基于机器学习的加密流量分类研究综述

付钰[1]，刘涛涛[1]，王坤[1,2]，俞艺涵[3]
（1.海军工程大学信息安全系，湖北 武汉 430033；2.信阳职业技术学院数学与信息工程学院，河南 信阳 464000；
3.海军工程大学作战运筹与规划系，湖北 武汉 430033）

摘　要：加密流量分类是网络管理和安全防护的重要组成部分，不过当前网络流量环境复杂多变，致使传统的分类方法已基本失效。而机器学习，尤其是深度学习，凭借强大的特征提取能力已广泛应用于加密流量分类领域。为此，对机器学习驱动的加密流量分类最新成果进行系统性综述，首先将加密流量分类工作划分为数据采集与处理、特征提取与选择及流量分类与性能评估3个部分，分别对应加密流量分类中的数据获取、显著特征构建及模型的应用与验证；接着将这3个部分内容细分为流量采集、数据集构建、数据预处理、特征提取、特征选择、分类模型及性能评估7个阶段；然后分别对这7个阶段进行全面的归纳、总结与分析；最后详细分析当前工作所面临的挑战并展望加密流量分类未来的研究方向。

关键词：流量分析；加密流量分类；机器学习；深度学习
中图分类号：TP393
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025006

Survey of research on encrypted traffic classification based on machine learning

FU Yu[1], LIU Taotao[1], WANG Kun[1,2], YU Yihan[3]
1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China
2. School of Mathematics and Information Engineering, Xinyang Vocational and Technical College, Xinyang 464000, China
3. Department of Operational Operations and Planning, Naval University of Engineering, Wuhan 430033, China

Abstract: Encrypted traffic classification was an important component of network management and security protection. However, the complexity and variability of the current network traffic environment rendered traditional classification methods largely ineffective. Machine learning, particularly deep learning, with its strong feature extraction capabilities, has been widely used in the field of encrypted traffic classification. To this end, a systematic review of the latest advancements in machine learning-driven encrypted traffic classification was provided. Firstly, the encrypted traffic classification work was roughly divided into three parts: data collection and processing, feature extraction and selection, and traffic classification and performance evaluation, which correspond to data acquisition, significant feature construction, and model application and validation in encrypted traffic classification. The content was further subdivided into seven stages: traffic collection, dataset construction, data preprocessing, feature extraction, feature selection, classification models, and performance evaluation. A comprehensive summary, synthesis, and analysis of these seven stages were then conducted. Finally, the challenges faced by current research were analyzed in detail, and the future research directions for encrypted traffic classification were prospected.

Keywords: traffic analysis, encrypted traffic classification, machine learning, deep learning

收稿日期：2024–09–29；修回日期：2024–12–13
通信作者：刘涛涛，liutaotaoh@163.com
基金项目：国家自然科学基金资助项目（No.62102422）；河南省科技攻关基金资助项目（No.242102211070）
Foundation Items：The National Natural Science Foundation of China (No.62102422), Henan Province Key Science and Technology Research Projects of China (No.242102211070)

0 引言

计算机技术的持续发展以及海量设备不断接入互联网，催生出大量以云上（OTT, over-the-top）应用为主体的网络应用服务。其中，网络流量作为不同用户在不同应用中进行网络交互的重要数据传输媒介，可在隐私保护的前提下被合法、透明地访问，故互联网服务提供商（ISP, Internet service providers）为提升网络服务质量（QoS, quality of service）以及用户体验效果（QoE, quality of experience），通常需要对网络流量进行分析。因此，流量分析已成为网络管理和安全防护的重要组成部分[1-2]。流量分析的主要任务是对所捕捉的网络流量数据包进行处理，从而实现流量的检测、分类与识别。其中检测以二分类结果为目的，分类和识别以多分类结果为目的，因此流量分析可看作一个分类问题。此外，准确的流量分类不仅从流量监测的角度提升了QoS和QoE，也在网络动态规划、入侵检测等领域中发挥关键作用，已成为网络安全研究中的热点问题[3-5]。

近年来，随着企业和用户对互联网隐私问题的日益关注以及用户对个人数据隐私保护的迫切需求[6-7]，加密技术的应用越来越广泛，网络流量呈加密化趋势，完全加密的时代已悄然来临。Google透明度报告显示，截至2022年9月，加密流量占比已达到95%[8]。Firefox的研究进一步指出，使用HTTPS协议进行加载的网页已从2015年的32%上升至2023年的83%，并且使用SSL/TLS安全协议的美国用户比例已从2017年的55%上升到2023年的93%[9]。在该前提下，加密流量分类方法通过利用有效的流量特征对加密流量进行分类可实现网络应用的精准分析。

然而，不断增长的加密流量在给企业和用户带来便利的同时，也给网络安全带来了不小的挑战。复杂多变动态的网络环境使得传统的网络流量分类方法难以进行准确的细粒度分析。过去传统的加密流量分类方法主要依靠端口和深度包检测（DPI, deep packet inspection），许多商业产品[10-11]和开源软件[12-13]都是基于这2种方法，例如17-filter网站以及Snort网站[14]。基于端口的方法是利用端口与协议之间的对应关系进行分类，但随着未注册、随机端口的激增而变得无效。基于DPI的方法通过分析数据包识别特定的协议和应用数据，不过网络流量经加密后其有效载荷信息不再可用，故该方法也不再可靠。同时由于恶意流量为隐藏自身行为会选择流量加密的方式来逃避检测，网络安全的主要威胁在不断变化[15]，因此，亟须探索新的技术方法对加密流量进行分类。

当前，学术界逐渐将机器学习（ML, machine learning）和深度学习（DL, deep learning）引入加密流量分类领域，以应对流量加密化带来的挑战。ML方法主要依赖于分类器提取流量特征，无须利用数据包的有效载荷信息便可实现分类识别，同时其所使用的特征信息具有较好的鲁棒性。相比之下，DL方法则引发了一场关于自主特征学习的研究热潮，通过神经网络自动提取流量特征，取得较好的效果，并省去了人工特征提取的步骤。目前现有的大多数加密流量分析综述文章基本都是从传统ML和DL两方面进行阐述分析，表1将本文与现有相关综述进行了总结分析，具体情况如下所示。

Velan等[16]研究了不同加密协议的传统机器学习方法。首先详细介绍了不同互联网加密协议的原理和用途，然后概述了一些关于传统机器学习的加密流量分析方法以识别不同的加密应用协议，最后

表1 本文与现有相关综述的对比

文献	问题领域	描述
文献[16]	分类	总结加密流量分析方法，主要集中于传统机器学习方法
文献[17]	分析	从网络资产识别、网络特征、隐私泄露检测和异常检测4类目标介绍用于加密流量分析的机器学习方法
文献[18]	分类	按照监督学习、半监督学习和无监督学习对加密流量分类技术进行研究
文献[19]	分类	总结了用于加密流量分类的深度学习方法
文献[20]	识别	总结了用于加密流量识别的深度学习方法
文献[21]	检测	回顾了基于深度学习的加密数据入侵检测方法
本文	分类	总结了机器学习驱动的加密流量分类工作，涵盖了数据采集与处理、特征提取与选择、模型分类与评估3个部分

进行对比分析。

Shen 等[17]全面回顾了机器学习在加密流量分析领域中的研究方法并提炼出具体的步骤流程，然后根据不同的分析目标，按照网络资产识别、网络特征化、隐私泄露检测和异常检测 4 个部分进行详实而全面的阐述，最后对该领域的未来研究方向和存在的重大挑战进行讨论并给出具体的应对措施。

