面向边缘计算的TCA1C DDoS检测模型

申秀雨[1],姬伟峰[1*],李映岐[2],吴玄[3]

(1.空军工程大学信息与导航学院,陕西 西安 710077; 2.93107部队,辽宁 沈阳 110000; 3.94701部队,安徽 安庆 246000)

摘 要: 边缘计算弥补了传统云计算数据传输开销大的不足,但边缘网络中存储和计算资源受限的特殊性限制了其部署复杂安全算法的能力,更易受到分布式拒绝服务(DDoS)攻击。针对目前边缘网络中DDoS攻击检测方法性能不高、未对卸载任务分类处理、对多属性的流量处理能力弱的问题,提出一种基于任务分类的Attention-1D-CNN DDoS检测模型TCA1C,对通信链路中的流量按不同的卸载任务进行分类,使单个任务受到攻击时不会影响整个链路中计算任务卸载的安全性,再对同一任务下的流量提取属性值并进行归一化处理。处理后的数据输入到Attention-1D-CNN,通道Attention和空间Attention学习数据特征对DDoS检测的贡献度,利用筛选函数剔除低于特征阈值的冗余信息,降低模型学习过程的复杂度,使模型快速收敛。仿真结果表明:TCA1C模型在缩短DDoS检测所用时间的情况下,检测准确率高达99.73%,检测性能优于DT、ELM、LSTM和CNN;当多个卸载任务在面临特定攻击概率时,卸载任务分类能有效降低不同任务的相互影响,使终端设备的计算任务在卸载过程中保持较高的安全性。

关键词: 边缘计算;分布式拒绝服务攻击检测;任务分类;注意力机制;1D-CNN模块

中图分类号: TP393 **文献标志码:** A **DOI:** 10.19678/j.issn.1000-3428.0067572

TCA1C DDoS Detection Model for Edge Computing

SHEN Xiuyu[1], JI Weifeng[1*], LI Yingqi[2], WU Xuan[3]

(1.Information and Navigation School, Air Force Engineering University, Xi'an 710077, Shaanxi, China; 2.Unit 93107, Shenyang 110000, Liaoning, China; 3.Unit 94701, Anqing 246000, Anhui, China)

【Abstract】 Edge computing compensates for the traditional cloud computing data transmission overhead. However, limited storage and computing resources in the edge network restrict its ability to deploy complex security algorithms, making it more vulnerable to Distributed Denial of Service (DDoS) attacks. This paper proposes a task classification-based Attention-1D-CNN detection model, TCA1C, aimed at solving problems in current edge networks, such as low performance in detecting DDoS, lack of a task classification mechanism, and weak ability to deal with multi-attribute traffic. First, the model classifies the traffic in the communication link according to different offloading tasks such that the overall offloading security is not affected when some tasks are attacked, and the attribute values of the traffic under the same task are extracted and normalized. Next, the model inputs the processed data into an Attention-1D-CNN. Channel and spatial attention determine the contribution of data features for classification and eliminate redundant information below the feature threshold, thereby reducing the complexity of the model learning process and allowing the model to converge quickly. The simulation results show that the accuracy of the TCA1C model in DDoS detection is as high as 99.73%, and the performance of the TCA1C model is better than those of the DT, ELM, LSTM, and CNN, with reduced detection time. When different offloading tasks face certain attack probabilities, traffic classification can effectively reduce the mutual influence of different tasks such that the computing tasks of the terminal equipment can maintain a high level of security during offloading.

【Key words】 edge computing; Distributed Denial of Service (DDoS) attack detection; task classification; attention mechanism; 1D-CNN module

0 引言

随着通信技术的发展,各类终端设备以指数爆炸的趋势接入互联网,万物互联(IoE)的时代即将到来。边缘计算[1]作为一种新型计算模型应运而生,将计算任务放在靠近数据源的边缘侧进行,能够降低终端与云中心的信息传输开销。边缘基础设施的存储资源和计算资源都较为薄弱,许多边缘设备在设计之初只考虑了可用性而忽略了安全性,这些设备暴露在互联网上极易受到网络攻击。分布式拒绝服务(DDoS)攻击[2]是最常见的网络安全威胁之一,其因攻击成本低、危害范围大被广泛关注。近年来,

收稿日期: 2023-05-08 **修回日期:** 2023-07-13

基金项目: 空军工程大学教育创新计划(CXJ2022027)。

通信作者 E-mail: *jiwf@yeah.net

计算机工程 www.ecice06.com

DDoS攻击强度越来越大，AWS发布报告称2020年受到的DDoS攻击量为2.3 Tb/s[3]。在边缘计算环境中，DDoS攻击可以轻易地实施于边缘节点，并通过计算卸载[4]将海量的恶意流量发送到边缘网络的所有设备，造成边缘网络瘫痪，因此，需要研究一种面向边缘计算卸载的DDoS攻击检测模型，以便有效保护边缘计算资源并提高边缘设备可用性。

目前，边缘计算中对计算卸载的研究主要集中在卸载方式、卸载粒度、卸载决策上，通过综合考虑终端设备性能、信道质量、边缘服务计算能力等因素[5]对时延[6]、能耗[7]以及多指标联合效用[8]进行优化，对卸载安全方面的研究比较少，而卸载安全问题被很多专家学者认为是不容忽视的新方向[9-11]。

基于机器学习的边缘智能[12]方法已经用在边缘计算的DDoS检测中。文献[13]在WEKA工具中实施6种不同的机器学习(ML)算法对CICDDoS2019数据集进行分析，其中决策树(DT)和随机森林(RF)算法获得99%的最佳检测结果，DT在时间上优于RF算法。虽然决策树预测效率高，但预测模型对训练样本的要求较高，受样本不平衡的影响较大。文献[14]提出一种基于随机森林和深度森林的无线传感器网络入侵检测模型，获得了比传统机器学习方法更高的检测准确率，但不及CNN和Autoencoder SVM。

