专题：内生安全

基于机器学习和深度学习的网络流量分类研究

顾玥[1]，李丹[1,2]，高凯辉[2]

（1. 清华大学，北京 100084；2. 清华大学深圳国际研究生院，广东 深圳 518055）

摘　要：随着互联网技术的不断发展以及网络规模的不断扩大，应用的类别纷繁复杂，新型应用层出不穷。为了保障用户服务质量（QoS）并确保网络安全，准确快速的流量分类是运营商及网络管理者亟须解决的问题。首先给出网络流量分类的问题定义和性能指标；然后分别介绍基于机器学习和基于深度学习的流量分类方法，分析了这些方法的优缺点，并对现存问题进行阐述；接着围绕流量分类线上部署时会遇到的 3 个问题：数据集问题、新应用识别问题、部署开销问题对相关工作进行阐述与分析，并进一步探讨目前网络流量分类研究面临的挑战；最后对网络流量分类下一步的研究方向进行展望。

关键词：QoS；网络安全；流量分类；数据采集；新应用识别

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2021052

Research on network traffic classification based on machine learning and deep learning

GU Yue[1], LI Dan[1,2], GAO Kaihui[2]

1. Tsinghua University, Beijing 100084, China
2. Tsinghua Shenzhen International Graduate School, Shenzhen 518055, China

Abstract: With the continuous development of Internet technology and the continuous expansion of network scale, there are many different types of applications , and various new applications have endlessly emerged. In order to ensure the quality of service (QoS) and ensure network security, accurate and fast traffic classification is an urgent problem for both operators and network managers. Firstly, the problem definition and performance metrics of network traffic classification were given. Then, the traffic classification methods based on machine learning and deep learning were introduced respectively, the advantages and disadvantages of these methods were analyzed, and the existing problems were expounded. Next, the related work by focusing on the three problems encountered elaborated and analyzed in traffic classification when considering online deployment: dataset, zero-day application identification and the cost of online deployment, and further discusses the challenges faced by the current network traffic classification researches. Finally, the next research direction of network traffic classification was prospected.

Key words: QoS, network security, traffic classification, data collection, zero-day application identification

收稿日期：2021−02−01；**修回日期：**2021−03−01

基金项目：国家重点研发计划项目（No.2018YFB1800500）；广东省重点领域研发计划项目（No.2018B010113001）；国家自然科学基金项目（No.61772305, No.61672499）

Foundation Items: The National Key Research and Development Program of China(No.2018YFB1800500), Guangdong Provincial Key Research and Development Program (No.2018B010113001), The National Natural Science Foundation of China(No.61772305, No.61672499)

1 引言

随着互联网的不断发展，不同类型的应用程序不断涌现。应用程序会产生大量的网络流量，而不同类型的流量会呈现出不同的特征。流量分类的目标就是根据流量的区分性特征识别流量的类别[1]。网络流量分类对网络运营商是十分必要的：一方面，从用户服务质量（QoS）的角度来说，流量分类是保障 QoS 的第一步，是根据不同业务类型的要求为业务提供区分服务的前提[1]；另一方面，从安全的角度来说，流量分类是异常网络流量检测的第一步，可以更好地保护网络安全[2]。近几年，随着用户对隐私保护需求的不断增加，以及加密技术的不断发展，越来越多的流量被加密处理，这对网络流量分类提出了新的挑战。

传统的流量分类方法有两类：一类是基于端口号的识别方法，即根据端口号对应的协议号进行识别，但随着端口混淆技术的出现，这种方法渐渐失效[1]；另一类是基于 DPI 的识别方法，即基于预定义的各个类别的正则表达式，匹配数据包负载以确定类别。但这种方法随着流量加密也渐渐不可行[1]。

随着传统的流量分类方法的失效，研究者开始探索新的流量分类方法。近年来不断发展的机器学习技术受到了研究者的广泛关注。机器学习技术相较于传统分类方法更加自动化和智能化，可以根据流的统计特征分类，避免了流量加密带来的影响。鉴于这个优势，研究者提出基于机器学习算法做流量分类的方法，目前广泛使用的机器学习算法有决策树算法、随机森林算法、支持向量机算法等。这些分类方法都具有良好的分类准确性，并且得到了学术界和工业界的广泛认可。然而基于机器学习的流量分类方法需要专家经验提取和筛选流量的特征，这会消耗大量的人力资源。考虑到这一点，研究者又提出了基于深度学习的端到端的流量分类方法[3]。基于深度学习的方法可以直接基于原始的流量数据进行分类，不需要人为提取特征，一方面节省了人力，另一方面保证了分类准确性，成为学术界研究的热点[3]。