于治平等[18]从监督学习、半监督学习以及无监督学习 3 个方面对分类技术进行总结，并简要描述了私有协议应用广泛以及特征高维性所带来的挑战。

在深度学习方面，Rezaei 等[19]概述了一个通用框架，并且将其分类目标分为以下几种：协议、应用程序、流量类型、网站、用户行为、操作系统及浏览器，最后详细介绍了零日攻击、更强的加密协议、中间流分类等开放问题下的研究思路。

郭宇斌等[20]使用深度学习进行加密流量分类识别，从数据集、模型构造等方面对以往部分研究工作进行回顾，此外，该文还对现存问题进行阐述，例如新型加密协议的普及使得部分基于明文的方法失效以及加密流量数据集类不平衡分布等。

Hendaoui 等[21]从隐私保护的角度对基于深度学习的加密数据入侵检测系统进行了系统性的综述，旨在指导研究人员如何选择合适的工具在加密数据上建立具有隐私保护的入侵检测系统。该文研究了多种深度学习方案并对深度学习的数据集、模型及加密工具进行了全面的评估。同时明确了加密数据入侵检测系统进行隐私保护应采取的步骤。

当前加密流量分类领域的研究综述覆盖面较广，清晰地表明了当前可采用的技术手段，不过鲜有从特征的角度对现有加密流量分类方法进行归纳总结。作为加密流量分类中至关重要的部分，特征一直是工业界和学术界研究的重点，决定了分类器的好坏。在面对各种分类器及分类任务时所选择的特征也不相同，一个合适的加密流量特征可以大幅度提升分类性能，还能加密流量建模阶段的困难。因此，本文基于加密流量分类各流程之间的层层递进关系，聚焦于加密流量特征流动的分类过程，将加密流量分类工作划分为蕴含特征的加密流量数据采集与处理、蕴含特征的加密流量特征提取与选择及蕴含特征的加密流量分类过程与性能评估。然后根据任务的不同将上述 3 个部分内容细分为 7 个阶段：流量采集、数据集构建、数据预处理、特征提取、特征选择、分类模型以及性能评估，具体如图 1 所示。

纵观当前国内外关于加密流量分类技术的研究，大体上也符合图 1 所示的工作流程。对于加密流量分类而言，首先通过流量采集工具从网络中的各个节点（例如路由器、网关等）捕获流量并将其构造成数据集；然后对加密流量数据进行预处理，且经过特征提取及特征选择阶段，可将高维流量数据映射成低维特征参数；最后，选取合适的分类模型进行训练，并且通过多个评价指标来评估模型性能。本文将以这 7 个阶段为主旨对机器学习驱动的加密流量分类最新成果进行系统性归纳总结。

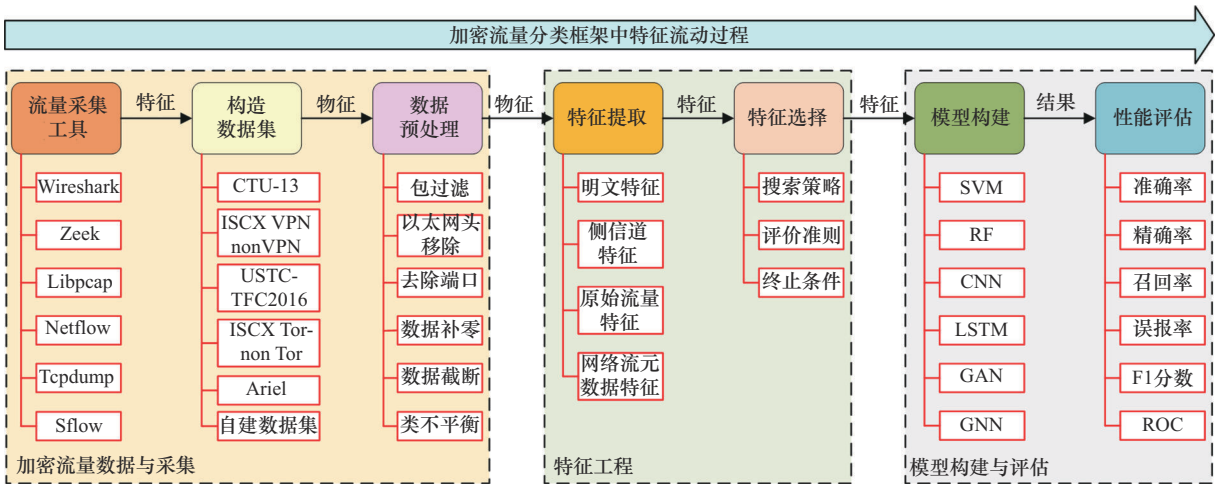

图 1　加密流量分类流程

1 加密流量数据采集与处理

1.1 加密协议介绍

为保障通信安全，加密协议在通信过程中得到广泛应用，从而生成加密流量。因此在介绍加密流量数据采集与处理之前，本文先对当前所使用的加密协议进行总结[17]，具体如表2所示。

1) SSL/TLS[22]。SSL为安全套接层协议，通过为通信双方提供加密通道以确保数据传输安全，通常位于面向连接的网络层协议和应用层协议之间。TLS为安全传输层协议，通过在SSL3.0的基础上设计而来，更安全可靠。其独立于应用层协议，可直接在TCP上提出传输层安全，当前主要使用TLS-1.2协议，不过在某些领域已开始使用TLS-1.3协议，常用于电子邮件、在线交易等多种互联网应用。

2) HTTPS[23]。HTTPS为超文本传输安全协议，由HTTPS协议和SSL/TLS协议结合而成，主要应用于金融等机构网站或敏感数据传输。

3) QUIC[24]。QUIC为快速UDP互联网连接服务协议，是一种特殊的应用层协议，既能保证可靠性又能降低网络时延，已广泛应用于Google旗下各种服务，同时也用于对实时性要求高的应用或服务。

4) SSH[25]。SSH为安全外壳协议，其通过在客户端和服务器之间建立安全通道以实现通信双方之间的安全连接，主要在应用层中使用，广泛用于远程登录、文件传输等场景。

5) IPSec[26]。IPSec为互联网安全协议，可用来提高IP网络的安全性，主要在网络层通信中使用，常用于构建企业网络或云服务。

1.2 加密流量采集

数据是科学研究的基础，流量采集通常被认为是加密流量分类的起点。目前，研究人员利用流量采集工具在网络中各个节点或特殊网络结构[27-28]中捕获流量，因此，本节将介绍典型的流量采集工具。

1) Wireshark[29]。常见的网络数据包分析工具，可在线截取各种网络封包，也可分析已有的报文数据，具有多种过滤规则和较好的直观性，允许用户提出各种特定要求。

2) Zeek[30]。开源的被动网络流量分析软件，适合检测所有链路上的流量与恶意行为。其优势在于可生成大量日志文件，不仅有链接的全面记录，还包括应用程序层记录，但缺少部分内置功能。

3) Libpcap[31]。基于C/C++的网络数据包捕获函数库，可提供采集网络统计信息、安全监测等功能。同时由于Libpcap的开放性和对多种网络协议的支持，使得很多流量采集工具都基于此函数库设计实现[17]。

4) Tcpdump[32]。基于Libpcap库的Linux和Unix网络抓包工具，通过正则表达式过滤数据包。功能与Wireshark类似，不过需要通过命令行操作。

5) Netflow[33]。Cisco开发的广泛扩展的协议，用于记录和分析流量，而不只是用来监控，但不适用于非IP流量的数据链路层分析。

6) Sflow[34]。流量采样技术，旨在兼容各种不同的设备，适合用于网络异常监控及定位，可快速提供实时数据，减轻设备负载。

总体而言，现有的流量采集工具大多基于Libpcap进行设计，同时在选择采集工具时应结合具体的应用场景和需求，考虑其性能和扩展性。

1.3 数据集描述

合适的数据集是提升加密流量分类性能的重要因素，经采集工具捕获的流量通常被制作成公开数据集或自建数据集。研究人员在选择数据集时应注意以下要求：首先是可用性和隐私性，保护用户数据的隐私是前提，因此必须保证数据的可用性和隐私性；其次是真实性和多样性，为了更好地评估模