深度学习算法[15]比其他机器学习算法具有更高的准确率，但由于结构复杂、参数较多，模型训练需要大量的时间和计算资源，因此需要对深度学习算法进行轻量化设计来适应边缘计算环境，并同时保证较高的检测效率。

文献[16]利用FastRNN和FastGRNN构建一层128个神经元的轻量型Edge-Detect模型，与标准LSTM、GRU相比，精度提高了1%，模型尺寸缩减了66%。但该模型仅做到了对DDoS攻击的二分类。文献[17]针对一维时间序列数据无法作为卷积层输入、CNN池化层存在信息丢失和RNN处理长时序时存在梯度消失的问题，在初始CNN、RNN基础上引入格拉姆角场(GAF)、SoftPool池化层和多头注意力机制(MHS)，选用Bi-GRU代替传统的RNN算法，达到减少模型参数的目的，所构建的物联网入侵检测模型(GSM-IDS)在多分类中具有较好表现，但其在处理模型输入的数据时采用升维的方式，增加了模型处理数据的复杂度。

文献[18]提出LUCID模型，建立了适用CNN输入的在线流量预处理机制，其将流量样本转化为二维矩阵，让所有卷积核使用相同参数，简化了CNN参数学习方式，从而得到更加轻量级的训练模型，训练过程中学习参数、计算量、内存占用均减少，与LSTM达到相同检测精度时，分类速度快了40倍，所以，CNN在资源有限的环境中，既能最大限度地减小运算规模，同时又能保持高性能。但LUCID模型的输入仍然需要人为筛选出流量的11个属性，不能实现自主区分多属性在检测中的重要性。以上方法大多都是针对通信链路中的全部数据直接进行检测，检测到攻击后对所有卸载任务进行阻断，未考虑通过对卸载任务进行分类来降低单个任务受到攻击时对整个链路中计算任务安全卸载的影响。

基于以上讨论，考虑到边缘网络中计算和存储资源有限的特殊性，针对现有DDoS检测方法性能有待提高、未对计算卸载任务进行分类处理、CNN模型不能自主过滤冗余特征的问题，本文提出一种边缘计算中基于任务分类的Attention-1D-CNN DDoS检测模型TCA1C，其中包括卸载任务分类处理模块和Attention-1D-CNN模块，可以在线收集边缘网络中的实时流量数据并及时检测DDoS攻击，进而阻断DDoS攻击对边缘服务器的影响。

TCA1C模型的卸载任务分类处理模块对混杂在通信链路中的卸载数据进行分类识别，降低了不同任务受到攻击时的相互影响。同时，在同一计算任务下提取数据的属性值并进行归一化，生成可直接输入检测模型的数据样式。

TCA1C模型的Attention-1D-CNN模块对输入数据进行检测，其中，通道注意力(CA)机制对1D-CNN不同通道的特征图进行筛选，空间注意力(SA)机制对同一特征图中不同位置的信息进行筛选，将低于筛选阈值的特征作置零处理，减少1D-CNN的学习参数，提高模型收敛速度。

1 TCA1C模型

为了解决边缘网络中卸载任务种类不同、属性值多样，不利于快速完成DDoS检测的问题，本文提出一种TCA1C模型。该模型部署在边缘服务器上，由卸载任务分类处理模块和Attention-1D-CNN模块构成，是一个对边缘网络中DDoS攻击进行检测的轻量级模型。该模型架构由卸载任务分类处理、模型训练、攻击检测3个阶段构成，如图1所示(彩色效果见《计算机工程》官网HTML版，下同)。

卸载任务分类处理模块主要完成卸载任务分类和数据处理任务，将终端设备卸载到边缘网络中的计算任务处理为可直接输入检测模块的数据样式，为检测每个计算任务是否受到DDoS攻击做好数据准备工作。

Attention-1D-CNN模块主要完成模型训练和攻击检测任务，1D-CNN完成特征提取和异常检测，CA和SA机制对1D-CNN提取的特征进行筛选，去除不必要的冗余特征。

计算机工程 www.ecice06.com

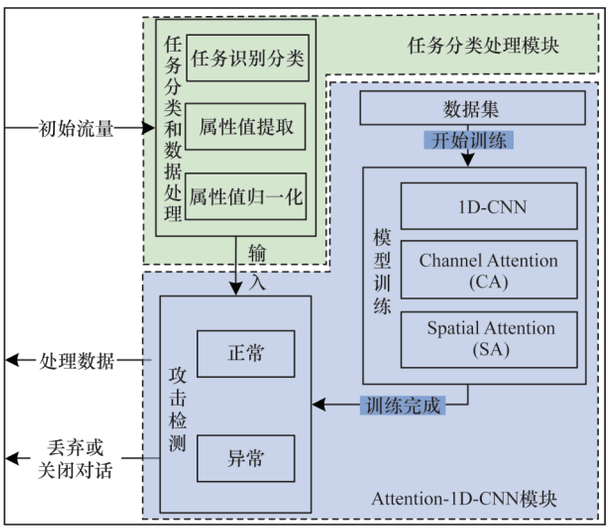


图1 TCA1C模型架构

Fig.1 TCA1C model architecture

1.1 卸载任务分类处理模块

终端设备将计算任务卸载到边缘服务器时，不同设备以及同一设备的不同任务之间会共用终端设备与边缘服务器的通信链路。直接在通信链路上采样进行检测会将不同任务的数据包混在一起，当检测出有异常时，不能立刻确定是哪个任务中出现了DDoS攻击，不利于精确实施防御措施。因此，需要将通信链路中混杂的数据包按卸载任务进行分类、重组，并处理成可以直接输入检测模型的数据样式。

