计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(7):113−120 [doi: 10.15888/j.cnki.csa.009158]

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

基于自编码器的网络游戏流量分类①

宁安安[1], 张　俊[1,2], 年　梅[1]

[1](新疆师范大学 计算机科学技术学院, 乌鲁木齐 830054)
[2](中国科学院 新疆理化技术研究所, 乌鲁木齐 830011)
通信作者: 年　梅, E-mail: 2468830639@qq.com

摘　要: 加密和动态端口技术使传统的流量分类技术不能满足网络游戏识别的性能需求, 本文提出了一种基于自编码器降维的端到端流量分类模型, 实现网络游戏流量的准确识别. 首先将原始流量预处理成 784 B 的一维会话流向量, 利用编码器进行无监督降维, 去除无效特征; 接着探索构建卷积神经网络与 LSTM 网络并联算法, 对降维后的样本进行空间和时序特征的提取和融合, 最后利用融合特征进行分类. 在自建的游戏流量数据集和公开数据集上测试, 本文模型在网络游戏流量识别方面达到了 97.68% 的准确率; 与传统端到端的网络流量分类模型相比, 本文所设计的模型更加轻量化, 具有实用性, 并且能够在资源有限的设备中方便部署.

关键词: 网络游戏流量分类; 自编码器; 无监督降维; 卷积神经网络; LSTM 网络

引用格式: 宁安安,张俊,年梅.基于自编码器的网络游戏流量分类.计算机系统应用,2023,32(7):113–120. http://www.c-s-a.org.cn/1003-3254/9158.html

Online Game Traffic Classification Based on Autoencoder

NING An-An[1], ZHANG Jun[1,2], NIAN Mei[1]

[1](College of Computer Science and Technology, Xinjiang Normal University, Urumqi 830054, China)
[2](Xinjiang Technical Institute of Physics and Chemistry, Chinese Academy of Sciences, Urumqi 830011, China)

Abstract: Encryption and dynamic port technology make the traditional traffic classification technology fail to meet the performance requirements of online game identification. In this study, an end-to-end traffic classification model based on auto-encoder dimension reduction is proposed to accurately identify online game traffic. First, the original traffic is preprocessed into a one-dimensional session flow quantity of 784 B, and the encoder is used for unsupervised dimension reduction and removing invalid features. Then, the parallel algorithm of the convolutional neural network and LSTM network is explored and constructed to extract and fuse spatial and temporal features of samples after dimension reduction. Finally, the fusion features are used for classification. When tested on the self-built game traffic dataset and the open dataset, the proposed model achieves an accuracy rate of 97.68% in online game traffic identification. Compared with the traditional end-to-end network traffic classification model, the model designed in this study is more lightweight and practical and can be easily deployed on devices with limited resources.

Key words: online game traffic classification; autoencoder; unsupervised dimension reduction; convolutional neural network (CNN); LSTM network

1　引言

网络游戏是目前人们重要的娱乐方式和社交手段, 根据 CNNIC (中国互联网信息中心) 第 49 次《中国互联网络发展状况统计报告》显示, 截至 2021 年 12 月, 我国网民规模达 10.32 亿, 其中我国网络游戏用户规模达 5.54 亿, 占网民整体的 53.6%. 和平精英、王者荣

① 基金项目: 国家重点研发计划 (E1182101)
收稿时间: 2022-12-29; 修改时间: 2023-01-19; 采用时间: 2023-02-09; csa 在线出版时间: 2023-04-23
CNKI 网络首发时间: 2023-04-24

耀、荒野行动、穿越火线、英雄联盟等是高校学生广泛喜爱的游戏, 部分学生因沉溺于网络游戏而荒废学业, 无法顺利完成学业. 对高校校园网管理部门, 游戏流量占用了校园网大量的带宽若不加以控制, 会影响高校正常教学、科研以及管理业务流量的顺畅传输. 为了精确了解校园网网络游戏的占用校园网资源的情况, 并在必要的情况下能够对游戏流量的带宽加以适当的管控, 需要精确识别游戏流量, 为提升数字校园为学校教学科研服务的质量提供技术支持.