表2 加密协议对比

协议	优点	缺点
SSL/TLS	安全性高，在传输过程中可确保数据完整	计算资源消耗较大，协议较复杂
HTTPS	兼容性好，可确保服务器的身份是可信的	速度较慢，需要进行加密和解密操作
QUIC	时延低，可快速重传和恢复数据包	性能损耗较大，普及程度不高
SSH	可跨平台应用，灵活性较强	速度较慢，所需的计算资源较高
IPSec	无须修改客户端或服务器上的任何应用程序	配置和管理复杂，灵活性较差

型，数据必须贴近现实生活场景并包含多种类型；最后应保证有足够的数据支撑模型进行有效学习。本节将对常见的加密数据集进行介绍。

1) USTC-TFC2016[35]由中国科学技术大学创建，包含了10类恶意样本和10类良性样本，具体使用情况可参考文献[36-38]。

2) ISCX VPN-nonVPN[39]由加拿大达尔豪斯（Dalhousie）大学网络安全实验室通过VPN收集而成，常用于访问被阻塞的网站或服务[40]，包括7类良性样本及7类协议封装样本，不过通常只使用6类，使用情况可参考文献[41-42]。

3) ISCX Tor-nonTor[43]与ISCX VPN-nonVPN数据集类似，只不过其是在洋葱路由Tor上收集流量，包括8类常规流量及8类Tor流量，使用情况可参考文献[44-45]。

4) CTU-13[46]是捷克技术大学在13个不同场景中捕获特定软件的恶意流量所创建的数据集，包括多种类型的恶意流量，具体可参考文献[47-48]。

5) Ariel(BOA2016)[49]是Dubin等使用Selenium网络爬虫收集实验室浏览器流量构造的数据集，包含浏览器流量及非浏览器流量，使用情况可参考文献[50-51]。

6) UNSW-NB15[52]由澳大利亚网络安全中心所创建，包括10个流量类别，使用情况可参考文献[53-54]。

7) NSL-KDD[55]由加拿大网络安全研究所发布，该数据集包含4个文件，具体使用情况可参考文献[53, 56]。

8) CICIDS2017[57]也是由加拿大网络安全研究所创建而成的，是当前最大、最新的入侵检测数据集之一，使用情况可参考文献[54, 58]。

9) 自建数据集是论文作者为实现某些特定的目的（如保证数据的多样性和真实性）构造而成，使用情况可参考文献[59-60]。

本文对当前的加密流量数据集进行了详细对比和总结，具体结果如表3所示。总体来看，现有数据集种类较多，涵盖了不同类型的流量，且大部分数据集专注于恶意流量或特殊流量的分类。不过这些数据集中存在较多冗余数据，同时近年来缺乏针对新型加密流量类型的数据集，导致在适应复杂多变的网络环境方面受到一定限制。

1.4　数据预处理

研究人员构造的数据集通常无法直接用于特征

表3　　加密流量数据集对比

数据集	流量类型	主要内容
USTC-TFC2016[35]	Benign	BitTorrent、Facetime、FTP、Gmail、MySQL、Outlook、Skype、SMB、Weibo、World Of Warcraft
	Malware	Cridex、Geodo、Htbot、Miuref、Neris、Nsis-ay、Shifu、Tinba、Virut、Zeus
ISCX VPN-nonVPN[39]	VPN	Email、Chat、Streaming、File transfer、VoIP、P2P
	nonVPN	Email、Chat、Streaming、File transfer、VoIP、P2P
ISCX Tor-nonTor[43]	Tor	Browsing、Emial、Chat、Audio、Video、FTP、VoIP、P2P
	nonTor	Browsing、Emial、Chat、Audio、Video、FTP、VoIP、P2P
CTU-13[46]	Benign	Neris、Rbot、Virut、Mentri、Sogou、Merli、Nsis-ay
	Malware	Neris、Rbot、Virut、Mentri、Sogou、Merli、Nsis-ay
Ariel(BOA2016)[49]	OS	Windows、Linux-Ubuntu、OSX
	Browsers	Chrome、Internet Explorer、Firefox、Safari
	Applications	YouTube、Facebook、Twitter
UNSW-NB15[52]	Normal	Normal
	Attack	DoS、Fuzzers、Analysis、Backdoor、Exploits、Generic、Reconnaissance、Shellcode、Worms
NSL-KDD[55]	Normal	Normal
	Attack	DoS、Probe、R2L、U2R
CICIDS2017[57]	Benign	Benign
	Attack	DoS Hulk、PortScan、DDoS、Heartbleed、Bot、DoS GoldenEye、FTP-Patator、Infiltration、SSH-Patator、DoS slowloris、DoS Slowhttptest、Web Attack XSS、Web Attack Brute Force、Web Attack Sql Injection

提取，这主要是因为加密流量数据（例如header和payload）中包含了较多不相关或冗余的信息，例如源和目的IP地址及协议信息，这些信息可能会影响后续的分类性能。同时，网络环境的短暂波动或其他潜在原因，使流量中可能会出现大量的坏包及重传包，从而导致特征的分布形式发生改变，使得数据集中引入了过多噪声，因此需要对其进行预处理，通常可归纳为以下部分。1) 数据包过滤。由于DNS和ICMP等数据包与应用分类或服务分类无关，因此可对其进行过滤。同时对于一些方法而言，空流和超长流中的数据包也会被过滤，因为空流中几乎不包含有助于分类的信息，而超长流中所含的数据包太多，可能存在大量的坏包和重传包，故也应对其进行过滤。2) 去除以太网头和端口，由于以太网头及端口中不包含与流量分类有关的信息，因此需删除以太网头以避免其带来的潜在干扰。3) 数据截断/数据补零。由于数据传输需求不同，数据长度都不相同，为了统一数据长度输入模型中，应该对过长的数据进行截断，对长度不足的数据进行补零[35, 39]。

此外，网络流量数据集实际上可看作长尾数据集，因为在实际网络活动中，异常事件发生的概率极低，能采集到的异常流量样本（尾类）较少，大部分都为正常流量样本（头类），这种类不平衡问题导致模型更倾向于正常流量样本，而忽略了异常流量样本。但对于加密流量分类来说，少数类异常样本的分类至关重要，若被误分类为正常流量将给用户设备造成更大的损失。

类不平衡问题是现实场景中较常见的问题，当前解决方法主要分为2种：数据级方法和算法级方法。数据级方法主要是通过修改数据集以平衡加密流量样本，也是目前应用最广泛的方法。文献[61]对多数类样本进行欠采样以平衡加密流量数据，并在ISCX VPN-nonVPN数据集上实现了94%的召回率，其中召回率反映了实际的正样本中被预测为正样本的概率，但易受噪声干扰，可能会导致信息丢失等问题。文献[53]将聚类的合成少数类过采样技术（SMOTE, synthetic minority over-sampling technique）与K-Means的欠采样技术相结合，既能避免SMOTE所带来的成本代价过高，又能消除随机欠采样丢失重要信息的问题。文献[62]提出基于长短期记忆（LSTM, long short term memory）网络和核密度估计的数据增强方法，不仅能为少数类生成流量数据包，还能复制每个类的数值化特征，有效提升了DL模型性能。近年来，随着生成式方法的进步，研究人员开始通过生成式模型生成样本。文献[63]利用条件生成对抗网络（CGAN, conditional generative adversarial network）来学习原始加密流量数据特征分布，以为少数类生成流量数据。文献[64]提出了一种辅助分类器生成对抗网络（ACGAN, auxiliary classifier generative adversarial network），该方法将随机噪声和类别标签同时作为输入，以便相应地生成输入类别标签的加密流量样本，不过实验数据集仅由SSH和非SSH两类组成，适用面较窄，普适性不强。