卸载任务分类处理就是根据终端设备所卸载任务的ID信息，对链路中的流量数据按不同卸载任务进行分类整合，对同一个计算任务中的数据包提取属性值并做归一化处理，具体分为卸载任务识别分类、数据属性值提取、属性值归一化3个步骤，该过程所涉及的参数如表1所示。

表1 任务分类处理的参数

Table 1 Parameters in task classification processing

参数	含义
I	卸载任务的标识
n	卸载任务数量
N	每个计算任务的数据包数量
f	每个数据包所具有的属性数目
$\boldsymbol{A}$	N行f列的矩阵
h	每个计算任务一次输入TCA1C的包数量
t	获取流量的时间窗口
s	时间窗口的数量

1)卸载任务识别分类。在捕获流量的时间窗口内，通信链路中会有一个或若干个卸载任务的数据包，每个数据包都有自己对应的任务标识(I)。根据数据包所携带的任务标识对混杂在一起的数据包进行分类，每个卸载任务的数据包被组合在一起，直到收集完该任务的所有N个数据包，如图2所示。

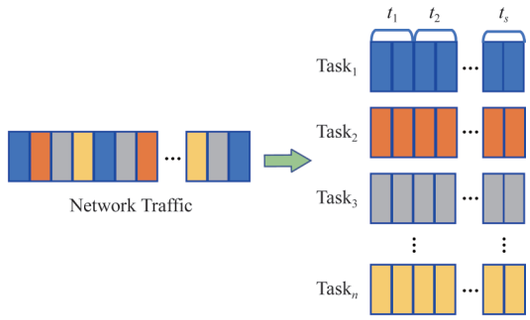


图2 卸载任务分类过程

Fig.2 Offloading task classification process

2)数据属性值提取。对每个数据包提取f个属性，包括Protocol、Timestamp、Total Fwd Packets等，提取的属性保存为$N\times f$的矩阵，N行表示有N个数据包，每一行表示数据包的所有属性值，f列表示每个数据包的f个不同属性，详细属性如表2所示。

表2 每个卸载任务的数据包属性

Table 2 Data packet attributes of each offloading task

行数	列数				
	0	…	…	…	$f-1$
	Protocol	…	Timestamp	Total Fwd Packets	…
0	6	…	51:40.4	26	…
1	6	…	51:40.5	9	…
2	0	…	51:41.3	56	…
⋮	⋮	⋮	⋮	⋮	⋮
N	6	…	52:19.9	2	…

3)属性值归一化。对有空值的行进行剔除，留下的行将属性值归一化到[0,1]，每一行的数组($1\times f$)就是一个单独的样本，在检测DDoS攻击时，作为模型的输入。

算法1给出了卸载任务分类处理过程，步骤1对需要的参数进行初始化，步骤2~11为整个处理过程，步骤3~5对数据包按任务I进行分类，步骤6~10对所有数据包的属性值进行标准化处理，所有的处理过程都在时间窗口t内完成。

算法1 卸载任务分类处理算法

输入 网络流量(NT)，获取流量的时间窗口t，卸载任务数量n，不同卸载任务的标识I

输出 按任务I分类并经过标准化处理的数据

```
1.Initialization:t,n,I
2.if NT∈(NT.start_time,NT.start_time+t) do
3.for packet.I∈n do
4.task←packet.ID
//按I进行任务分类
5.end for
6.for i=0;i<n;i++ do
7.for j=0;j<=task(i).N,j++ do
8.Packet←normalization(Packet)
//属性值标准化
```

计算机工程 www.ecice06.com

9.end for
10.end for
11.end if

1.2 Attention-1D-CNN 模块

模型训练和 DDoS 攻击检测阶段都在 Attention-1D-CNN 模块中完成，具体流程如图 3 所示。

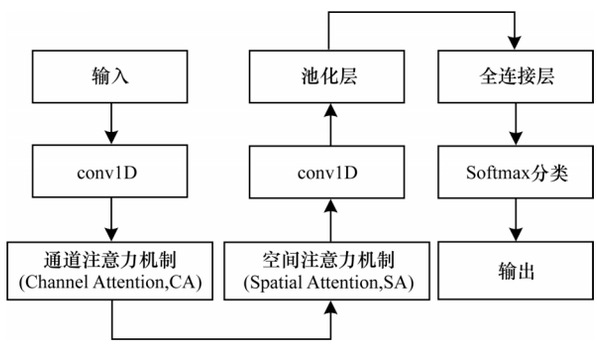


图 3 Attention-1D-CNN 模块流程

Fig.3 Procedure of Attention-1D-CNN module

1D-CNN[19]包括卷积层、池化层、全连接层，卷积层完成 1D-CNN 和激活函数的运算[20]，池化层完成下采样，全连接层与传统多层感知机（MLP）类似，完成权重学习和逻辑回归。1D-CNN 在处理一维流信息时的计算复杂度为 $O(pq)$，其中，p 为样本大小，q 为卷积核大小，所以，1D-CNN 在实时性高、资源有限的硬件上更容易实现。

1D-CNN 每层的卷积过程为：

$$\boldsymbol{X}_l=\boldsymbol{b}_l+\text{conv1D}(\boldsymbol{W},\boldsymbol{S}_{l-1}) \tag{1}$$

