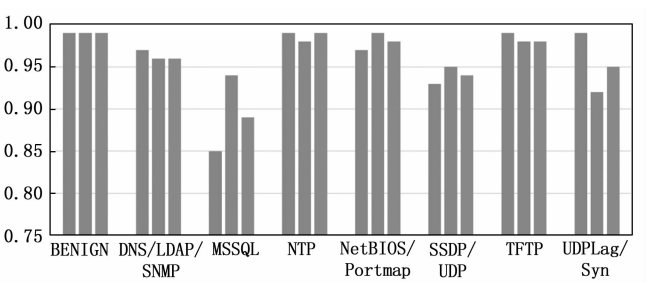

图 11　实验场景一分类情况统计图

3　模型与相关工作对比

表 5、表 6 展示了本文提出的模型在上述两种实验场景下的结果指标和其他相关工作的结果对比。

表 5 实验场景一下本文与相关工作的结果比较

作者/参考文献	方法	结果指标 精确率/召回率/F1% (或准确率)
Sharafaldin 等人[7]	朴素贝叶斯	30.30/17.51/7.35
	支持向量机	62.44/57.97/55.50
	决策树	61.15/58.32/55.15
	随机森林	50.76/36.91/39.57
Can[8]	82 种特征+FS	91.16/79.41/79.43
Ferrag 等人[9]	DNN	92.12
	RNN	94.88
	CNN	93.88
Chartuni A 等人[10]	DNN	94.21/94.03/94.12
本文	本文提出的模型	96/96/96(96.8)

表 6 实验场景二下本文与相关工作的结果比较

作者/参考文献	方法	结果指标 准确率/精确率/ 召回率/F1 %
Sharafaldin 等人[7]	朴素贝叶斯	51//76.5/58.5/44
	支持向量机	93/93.5/93.5/93
	决策树	77/84/76.5/76
	随机森林	86/89/87/86.5
	逻辑回归	95/96/94/95.5
	XGBoost	84/87.5/83/83
本文	本文提出的模型	99.8/99/99/99

可以看出本文提出的模型在结果指标上明显优于相关工作提出的方法，本模型获得的指标提升应该归因于一个更适合的新模型框架，以及研究的预处理阶段和之前提出的标签融合。但是，本文的模型受到训练阶段使用的标签的限制，那么在实际部署后检测到新攻击带来的恶意网络流量时，如果新攻击的流量特征和之前学习到的攻击有相似，模型将会把其归类为 DDos 攻击，但会错误归类到已存在的攻击类型。为应对这一情况，可以在后续模型训练阶段增加新标签以定义新的攻击类型，此法可有效减少输出的模糊性。轻量化后的模型，其总参数量适当，能够适应边缘计算环境下边缘节点算力受限、存储受限的实际场景。

4 结束语

随着边缘计算的蓬勃发展，边缘计算环境下所面临的网络安全攻击危害也日益严重，DDos 攻击作为边缘计算环境遭受的一种最主要的网络攻击带来了巨大的威胁。由于边缘计算环境下的边缘节点存在算力受限、储存受限的情况，传统的 DDos 防御和检测手段很难适应，所以，本文基于深度学习提出了一种检测模型，并对模型进行了剪枝轻量化，用以在该场景下防御 DDos 攻击。本文采用了 CIC-DDos-2019[7]数据集来模拟遭受 DDos 攻击时的，存在网络波动大、条件受限情况下的网络流量数据。针对数据集存在脏数据、属性值区间大、类别不平衡等情况，通过实验提出了针对性强的数据预处理解决方案。对于数据标签存在强相似性使标签混淆的问题，本文对数据的属性进行了相似性分析，提出了一种针对性强的标签融合方案，得到了两种合理性强的实验场景。本文设计了一种基于 Bilstm 和一维卷积的模型结构，并通过剪枝操作实现了模型的轻量化，以此来达到在边缘计算环境下检测 DDos 攻击的目标，实验场景一进行 DDos 攻击八分类任务准确率达到了 96.8%，实验场景二进行 DDos 攻击二分类任务准确率达到了 99.8%。

未来的工作中，对于个别类还存在混淆情况，可以对数据属性进行更深入的分析或是调整模型框架来解决。本文的模型分类结果可解释性较差，后续可考虑增强可解释性。下一步将在实际边缘计算场景下训练和调整本文的模型，增加新攻击类型标签，降低可能存在的预测模糊性。

参考文献：

[1] 汤 辉，贺余盛，徐 宁. 物联网 DDoS 僵尸网络恶意程序监测分析研究 [J]. 江西通信科技，2020 (3)：42-44.

[2] 李柏松，常安琪，张家兴. 物联网僵尸网络严重威胁网络基础设施安全——对 Dyn 公司遭僵尸网络攻击的分析 [J]. 信息安全研究，2016，2 (11)：1042-1048.

[3] 凌 捷，陈家辉，罗 玉，等. 边缘计算安全技术综述 [J]. 大数据，2019，5 (2)：34-52.

[4] HE Z，ZHANG T Z，LEE R B. Machine learning based DDoS attack detection from source side in cloud [C] //2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE，2017：114-120.

[5] STAUDEMEYER R C，OMLIN C W. Evaluating performance of long short-term memory recurrent neural networks on intrusion detection data [C] //South African Institute for Computer Scientists & Information Technologists Conference，2013：218.

[6] ELSAYED M S，LE-KHAC N A，DEV S，et al. Ddosnet：A deep-learning model for detecting network attacks [C] //2020 IEEE 21st International Symposium on "A World of Wireless，Mobile and Multimedia Networks" (WoWMoM). IEEE，2020：391-396.

[7] SHARAFALDIN I，LASHKARI A H，HAKAK S，et al. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy [C] //2019 International Carnahan Conference on Security Technology (ICCST). IEEE，2019：1-8.

[8] CAN D C，LE H Q，HA Q T. Detection of distributed denial of service attacks using automatic feature selection with enhancement for imbalance dataset [C] //Asian Conference on Intelligent Information and Database Systems. Springer，Cham，2021：386-398.

[9] FERRAG M A，SHU L，DJALLEL H，et al. Deep learning-based intrusion detection for distributed denial of service attack in Agriculture 4.0 [J]. Electronics，2021，10 (11)：1257.

(下转第 168 页)