虽然目前有大量的流量分类研究工作，但大部分流量分类方法在线上部署时仍面临着很多问题。首先，由于运营商倾向于在骨干网边缘上进行流量分类，无论在高速的骨干网络中进行流量采集还是在线下做骨干网流量数据标注都非常困难。即使能够在网络边缘设备上采集到流量数据，也会因为无法控制采集的流量类型而出现样本不均衡问题，影响分类的准确性[4]。其次，如何将流量分类器部署到边缘网络设备中也是一个需要考虑的问题。在网络设备中，存储空间和 CPU 性能都非常有限[5]，这对分类器的部署来说是很大的挑战。最后，新应用程序的层出不穷使得分类器应该具有对新流量进行准确识别的能力[6]，而新流量呈现的新特性加大了流量分类的难度。

2 网络流量分类问题概述

2.1 问题定义

（1）流

网络流是网络数据包的集合。把具有相同五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、协议号）的数据包集合定义为一条流。流根据其方向性，可以分为单向流（源、目的不可互换）和双向流（源、目的可互换）两种。

（2）流量分类

流量分类的目标就是根据流量的区分性特征将流量的类别识别出来[1]。

（3）特征选择

流量的特征分为包级特征和流级特征两种。包级特征即包大小、包时间间隔、包的原始字节（又分为包头的原始字节和包负载的原始字节）等。流级特征即流的长度（即包的个数）、流的持续时间等。

以上是基本的流量特征选择，不同的研究工作会在此基础上进行特征选择。

（4）分类粒度

网络流量分类问题有 3 种不同的分类粒度：应用识别、大类识别、用户行为识别。不同的流量分类场景要求不同的分类粒度。如果运营商想要监测各应用程序流量占比情况，或想要识别恶意应用程序，那么分类粒度就是应用识别，即识别应用程序的名称，例如微信、QQ、爱奇艺等应用程序；如果运营商想要为不同类型应用程序提供区分服务，以满足不同的需求，那么分类粒度就是大类识别，即识别不同应用程序的类型，例如即时通信类应用、文件传输类应用、视频类应用；如果运营商想要掌握用户在使用应用程序时的用户行为，那么分类粒度就是用户行为识别，例如发送图片、语音、文字等用户行为。

2.2　性能指标

流量分类的分类指标有两个，一个是准确性，另一个是实时性。准确性是分类问题的重要指标，是评判分类效果的重要标准。准确性度量指标有 4 个：准确率（accuracy）、精度（precision）、召回率（recall）、F1 分数（F1-score）。计算过程如下。

- 真正（true positive，TP）：表示被分类模型正确预测的正样本数。
- 假负（false negative，FN）：表示被分类模型错误预测的正样本数。
- 假正（false positive，FP）：表示被分类模型错误预测的负样本数。
- 真负（true negative，TN）：表示被分类模型正确预测的负样本数。

$$\text{accuracy}=\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{1}$$

$$\text{precision}=\frac{\text{TP}}{\text{TP+FP}} \tag{2}$$

$$\text{recall}=\frac{\text{TP}}{\text{TP+FN}} \tag{3}$$

$$\text{F1-score}=\frac{2\ \text{precision}\cdot\text{recall}}{\text{precision+recall}} \tag{4}$$

此外，有些应用是时延敏感型应用，例如在线搜索、社交网络、在线零售等。这些应用的服务时间直接影响应用的用户体验甚至运营商的效益。时延敏感型应用的数据流大部分是短流，持续时间为几十到几百微秒。因此为了满足这些时延敏感型应用的性能需求，需要保证分类的实时性，即实现快速分类。实时性即对整个分类过程所花费的时间进行度量。整个流量分类的过程分为两步：特征获取和分类器分类。因此实时性指标度量公式定义如下：