其中：$\boldsymbol{S}_{l-1}$ 是第 $l-1$ 层所有神经元的输出构成的数组，同时作为第 l 层卷积运算的输入；$\boldsymbol{W}$ 是第 $l-1$ 层神经元到第 l 层神经元的卷积核；$\boldsymbol{b}_l$ 是由第 l 层神经元的偏置构成的数组；$\boldsymbol{X}_l$ 是第 l 层所有神经元卷积输出构成的数组；conv1D 是使用无填充 valid 模式的一维卷积运算。式（1）所示即第 $l-1$ 层神经元的输出 $\boldsymbol{S}_{l-1}$ 与第 $l-1$ 层到第 l 层的卷积核 $\boldsymbol{W}$ 进行一维卷积运算，再加上第 l 层神经元的偏置 $\boldsymbol{b}_l$，得到第 l 层神经元卷积的输出 $\boldsymbol{X}_l$。

激活过程表示为：

$$\boldsymbol{Y}_l=g(\boldsymbol{X}_l) \tag{2}$$

其中：$\boldsymbol{Y}_l$ 是 $\boldsymbol{X}_l$ 经过激活函数进行非线性映射后的输出结果，同时作为下一步池化过程的输入；g 为激活函数，通常有 Tanh、ReLU、Sigmoid、Softmax 等，此处选用 Sigmoid。Sigmoid 函数可将特征转化为权重，其表达式为：

$$\text{Sigmoid}(x)=1/(1+\text{e}^{-x}) \tag{3}$$

池化过程为：

$$\boldsymbol{S}_l=\boldsymbol{Y}_l\downarrow\boldsymbol{S} \tag{4}$$

其中：$\boldsymbol{S}_l$ 为 $\boldsymbol{Y}_l$ 经过下采样后的输出，也是下一层卷积的输入；$\downarrow\boldsymbol{S}$ 表示带有采样因子 $\boldsymbol{S}$ 的下采样操作。

虽然标准 1D-CNN 具有计算复杂度低的优势，但仍有 2 个不足：1）在同一卷积层中，由不同通道的卷积核生成的特征图不同，不能识别哪些特征图是必要的，哪些特征图在参数学习上的贡献度低；2）同一特征图中不同位置的特征信息也不同，不能区分哪些特征信息是必要的，哪些信息对参数的贡献度低。低贡献度特征对模型训练和 DDoS 检测作用不大，但增加了参数学习过程的计算复杂度，因此，本文在标准 1D-CNN 上引入 CA 和 SA 机制，利用筛选函数剔除低贡献度的特征。

注意力机制[21]与 CNN 结合，不仅可以通过捕获 CNN 不同通道的权重关系给不同通道的特征进行加权，而且可以捕获一个特征图不同位置的权重信息，从而有效地进行特征筛选并增强特征[22-23]。

在 CA 机制中，不同通道的特征图被拼接在一起得到 L_{in}，L_{in} 为 CA 机制的输入。L_{in} 经过平均池化和最大池化分别得到 2 个长度与通道数量相等的一维向量，利用大小与通道数量成正比的卷积核对 2 个一维向量进行卷积，将得到的 2 个卷积结果利用乘法融合，再通过 Sigmoid 激活函数得到代表不同通道权重值的权重向量 $\boldsymbol{\mu}$，平均池化的一维向量与权重向量点积，得到筛选通道的阈值 λ。不同通道的特征图与阈值 λ 作为通道筛选函数 F_{C} 的输入，筛选出必要的特征图得到 L_{out}，减少不必要的计算量。CA 机制如图 4 所示。

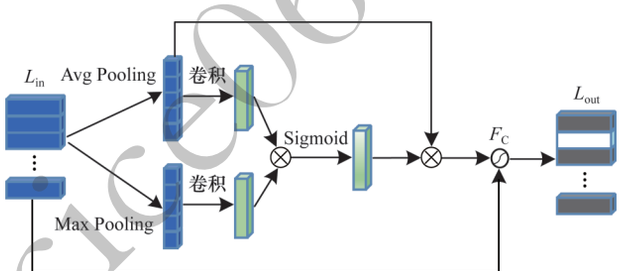


图 4 CA 机制

Fig.4 CA mechanism

通道筛选函数 F_{C} 的定义如下：

$$L_{\text{out}}=F_{\text{C}}(L_{\text{in}},\lambda)=\begin{cases}0, & |L_{i,\text{in}}|<\lambda\\ L_{i,\text{in}}, & |L_{i,\text{in}}|\geqslant\lambda\end{cases}$$

$$i=1,2,\cdots,l_{\text{len}}(L_{\text{in}}) \tag{5}$$

其中：$|L_{i,\text{in}}|$ 为第 i 个通道特征图的绝对值；λ 为特征图的筛选阈值。当特征图绝对值小于 λ 时，该特征图被置为 0，即 L_{out} 的值取 0，以达到减少计算复杂度的目的，如图 4 中 L_{out} 的空白部分所示；当特征图绝对值大于等于 λ 时，L_{out} 的值与 L_{in} 保持一致。

在 SA 机制中，每个卷积通道得到的特征图 M_{in} 经过一维卷积得到代表特征图信息的向量 $\boldsymbol{\alpha}$，$\boldsymbol{\alpha}$ 经过 Sigmoid 激活得到该特征图不同位置的权重向量 $\boldsymbol{\beta}$，M_{in} 的平均池化结果与 $\boldsymbol{\beta}$ 相乘，得到空间筛选阈值向量 $\boldsymbol{\gamma}$，M_{in} 和 $\boldsymbol{\gamma}$ 作为空间筛选函数 F_{S} 的输入，筛选出每个特征图中的必要信息，剔除低于阈值但增加计算复杂度的冗余信息，得到 M_{out}。SA 机制如图 5 所示。

