重庆理工大学学报(自然科学)
Journal of Chongqing University of Technology(Natural Science)
2021 年第 35 卷第 6 期
Vol. 35 No. 6 2021
doi: 10.3969/j. issn. 1674-8425(z). 2021. 06. 021

# 集成分类器的加密 YouTube 流量精细化分类方法

邹乐述[1], 翟江涛[2]

(1. 江苏科技大学 电子信息学院, 江苏 镇江 212003;
2. 南京信息工程大学 电子与信息工程学院, 南京 210044)

**摘 要**:为提升网络服务质量,实现流量精细化可管可控,针对特征失效问题,提出一种加密 YouTube 视频流量的精细化分类方法。设计快捷有效的特征提取方法,同时,为解决机器学习单个分类器度量手段单一问题,选取不同种类分类器,经过特征筛选后为每个分类器输入不同的特征数量组合。通过设置权值和阈值,根据分类精度进行权值更新,最终实现高精度分类。实验结果表明:所提方法较现有模型对加密应用下流量识别效果提升 3% 左右。

**关 键 词**:YouTube 视频流量;特征提取;集成学习;权值更新;流量分类
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1674-8425(2021)06-0165-09

# An Integrated Classifier to Encrypt YouTube Traffic Fine Classification Method

ZOU Leshu[1], ZHAI Jiangtao[2]

(1. College of Electronics & Information, Jiangsu University of Science & Technology, Zhenjiang 212003, China; 2. College of Electronics & Information Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China)

**Abstract**: Application classification of encrypted traffic is one of the hot topics in current research. However, the current algorithm has the problem that classification particles are too thick to meet the current needs. In order to improve the service quality of the network and realize the traffic fine and controllable, a fine classification method of encrypting YouTube video traffic is proposed for the

**收稿日期**:2020-05-26
**基金项目**:国家自然科学基金项目(61702235)
**作者简介**:邹乐述,男,硕士研究生,主要从事人工智能与信息安全研究,E-mail:1374404664@qq.com;通讯作者 翟江涛,男,博士,副教授,主要从事人工智能与信息安全研究,E-mail:jiangtaozhai@gmail.com。

**本文引用格式**:邹乐述,翟江涛. 集成分类器的加密 YouTube 流量精细化分类方法[J]. 重庆理工大学学报(自然科学),2021,35(6):165-173.

**Citation format**: ZOU Leshu, ZHAI Jiangtao. An Integrated Classifier to Encrypt YouTube Traffic Fine Classification Method[J]. Journal of Chongqing University of Technology(Natural Science),2021,35(6):165-173.

feature failure problem. First, a fast and effective feature extraction method is designed. At the same time, in order to solve the single measurement method of a single classifier in machine learning, different types of classifiers are selected and different number combinations of features are input for each classifier after feature screening. By setting the weights and thresholds, the weights are updated according to the classification accuracy, and the classification with high precision is finally realized. The experimental results show that the proposed method is about 3% more effective than the existing model in traffic recognition.

**Key words**: YouTube video traffic; feature extraction; integrated learning; weight update; traffic classification

据 CNNIC(China internet network information center)2019 年 8 月 30 日发布的第 44 次《中国互联网络发展状况统计报告》显示,截至 2019 年上半年,我国互联网普及率已超过 6 成。截至 2019 年 6 月,我国网民规模达 8.54 亿。人们在享受互联网技术带来便利的同时也产生了一些新的问题,近年来互联网安全[1]事件频发,僵尸网络[2-3]、APT(advanced persistent threat)[4-5]、木马[6-7]等为主要形式的网络攻击事件愈演愈烈。2018 年就有勒索病毒 GlobeImposter、Facebook 用户数据泄露、前程无忧 195 万条个人求职简历泄露等事件。随着人们的安全意识的增强,对数据保护意识也越来越强烈,为提升网络服务质量,流量加密技术成为保护数据的重要手段,当前加密流量已经成为当前主要的流量之一。流量加密在保护数据的同时也给网络安全带来了新的问题,在保护数据安全的同时也隐藏了恶意流量,因此加密流量分类成为当前研究的热点问题之一。随着加密技术、端口伪装技术、端口随机分配等方法的使用,使得现有的特征失效,很多传统的网络流量分类技术分类效果往往不佳,如普遍使用的 DPI(deep packet inspection)、基于端口识别技术等。