流量分类时间开销 = 特征获取时间 + 分类器分类时间　　（5）

3　网络流量分类方法

3.1　基于机器学习的方法

基于机器学习的流量分类方法的分类过程包括两个阶段：特征提取和分类器分类。整个流程如图 1 所示。

特征提取/特征选择阶段通常是对数据流的包大小、包时间间隔等包级特征求取平均值、方差、中位数、分位数等统计特征，并进一步做特征分析，选取有效特征。由于这一阶段需要收集足够多的数据包，并且往往都伴随着一定时间的特征计算和特征选择，因此不利于分类的实时性。

图 1　基于机器学习的分类方法流程

目前有大量基于机器学习的流量分类方法被提出。Auld 等[7]提出了一种贝叶斯神经网络，该网络经过训练可以对包括 Kazaa、BitTorrent、GnuTella 等著名的 P2P 协议进行分类，并实现 99%的准确率。Moore 等[8]使用朴素贝叶斯分类器和核密度估计器，基于流的统计特征来分类，统计特征包括流内包大小、包时间间隔的平均值、方差、中位数、分位数等特征，最终分类准确率达到 96%。Draper 等[9]使用 *k*-NN 和 C4.5 决策树算法，基于包的到达时间间隔最大最小值等时间相关特征表征网络流量，最终分类召回率高达 92%。使用 C4.5 算法，在 VPN 数据集上也达到了大约 88%的召回率。Yamansavascilar 等[10]手动选择了参考文献[11]中描述的 111 个流特征，使用 *k*-NN 算法，在对 14 类应用进行分类的过程中获得了 94%的准确率。然而在使用 *k*-NN 分类器用于预测时，算法的执行时间是需要考虑的问题。2016 年 Taylor 等[12]则提出基于突发数据流进行分类，考虑数据流传输的两个方向（源、目的地址互换），分别统计流的包大小序列，对于每个序列分别计算平均值、最小值、最大值、分位数等 18 个统计特征，最后使用支持向量回归算法和随机森林算法取得了 99%的分类准确率。2019 年 Shen 等[13]提出了一种去中心化应用识别方法，提出在双向数据流的统计特征的基础上使用核函数进行特征融合，再进一步进行特征筛选，最后实现 92%的分类准确率。

基于机器学习的流量分类方法的主要缺点是需要专家经验提取和筛选特征，因此这些方法既耗时又昂贵，而且容易出现人为错误。于是，研究者渐渐把目光放到可以自主学习特征的深度学习上来。

3.2 基于深度学习的方法

基于深度学习的方法避免了根据专家经验选择特征的过程，可以通过训练自主学习特征。这一特点使得深度学习成为一种非常理想的流量分类方法。而且深度学习模型是端到端的模型，可以直接学习到原始输入和对应输出之间的非线性关系，不需要将问题分解为特征获取和分类器分类两个问题。基于深度学习的分类过程如图 2 所示。

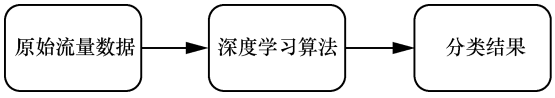

图 2 基于深度学习的分类过程

基于深度学习的流量分类方法分为两类：基于数据包的原始字节特征和基于流内数据包序列特征。基于数据包的原始字节特征的方法指分类器的输入是数据包原始字节内容，基于流内数据包序列特征的方法指分类器的输入是流内数据包包大小、包时间间隔序列等特征。

Lotfollahi 等[1]提出的 DeepPacket 是基于数据包原始字节特征的深度学习方法的代表，它提出以每个数据包作为输入样本，不需要专家经验提取特征，只需要把数据包的原始字节作为特征，分类模型为一维卷积神经网络（1DCNN）和稀疏自动编码机（SAE），最终取得 98%的分类准确率。Wang 等[3]提出使用每条数据流（单向流/双向流）的前 784 字节作为模型输入，并分别基于一维卷积神经网络（1DCNN）和二维卷积神经网络（2DCNN）两个模型做实验，实验结果表明：1DCNN 的效果更好，可以达到 90%以上的准确率。Li 等[14]将循环神经网络（RNN）引入网络流量分类中，设计了一种新的神经网络——字节段神经网络（BSNN）。BSNN 直接将数据包作为模型输入，实验结果表明，在对 5 个协议分类的过程中，BSNN 的 F1-score 平均值约为 95.82%。Xie 等[15]提出了一种基于自注意力机制的流分类方法 SAM，把每个数据包的包头原始字节作为模型输入，这种方法在协议识别和应用识别上分别取得了 98.62%和 98.93%的 F1-score 平均值。