早期, 研究者主要采用基于端口、基于深度包检测 (DPI)、基于传输层行为等传统的网络游戏流量识别方法进行课题的研究. 文献 [1] 利用 Wireshark 工具抓取不同类型的网络游戏流数据, 采用协议过滤和 IP 过滤的方法对数据进行预处理, 并通过大量的统计特征分析找出适合于游戏流分类的特征, 实验结果表明, 利用 IP 过滤和提取出的特征组合可以有效地提高识别准确率. 文献 [2] 通过对游戏报文的内容研究, 提取出识别游戏流量的特征规则库, 并基于 EGT-PC 算法提出了一种高效的游戏流量分类方法. 文献 [3] 利用网络游戏流量有效载荷的统计特征, 构建了决策树、贝叶斯网络等不同的机器学习识别模型, 对比了不同模型的识别准确性和性能, 实验结果表明, 机器学习模型能够以非常高的准确率识别网络游戏流量. 然而现如今大多数网络游戏都采用了动态端口及加密模式传输, 传统的流量分类技术已不能满足网络游戏流量识别的需求.

当前, 深度学习在网络流量分类领域取得了很好的成绩, 利用其自动提取特征的优势实现了端到端的网络流量分类. 其中, 文献 [4,5] 首次提出了一种基于深度学习的端到端的流量分类模型, 对原始的流量转换得到灰度图, 利用 CNN 进行特征提取并分类, 实现恶意流量的检测. 在此基础上, 许多研究者进行了模型的优化. 如文献 [6] 使用了基于 VGG-Net 的神经网络进行特征提取, 构建了跨层多特征融合模块进行特征组合, 使网络流量的分类准确率达到 97.8%. 文献 [7] 用 VGG16 模型作为特征提取网络构建了孪生神经网络模型, 实现恶意流量的检测, 取得了很好的检测效果. 文献 [8] 则构建基于一维卷积神经网络模型进行流量分类, 达到了 81% 的分类准确率. 文献 [6–12] 优化传统的 VGG、ResNet 等模型构建网络端到端的网络流量分类模型, 以上研究均将网络流量转换为灰度图, 但由于灰度图颜色单一, 各点像素值非常接近, 导致像素值冗余问题, 若直接将灰度图送入深度学习中进行特征提取和分类, 冗余的像素值会浪费计算资源和内存资源, 降低流量分类模型的实用性. 本文针对端到端的网络流量分类模型的数据信息冗余问题, 构建了自编码器模型对数据集先进行特征降维, 然后再提取特征向量, 构成端到端网络游戏流量的粗粒度分类模型. 在特征提取模型中, 参考文献 [4] 和文献 [13] 利用 CNN 网络结构与 LSTM 网络结构进行串联构成了层次化的时空特征提取模型的研究, 为了避免 CNN 网络结构与 LSTM 网络结构进行串联时互相之间的影响. 本文将提取空间特征的卷积神经网络与提取时序特征的 LSTM 网络进行并联, 构建了类似于伪孪生神经网络的特征提取模型架构提取特征. 实验证明, 本文提出的并联时空特征提取模型架构在网络游戏流量分类方面取得了很好的效果, 识别准确度达 97.68%, 同时本文所设计的模型更加轻量化.

2 网络游戏流量分类模型的构建

本网络流量分类模型由 3 个模块构成: 一是数据预处理模块, 将 PCAP 原始流量文件利用文献 [7] 预处理工具切分为会话并转为特征向量的格式; 二是自编码器降维模块, 采用自编码器将流量特征向量压缩, 除去无用的特征, 保留有效的特征向量; 三是特征提取与分类模块, 先分别利用卷积神经网络结构提取空间特征、LSTM 网络结构提取时序特征, 将空间特征和时序特征进行拼接融合, 然后送入 Softmax 分类器进行分类. 模型的整体架构如图 1 所示.

2.1 数据集预处理

本文使用了文献 [14] 构建数据集进行网络游戏流量粗粒度分类模型性能的研究, 该数据集由自建游戏流量数据和 ISCX VPN2016 数据并集构成. 其中游戏流量包括了 LOL、CF、炉石传说、英雄联盟、CSGO 等主流游戏样本集. ISCX VPN2016 数据集包括 Chat、Email、VoIP、File、 P2P、Streaming 这 6 种应用程序流量样本. 原始流量数据集包含完整的 PCAP 流量, 利用图 1 预处理流程将原始流量处理为会话流向量 NPY 文件.