目前,在非加密流量分类方面已有众多相关文献给出了诸多较好的方法,国内外学者取得了较多成果,Ruixi 等[8]采用一种基于 SVM(support vector machine)的方式可实现高精确度流量分类。在 2018 的互联网报告中,加密流量占比已经超过一半,而且还在急速增长之中,相信不久互联网流量将会基本以加密流量为主。将识别非加密流量的方法和特征直接应用于加密流量将不再适用。现有对加密流量分类相关文献也已取得十分不错的成果[9-11],Grimaudo 等[12]提出自学习分类器也取得了不错的效果。Shen 等[13]引入了 Certificate 报文大小增加 Markov 链的状态多样性,并建立二阶 Markov 链模型对 HTTPS(hyper text transfer protocol over securesocket layer)应用进行分类。Lotfollahi 等[14]采用 CNN(convolutional neural networks)建立模型对流量进行分类。赵博等[15]提出了一种基于加权累积和检验的时延自适应加密流量盲识别算法,通过实验表明该方法能有效区别加密流量。当前,在不同方向都已取得了一些不错的研究成果,如加密协议的识别[16-18]、加密应用的识别[19-20]等,但上述方法大都存在分类颗粒度较粗的问题,在针对具体某一应用下流量精细化分类问题,国内相关文献较少。很多特征在具体的某一应用下的精细化识别实验效果往往不理想。加密流量之下特征的转变,不仅使得传统常用的特征失效,而且也使加密之后流量的精细化识别难度加大,在某一个应用之下,流量的相似性更大,很难寻找到有效的特征。加密流量之中视频流量所占比例较高,为提升网络服务质量,实现流量更精细化可管可控,本文提出一种基于集成分类器的加密 YouTube 视频流量精细化标题分类方法。实验表明,本文中所提方法较现有模型对加密应用下流量分类效果提升 3% 左右。

## 1 加密 YouTube 流量精细化分类方法

### 1.1 流量特征获取

本文的识别目标为加密 YouTube 视频流量精

细化分类,针对传统特征失效问题,采用一种快捷且有效的特征提取方法。

### 1.1.1 数据集的获取及预处理

本研究所做实验采用的数据集来源是 Ran 等[21]所公开的数据集,如表 1 所示。

表 1 实验数据集

| 标题 | 数据包个数 | 数据流条数 | 加密协议 |
|---|---|---|---|
| 2pac_Changes | 1 236 975 | 100 | TLS |
| Akon_Right_Now | 2 175 826 | 100 | TLS |
| Albatross | 1 182 457 | 100 | TLS |
| Alexis_y_Fido | 4 916 187 | 100 | TLS |
| Ali_G_NBA_interviews | 7 513 659 | 100 | TLS |
| American_Hustle | 1 102 624 | 100 | TLS |
| Avengers | 2 210 823 | 100 | TLS |
| Avicii_Waiting | 3 660 021 | 100 | TLS |
| bara_bere | 2 976 735 | 100 | TLS |
| Black_Eyed_Peas_Where_Is_The_Love | 2 801 729 | 100 | TLS |

该数据集是一个拥有 10 000 个 YouTube 视频流的大数据集,所使用的视频标题是来自不同类别的热门 YouTube 视频,比如体育、新闻、自然以及视频动作预告片和 GoPro 视频等。因为 Chrome 浏览器在市场上是最受欢迎的浏览器,并且其受欢迎程度正在不断增长,所以 YouTube 视频集采集浏览是通过 Chrome 浏览器,使用的播放模式是 YouTube 的默认的自动播放模式(播放器会根据客户端网络状况的估计决定下载哪种质量)。所使用的是 Selenium 网络自动化工具和 ChromeDriver 作为爬虫,因此它将模拟完全相同的普通用户视频下载行为方式。为此,在数据集中,其中包含 10 000 个 YouTube 流(通过真实世界的互联网连接在一个月内通过不同的真实网络条件下载)。

在获取数据集后,首先根据流量的五元组将流量进行划分(protocol、src IP、dst IP、src port、dst port),决定每个流是否为 YouTube 流,过滤掉其他存在的干扰流,先可基于客户端消息 SNI(Server Name Indication)中的服务名称中的字段完成,如在(SNI)中找“googlevideos. com”的字段则将其留下。同时,去除其音频包,相比于视频包,音频包对识别分类的影响是有限的。本次预处理还可通过 wireshark 进行 IP 过滤筛选,wireshark 分析数据样本如表 2 所示,同时将其中的重传包进行过滤(重传一般都是由于网络原因所造成的)。