Liu 等[16]提出的 FS-Net 是基于流内数据包序列特征的深度学习方法的代表，时序特征采用的是流内数据包大小序列，并基于此提出一种基于自动编码机（auto-encoder）的重构机制，这种重构机制使得模型能够学习到最有利于分类且最能代表这条数据流的特征，最终的分类准确率高达 99%。Lopez-Martin 等[17]提出基于数据流前 20 个数据包的端口号、包负载长度、包间隔时间、窗口大小等属性构成 20×6 的矩阵，并输入给卷积神经网络（CNN）和长短期记忆循环神经网络（LSTM）的组合模型，最终准确率可以达到 96%以上。Shapira 等[18]提出根据单向数据流的包大小、包到达时间将数据流转换成图片，然后通过 CNN 模型做分类，最终分类准确率可以达到 99.7%。

无论是基于数据包原始字节特征的深度学习方法还是基于流内数据包序列特征的深度学习方法都有各自的优缺点。基于数据包原始字节特征的深度学习方法的优点是可以直接根据数据包的字节内容做推理，做到实时分类，但分类结果依赖于数据包负载的内容。当流量加密时，数据包负载部分不再可用；而数据包的 IP 地址和端口字段也会对分类效果造成极大的影响，带来过拟合问题。基于流内数据包序列特征的深度学习方法的优点是不依赖于数据包原始内容，对于加密流量更灵活，但需要等待一段时间的数据包以构成时序序列，因此分类实时性差。

通过对基于机器学习和基于深度学习的流量分类方法的阐述与分析，本文从是否需要人为特征提取、是否适用于加密流量、是否能够满足实时性和准确性 4 个角度总结了这两类方法的优缺点，见表 1。

基于机器学习的流量分类方法由于需要专家经验提取和筛选特征，因此既耗时又昂贵，而且容易出现人为错误。而基于深度学习的方法可以通过训练自主学习到原始输入和对应输出之间的非线性关系，不需要将问题分解为特征获取和分类器分类两个问题，因此避免了依据专家经验选择特征的过程。然而无论是基于机器学习的方法还是基于流内数据包序列特征的深度学习方法，由于都需要收集一段时间的数据包以计算统计特征或者获取数据包时序序列，因此都无法做到实时分类。基于数据包原始字节特征的深度学习方法则可以对一个数据包进行分类，满足实时性的要求，但由于依赖包的字节内容，因此容易导致过拟合，影响分类效果。

从表 1 可以看出，当考虑实时性、准确性两个指标时，无论是基于机器学习还是基于深度学习的流量分类方法都不是完美的，还有一定的改进空间。与此同时，运营商为了更好地提供服务，需要将整个分类系统落地，这就会给分类系统带来更多的问题和挑战。

4　网络流量分类的线上部署及挑战

从运营商的角度来看，为了保障用户的服务质量，更好地做流的优先级调度，运营商会选择在骨干网的边缘设备上部署流量分类模型，运营

表 1　基于机器学习与基于深度学习的流量分类方法优缺点

	是否需要人为特征提取	是否适用于加密流量	是否能够满足实时性	准确性
基于机器学习方法	是	是	否	较高
基于数据包原始字节特征的深度学习方法	否	若仅基于包负载字节内容分类则不适用；若仅基于包头字节内容则适用	是	较高
基于流内数据包序列特征的深度学习方法	否	是	否	极高