网络游戏以 TCP 流和 UDP 流在网络中传输, 可基于五元组进行会话流的切割与重组. TCP 流可以根据 3 次握手与 4 次挥手确定一条有序流. UDP 流则根据数据包的开始发送时间和结束时间确定. 经过删除

无效的、重复的流以及 MAC 和 IP 等干扰数据后, 若长度大于 784 B 则截取, 小于则用 0 填充, 最终形成 784 B 的一维向量. 该会话流用一维向量 X_i=[x_{i1}, x_{i2}, x_{i3}, x_{i4}, ⋯, x_{ij}] 表示, 其中 i 代表 n 个一维向量中的第 i 个向量, j 代表第 i 个向量中的第 j 个元素, 即会话流样本中的字节所对应的十进制数值赋值为向量中的对应分量. 一维向量的取值范围为 [0, 255], 为了加快模型的训练速度以及收敛速度, 降低模型的计算复杂度, 归一化处理使每个向量值的范围在 [0, 1], 归一化算法如式 (1) 所示.

$$X_i' = \frac{X_i}{255} \tag{1}$$

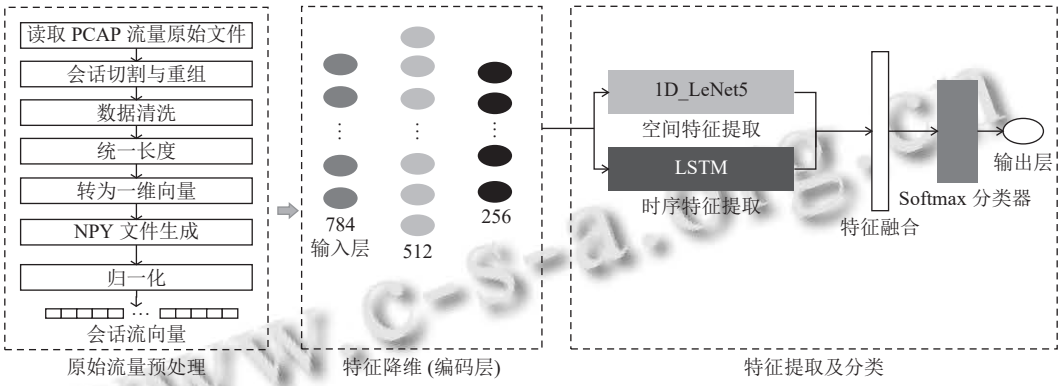

图 1 网络游戏流量分类模型的整体架构

2.2 自编码器降维

由于缺乏权威带标签网络游戏流量样本, 选择使用无监督算法进行降维. 无监督降维主要包括 PCA 算法和自编码器算法. PCA 算法[15] 属于线性降维, 不适合对非线性关系的网络流量数据集进行降维, 故本文选择自编码器进行特征降维. 自编码器网络模型[16] 由编码器和解码器构成, 自编码器的结构如图 2 所示. 输入向量用隐藏层压缩成潜在空间表征编码, 该编码值代表了输入向量的重要程度. 然后解码器对该编码进行重构输出.

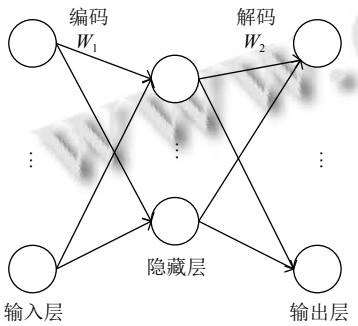

图 2 自编码器结构图

编码器的函数关系式如式 (2) 所示.

$$h = f(W_1 \cdot X + b_1) \tag{2}$$

其中, f 表示编码层的激活函数, X 表示输入数据, W_1 表示编码层的权重, b_1 表示编码层的偏置项, h 表示经编码函数 f 压缩后的潜在空间表征向量. 解码器则是将潜在空间表征向量 h 进行解码, 其函数关系如式 (3).

$$X' = g(W_2 \cdot h + b_2) \tag{3}$$

其中, g 表示解码层的激活函数, W_2 表示解码层的权重, b_2 表示解码层的偏置项, h 为编码器处理后的潜在空间表征, X'则是通过解码函数. g 重构得到输出向量. 在自编码器训练的过程中, 利用反向传播算法, 并且通过多次迭代不断更新 W_1、b_1、W_2、b_2 参数, 使得X'与X的重构误差较小, 其采用的重构损失函数为均方误差 (mean square error, *MSE*) 函数, 重构损失函数如式 (4) 所示.

$$e = MSE = \frac{1}{M}\sum_{i=1}^{M} |X_i - X_j'|^2 \tag{4}$$

图 3 为本文设计的 AE 自编码器的结构, 其中参数 N 表示降维后的特征向量维数. 本文自编码器包含一个 784 维度的输入层, 两个 512 维度的隐藏层和一个 N 维度的隐藏层, 以及一个 784 维度的输出层. 模型降维的目标是找出最小特征向量维度 N, 利用该维度的特征向量能够使解码器实现原始特征向量的重构, 即降维但不影响分类效果. 为此, 分别将 N 设置为 128、256、512 等不同的维度, 使用 Softmax 分类函数对不同 N 维特征进行分类, 根据分类结果选择最佳维度 N. 结果如表 1 所示.