表 2 数据集样本分析

| No | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 5 | 0.015 170 | 10.0.0.4 | 81.218.16.208 | TLSv1.2 | 285 | Client Hello |
| 8 | 0.015 497 | 10.0.0.4 | 81.218.16.208 | TLSv1.2 | 285 | Client Hello |
| 11 | 0.034 054 | 81.218.16.208 | 10.0.0.4 | TLSv1.2 | 1 414 | Server Hello |
| 16 | 0.035 537 | 81.218.16.208 | 10.0.0.4 | TLSv1.2 | 934 | Certificate, Server Key Exchange, Server Hello Done |
| 22 | 0.066 268 | 10.0.0.4 | 81.218.16.208 | TLSv1.2 | 1 308 | Application Data |
| 36 | 0.093 201 | 81.218.16.208 | 10.0.0.4 | TLSv1.2 | 195 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |

### 1.1.2 特征提取

通过分析流量的传输,提取传输过程的时间戳及对应时间传输的包长,如表 2 所示 Time、Length。选取 Time 前 $T$ 时间内传输的数据包长 Length,根据时间 $T$ 将它平均切分成 $n$ 份,将每段时间传输数据包长之和作为特征,$n$ 段即可得 $n$ 个特征,如上表取 $T$、$n$ 分别为 0.1、2,即可得 2 个特征,特征 1 为前 Time0.05 时间 Length 长度之和为

2 918(285 + 285 + 1 414 + 934),特征 2 为 1 503(1 308 + 195)。

### 1.1.3 流量特征对比

当 $T$ 取 20、$n$ 为 20,如图 1 所示,随机在某一类中选取 10 个样本,通过对比同类别之间的特征区别,可以从同类特征表现图中发现样本之间同类特征表现具有极大的相似性。如图 2 所示,随机选取其中 4 类中各一个样本,通过对比非同类样本之间的特征表现,可以发现不同类之间总存在某一特征时刻与其他样本之间差别较大。且本方法提取的特征经实验部分验证具有较强的可行性。

经特征提取后分别标上对应的类别标签,如表 3 所示,随机抽取了 7 个样本,为方便展示,表中数据集样本为 $T$ 为 20、$n$ 为 5 的数据,同时通过实验发现,$T$ 取不同值时,对分类精确度存在一定的影响,将在实验部分对比 $T$ 和 $n$ 取不同值时对分类的影响。

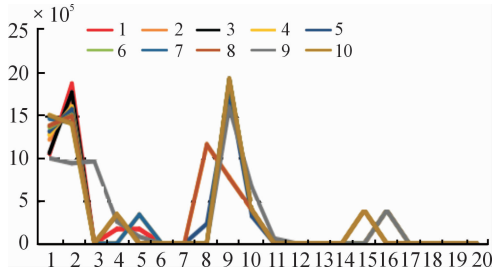


图 1 同类特征对比曲线

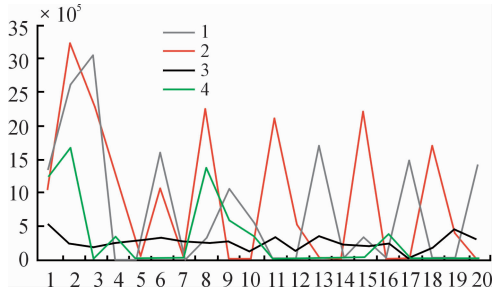


图 2 非同类特征对比曲线

表 3 数据集特征样本

| | Feature1 | Feature2 | Feature3 | Feature4 | Feature5 | 类别 |
|---|---|---|---|---|---|---|
| 1 | 2 898 700 | 336 300 | 2 329 025 | 390 904 | 1 336 | Akon_Right_Now |
| 2 | 1 262 287 | 940 876 | 1 370 146 | 882 846 | 1 565 201 | Albatross |
| 3 | 7 744 023 | 2 192 154 | 3 917 410 | 3 021 548 | 2 106 537 | Alexis_y_Fido |
| 4 | 7 041 932 | 1 577 425 | 1 965 483 | 2 413 453 | 2 297 115 | Ali_G_NBA_interviews |
| 5 | 3 673 176 | 335 871 | 3 601 924 | 335 898 | 3 329 201 | American_Hustle |
| 6 | 2 300 675 | 1 761 507 | 10 727 917 | 405 417 | 2 593 849 | Avengers |
| 7 | 2 268 501 | 2 066 376 | 9 436 110 | 406 751 | 3 675 319 | Avengers |