算法级方法通过改变损失权重来降低误报率，其表示负样本被预测为正样本占总的负样本的比例。文献[65]利用代价敏感方法解决类不平衡问题，通过添加代价表示分类器对少数类样本的敏感性，从而修改学习过程。文献[66]也利用代价敏感方法平衡加密流量数据集，通过样本数量设置代价惩罚矩阵，将较高的成本分配给少数类并为每个类分配不同代价，然后在训练过程中调整代价来更新权重以更敏感地识别少数类样本。此外，文献[56]采用均衡损失函数EQL v2（equalization loss v2）作为模型的损失函数，从而使模型关注少数类而不被多数类给淹没，提升了多个数据集的分类性能。文献[67]将注意力机制应用到物联网的流量分类区域，然后使用改进焦点损失函数解决类不平衡问题。文献[68]提出一种改进的交叉熵损失函数，主要将单个类别对总损失的影响平均分给其余类别，以缓解多数类主导总损失优化方向的现象。

类不平衡方法的对比如表4所示。总体而言，当前方法主要着眼于数据生成或删除及损失函数改进上，但易损失信息、鲁棒性不强且不适应动态的加密流量环境，因此未来应更加关注流量数据样本的采集。

2 加密流量特征提取与选择

本节首先详细介绍加密流量分类工作中所提取的特征，然后针对特征选择过程进行具体描述。

2.1 加密流量特征提取

传统的流量分类方法依靠端口和有效载荷等特

表4　类不平衡方法的对比

方法	文献	数据集	类不平衡策略	优点	缺点
数据级方法	文献[53]	UNSW-NB15、CICIDS2017	Cluster-SMOTE 过采样与K-Means欠采样	对不平衡数据的覆盖率优于单一欠采样技术	易受噪声干扰,在复杂环境下效果不如GAN等生成模型
	文献[61]	ISCX VPN-nonVPN	多数类中进行欠采样技术	降低数据集规模,适合资源受限场景	信息有所丢失,影响模型泛化能力
	文献[62]	自建数据集	基于LSTM与核密度估计的数据增强技术	性能优于常规的采样技术	计算复杂度高,适用于算力较强的场景
	文献[63]	USTC-TFC2016	CGAN	挖掘流量深层特征,生成的样本比传统采样方法丰富	容易生成无意义的样本,性能略低于ACGAN
	文献[64]	NIMS	ACGAN	提高生成数据质量,适用于高维数据集的生成任务	模型结构复杂,适用于算力较强的场景
算法级方法	文献[56]	UNSW-NB15、NSL-KDD、CICIDS2017	均衡损失函数EQL v2	相较一般的代价敏感方法更能平衡梯度,适合深度学习场景	计算复杂度较高,在实时场景下对计算资源的需求较大
	文献[65]	ISCX VPN-nonVPN	改进代价惩罚矩阵和交叉熵损失函数	改善了多数类的主导作用,效果优于传统损失函数	仅支持固定不变的样本,无法适应动态变化的实时流量
	文献[66]	ISCX VPN-nonVPN	代价敏感深度学习	提高了少数类分类性能,与代价矩阵结合更有效	未能考虑到模型输出概率之和为1的问题
	文献[67]	BoT-IoT	注意力机制和改进焦点损失函数	增强了少数类的分类,表现优于一般的损失函数	动态调参难度较大,泛化性略低于其他方法
	文献[68]	ISCX VPN-nonVPN	改进交叉熵损失函数	提升少数类性能同时还可保持多数类性能	无法自适应参数寻优,灵活性不如其他方法

征可有效地分类网络流量。然而，随着网络加密协议的日益复杂，以及攻击人员通过私有加密协议逃脱监管，仅仅利用上述特征已难以适应当前用户隐私保护的需求。因此，研究人员逐渐开始研究其他分类特征，主要可分为4类：网络流元数据特征、明文特征、侧信道特征以及原始流量特征[1, 15]，具体组成如图2所示。

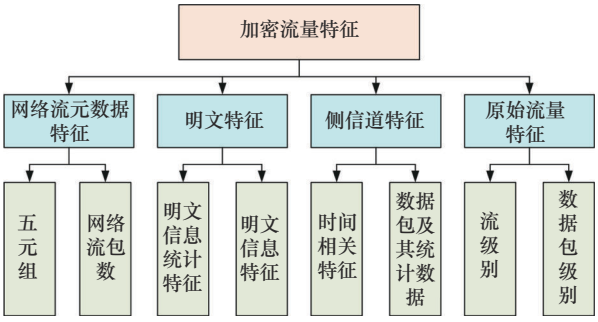

图2　加密流量特征组成

2.1.1　网络流元数据特征

网络流元数据特征是一种基本特征，指的是从网络流量中提取出与协议无关的特征，例如五元组（源IP地址、源端口、目的IP地址、目的端口、传输层协议）、网络流包数等数据流的基本信息。提取方法包括包大小分布、流持续时间和包间隔时间。其中，包大小分布主要统计流中数据包的大小，并计算均值、方差等统计量；流持续时间通过记录流的第一个和最后一个数据包的时间戳，计算流的持续时间；包间隔时间则计算连续包之间的时间间隔，并基于这些间隔生成统计特征。

McGrew等[69]从加密流量中提取源/目的端口、字节数及数据包数等网络流元数据特征，然后使用基于逻辑回归的分类器来识别加密流量并取得95.68%的平均准确率，其中准确率是指正样本和负样本中预测正确的数量占总数量的比例。秦鸣乐[70]将客户端和服务器中传输的源/目的端口等特征作为所选特征的一部分，并在集成多分类模型上取得了97.21%的准确率。姜鹏[71]提取心跳周期性、字节分布等特征构建数据集，在双向LSTM上实现了98.99%的准确率。霍跃华等[72]利用流元数据特征和证书特征，然后构建多视图协同训练分类器模型进行加密恶意流量分类并实现了99.17%的平均准确率。汪洋等[73]基于VPN测速特点对元数据进行划分，并在其基础上增加了目的端口平均大小在内的10个特征，通过随机森林进行识别并取得90.3%的精确率。不过网络流元数据特征通常与其

他特征进行结合，而不单独作为分类特征，故不再多加赘述。

2.1.2 明文特征

明文特征指的是可直接提取的明文信息特征及明文信息统计特征，提取方法包括协议字段解析和明文数据统计。协议字段解析通过解析网络流量中的明文字段，提取关键信息；明文数据统计则从非加密的字段或内容中提取长度、频率分布等统计信息，以捕捉特征的分布特性。

Akbari等[74]针对加密的TLS流量进行分类，从公开数据集Orange’20中提取了3类特征：数据包时间序列特征、流统计特征以及TLS握手的原始载荷字节，然后使用一维卷积神经网络（1DCNN, 1D convolutional neural network）和LSTM构成的多模态神经网络进行处理，取得了97.08%的准确率。Luxemburk等[75]创建了一个仅由TLS流组成的加密流量数据集，包含了完整的TLS握手流量，提取其统计信息特征并通过1DCNN和线性层实现了97.41%的准确率。周益旻等[76]利用负载明文特征和流统计特征提出IPSec VPN加密流量识别方法，通过随机森林（RF, random forest）模型取得了96.7%的精确率。此外，还可使用明文特征TLS证书内容进行识别，Chen等[77]提出一种多属性关联指纹方法，具体来讲，该方法利用加密TLS流握手中X.509证书对不用的加密应用进行分类，克服了因证书可用性而导致缺少属性的问题，在由16个应用组成的真实世界跟踪集上实现了98.69%的精确率，不过由于X.509证书字段本身并不包含应用的特定行为或独有特征，因此当多个用户拥有相同常用名、机构名等字段时，该方法难以对应用的TLS流进行准确的分类。Liu等[78]设计了一种加密恶意软件流量检测结构，首先使用流量采集工具Libpcap捕获2个已建立TLS连接主机之间的数据包，然后只提取加密流量前8个数据包中的特征，即数据包特征、TLS协议特征和证书特征，最后使用在线RF模型作为分类器以缩短训练时间，在CTU-13和MCFP构造的混合数据集中对Susp类的误报率仅为0.02%。