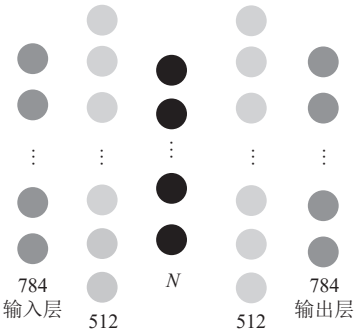

图 3 本文设计的 AE 自编码器结构

表 1 不同隐藏层维度 N 的分类效果 (%)

隐藏层维度	A	P	R	$F1$
AE-Softmax (128)	92.47	92.33	90.89	91.16
AE-Softmax (256)	96.56	95.62	94.46	95.03
AE-Softmax (512)	95.99	94.37	93.29	93.81

表 1 为 AE 自编码器网络结构选择不同的维度 N 降维后, Softmax 分类器的结果, 表 1 表明, 当会话流维度降为 256 时, 其准确率、精准率、召回率、$F1$ 值均高于其他两种维数, 说明 256 维的特征向量能够保留更好的表征特征, 更有利于模型的分类.

2.3 特征提取及分类模块

网络流量的层次化特征体系如图 4 所示, 原始流量是由流量字节, 数据包, 网络流构成, 即原始流量是一种结构化信息. 网络流量中的数据包之间和每条流之间存在着时序特征关系. 本文参考文献 [4] 思路的基础上, 提出了优化模型用于网络游戏流量特征提取, 即提出了将卷积神经网络 (convolutional neural networks, CNN) 提取的空间特征和长短期记忆网络 (long short term memory network, LSTM) 提取的时序特征并行融合的算法, 最后基于时空特征进行分类的模型.

2.3.1 空间特征提取

经典的 LeNet5 卷积神经网络[17] 结构简单、计算量较少, 在图像识别领域已取得了很好的分类效果, 本文选择该模型提取数据包特征. LeNet5 网络结构如图 5 所示, 该模型的网络结构共 6 层, 由两个卷积层、两个池化层和两个全连接层组成. 其卷积层是二维结构. 而本文数据集是一维向量, 故需要将 LeNet 网络进行改造, 即卷积层卷积核由 5×5 改为 1×5, 池化层由 2×2 改为 1×2. 改造后的 LeNet 网络结构如图 6 所示. 经过 AE 无监督降维后形成 256 维的特征向量, 使用一维的 LeNet5 网络结构自动学习与提取数据包特征向量, 最终得到 84 维的空间特征. 改进后的 LeNet5 称为 1D_LeNet5.