## 1.2 集成加密流量精细化识别方法

### 1.2.1 现有典型分类器

随机森林主要是以 bagging 算法为基础,也是一种集成学习的算法,由多棵决策树构成,且具有随机性,从总体的特征之中随机选取特征,就可以很好地降低过拟合的现象,使其具有比较好的泛化能力,这是比较常用的算法,但在数据集样本噪声干扰比较大时,随机森林所训练的模型容易陷入过拟合。同时,当存在取值划分特征较多时就很容易对随机森林所训练的模型产生更大的影响,最终对模型的评估产生影响。

KNN(k-nearest neighbor)是一种常见的算法,因为它非常有效,所以经常在实验当中使用。它的原理也非常的简单,主要包括 3 个要素:$K$ 值的选择、距离的度量以及决策的规则。对于 $K$ 值的选择通常采用交叉验证的方式选取最优 $K$ 值,常使用的距离的度量方式是欧氏距离,分类决策规则往往是多数表决的方式。现将已有的带标签的数据集分布在空间当中。当需要预测新的数据时,将找到它在空间坐标之中对应的位置,并选取

计算距离它最近的 $K$ 个点,并且找到这 $K$ 个点对应的类别,最终将预测的数据类别划归为这 $K$ 个点种类别最多的一类。KNN 虽然原理非常简单,但是存在一些缺点,当类别不平衡时对数据量稀少的类别预测准确率极低。所以相对来说仅仅使用某一种算法来分类,虽然能取得的效果还算不错,但是分类评估手段比较单一,如 $K$ 近邻算法仅采用计算距离的方式来评估所属类别,决策树通过信息增益来进行分类。这种依靠单一度量属性的方法相对集成多种方法的方式来说鲁棒性较差,分类效果也不如集成之后的方法。

### 1.2.2 本文方法

主要思想是基于特征维度和模型集成 2 个部分去提升分类效果,① 通过改变特征的输入组合以及数量,使得分类器输入不同的特征维度;② 通过集成不同模型分类结果进行最终分类。集成分类方法如图 3 所示。

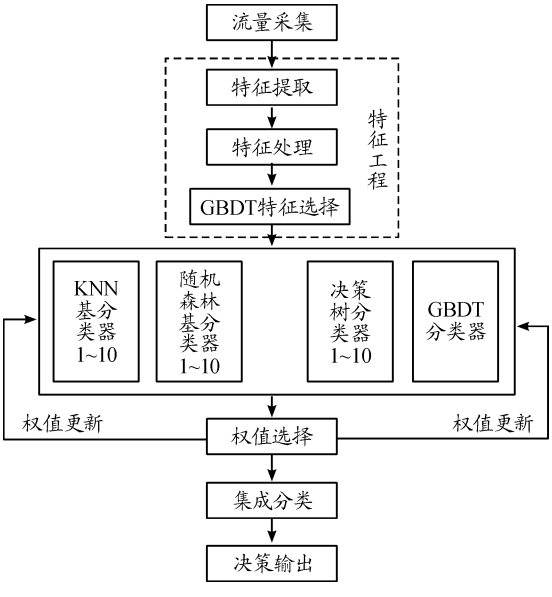


图 3 集成分类方法框图

### 1.2.3 数据处理及特征选择

由于不同的基分类器对于特征要求不同,本文对于同样的数据特征根据不同的基分类器进行相应的特征处理,针对 KNN 基分类器对数据进行了归一化数据处理。

特征选择对分类器的结果起着至关重要的作用,对于每一份数据来说都拥有不止一个属性特征,但是部分特征对分类识别比较重要,同时也存在某些特征对分类有反作用影响。同时特征选择可以规避维数灾难,当对分类器性能要求较高时,选取其中比较重要的特征,可提高运行性能,简化分析。比较常见的特征选择方法分为 3 类,过滤式、包裹式、嵌入式。过滤式方法是先对数据进行处理,而不管后续使用的是什么分类器。包裹式方法是直接将学习器的性能作为特征的评价指标,但是当然它的开销也比过滤式的大。嵌入式方法是直接将特征选择与学习器结为一体,即在学习的过程之中自动进行特征选择,比如决策树等。