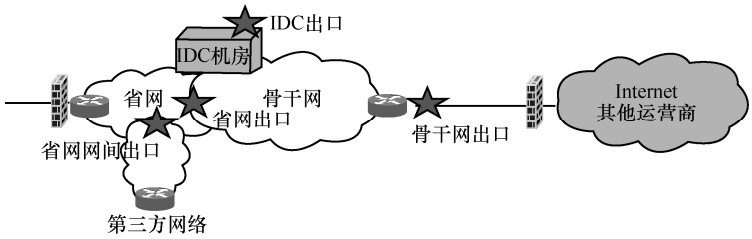

图 3　运营商流量分类模型部署点（五角星位置）

商流量分类模型部署点如图 3 所示。

从图 3 可以看出，运营商选择将分类模型部署在网络边缘设备（交换机、路由器等）。这样的部署方式会带来 3 个问题：首先，由于模型的线下训练需要大量的流量数据，因此需要在骨干网采集流量。一方面，骨干网的流量速率>40 Gbit/s[19]，在这样的高速网络环境下对数据采集的要求极高，准确的线下数据标注也是难题；另一方面，对骨干网流量进行采集时，由于无法限制各类别流量的比例，因此会导致数据集样本不均衡问题，影响分类的准确率。其次，在网络设备上部署分类模型需要考虑 3 个开销：内存开销、时间开销和计算开销。一方面，设备的存储空间有限，如果想达到快速分类的目的，模型和数据的存储开销需要小于 CPU 上缓存的存储空间，也就是小于几兆字节[20]；另一方面，由于在骨干网中数据流的速度非常快，并且需要应对大量的并发流，因此对特征获取速度和分类速度提出了更高的要求；而且，由于网络设备的计算资源有限，因此也要求尽量减少特征处理和模型推理时导致的 CPU 资源开销。最后，在线上分类时，分类器会对各种各样类型的流量分类，然而随着互联网技术的发展，越来越多的新应用不断涌现，这就要求线上分类时能够及时识别出新应用的流量。由于新应用的流量呈现出新的特性，因此给新应用识别带来了难度。

虽然目前无论是基于机器学习方法还是基于深度学习方法已经有大量的流量分类研究工作，但把现有的工作直接进行线上部署是不可行的：根据表 1 可知，基于机器学习的流量分类方法和基于流内数据包序列特征的深度学习方法都面临分类实时性的问题，而且无论是哪种方法在训练时都是固定类别数进行训练的，所以都无法应对新应用流量的识别问题。因此，有研究者提出在机器学习方法和深度学习方法的基础上针对这 3 个问题做出一些改进。

4.1　数据集

由于在骨干网络中数据集采集是不可控的，无法控制采集的流量类别，因此会带来数据集样本分布不均衡的问题。目前针对流量数据集样本不均衡问题有很多研究工作。除了传统的欠采样、过采样方法，有研究者提出使用生成对抗网络（GAN）解决样本不均衡问题。Ly 等[21]提出使用 ACGAN 为少样本生成合成数据以达到数据均衡的效果，并基于这种方法使得流量分类的准确性得到很大的改善。Zheng 等[4]提出一种名为 RBRN 的框架，这个框架基于 Glow 模型[22]构建一个名为“hallucinator”的流量生成器应对样本不均衡问题，并基于元学习（meta-learning）方法进行小样本学习。这两个工作的对比结果见表 2。

表 2　ACGAN 与 RBRN 对比

对比项	准确率	精度	召回率	F1 分数
ACGAN	0.926 3	0.951 6	0.916 7	0.933 8
RBRN	0.956 3	0.956 9	0.959 0	0.957 9

然而，事实上数据样本不均衡只是数据集问题的一小部分，数据集最难也最关键的问题是如何在高速骨干网络下进行数据采集和做线下数据

标注。目前的骨干网流量标注方法仍然是基于深度包检测（deep packet inspection，DPI）的方法，这种方法随着加密流量的逐渐增多而逐渐失效，因此目前并没有任何工作能够解决骨干网络数据采集难和标注难的问题。

4.2　部署开销

目前流量分类的研究工作关注点有两个：如何获取有效的流量特征和如何提高分类的准确率。然而对于线上部署来说，一方面由于需要面对网络中的高速并发流，另一方面由于网络设备的存储资源和 CPU 资源非常有限，因此流量分类的研究工作也应该考虑存储开销、计算开销和时间开销。为了减少特征的计算开销，实现更快速的流量分类，Garcia 等[23]提出一种离散优化算法 KSD，通过基于统计特征数据分布构建直方图的方式将特征离散化，这种方式大大减少了计算资源，并实现了更快速的分类。在此之后，Garcia 等[24]又进一步基于 KSD 算法提出了一种基于离散优化算法的分类器 DISCO。除了特征离散化这种方式以外，Garcia 等[25]也曾提出用低计算开销特征（例如：给定包大小范围的数据包比例）代替高阶统计特征（例如：数据包大小的分位数），这种方式不但没有影响分类准确率，反而提高了分类速度，减小了计算资源的开销。