2.1.3 侧信道特征

侧信道特征是当前应用较广泛、较频繁的网络通信特征，通过直接观测加密流量数据而获取，包含时间相关特征、数据包及其统计数据，具备简单易处理等优势。常见的提取方法包括时间特征提取、流量速率分析及行为模式分析。时间特征提取是统计包的时间间隔分布、包到达的时间序列，获取流量的时间特性；流量速率分析通过分析流的传输速率变化，提取特定流量模式；行为模型分析则是基于流的通信行为模型，提取相关特征。

Yao等[79]利用循环神经网络（RNN, recurrent neural network）将加密流量建模为时间序列，并且把数据包长度与其他特征合并到同一个特征矩阵中，然后引入LSTM、分层注意力网络（HAN, hierarchical attention network）2个模型辅助网络流量分类，该方法在ISCX VPN-nonVPN数据集上的准确率为91.2%。Shen等[80]针对网络指纹识别提出一种细粒度网页指纹识别方法，通过提取数据包长度累积和块、序列特征、统计特征输入RF、K近邻（KNN, k-nearest neighbor）等传统ML算法中以创建网络指纹，从而实现细粒度识别。孙云霄等[81]针对IPSec VPN加密流量在开放型网络和闭合型网络上的区别，提取TCP最大分片长度值的信息熵以及帧长序列的标准差作为特征，然后在支持向量机（SVM, support vector machine）、RF、ID3这3类算法上进行测试，实验表明，在自采集数据集上ID3算法的性能较好，能达到97.6%的平均准确率。He等[82]提出基于数据倾斜的TLS应用未知加密流量方法，不仅准确地对已知流进行分类，还能较好地检测出未知流。该方法从数据包长度和数据包字节序列2个角度出发构建特征向量，在含60%的未知应用程序的真实加密流量数据集上取得了4.11%的误报率。Koumar等[83]设计了一种新颖的流量特征扩展方法，并基于统计、时间、频率、分布和行为提出69个通用特征，然后在15个知名的公开数据集上使用RF、K近邻及SVM在内的14个传统机器学习算法进行验证，实验表明，极限梯度提升（XGBoost, extreme gradient boosting）算法的性能最佳，在ISCX-VPN和UNSW-NB15数据集上分别取得了94.35%和98.49%的分类准确率。

2.1.4 原始流量特征

原始流量特征是加密流量分类领域中一类特殊的特征，归因于计算机算力的提升以及深度学习的迅速发展，逐渐成为当前研究热门，其提取方法主要包括原始包序列输入和字节流特征。原始包序列输入是通过深度学习模型直接处理流的原始包序列

以提取特征；字节流特征则是通过滑动窗口对字节流进行特征提取，以捕捉数据流的深层次特征。基于原始流量的分类模型如图3所示。

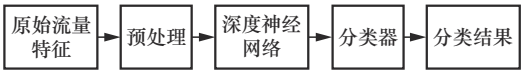

图3　基于原始流量的分类模型

Wang等[37]最早将原始流量作为特征引入加密流量分类领域，创建了加密恶意流量数据集USTC-TFC2016并将其原始流量转换为二维灰度图，然后通过不同加密恶意流量在二维图像素值上存在明显差异这一特点采用2DCNN进行端到端加密流量分类，实验在流+所有层、流+应用层、会话+所有层以及会话+应用层4种流量表示形式上展开，最后确定会话+所有层的性能最佳，二分类精度能达到100%，二十分类精度也能达到99.17%。Long等[84]设计了一种并行自动特征提取的加密流量检测框架，首次对流量数据包进行预处理，然后对其前784个字节进行分块，以28个字节为一块划分，最后通过多个并行的小型多层栈式自编码机提取局部流量特征，在CTU-13数据集上取得了99.998%的准确率，具有较好的鲁棒性。Zhang等[85]提出了一个自主学习框架以解决无法对未知加密流量进行正确分类的问题，该框架由一个基于DL的分类器、一个自学习的判别器和一个自标注模型组成，同时将数据包中的前1 456个字节向量分别转换为1×1456、39×39、22×22×3这3种形式以满足1DCNN、2DCNN、3DCNN的需求，该方法在ISCX VPN-nonVPN和真实网络应用的混合数据集上未知类可实现97.1%的分类性能。此外，流级别的原始流量同样可进行分类，Zou等[86]将CNN用于提取单个数据包的数据包特征，然后基于流中的数据包特征来训练LSTM，从而挑选流特征，在ISCX VPN-nonVPN数据集上取得了91%的精确率，不过CNN缺乏提取交互信息的能力，因此通常需要结合CNN与LSTM来提取流特征，但是LSTM又依赖上一个单元的输出，所以该方法非常耗时。Gonzalo等[87]分别将数据包级别和流级别的原始流量作为输入，然后设计2种DL模型进行特征提取，其中数据包级别采用1DCNN与LSTM相结合，而流级别只采用1DCNN，此外，数据包级别取前1 024个字节进行实验，流级别中每个流只保留前2个数据包，每个数据包长度固定为100个字节，最后在CTU公开的数据集上数据包级别达到了77.6%的准确率，流级别则达到了98.6%的准确率。

加密流量特征提取方法对比如表5所示，同时图4展示了上述方法在准确率和精确率方面的对比。值得注意的是，图4中的指标值皆为相关方法所能达到的最优水准，即当数据集、Epoch等参数有所变化后，同一方法可能会获得较低的性能，这主要是因为不同方法所采用的数据集和实验环境存在显著差异。不过图4还是能为后续相关人员的研究提供一定程度的参考价值。总体而言，基于原始流量特征的加密流量分类方法所取得的性能最好，因为其通过神经网络自动提取特征，而网络流元数据特征、明文特征和侧信道特征则是通过人工从网络流量中进行特征，信息有所损耗。因此，随着加密协议的不断应用，未来加密流量分类特征应关注原始流量特征的应用，同时其他特征也能取得较好的性能，故也应该着眼于多种类型特征相结合，以适应不断动态变化的加密流量环境。

2.2　加密流量特征选择

与加密流量特征提取相比，加密流量特征选择往往被忽视，但是现有的大多加密流量数据集中都存在较高的特征维度。同时经特征提取后的特征向量也可能存在冗余特征现象，这些不相关特征使得不同类样本之间的差异不显著，从而在一定程度上影响分类性能，增加计算成本。特征选择主要关注如何从一系列的特征中确定出一组具有代表性的特征，目的是防止因维数过高而导致模型性能下降，即“维灾害”和“峰值”现象[88]，因此加密流量在经过特征提取后应进行特征选择作为其后续步骤。

一般来说，特征选择框架主要包括3个部分：搜索策略、评价准则及终止条件，具体如图5所示。搜索策略算法是用来生成待评价的特征子集，常见的搜索策略有全局搜索、序列搜索及随机搜索等。全局搜索可找到全局最优解，但是其成本较高、效率低下，面临“状态空间爆炸”问题；序列搜索的速度较快，计算复杂度相对较小，但是容易陷入局部最优；随机搜索则综合了上述2种搜索方法的优势，在提高效率的同时又能寻找到近似最优解。评价准则是指通过某种度量准则对特征子集的好坏进行评价的手段。对于加密流量分类而言，其