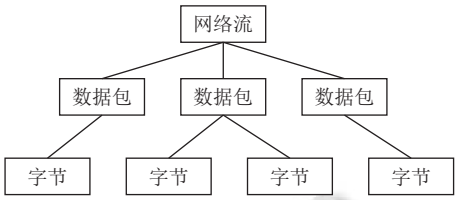

图 4 网络流量的层次化结构

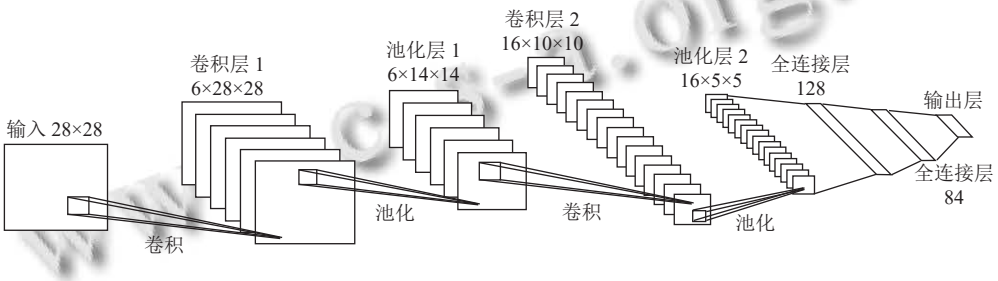

图 5 LeNet5 网络结构图

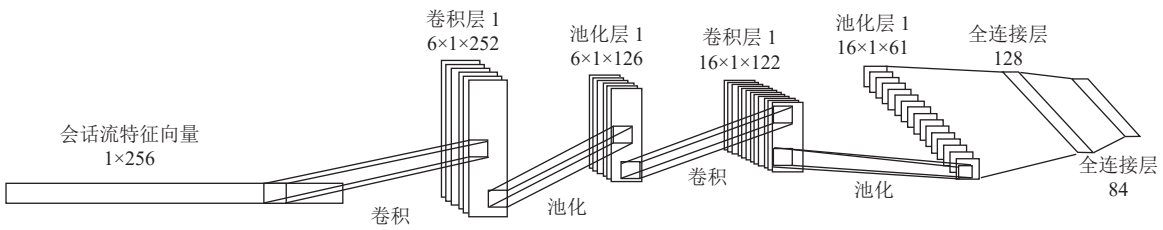

图 6 网络游戏流量空间特征提取模型结构图

2.3.2 时序特征提取

本文利用长短期记忆网络[18]模型提取流之间的时序特征, LSTM 是一种特殊类型的 RNN, 能够学习流量包之间长期的依赖关系.

输入向量为 256 维, 选择 LSTM 模型中的参数 t 为 16, 即将含有 256 B 的一维向量分别在 16 个时间点输入到网络中, 每个时间点输入数据的长度也为 16. 模型的隐藏层的节点数设置为 128. 其 LSTM 模型架构如图 7 所示.

2.3.3 时空特征融合和分类算法

在特征提取模型中, 参考文献 [4] 和文献 [13] 利用 CNN 网络结构与 LSTM 网络结构进行串联构成了层次化的时空特征提取模型的研究. 本文利用实验证实, 空间特征的提取与时序特征的提取, 它们之间的先后顺序位置对模型的分类结果有一定影响的猜想.

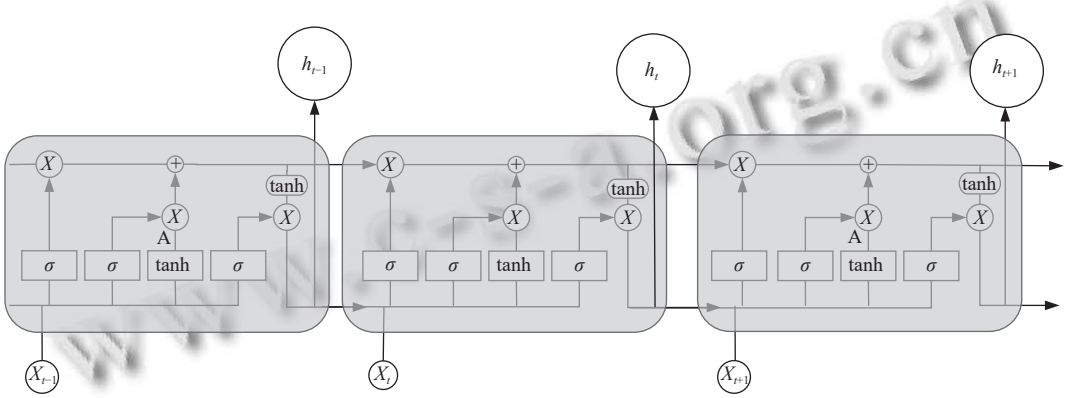

图 7 网络游戏流量时序特征提取的 LSTM 模型架构

因此为了提高分类的准确度, 将 1D_LeNet5 模型提取的空间特征和 LSTM 模型提取的时序特征使用 Keras 深度学习框架中的 concatenate 函数进行融合. 假设空间特征的通道分别为 X_1, X_2, X_3, …, X_n 和时序特征的通道分别为 Y_1, Y_2, Y_3, …, Y_m. 然后将空间特征和时序特征进行融合, 其融合算法如式 (5) 所示.

$$Z=\sum_{i=1}^{n}X_i\cdot K_i+\sum_{i=1}^{m}Y_i\cdot K_i \tag{5}$$

其中, ·代表卷积操作, K_i 代表第 i 个卷积核. 参数 n、m 分别代表空间特征和时序特征的通道数. 经过特征融合后, 得到一个新的特征图 Z, 其通道数为 m+n.

融合后的特征最后用 Softmax 分类器进行分类. Softmax 函数如式 (6) 所示.

$$\partial_i(X)=\frac{\exp(x_i)}{\sum_{j=1}^{m}\exp(x_j)} \tag{6}$$

其中, m 为类别数, x_i为第 i 个节点的输出值, 结果是某流量样本在 m 个分类上的概率分布, 输出不同类别之间的相对概率, 概率值最高的一类可作为模型的分类结果.

同时本文结合时空特征的融合模型与文献 [4] 和文献 [13] 利用 CNN 网络结构与 LSTM 网络结构思想进行串联构成了层次化的时空特征提取模型分别做了 3 组对比实验, 实验结果如图 8 所示.