虽然这几个工作于提高分类速度以及减少计算资源开销起到了一定的作用，但是这几个工作并不适合线上部署。由于 KSD 算法和使用低开销替换特征的方式都需要大量的预处理时间，这不利于在网络设备上的实时推理。

4.3　新应用识别

目前已经有研究工作关注到新应用识别这个问题。RTC[6]是一种结合监督学习和半监督学习方法的解决方案，RTC 动态训练一个新应用类别判别器，随着人为标注动态调整判别器。Zhang 等[26]提出的方法和 RTC 方案相似，都是根据线上分类结果动态训练一个新应用类别判别器，区别在于此方法是基于深度学习的分类方法。无论是 Zhang 等[6]提出的方法还是 RTC 方案，都需要做两次推理才能得到分类结果，这会严重影响分类的实时性。而且这两种方法都要求已知训练集数据的应用类别。Ede 等[27]提出的 FLOWPRINT 则不要求任何的类别先验知识，也无须训练过程。通过半监督学习的方式基于数据流的目的 IP 地址聚类获得应用程序的“指纹”，从而达到区分各个应用程序的目的，同时能够很准确地识别出新应用的流量。但 FLOWPRINT 需要获取足够多的数据流（5 min 内的数据流）以得到应用程序指纹，因此也不利于分类的实时性。

通过对线上部署时面临的 3 个问题的相关工作的阐述与分析，虽然目前很多工作试图在解决这些问题，但解决办法仍然不完善，这就给未来的流量分类工作带来了挑战：如何在高速网络下实现快速数据采集？如何在线下实现准确数据标注？如何减小分类模型的部署开销？如何快速地识别出新应用流量？这就是未来的研究工作在线上部署时亟须商榷和解决的问题。

5　结束语

网络流量分类一直是网络管理和网络安全的重要任务，准确并快速地流量分类对保障用户服务质量和用户安全是十分重要的。本文对网络流量分类的研究工作进行了梳理和总结。由于传统的基于端口号和基于 DPI 的流量分类方法随着端口混淆技术的使用和加密流量的出现逐渐失效，越来越多的研究工作选择采取机器学习和深度学习的方法解决流量分类问题。基于机器学习的流量分类方法虽然适用于加密流量，但其需要专家经验，且实时性差；基于深度学习的流量分类方法分为两类：基于数据包原始字节特征的深度学习方法和基于流内数据包序列特征的深度学习方法，这两类方法在实时性和准确性上也有着各自的优缺点。虽然目前流量分类已经有大量的研究

工作，但是当在高速网络中线上部署时还是会遇到数据集采集难、部署开销大以及新应用识别实时性差的问题。由于目前还没有任何一种方案能真正满足线上部署的要求，因此如何实现合理有效的线上部署仍然是一个待解决的问题。

参考文献：

[1] LOTFOLLAHI M, SIAVOSHANI M J, ZADE R S H, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.

[2] WANG W, ZHU M, ZENG X W, et al. Malware traffic classification using convolutional neural network for representation learning[C]//Proceedings of 2017 International Conference on Information Networking (ICOIN). Piscataway: IEEE Press, 2017: 712-717.

[3] WANG W, ZHU M, WANG J L, et al. End-to-end encrypted traffic classification with one-dimensional convolution neural networks[C]//Proceedings of 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). Piscataway: IEEE Press, 2017: 43-48.

[4] ZHENG W, GOU C, YAN L, et al. Learning to classify: aflow-based relation network for encrypted traffic classification[C]//Proceedings of the Web Conference 2020. [S.l.:s.n.], 2020: 13-22.

[5] WANG S H, SUN C, MENG Z L, et al. Martini: bridging the gap between network measurement and control using switching ASICs[C]//Proceedings of 2020 IEEE 28th International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2020: 1-12.

[6] ZHANG J, CHEN X, XIANG Y, et al. Robust network traffic classification[J]. IEEE/ACM Transactions on Networking, 2015, 23(4): 1257-1270.

[7] AULD T, MOORE A W, GULL S F. Bayesian neural networks for internet traffic classification[J]. IEEE Transactions on Neural Networks, 2007, 18(1): 223-239.

[8] MOORE A W, ZUEV D. Internet traffic classification using bayesian analysis techniques[C]//Proceedings of the 2005 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems. Piscataway: IEEE Press, 2005: 50-60.