采用 GBDT(gradient boosting decision tree)嵌入式的特征选择模块,综合考虑选择不同维度特征,从低维到高维,当 $n$ 取 20 时,通过 GBDT 分类器的获取各特征在分类器中的重要程度,选择特征数量为 11 ~20,共 10 种特征组合。

### 1.2.4 基分类器、权重选择以及集成决策

为克服单个分类算法度量单一,如 KNN 仅通过单一的距离度量手段,决策树通过信息增益或信息增益比的方式来度量。本文提出采用集成多分类器的方法,由于本文实验是针对 YouTube 视频流量具体精细化分类,通过选取其中一些针对 YouTube 视频流量具体精细化分类效果较好的分类算法,如 KNN、随机森林、贝叶斯算法、决策树算法、GBDT(梯度提升树),将其作为基分类器,且从机器学习框架 sklearn 的 model_selection 模块中使用 GridSearchCV 调参算法选择出每个基分类器相对最优参数。选择 KNN、随机森林、贝叶斯算法、决策树算法分类模型每种模型 10 个,4 种算法分类模型总共 40 个模型分类器。将特征选择模块获得的 10 种特征组合输入各分类器,如分类器 KNN1 输入特征数 11、分类器 KNN2 输入特征数 12…分类器 KNN10 输入特征数 20,随机森林、贝叶斯算法、决策树算法分类模型也类似。由于 GBDT 分类效果相对更好,将其单独拿出直接输入所有特征,并在之后权值模块将其权值设置为

1 100。

将数据集按 0.7、0.1、0.2 的比例切分为训练集、验证集、测试集。在权重选择模块上,设置阈值 $X$,将分类效果相对较差的模型剔除不参与最终决策。将阈值 $X$ 设置为 80%,它最终决定有多少基分类器能参与决策,分类能力比较低的基分类器模型将会被剔除不能参与集成决策,否则将影响最终的集成分类效果。同时还为每个分类器在最终决策时设置权重,权值决策分类如图 4 所示。

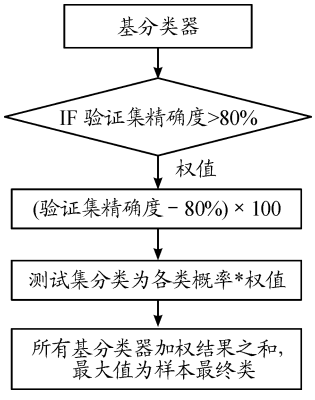


图 4 集成权值分类决策流程框图

例如基分类器 1 验证精确度 91% 分类样本 1 的所属各类概率(0.1,0.15,0.6,0,0,0,0,0,0.15,0),权值为(91% ~ 80%) × 100 等于 11,基分类器 1 分类结果为(0.1,0.15,0.6,0,0,0,0,0,0.15,0) × 11 等于(1.1,1.65,6.6,0,0,0,0,0,1.65,0)。将所有基分类器分类结果相加求和,将该样本分类为其中的最大值的类别。由于在分类实验中分类器 GBDT 明显效果好于其他分类器,且 GBDT 分类器只有一个,所以将权值部分的 100 加大为 1 100。为了拉开基分类器之间的权值差距,权值计算部分使用了验证集精确度减去 0.8,如直接使用验证精确度 ×100 作为权值则各基分类器对最终决策影响几乎一样。为减少切分的偶然性,采用 $k$ 折交验证进行权值更新,选择 $k$ 次验证权值的平均为最终权值。

通过 $k$ 折交叉验证根据分类精确度调整更新分类权值,分类效果相对较好的基分类器将在最终的分类决策时所占权值高一些。对于分类效果高于阈值,但相比对其他基分类器来说,它的效果较低时,将它的权值设置较低。总之,每个对于基分类器在总决策分类时所占的比重与它分类的准确度是成正相关的。本文设置 $k$ 折交叉验证在每次验证之后,模型将对每个基分类器分类的验证后的效果进行权值反馈更新。在最终的决策预测时,将每个基分类器对于每个样本分类概率乘权值求和,概率最高则将其分为该类。本方法存在较好的可扩展性,即存在其他分类器模型在所分类的数据集取得较好的效果时,本方法可将它加入其中扩充基分类器。由于每个基分类器都参与决策,而不由某一分类器或者某一类分类器单独决定,最终分类效果一般比较理想。同时,基分类器间相互独立且输入特征互异,可高度并行训练,所以在训练时间上与训练单个分类器基本相同。