其中 AE-1D_LeNet5-LSTM 为本文设计的时空特征融合模型, 同时参考文献 [4] 和文献 [13] 的时空特征提取模型结构本文针对 LSTM 所在位置设计了两个模型分别为 AE-1D_LeNet5 (before)-LSTM 和 AE-LSTM (before)-1D_LeNet5.

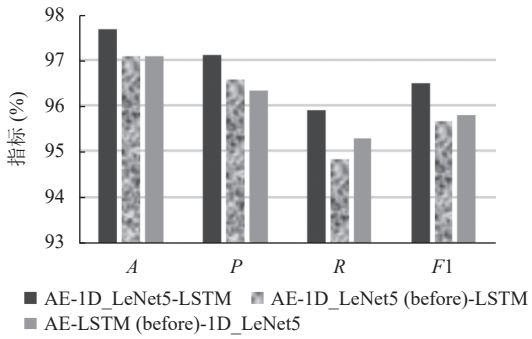

图 8 时空特征提取模型对比实验结果

通过图 8 实验结果可以看出, LSTM 模型所在的位置会影响模型的分类效果, 该实验结果验证了本文

的猜想. 其原因在于先提取空间特征, 然后再从空间特征中提取时序特征, 由于 1D_LeNet5 模型中通过一维卷积层的计算和下采样操作提取比较重要的空间特征的同时也可能会失去一些重要的时序特征, 这样会影响 LSTM 模型对时序特征的提取, 从而影响模型分类的效果. 反言而止, 若 LSTM 模型在 1D_LeNet5 模型之前, 虽然通过 LSTM 模型获得了重要的时序特征, 但是在提取时序特征的过程中也会失去一些潜在的空间特征. 因此 1D_LeNet5 模型与 LSTM 模型若进行前后位置的组合, 他们之间会互相影响, 同样也与模型的参数有关, 例如 1D_LeNet5 的卷积核的大小, 神经元的个数, LSTM 模型中的隐藏层输出的数量, 输入的维度等参数. 鉴于此, 为了降低 1D_LeNet5 模型与 LSTM 模型之间的相互影响, 本文所设计的模型就是将 1D_LeNet5 与 LSTM 并联构建出类似于伪孪生神经网络的特征提取模型, 即 AE-1D_LeNet5-LSTM, 通过并联的方式使得他们之间互不干扰.

3 实验结果与分析

将数据集按照 7:2:1 的比例划分为训练集、测试集、验证集, 根据实验结果测试本文模型的性能. 实验环境为: CPU 使用了 Intel(R) Xeon(R)W-2235 处理器, 匹配了 NVIDIA GeForce RTX 3080 显卡, 操作系统为 Windows 10 专业版, 开发软件为 PyCharm, 深度学习框架为 Keras 2.8.0, 编程语言使用了 Python 3.8.

3.1 评价指标

本模型将各种游戏流量作为一类进行识别, 非游戏流量则按照 ISCX VPN2016 数据集的应用程序类别进行分类. 为了更好地评估本文模型的性能, 选取准确率 (A)、召回率 (R)、精确率 (P) 以及 $F1$ 分数作为评价指标. 其中 TP 定义为游戏流量类别中样本正确地归类为游戏流量的百分比; FN 定义为游戏流量类别中样本被错误归类为其他流量类别样本的百分比; FP 是指其他流量类别的样本被错误归类为游戏流量样本的百分比. 评估指标表达式如式 (7)–式 (11) 所示:

$$A = \frac{TP+TN}{TP+FP+FN+TN} \tag{7}$$

$$P = \frac{TP}{TP+FP} \tag{8}$$

$$R = \frac{TP}{TP+FN} \tag{9}$$

$$F1 = \frac{2\cdot P\cdot R}{P+R} \tag{10}$$

此外, 本文用空间复杂度和计算复杂度对模型的复杂性进行了分析. 空间复杂度即为模型运行所占的内存空间. 计算复杂度, 用模型的浮点型计算量 (floating point operations, *FLOPs*) 进行评估, 其计算公式如式 (11) 所示.

$$FLOPs = \sum_{i=1}^{i=n}\left[\left(2\cdot k_{w_i}\cdot k_{h_i}\cdot c_{\mathrm{in}_i}\right)\cdot c_{\mathrm{out}_i} + c_{\mathrm{out}_i}\right]\cdot H\cdot W \tag{11}$$

其中, k_{w_i}表示每一层卷积核的宽度, k_{h_i}表示每一层卷积核的高度, 一维卷积神经网络中卷积核的高度为 1, c_{in_i}表示每一层输入的通道数量, c_{out_i}表示每一层输出的通道数量. H、W 表示输出特征图的高和宽, 经过一维卷积神经网络每次卷积后获取特征向量, 所以 H 为 1. 通过计算每一层的计算量, 然后求和得到模型的浮点型计算量来评估模型的计算复杂度.