表5 加密流量特征提取方法

类别	文献	所用特征	分类模型	数据集	优点	缺点
网络流元数据特征	文献[69]	源/目的端口、字节数及数据包数	逻辑回归	自建数据集	简单易实现，训练速度快，适用于基础场景	方法较老旧，适用面较窄，不适合处理高维数据
	文献[70]	源/目的端口	集成学习	混合数据集	多分类器的性能优于单一分类器	特征较简单，难以区分复杂流量
	文献[71]	心跳周期性、字节分布	双向LSTM	自建数据集	分类性能优于传统机器学习	适用面窄，难以推广到其他场景
	文献[72]	流元数据特征、证书特征	XGBoost、RF	CTU-13	分类准确率较高，在分析TLS流量时效果较好	依赖于特定的特征，适应性较差
	文献[73]	五元组等10个特征	RF	自建数据集	泛化性较强，适合常规流量分析	无法挖掘深层次特征，性能低于深度学习模型
明文特征	文献[74]	数据包时间序列、流统计、TLS握手原始载荷字节	1DCNN、LSTM	Orange'20	适合具有时序信息的加密流量分类	计算成本较高，不适用资源受限场景
	文献[75]	明文信息统计特征	1DCNN、线性层	自建数据集	分类速度较快，对实时流量处理较有效	在复杂流量场景下的效果一般
	文献[76]	负载明文、流统计特征	RF	自建数据集	在简单明文流量分类中效果较好	模型较简单，难以捕捉复杂信息
	文献[77]	X.509证书	XGBoost	自建数据集	对证书类流量特征处理的性能较高	难以推广到其他非证书特征场景
	文献[78]	数据包、TLS协议、证书特征	在线RF	CTU-13、MCFP	误报率较低，适合流量监控场景	仅限于特定证书和协议特征
侧信道特征	文献[79]	数据包长度、时间特征	LSTM、HAN	ISCX VPN-nonVPN	时间开销小，可进行实时流量处理	特征较多，需要较大的计算资源
	文献[80]	数据包长度累积、块和序列、统计特征	XGBoost	自建数据集	能处理多种侧信道特征，具有较高的分类准确率	泛化性较低，对少数类流量分类困难
	文献[81]	TCP最大分片长度值的信息熵、帧长序列的标准差	ID3	自建数据集	分类速度快，能有效处理特定特征	模型简单，无法处理复杂流量
	文献[82]	数据包长度、数据包字节序列	分类回归树	自建数据集	能有效降低特定类型流量的误报率	效果一般，性能低于深度学习模型
	文献[83]	基于统计、时间、频率、分布、行为等69个通用特征	XGBoost	ISCX VPN、UNSW-NB15	准确率较高，适合多种流量分类任务	特征数量较多，不适合资源受限场景
原始流量特征	文献[37]	数据包级别	2DCNN	USTC-TFC2016	首次引入原始流量特征	模型较简单，性能有限
	文献[84]	数据包级别	栈式自编码机	CTU-13	准确率较高，可捕获复杂特征	容易陷入局部最优
	文献[85]	数据包级别	CNN	ISCX VPN-nonVPN	效果有所提升，可处理高维特征	模型较复杂，计算资源需求较高
	文献[86]	流级别	CNN、LSTM	ISCX VPN-nonVPN	适用于具有时间依赖的流量分类	时间花销较高，不适合低时延场景
	文献[87]	流级别	CNN、LSTM	CTU数据集	考虑较全面，可提取时域信息	数据包级别精度较低

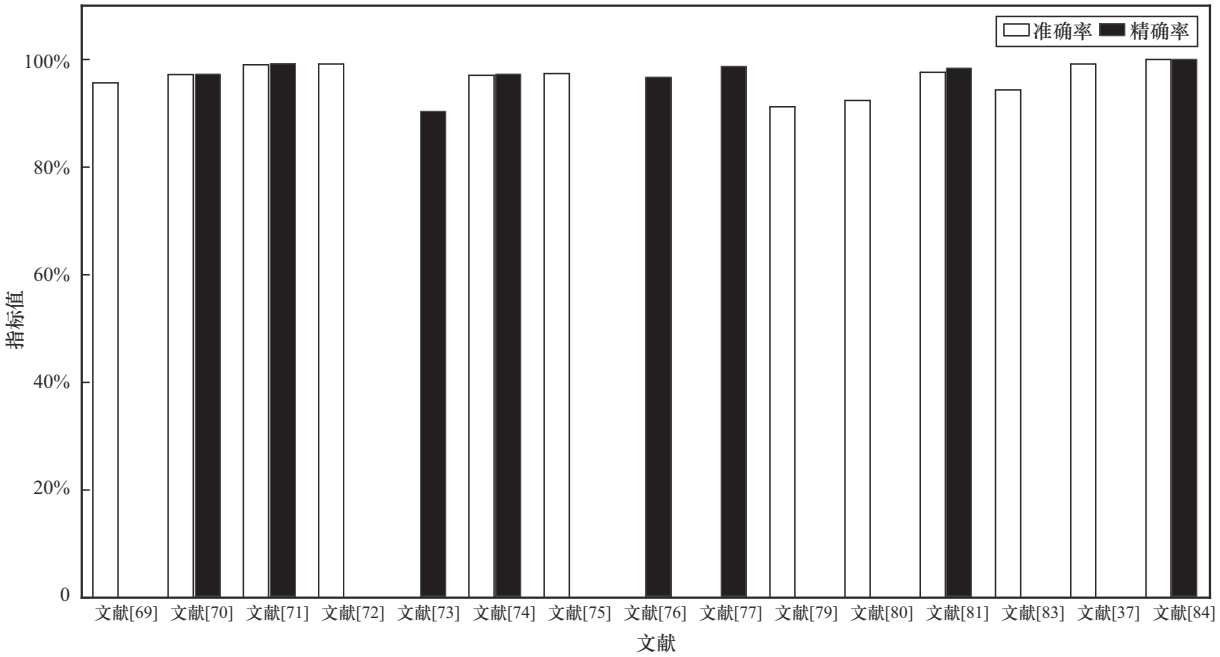

图4　加密流量特征提取方法性能对比

评价准则大体可分为过滤式、封装式和嵌入式3种。过滤式是根据离散度和相关性对每个特征进行评分，然后通过所设阈值筛选特征；封装式则是基于目标函数，一次选择或排除几个特征；嵌入式是采用传统机器学习得到每个特征的权重系数，然后进行排序筛选[89]。