## 2 实验结果及其分析

### 2.1 本次实验所配环境

实验采用的设备:Windows10,处理器:4 核 Intel(R) Core(TM) i3 - 4170 CPU @ 3.70GHz,RAM:8.00GB,系统类型:64 位,基于 x64 的处理器。同时还有其他的一些第三方软件:Wireshark、Python、pycharm、anaconda、Google 浏览器、机器学习 sklearn 框架等。

### 2.2 实验结果与分析

#### 2.2.1 评价指标

为了公正的判断本实验方法的有效性,采用准确率(accuracy)、召回率(recall)、精确率(Precision)、$F1$-score 作为评价指标,可以通过混淆矩阵来进行计算准确率。准确率是被分类的样本的正确率,当正确率越高,一般来说就分类器越好,它主要反应分类器将正判别为正、负判别为负的能力。召回率主要是指某一类正确被分为该类的所占的比例。精确率表示正确预测为正的占全部预测为正的比例。$F1$-score 它同时兼顾了分类模型的精确率和召回率。$F1$-score 可以看作是模型精确率和召回率的一种调和平均,它的最大值是 1,

最小值是 0。

$$\mathrm{Acc} = \frac{TP + TN}{TP + TN + FN + FP} \tag{1}$$

$$R = \frac{TP}{TP + FN} \tag{2}$$

$$P = \frac{TP}{TP + FP} \tag{3}$$

$$F1 = \frac{2PR}{P + R} \tag{4}$$

式中:$TP$(true positive)是将正类预测为正类的数目;$FP$(false positive)是将负类预测为正类的数目;$TN$(true negative)是将负类预测为负类的数目;$FN$(false negative)是将正类预测为负类的数目。

### 2.2.2 时间 $T$ 取值长度不同之间的对比

实验通过选取 $n$ 为 20,分别选择时间长度 $T$ 分别为 5、10、20 进行对比,图 5 为实验对比图,横轴为实验次数,纵轴为分类准确度,从图中可以看出,当时间 $T$ 取值越大分类效果越好,且对分类准确度影响较大。同时从实验中可看出,如存在实时检测性能的要求,可将 $T$ 设置为更小,当然分类精确度也相对较低。

### 2.2.3 提取特征数 $n$ 不同之间的对比

实验在相同的流时间间隔内,通过提取流量特征 $n$ 为不同数目,相互之间对比,得到适合的特征数目。主要设置特征数 $n$ 分别为 15、20、25。图 6 为不同特征数量之间的分类效果对比图,可以看出,当取不同的特征数目对分类效果的影响。15、20、25 分别对应黄、蓝、灰线,经过 20 次实验分类效果的平均值分别为 97.532 5、98.028 5、97.921,所以通过对比本文最终选取特征数 $n$ 为 20。

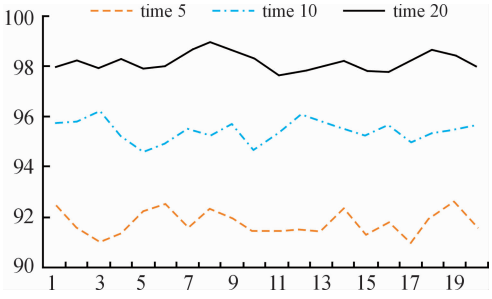


图 5 $T$ 取不同值时分类效果对比曲线

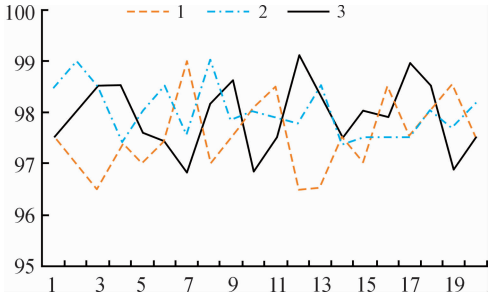


图 6 不同特征数分类效果对比曲线

基分类器模型在验证集分类准确度删选阈值 $X$ 选取实验对比如表 4 所示。主要参数如表 5 所示。

表 4 不同阈值分类效果对比

| $X$ | 集成分类准确度 |
|---|---|
| 70% | 96.5 |
| 80% | 98.1 |
| 90% | 97.4 |

表 5 主要参数

| 主要参数 | 取值 |
|---|---|
| $T$ | 20 |
| $n$ | 20 |
| $X$ | 80% |

其余非主要参数主要通过 GridSearchCV 调参算法自动选出,如 KNN 算法中的 $K$ 的取值,给定 GridSearchCV 算法 1 ~ 10 的范围,步长为 1,GridSearchCV 算法最终通过范围搜索得到使 KNN 分类器分类效果最好的 $K$ 值,如图 7 所示。