计算机工程 www.ecice06.com

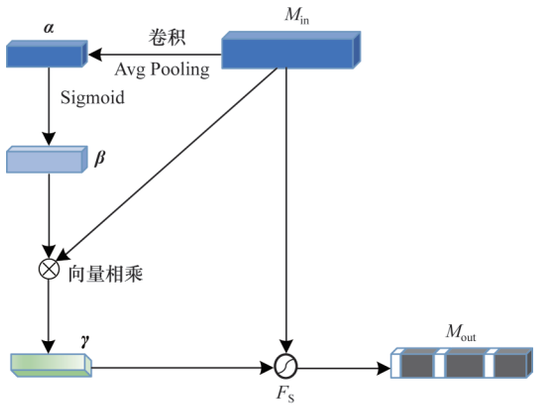


图 5 SA 机制

Fig.5 SA mechanism

空间筛选函数 F_S 定义如下：

$$M_{out}=F_S(M_{in},\boldsymbol{\gamma})=\begin{cases}0, \left|M_{j,in}\right|<|\gamma_j| \\ M_{j,in}, \left|M_{j,in}\right|\geqslant|\gamma_j|\end{cases}$$

$$j=1,2,\cdots,l_{len}(M_{in}) \tag{6}$$

其中：$\left|M_{j,in}\right|$ 为特征图 M_{in} 第 j 个位置信息的绝对值；$|\gamma_j|$ 为对应第 j 个位置的筛选阈值。当第 j 个位置信息的绝对值小于筛选阈值 $|\gamma_j|$ 时，将该位置的值置为 0，即 M_{out} 的值取 0，达到减少计算复杂度的目的，如图 5 中 M_{out} 的空白部分所示；当第 j 个位置信息的绝对值大于等于筛选阈值 $|\gamma_j|$ 时，M_{out} 的值与 M_{in} 保持一致。

2 数据集和预处理

本文采用 CICDDOS2019 数据集验证所提模型效果。CICDDOS2019 数据集由真实的网络系统生成，包括良性流量和最新常见的 DDoS 攻击，从原理上 DDoS 攻击被分为基于反射的 DDoS 攻击和基于漏洞的 DDoS 攻击，从协议上被分为基于 TCP、UDP 及 TCP、UDP 集成的攻击[24]，详细的分类情况如表 3 所示。

表 3 CICDDOS2019 数据集 DDoS 攻击的详细分类

Table 3 Detailed classification of DDoS attacks in CICDDOS2019 dataset

按原理分类	按协议分类	详细分类
基于反射的 DDoS	基于 TCP 的攻击	MSSQL
		SSDP
	基于 TCP/UDP 的攻击	DNS
		LDAP
		NETBIOS
		SNMP
		PORTMAP
	基于 UDP 的攻击	CharGen
		NTP
		TFTP
基于漏洞的 DDoS	基于 TCP 的攻击	SYN Flood
	基于 UDP 的攻击	UDP Flood
		UDP-Lag

原始数据集按攻击类型分为 11 个文件，每个文件所包括的 DDoS 攻击实例数量和实验所用到的实例数量如表 4 所示。CICDDOS2019 数据集中的实例包括 56 863 个正常流量包和 12 类共 50 006 249 个攻击流量包（WebDDoS 只有 439 个），每个实例都有 88 个特征，其中 1 个为分类标签。因为原始数据集的实例数量过大，所以在训练和测试所提的模型时，从原始数据集中选取部分样本构建训练和测试样本集，样本集中包含从 11 文件中选取的正常实例共 56 863 个，在 11 类攻击实例中，每类都选取 56 863 个。

表 4 CICDDOS2019 数据集实例分析

Table 4 Example analysis in CICDDOS2019 dataset 单位：个

DDoS 攻击类型（标签）	数据集包含的实例数量			训练和测试样本集数量	
	正常	异常	合计	正常	异常
DrDoS_DNS	3 402	5 071 011	5 074 413	56 863	56 863
DrDoS_LDAP	1 612	2 179 930	2 181 542		56 863
DrDoS_MSSQL	2 006	4 522 492	4 524 498		56 863
DrDoS_NetBIOS	1 707	4 093 279	4 094 986		56 863
DrDoS_NTP	14 365	1 202 642	1 217 007		56 863
DrDoS_SNMP	1 507	5 159 870	5 161 377		56 863
DrDoS_SSDP	763	2 610 611	2 611 374		56 863
DrDoS_UDP	2 157	3 134 645	3 136 802		56 863
Syn	392	1 582 289	1 582 681		56 863
TFTP	25 247	20 082 580	20 107 827		56 863
UDP-lag（含 WebDDoS）	3 705	366 900	366 900		56 863
总数	56 863	50 006 249	50 063 112	56 863	625 493

3 仿真分析

3.1 实验平台

模型的训练和测试在 Intel® Core™ i7-1165 处理器、16 GB RAM、Win10 64 位操作系统上完成，编程环境为 Jupyter Notebook 6.52，编程框架为 Python 3.8 和 TensorFlow 2.11，1D-CNN 的卷积核大小为 3，通道数为 64。

3.2 评价指标

TCA1C 模型的对比实验选取 DT 模型[13]、极限学习机（ELM）模型[25]、LSTM 模型[26]和 1D-CNN 模型[27]，本文采用准确率、召回率、精确率、F1 值和每步平均耗时作为评估 TCA1C 模型性能的指标。

准确率是阳性和阴性样本被正确区分的比例，表示对整体样本的分类能力，如式（7）所示；召回率是在真实的阳性样本中预测为阳性样本所占的比例，表示正确预测阳性样本全度的能力，如式（8）所示；精确率是在预测的阳性样本中真实阳性样本所占的比例，表示正确预测阳性样本精度的能力，如式（9）所示；F1 值是召回率和精确率的加权调和平均，可平衡单维度指标的缺陷，如式（10）所示。

$$A_{Accuracy}=\frac{T_P+T_N}{T_P+T_N+F_P+F_N} \tag{7}$$

计算机工程 www.ecice06.com

$$R_{\text{Recall}}=\frac{T_{\text{P}}}{T_{\text{P}}+F_{\text{N}}} \tag{8}$$

$$P_{\text{Precision}}=\frac{T_{\text{P}}}{T_{\text{P}}+F_{\text{P}}} \tag{9}$$

$$F_1=2\times\frac{P_{\text{Precision}}\times R_{\text{Recall}}}{P_{\text{Precision}}+R_{\text{Recall}}} \tag{10}$$