3.2 实验结果及分析

为了验证降维算法的性能, 设计了两组实验, 分别为:

(1) AE-1D_LeNet5-LSTM: 数据集经过 AE 自编码器降维后, 利用本文特征时空特征融合模型进行特征提取和融合后, 送入 Softmax 分类器进行分类.

(2) 1D_LeNet5-LSTM: 将未降维的 784 B 的特征向量, 利用本文模型提取时空特征, 融合后送入 Softmax 分类器进行分类.

结果如表 2 所示, 分别给出了经过 AE 自编码器降维前后不同类网络流量分类的精确率、召回率、$F1$ 值. 表 2 结果表明, 经过 AE 自编码器降维后, 除 P2P 流量识别性能持平外, 其他各种流量分类在精准率、召回率、$F1$ 值 3 个指标上均高于降维前, 尤其是各类流量分类的精确度明显提高. 对网络游戏流量, 降维后的精准率、召回率、$F1$ 值与降维前相比, 分别提高了 4.82%、2.83%、3.81%. 此外, 宏平均 (macro-averaging) 指标能较好地体现模型的整体分类效果, 从表 2 中看出, 各类流量降维后的宏平均的各项指标均高于降维前, 说明经过 AE 自编码器降维后的特征向量更有利于模型的特征提取, 能明显改善游戏流量的分类性能.

为了验证并行时空特征融合算法的性能, 使用常用的特征提取算法与融合算法进行了性能对比, 实验结果如表 3 所示. 设计了如下 3 组实验.

表 2 降维实验对比结果 (%)

流量分类	降维前 (1D_LeNet5-LSTM)			降维后 (AE-1D_LeNet5-LSTM)		
	P	*R*	*F*1	*P*	*R*	*F*1
Chat	83.99	97.56	90.27	99.12	98.65	98.89
Email	96.42	75.75	84.84	98.50	98.42	98.46
File	86.45	86.92	86.69	89.59	88.77	89.18
P2P	100	99.86	99.93	100	100	100
Streaming	90.28	84.79	87.45	97.97	91.63	94.70
Game	92.29	92.29	92.29	97.11	95.12	96.10
VoIP	96.83	97.35	97.09	97.60	98.66	98.13
macro-averaging	92.32	90.65	91.22	97.12	95.89	96.49
准确率		93.21			97.68	

表 3 特征提取模块实验结果 (%)

指标	AE-1D_LeNet5			AE-LSTM			AE-1D_LeNet5-LSTM		
	P	*R*	*F*1	*P*	*R*	*F*1	*P*	*R*	*F*1
macro-averaging	96.36	95.24	95.76	96.75	94.57	95.58	97.12	95.89	96.49
准确率	97.19			97.10			97.68		

(3) AE-1D_LeNet5: AE 自编码器降维后的特征向量通过 1D_LeNet5 模型进行会话流空间特征的提取和分类.

(4) AE-LSTM: AE 自编码器降维后的特征向量通过 LSTM 模型中进行时序特征的提取和分类.

(5) AE-1D_LeNet5-LSTM: 经过 AE 自编码器降维后的特征向量进行空间特征的提取与时序特征的提取, 然后将空间特征与时序特征进行融合再送入 Softmax 分类器进行分类.

实验结果如表 3 所示, 空间特征提取模型 AE-1D_LeNet5 与时序特征提取模型 AE-LSTM 的准确率相差不大, 仅相差 0.09%, 但是时空特征融合后的模型 AE-1D_LeNet5-LSTM 的准确率均高于前两者, 高达 97.86%. 说明时空特征的融合更有利于模型的特征学习能力, 提高模型分类器的分类效果.

为了验证本文模型的复杂度, 利用相同的数据集, 设计实验对 AE-1D_LeNet5-LSTM 模型与文献 [4] 端到端的网络流量分类模型 (称为 1D_CNN) 以及 ResNet[19] 、VGG[20] 等这些传统的深度学习模型, 从计算复杂度、参数大小、内存空间、准确率 4 个指标进行对比. 结果如表 4 所示.

从表 4 明显发现, 本文构建的网络游戏流量识别模型的准确率均比其他 3 个模型高于 1 个百分点以上. 同时在浮点型计算量、时间复杂度、内存空间 3 个指标比较, 本文模型均比其他 3 个模型更加轻量化, 更具有实用性.