[9] DRAPER-GIL G, LASHKARI A H, MAMUN M S I, et al. Characterization of encrypted and vpn traffic using time-related features[C]//Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP). Piscataway: IEEE Press, 2016: 407-414.

[10] YAMANSAVASCILAR B, GUVENSAN M A, YAVUZ A G, et al. Application identification via network traffic classification[C]//Proceedings of 2017 International Conference on Computing, Networking and Communications (ICNC). Piscataway: IEEE Press, 2017: 843-848.

[11] MOORE A, ZUEV D, CROGAN M. Discriminators for use in flow-based classification[R]. 2013.

[12] TAYLOR V F, SPOLAOR R, CONTI M, et al. Appscanner: automatic fingerprinting of smartphone apps from encrypted network traffic[C]//Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2016: 439-454.

[13] SHEN M, ZHANG J, ZHU L, et al. Encrypted traffic classification of decentralized applications on ethereum using feature fusion[C]//Proceedings of 2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS). Piscataway: IEEE Press, 2019: 1-10.

[14] LI R, XIAO X, NI S, et al. Byte segment neural network for network traffic classification[C]//Proceedings of 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS). Piscataway: IEEE Press, 2018: 1-10.

[15] XIE G R, LI Q, JIANG Y, et al.SAM: self-attention based deep learning method for online traffic classification[C]//Proceedings of the Workshop on Network Meets AI & ML. Piscataway: IEEE Press, 2020: 14-20.

[16] LIU C, HE L T, XION G, et al. Fs-net: a flow sequence network for encrypted traffic classification[C]//Proceedings of IEEE INFOCOM 2019-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2019: 1171-1179.

[17] LOPEZ-MARTIN M, CARRO B, SANCHEZ-ESGUEVILLAS A, et al. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things[J]. IEEE Access, 2017(5): 18042-18050.

[18] SHAPIRA T, SHAVITT Y. Flowpic: encrypted internet traffic classification is as easy as image recognition[C]//Proceedings of IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2019: 680-687.

[19] LIU Z X, BEN-BASAT R, EINZIGER G, et al. Nitrosketch: robust and general sketch-based monitoring in software switches[C]//Proceedings of the ACM Special Interest Group on Data Communication. Piscataway: IEEE Press, 2019: 334-350.

[20] RASHELBACH A, ROTTENSTREICH O, SILBERSTEIN M. A computational approach to packet classification[C]//Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication. [S.l.:s.n.], 2020: 542-556.

[21] VU L, BUIC T, NGUYEN QUANG U. A deep learning based method for handling imbalanced problem in network traffic

classification[C]//Proceedings of the Eighth International Symposium on Information and Communication Technology. Piscataway: IEEE Press, 2017: 333-339.
[22] KINGMA D P, DHARIWAL P. Glow: generative flow with invertible 1×1 convolutions[J]. rXiv:1807.03039, 2018.
[23] GARCIA J, KORHONEN T. Efficient distribution-derived features for high-speed encrypted flow classification[C]//Proceedings of the 2018 Workshop on Network Meets AI & ML. [S.l.:s.n.], 2018: 21-27.
[24] GARCIA J, KORHONEN T. On runtime and classification performance of the discretize-optimize (DISCO) classification approach[J]. ACM SIGMETRICS Performance Evaluation Review, 2018, 46(3): 167-170.
[25] GARCIA J, KORHONEN T, ANDERSSON R, et al. Towards video flow classification at a million encrypted flows per second[C]//Proceedings of 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). Piscataway: IEEE Press, 2018: 358-365.
[26] ZHANG J L, LI F H, YE F, et al. Autonomous unknown-application filtering and labeling for DL-based traffic classifier update[C]//Proceedings of IEEE INFOCOM 2020-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 397-405.
[27] EDE T V, BORTOLAMEOTTI R, CONTINELLA A, et al. Flowprint: semi-supervised mobile-app fingerprinting on encrypted network traffic[C]//Proceedings of Network and Distributed System Security Symposium. [S.l.:s.n.], 2020.

[作者简介]

顾玥（1997– ），女，清华大学博士生，主要研究方向为智能网络。

李丹（1981– ），男，清华大学计算机系教授、博士生导师，主要研究方向为数据中心网络、网络智能和可信任互联网。

高凯辉（1996– ），男，清华大学深圳国际研究生院博士生，主要研究方向为性能可预测的数据中心网络和网络智能。