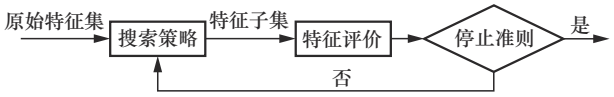

图5　传统特征选择框架

Shekhawat等[48]利用流量采集工具Zeek从加密流量的conn.log、ssl.log以及x509.log这3类文件中共提取了38个特征，然后通过XGBoost、SVM与RF在CTU-13、MCFP数据集上实现了较好的结果，同时使用信息增益和Pearson系数的过滤式特征选择方法来分析特征，实验表明，少量特征仍能取得不错的检测性能。Dong等[90]提出一种基于信息增益比和进化计算的多目标自适应特征选择算法，利用信息增益率过滤掉排名较低的特征，只保留前60%的特征，然后以不一致率和特征数量为目标，采用进化算法得到最优特征子集，在由6类多媒体流组成的加密流量数据集上通过多层KNN算法实现了98.6%的准确率。Long等[84]提出一种基于SVM和L1正则化的嵌入式特征选择方法，针对栈式自编码机所提取的特征并非都对分类任务有利，甚至会出现特征冗余这一情况，利用线性SVM损失函数中的缩放因子来控制L1权重强度，最后将特征贡献率较低的权重去除，以保留贡献率较高的特征。Manju等[91]根据每个特征在树中出现的次数作为权重进行特征排序，然后按照排序将特征逐个输入XGBoost，直至性能不再提升，此时所输入特征为最优特征子集，最后在2个不平衡数据集上分别取得了98.51%和93.54%的准确率。Wang等[58]针对工业信息物理融合系统中的流量提出基于可自适应搜索空间的二元灰狼优化特征选择算法，选取适应度函数值最低的作为特征子集，该算法在CICIDS2017数据集上实现了99.44%的准确率。McGaughey等[92]采用了基于封装式的特征选择方法，首先在由Tcpdump采集的自建加密流量数据集上提取了44个主要特征，然后通过快速正交搜索FOS算法筛选出10个代表特征，最后通过KNN算法进行对比，实验表明，所选特征子集的召回率为94.70%，仅比原始特征集的96.46%差了不足2%，但在时间上却是原始特征集的6倍，大大增加了计算成本。

加密流量特征选择方法对比如表6所示，同时图6展示了上述方法在准确率和召回率方面的对比。图6中的指标值仍为相关方法所能达到的最优水准。总体而言，基于3种评价准则的加密

表6 加密流量特征选择方法对比

评价准则	文献	使用方法	分类模型	数据集	优点	缺点
过滤式	文献[48]	信息增益、Pearson系数	XGBoost、SVM、RF	CTU-13、MCFP	能评估特征与离散目标变量之间的相关性	无法捕捉非线性关系
	文献[90]	信息增益比、进化算法	多层KNN	自建数据集	通用性强、算法复杂度高	忽略特征间的相关性
嵌入式	文献[84]	SVM、L1正则化	栈式自编码机	CTU-13	泛化能力强，避免过拟合	可能会忽略重要特征
	文献[91]	集成树模型	集成XGBoost	Cambridge dataset	计算效率有所提升	对异常值较敏感
封装式	文献[58]	二元灰狼优化算法	知识蒸馏	CICIDS2017	易辨识出关键特征	计算成本过高
	文献[92]	快速正交搜索算法	KNN	自建数据集	适应性强，可捕捉特征之间的相关性	难以处理多目标问题

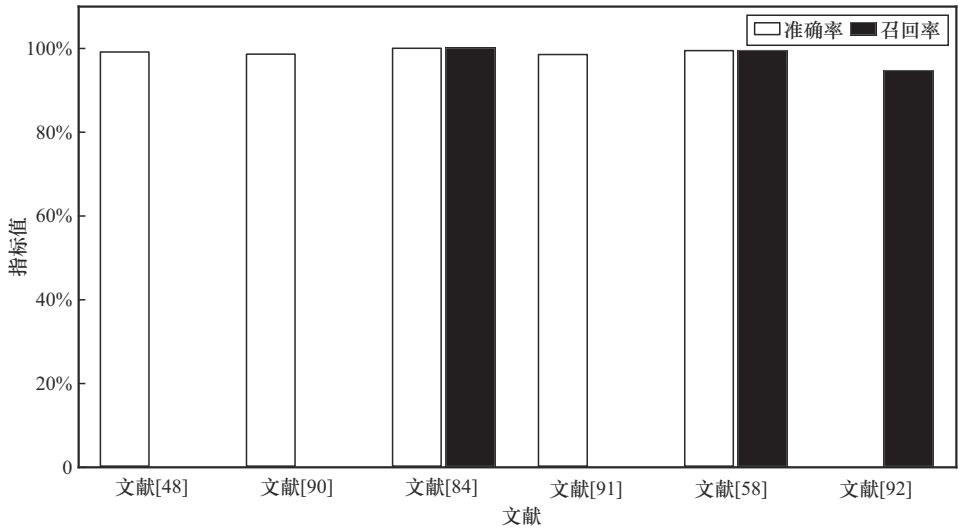

图6 加密流量特征选择方法性能对比

流量分类方法所取得的结果相差不大，都实现了较高的性能，因此研究人员可根据具体的场景和要求对评价准则进行选择。同时目前加密流量分类领域中特征选择的相关研究工作较特征提取来说要少很多，尤其是特征选择与深度学习相结合的工作，大部分特征选择方法都是通过传统机器学习算法来实现流量分类，因此，未来的加密流量分类研究应更加关注于特征选择在深度学习中的应用以降低计算成本。

3 加密流量分类过程与性能评估

本节首先详细介绍了基于机器学习的加密流量分类模型，包括传统机器学习方法和深度学习方法；然后对研究工作中所采用的评价指标进行描述。

3.1 加密流量分类模型

模型选择是加密流量分类领域中的关键组成部分，模型的优劣直接影响到整体方法的性能，因此选择一个合适的模型是至关重要的。现有机器学习模型按照复杂度进行区分大体上可分为传统机器学习和深度学习2种[93-94]，这主要是因为传统机器学习方法主要依赖于人工特征提取，只能用来分析数据之间的线性关系。而深度学习则是通过非线性单元的映射堆叠来挖掘数据内在隐藏抽象特征，能够处理好复杂的非线性问题[95-96]。因此，本节从传统机器学习和深度学习的角度，系统地阐述现有的加密流量分类模型方法，并对已有的研究工作进行总结分析。

3.1.1 基于传统机器学习的加密流量分类模型

传统机器学习方法主要依赖于人工提取的特征，在过去的几十年里一直都扮演着较重要的角色且应用较广泛，各类传统机器学习方法层出不穷并取得了良好的分类性能。传统机器学习可分为有监督学习、半监督学习、无监督学习和强化学习4种学习范式[21, 97]，具体分类如图7所示。

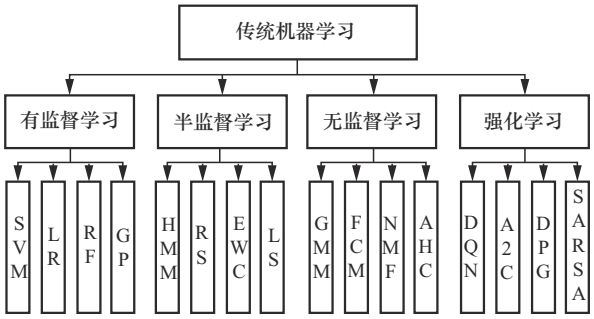

图7　传统机器学习分类

有监督学习的训练数据集既有特征又有标签，通过在含标签数据上进行训练以建立输入与输出之间的关系，从而使得模型可以对新数据进行分类或预测。Alshammari 等[98]针对 SSH 和 Skype 这 2 种加密流量的识别问题提出一种有监督学习方法，通过 C4.5、自适应增强（AdaBoost, adaptive boosting）和高斯过程（GP, gaussian process）3 个算法在 University Traces、DARPA99 Traces、AMP Traces、MAWI Traces 这 4 个数据集上进行实验，结果表明，3 个有监督传统 ML 方法可有效处理加密流量分类问题。同时其无须新的训练，便可将一个网络数据泛化到另一个网络数据，鲁棒性较强。Zaki 等[99]提出一种多标签的加密流量分类方法，通过将 2 个 RF 分类器链接在一起以对数据包有效载荷长度的 7 种统计特征进行处理，从而实现不同分类粒度的操作，该方法在 ISCX VPN-nonVPN 数据集上与 4 种基线分类器进行比较均保持不错的性能，可用于区分应用程序内的不同服务，具有较好的可靠性和灵活性。He 等[100]针对 Tor 流量提出一种基于两级滤波的 Obfs4 检测方案，首先通过数据包负载的随机性和时序特性进行粗粒度滤波以消除其他干扰流量，然后利用 SVM 算法对 Obfs4 的统计特征进行细粒度识别，最后在自建数据集上取得 99% 以上的准确率，即使在大流量环境下也能有效识别出 Obfs4。