表 4 与其他模型的对比结果

模型	浮点型计算量 (*GFLOPs*)	参数大小 (k)	内存空间	准确率 (%)
AE-1D_LeNet5-LSTM	0.001 48	745	8.61 MB	97.68
1D_CNN[4]	0.039 7	5 827	66.7 MB	95.72
VGG[19]	0.921	123 302	1.37 GB	95.40
ResNet18[20]	0.661	1 408	5.53 MB	92.79

4 总结

本文首先利用 AE 自编码器无监督降维消除了会话流向量中的部分数据冗余问题. 其次构建了一种类似于伪孪生神经网络的时空特征提取网络, 即将 1D_LeNet5 模型与 LSTM 模型进行并联, 该特征提取网络充分利用了深度学习自动提取特征的能力来挖掘会话流内部的空间关系和会话流间的时序关系, 有效提高了网络游戏流量的分类效果, 游戏流量的分类准确率达到了 97.68%, 并且也优化了其他非游戏流量的分类精度. 但本文只在单一的数据集上进行了实验, 在数据预处理的统一长度阶段采用了截取的方式, 这样会造成一些有效信息的丢失, 因此在后续研究中将采用不同的数据预处理方式使用更多的数据集进行研究, 以获取更好的模型分类效果.

参考文献

1 周锐, 董育宁. 网络游戏流特征分析与识别. 计算机工程与应用, 2016, 52(23): 135–141.

2 毕夏安, 张大方, 赵姣姣. 一种高效的游戏流量识别与分类技术. 计算机工程与应用, 2011, 47(23): 101–103, 111.

3 Williams N, Zander S, Armitage G. Evaluating machine learning methods for online game traffic identification. Technical Report, Melbourne: Swinburne University of Technology. 2006.

4 王伟. 基于深度学习的网络流量分类及异常检测方法研究 [博士学位论文]. 合肥: 中国科学技术大学, 2018.

5 Wei W, Zhu M, Wang JL, *et al*. End-to-end encrypted traffic classification with one-dimensional convolution neural networks. Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics. Beijing: IEEE, 2017. 43–48.

6 顾兆军, 郝锦涛, 周景贤. 基于改进双线性卷积神经网络的恶意网络流量分类算法. 信息网络安全, 2020, 20(10): 67–74.

7 李道全, 鲁晓夫, 杨乾乾. 基于孪生神经网络的恶意流量检测方法. 计算机工程与应用, 2022, 58(14): 89–95.
8 李道全, 王雪, 于波, 等. 基于一维卷积神经网络的网络流量分类方法. 计算机工程与应用, 2020, 56(3): 94–99.
9 潘嘉, 翟江涛, 刘伟伟. 基于改进递归残差网络的恶意流量分类算法. 计算机应用研究, 2020, 37(S2): 227–229.
10 薛文龙, 于炯, 郭志琦, 等. 基于特征融合卷积神经网络的端到端加密流量分类. 计算机工程与应用, 2021, 57(18): 114–121.
11 代志康, 吴秋新, 程希明. 一种基于 ResNet 的网络流量识别方法. 北京信息科技大学学报 (自然科学版), 2020, 35(1): 82–88.
12 石欣然, 张奇支, 赵淦森, 等. 一种基于少样本且不均衡的网络攻击流量检测系统. 华南师范大学学报 (自然科学版), 2021, 53(1): 100–108.
13 Zou Z, Ge JG, Zheng HB, *et al*. Encrypted traffic classification with a convolutional long short-term memory neural network. Proceedings of the 20th IEEE International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems. Exeter: IEEE, 2018. 329–334.
14 徐星晨, 张俊, 年梅. 基于表征学习的网络游戏流量识别. 计算机系统应用, 2021, 30(12): 172–179. [doi: 10.15888/j.cnki.csa.008203]
15 Shlens J. A tutorial on principal component analysis. International Journal of Remote Sensing, 2014, 51(2).
16 Michelucci U. An introduction to autoencoders. arXiv: 2201.03898, 2022.
17 LeCun Y, Jackel L D, Bottou L, *et al*. Learning algorithms for classification: A comparison on handwritten digit recognition. Neural Networks: The Statistical Mechanics Perspective, 1995, 261(276): 2.
18 Hochreiter S, Schmidhuber J. Long short-term memory. Neural Computation, 1997, 9(8): 1735–1780. [doi: 10.1162/neco.1997.9.8.1735]
19 He KM, Zhang XY, Ren SQ, *et al*. Deep residual learning for image recognition. Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016. 770–778. [doi: 10.1109/CVPR.2016.90]
20 Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition. arXiv:1409.1556, 2014.

(校对责编: 牛欣悦)