其中：T_{P}表示预测和实际都是阳性的样本数量；F_{P}表示将阴性误判为阳性的样本数量；T_{N}表示预测和实际都是阴性的样本数量；F_{N}表示将阳性误判为阴性的样本数量。

对于卸载任务分类处理模块，本文采用计算任务安全卸载概率K来评估模块的有效性。

当终端设备的计算任务在一定的攻击概率K_{attack}下进行卸载时，采用任务分类处理时，各个卸载任务的安全概率相互独立，表示为：

$$K_{\text{secure}}=\left(1-K_{\text{attack}}\right)\times F_1 \tag{11}$$

其中：K_{secure}为采用任务分类处理时的计算任务安全卸载概率；K_{attack}为计算任务受到攻击的概率。

当不采用任务分类时，各个卸载任务的安全概率取决于信道中所有卸载任务的安全情况，每个需要卸载任务的安全概率相互影响，表示为：

$$K'_{\text{secure}}=\left[\left(1-K_{\text{attack}}\right)\times F_1\right]^n \tag{12}$$

其中：K'_{secure}为不采用任务分类处理时的计算任务安全卸载概率。

3.3 仿真结果

模型训练的准确率收敛情况如图 6 所示。DT 在训练 10 轮时，准确率从 0.500 0 上升到 0.913 0，在 10 轮以后迅速收敛并稳定在 0.993 3 附近。ELM 收敛的波动幅度较小，从 0.954 6 稳定收敛到 0.965 8 附近。TCA1C 与 LSTM、1D-CNN 的收敛趋势大致相同，但 TCA1C 和 LSTM 比 1D-CNN 收敛得更快，在训练 10 轮时，TCA1C 和 LSTM 可以达到 0.993 0 以上的准确率，而 1D-CNN 在训练 40 轮时才能接近 0.993 0。TCA1C 在训练 10 轮以后，准确率稳定接近 0.997 5，而 LSTM 波动幅度很大，准确率最高为 0.993 5，最低为 0.955 0。从收敛速度和结果来看，TCA1C 明显优于其他对比模型。

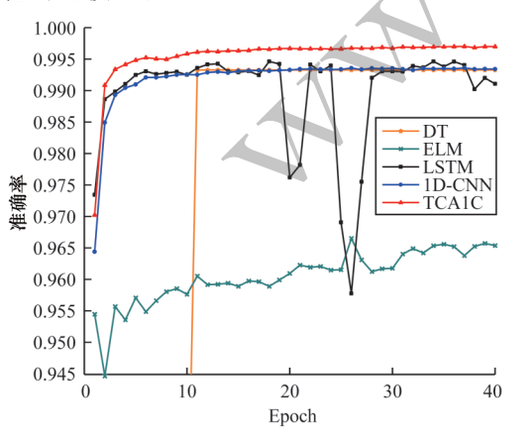


图 6 5 种模型准确率的收敛性

Fig.6 Convergence of accuracy for five models

5 种模型训练过程中每步平均耗时如图 7 所示。LSTM 在训练过程中学习的参数比其他模型更多，每步平均耗时最长且波动幅度大，最短为 11 ms，最长为 209 ms。ELM 在 10 轮以后每步平均耗时明显变长，在 20~60 ms 之间波动。DT、1D-CNN 和 TCA1C 每步平均耗时均在 15 ms 以下，由于 TCA1C 在训练过程中，通过 CA 和 SA 机制减少了冗余特征的学习，因此 TCA1C 比 1D-CNN 在耗时方面更占优势，90% 以上的每步平均耗时低于 1D-CNN，在准确率高于 DT 情况下，每步平均耗时与 DT 基本一致，稳定在 4~8 ms 之间。

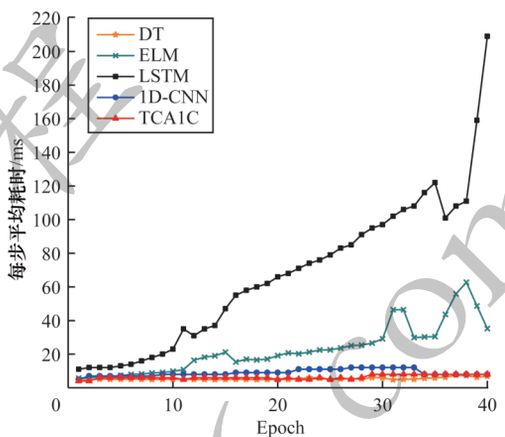


图 7 5 种模型每步平均耗时

Fig.7 Average time consuming per step of five models

5 种模型在精确率、召回率、F1 值上的表现情况如图 8 所示。各模型对数据集里 11 类 DDoS 攻击进行检测，对各类攻击检测的性能取平均值进行比较。DT 的综合表现为：精确率 0.993 43，召回率 0.993 51，F1 值 0.993 45。ELM 的综合表现为：精确率 0.960 74，召回率 0.960 31，F1 值 0.960 12。LSTM 综合表现为：精确率 0.995 50，召回率 0.995 42，F1 值 0.995 39。1D-CNN 综合表现为：精确率 0.996 86，召回率 0.996 80，F1 值 0.996 82。TCA1C 综合表现为：精确率 0.997 28，召回率 0.997 27，F1 值 0.997 25。TCA1C 整体上优于 DT、ELM、LSTM 和 1D-CNN 模型，并得到了更好的分类结果。