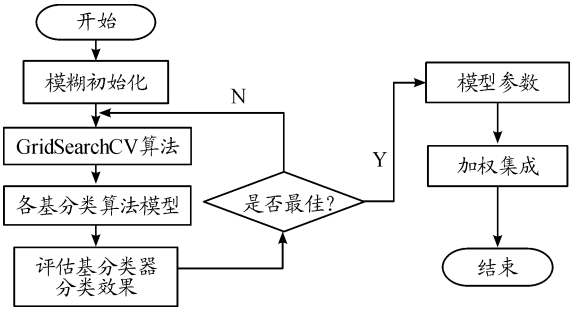


图 7 模型流程框图

### 2.2.4 与其他分类模型对比

当前,由于在某一应用下加密流量再精细化分类的相关研究成果较为有限,据 Ran 等[21]的研究,本文将与其提出的方法进行对比实验。

从图 8 中可以看出,经过 20 次实验对比,本方法的准确率平均为 98.01%,最高时可超过 99%。而文献[21]中方法的平均准确率为 95.26%,平均提升了 2.75%。同时本实验还对召回率进行了对比,可通过图 9 发现本方法的召回率平均为 98.092 5% 也是优于文献[21]中的 95.353 5%,平均提升 2.739%。从图 10 的精确率对比实验中得到本文方法的平均精确率为 98.672 5%,文献[21]的平均精确度为 95.486 0%,本方法精确率明显高于文献[21],提升了 3.186 5%。最后,对 2 个方法的 *F*1-score 进行对比,如图 11 所示,本文方法的平均 *F*1-score 为 98.380 5%,文献[21]的平均 *F*1-score 为 95.417 8%,本方法 *F*1-score 上也是高于文献[21],提升了 2.962 7%。综合 4 项指标对比实验可以看出本模型基本优于文献[21]中的方法。

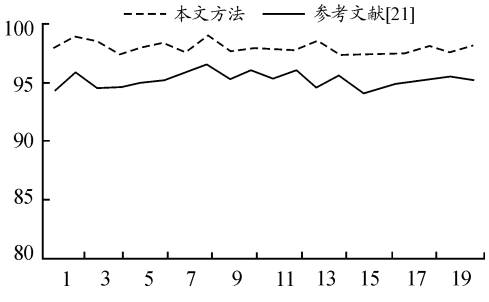


图 8 不同模型准确度对比曲线

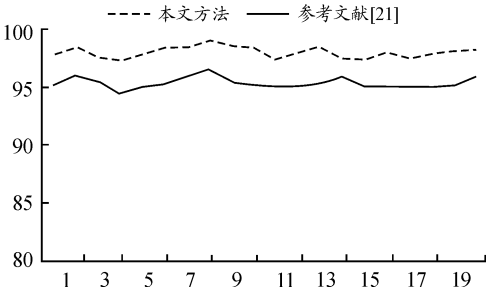


图 9 不同模型召回率对比曲线

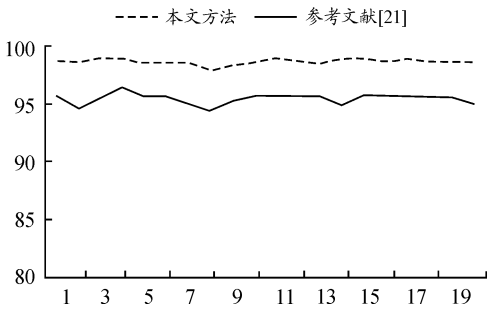


图 10 不同模型精确率对比曲线

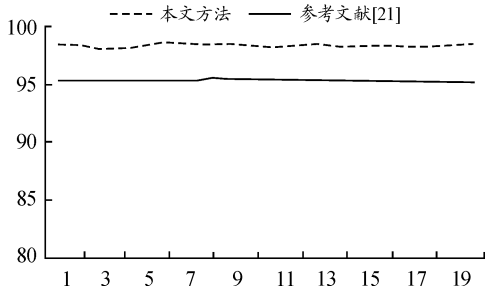


图 11 不同模型 F1 比对曲线

## 3 结论

针对加密的 YouTube 视频流量进行精细化分类算法研究,主要有 2 个方面。特征方面:提出一种快捷且有效的特征提取方法,模型方面:通过改变特征维度以及集成不同模型的方式,最终实现在公开数据集上最高识别率可达 99% 的良好效果。本文特征提取可将时间 *T* 设置相对更大,取得相对更好的分类效果。同时,本方法存在的一些不足之处也会在后续的研究中去改进,通过实验发现将文中提取出来的特征用较深层的深度学习模型进行分类识别,也能取得非常好的分类效果。