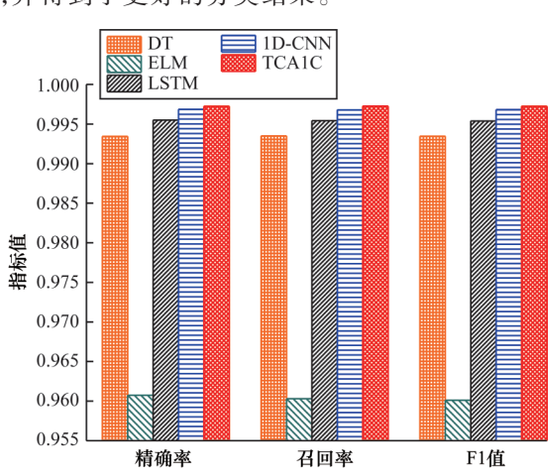


图 8 5 种模型性能对比

Fig.8 Performance comparison of five models

计算机工程 www.ecice06.com

当边缘网络中进行卸载的计算任务受到攻击概率为20%和40%时，各计算任务安全卸载概率如图9所示。需要卸载的计算任务经过任务分类处理，安全卸载概率相互独立，能保持较高水平。未经任务分类处理时，不同卸载任务的安全卸载概率互相影响，最终的安全卸载概率随着卸载任务数量的增加而快速降低，严重影响了卸载任务的安全性。

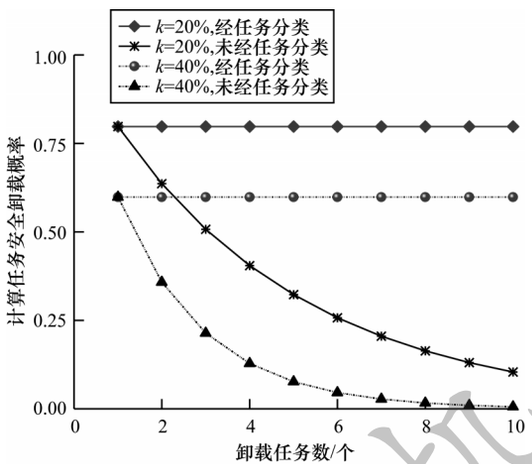


图9 计算任务安全卸载概率

Fig.9 Computing task security unloading probability

基于以上仿真结果和分析可知，TCA1C模型在DDoS检测方面具有明显优于ELM、LSTM和1D-CNN的准确率和时间性能，虽然时间性能与DT相当，但准确率明显优于DT模型，通过在线流量处理，可以解耦不同卸载任务的关联性，有效保障终端设备在进行计算卸载时整体的安全性。

4 结束语

本文针对边缘网络中防御DDoS攻击时资源受限的特点，研究和分析当前边缘网络DDoS防御方法存在的问题，提出了一种基于任务分类的Attention-1D-CNN DDoS检测模型TCA1C。该模型通过卸载任务分类处理机制对混杂在通信链路中的流量数据按任务分类并处理为可以直接输入到检测模块的数据样式；通过Attention-1D-CNN模块对每个计算任务进行DDoS检测，正常数据进入边缘服务进行处理，异常数据被丢弃或将该会话关闭。实验结果表明，TCA1C模型对DDoS攻击在降低整体用时的情况下，具有较高的检测准确率，当卸载任务面临一定攻击概率时，能使计算任务的卸载保持较高的安全性。TCA1C模型的优异性能表明，该模型是一种适合边缘网络环境的DDoS攻击检测方法。下一步工作将在此基础上，研究边缘网络中攻击强度、入侵响应策略对计算任务安全卸载的影响，寻求能够降低计算任务安全卸载所需成本的高效检测方案。

参考文献

[1] 施巍松，张星洲，王一帆，等. 边缘计算：现状与展望[J]. 计算机研究与发展，2019，56(1)：69-89.
SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89. (in Chinese)

[2] XU W, TAO Y D, GUAN X. The landscape of Industrial Control Systems (ICS) devices on the Internet [C]// Proceedings of International Conference on Cyber Situational Awareness, Data Analytics and Assessment. Washington D. C. , USA: IEEE Press, 2018: 1-8.

[3] AWS Shield. Threat landscape report-Q1 2020[EB/OL]. [2023-05-06]. https://aws-shield-tlr. s3. amazonaws. com/2020-Q1_AWS_Shield_TLR. pdf.

[4] CHOUHAN S. Energy optimal partial computation offloading framework for mobile devices in multi-access edge computing [C]//Proceedings of International Conference on Software, Telecommunications and Computer Networks. Washington D. C. , USA: IEEE Press, 2019: 1-6.

[5] 王婷婷，甘臣权，张祖凡. 面向工业物联网的移动边缘计算研究综述[J]. 计算机应用与软件，2023，40(1)：1-10，65.
WANG T T, GAN C Q, ZHANG Z F. Review on mobile edge computing for industrial Internet of Things [J]. Computer Applications and Software, 2023, 40(1): 1-10, 65. (in Chinese)

[6] KAO Y H, KRISHNAMACHARI B, RA M R, et al. Hermes: latency optimal task assignment for resource-constrained mobile computing[C]//Proceedings of IEEE Conference on Computer Communications. Washington D. C. , USA: IEEE Press, 2015: 1894-1902.

[7] YOU C S, HUANG K B, CHAE H, et al. Energy-efficient resource allocation for mobile-edge computation offloading[J]. IEEE Transactions on Wireless Communications, 2017, 16(3): 1397-1411.