## 参考文献:

[1] 贾子骁,徐原. 2019 年 8 月网络安全监测数据发布[J]. 信息网络安全,2019(10):93 - 94.

[2] MOHAMMAD A, NAUMAN A, MOUHAMMD A K, et al. An efficient reinforcement learning-based Botnet detection approach[J]. Journal of Network and Computer Applications,2019:1 - 51.

[3] ABDURRAHMAN P. Tankut acarman deep learning to

detect botnet via network flow summaries[J]. Neural Computing and Applications,2019,31(11):8021 - 8033.

[4] 刘海波,武天博,沈晶,等. 基于 GAN-LSTM 的 APT 攻击检测[J]. 计算机科学,2020,47(1):281 - 286.

[5] LV K, CHEN Y, HU C Z. Dynamic defense strategy against advanced persistent threat under heterogeneous networks[J]. Information Fusion,2019,49:216 - 226.

[6] 兰景宏,刘胜利,吴双,等. 用于木马流量检测的集成分类模型[J]. 西安交通大学学报,2015,49(8):84 - 89.

[7] 张晓帆. 基于通信流量的木马检测技术研究[D]. 天津:河北工业大学,2017.

[8] RUIXI Y,ZHU L,XIAOHONG G,et al. An SVM-based machine learning method for accurate internet traffic classification[J]. Information Systems Frontiers, 2010, 12(2):149 - 156.

[9] GIUSEPPE A, DOMENICO C, ANTONIO M, et al. MIMETIC: Mobile encrypted traffic classification using multimodal deep learning[J]. Computer Networks, 2019, 165:445 - 458.

[10] IRENA O, DARIO P, MIRKO S, et al. A machine learning approach to classifying YouTube QoE based on encrypted network traffic[J]. Multimedia Tools and Applications,2017,76(21):22267 - 22301.

[11] CIRILLO M, MAURO M D, LONGO M, et al. Detection of encrypted multimedia traffic through extraction and parameterization of recurrence plots[C]//Proceedings of 2016 International Conference on Sustainable Energy, Environment and Information Engineering (SEEIE 2016). Science and Engineering Research Center, 2016: 286 - 290.

[12] GRIMAUDO L, MELLIA M, BARALIS E, et al. Self-learning classifier for internet traffic [P]. 2013: 423 - 428.

[13] SHEN M, WEI M, ZHU L, et al. Classification of encrypted traffic with second-order Markov chains and application attribute bigrams[J]. IEEE Transactions on Information Forensics and Security,2017,12(8): 1830 - 1843.

[14] LOTFOLLAHI M, ZADE R S H, SIAVOSHANI M J, et al. Deep packet: A novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2017:1 - 13.

[15] 赵博,郭虹,刘勤让,等. 基于加权累积和检验的加密流量盲识别算法[J]. 软件学报,2013,24(6):1334 - 1345.

[16] 李进东,王韬,吴杨,等. 基于主成分分析和学习矢量量化的会话初始协议识别研究[J]. 计算机工程,2016,42(6):125 - 130.

[17] 蔡乐. 基于帧的通信协议识别技术的研究[D]. 成都:电子科技大学,2017.

[18] 闫晓明. 基于特征匹配的协议识别关键技术研究[D]. 长沙:国防科学技术大学,2015.

[19] 陈雪娇,王攀,刘世栋. 网络应用流类别不平衡环境下的 SSL 加密应用流识别关键技术[J]. 电信科学,2015,31(12):91 - 97.

[20] 陈琳,孔华锋,沈开心. P2P 应用多层次识别方法研究[J]. 华中科技大学学报(自然科学版),2014,42(11):117 - 120.

[21] RAN D, AMIT D, OFIR P, et al. I know what you saw last minute—encrypted HTTP adaptive video streaming title classifification [C]//IEEE Transactionson Information Forensicsand Security,2017(12):3039 - 3049.

(责任编辑 王 欢)