[8] 战俊伟，庄毅. 基于能耗与延迟优化的移动边缘计算任务卸载模型及算法[J]. 计算机与现代化，2022(8)：86-93.
ZHAN J W, ZHUANG Y. Mobile edge computing task offloading model and algorithm based on energy consumption and delay optimization[J]. Computer and Modernization, 2022(8): 86-93. (in Chinese)

[9] 陈璐，汤红波，游伟，等. 移动边缘计算安全防御研究[J]. 网络与信息安全学报，2021，7(1)：130-142.
CHEN L, TANG H B, YOU W, et al. Research on security defense of mobile edge computing[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 130-142. (in Chinese)

[10] 宋宇波，金星妤，燕锋，等. 车联网中移动边缘计算的安全高效节能卸载策略[J]. 清华大学学报(自然科学版)，2021，61(11)：1246-1253.
SONG Y B, JIN X Y, YAN F, et al. Secure and energy efficient offloading of mobile edge computing in the Internet of vehicles[J]. Journal of Tsinghua University (Science and Technology), 2021, 61(11): 1246-1253. (in Chinese)

[11] HUANG Z Y, XIA G M, WANG Z H, et al. Survey on edge computing security [C]//Proceedings of International Conference on Big Data, Artificial Intelligence and Internet

计算机工程 www.ecice06.com

of Things Engineering. Washington D. C., USA: IEEE Press, 2020: 96-105.

[12] 张晓东,张朝昆,赵继军. 边缘智能研究进展[J]. 计算机研究与发展,2023,60(12):2749-2764,2769.
ZHANG X D, ZHANG C K, ZHAO J J. Research progress of edge intelligence [J]. Computer Research and Development, 2023, 60(12): 2749-2764, 2769. (in Chinese)

[13] ALZAHRANI R J, ALZAHRANI A. Security analysis of DDoS attacks using machine learning algorithms in networks traffic[J]. Electronics, 2021, 10(23): 2919.

[14] 董瑞洪,闫厚华,张秋余,等. 基于深度森林算法的分布式 WSN 入侵检测模型[J]. 兰州理工大学学报,2020,46(4):103-109.
DONG R H, YAN H H, ZHANG Q Y, et al. Distributed WSN intrusion detection model based on deep forest algorithm [J]. Journal of Lanzhou University of Technology, 2020, 46(4): 103-109. (in Chinese)

[15] 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.
TIAN T, YU Y K, NIU X Z. DDos detection based on deep learning in edge computing environment[J]. Computer Measurement & Control, 2023, 31(7): 28-34, 168. (in Chinese)

[16] SINGH P, JAYKUMAR J, PANKAJ A, et al. Edge-detect: edge-centric network intrusion detection using deep neural network[C]//Proceedings of the 18th Annual Consumer Communications and Networking Conference. Washington D. C., USA: IEEE Press, 2021: 1-6.

[17] 李晓佳,赵国生,汪洋,等. 面向 CNN 和 RNN 改进的物联网入侵检测模型[J]. 计算机工程与应用,2023,59(14):242-250.
LI X J, ZHAO G S, WANG Y, et al. Improved intrusion detection model of Internet of Things for CNN and RNN[J]. Computer Engineering and Applications, 2023, 59(14): 242-250. (in Chinese)

[18] DORIGUZZI-CORIN R, MILLAR S, SCOTT-HAYWARD S, et al. LUCID: a practical, lightweight deep learning solution for DDoS attack detection [J]. IEEE Transactions on Network and Service Management, 2020, 17(2): 876-889.

[19] KIRANYAZ S, AVCI O, ABDELJABER O, et al. 1D convolutional neural networks and applications: a survey[J]. Mechanical Systems and Signal Processing, 2021, 151: 107398.

[20] KIRANYAZ S, GASTLI A, BEN-BRAHIM L, et al. Real-time fault detection and identification for MMC using 1-D convolutional neural networks[J]. IEEE Transactions on Industrial Electronics, 2019, 66(11): 8760-8771.

[21] 刘达山,刘潞琦,张光驰,等. 基于深度学习的 Attention 机制文献综述[J]. 信息技术与信息化,2023(1):189-194.
LIU D S, LIU L Q, ZHANG G C, et al. Literature review of attention mechanism based on deep learning [J]. Information Technology and Informatization, 2023(1): 189-194. (in Chinese)

[22] WANG Q L, WU B G, ZHU P F, et al. ECA-Net: efficient channel attention for deep convolutional neural networks[C]// Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition. Washington D. C., USA: IEEE Press, 2020: 11531-11539.

[23] WOO S, PARK J, LEE J Y, et al. CBAM: convolutional block attention module[C]//Proceedings of ECCV 2018. Berlin, Germany: Springer, 2018: 1-10.

[24] SHARAFALDIN I, LASHKARI A H, HAKAK S, et al. Developing realistic Distributed Denial of Service (DDoS) attack dataset and taxonomy[C]//Proceedings of 2019 International Carnahan Conference on Security Technology. Washington D. C., USA: IEEE Press, 2019: 1-10.

[25] 李忠成,高惠燕,张文祥. 边缘计算中改进 ELM 的高效入侵检测算法[J]. 计算机测量与控制,2021,29(7):223-228,234.
LI Z C, GAO H Y, ZHANG W X. An efficient edge computing intrusion detection algorithm based on improved ELM[J]. Computer Measurement & Control, 2021, 29(7): 223-228, 234. (in Chinese)

[26] MYNENI S, CHOWDHARY A, HUANG D J, et al. SmartDefense: a distributed deep defense against DDoS attacks with edge computing[J]. Computer Networks, 2022, 209: 108874.

[27] HUANG H C, YE P X, HU M, et al. A multi-point collaborative DDoS defense mechanism for IIoT environment[J]. Digital Communications and Networks, 2023, 9(2): 590-601.

编辑 金胡考

计算机工程 www.ecice.com