与之相反，无监督学习则试图在没有标签的情况下发现数据隐藏的模式和结构，有助于学习更复杂的任务。Han 等[101]针对加密恶意流量提出一种轻量级无监督分类模型，首先对从数据包中提取到的统计信息进行特征压缩，从而提高了模型运行效率，然后采用经典的 K-means 算法实现分类，解决了实际场景中难以获得丰富的高质量标签问题，最后在公开加密恶意软件流量数据集 DataCon2020 上实现了 90% 以上的准确率。Carolina 等[102]仅提取基站收集的无线电连接迹线中的特征，并且依赖于聚合层次聚类（AHC, agglomerative hierarchical clustering）算法进行离线粗粒度分类，最后在实时收集的真实跟踪数据集上进行验证，实验表明，该算法无须在核心网中安装昂贵的探头就可完成加密流量分类，同时可扩展到其他无线接入技术，适用于 5G 系统。Yang 等[103]针对现有加密视频流量技术无法处理现实中未标记数据的问题，提出一种基于编辑距离相似度的谱聚类（SC, spectral clustering）算法用于加密视频流量的标题分析。在由 Chrome 浏览器收集的加密流量数据集上，该聚类算法在 25 个标题的视频流中取得了 95% 的准确率，其他指标也均保持在 90% 以上，无须大量标记样本进行训练便可实现良好的准确率。

半监督学习则介于两者之间，其训练数据集中既包含小部分标签数据，又存在大量的无标签数据，从而增强模型的泛化性能。He 等[104]提出了一种首次在网络级按应用程序类型对 Tor 流量进行分类的方法，首先选取突发体积和方向作为分类特征，然后使用 K-means 和多序列对比算法对数据进行预处理，最后利用隐马尔可夫模型（HMM, hidden Markov model）对未知 Tor 流量识别，实验验证了该方法的可行性。Fu 等[105]开发了一个系统，通过联合建模用户行为模式、网络流量特征和时间依赖关系，对移动消息应用程序的服务使用情况进行分类。该方法首先以分层的方式将互联网流量从流量流划分为具有多个对话的会话流，然后提取数据包长度和时间时延特征，最后基于聚类 HMM 从异常值中检测混合对话，并在现实世界流量数据集上验证了所提方法的有效性。Nguyen 等[106]针对 DoH 流量无法从 HTTPS 流量中识别从而导致加密 DoH 流量易泄露的问题，提出一种半监督学习算法对 DoH 流量进行分类，通过 CICFlowMeter 提取 PCAP 文件的统计特征，然后使用标签传播（LP, label propagation）、标签扩散（LS, label spreading）和半监督支持向量机（SSSVM, semi-supervised support vector machine）3 种半监督学习算法在恶意 DoH 数据集上进行实验并取得不错的效果，同时性能也优于其他分类方法。

强化学习是一种与环境交互的学习方式，通过其周围环境的作用进行决策，能有效处理复杂和动

态的环境。Dowling等[107]开发了一个利用强化学习与自动恶意软件进行交互的智能蜜罐，具体来说，该方法在Web服务器上将强化学习（RL, reinforcement learning）与状态−操作−奖励−状态−操作（SARSA, state-action-reward-state-action）技术结合使用，通过服务器充当蜜罐，对网络攻击和防御响应进行分类，该方法完全自动化进行，无须人为干预。Gupta等[108]针对基于VPN发起的加密攻击、混淆高级持续性威胁和恶意软件等问题，通过对深度强化学习（DRL, deep reinforcement learning）的迭代策略评估和改进来强化模糊K-means聚类增强的朴素贝叶斯模型，该方法在UNB-CIC VPN-nonVPN数据集上的精确率为94.4%，在一定程度上降低了计算成本。Rookard等[109]提出一种基于深度Q网络（DQN, deep Q-network）的强化学习方法以解决嵌入式系统和物联网设备等小型计算平台易遭受网络攻击的问题，并与其他结合强化学习的传统ML算法在TON-IoT数据集上进行对比分析，实验表明，该方法对正常流量的分类效果产生了积极影响，保护了计算机系统的安全。

基于传统机器学习的加密流量分类方法对比如表7所示，同时图8展示了上述方法在准确率和召回率方面的对比，图8中指标值仍为相关方法所能达到的最优水准。总体而言，基于有监督学习的加

表7 加密流量分类传统机器学习方法对比

学习范式	文献	分类模型	数据集	优点	缺点
有监督学习	文献[98]	C4.5、AdaBoost、GP	University Traces、DARPA99 Traces等	方法灵活、易理解	时间开销较大
	文献[99]	RF	ISCX VPN-nonVPN	训练速度较快	容易过拟合
	文献[100]	SVM	自建数据集	鲁棒性较强	难以处理大规模数据
无监督学习	文献[101]	K-means	DataCon2020	收敛速度较快	只能局部最优
	文献[102]	AHC	自建数据集	能处理大样本数据	复杂度较高
	文献[103]	SC	自建数据集	适应性较强	计算复杂度高
半监督学习	文献[104]	HMM	自建数据集	可捕捉数据中的动态结构	状态空间限制
	文献[105]	RF+HMM	自建数据集	适用面较广	参数估计困难
	文献[106]	LP、LS、SSSVM	DoH	计算复杂度较低	难以处理含噪声的流量数据
强化学习	文献[107]	SARSA	自建数据集	稳定性较强	收敛速度较慢
	文献[108]	DRL	UNB-CIC VPN-nonVPN	能自适应地学习最优策略	训练时间较长
	文献[109]	DQN	TON-IoT	通用性较强	复杂度较高

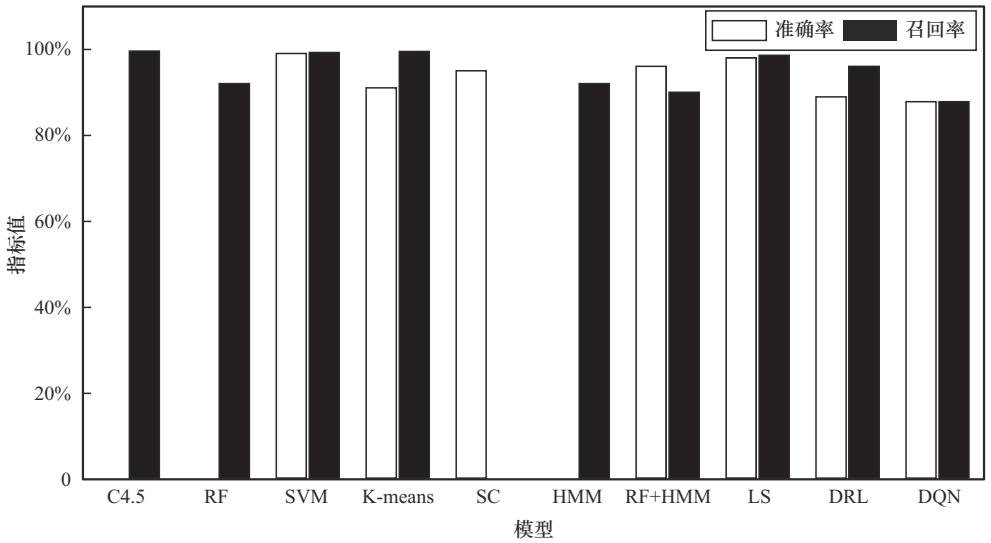

图8 加密流量分类传统机器学习方法性能对比

密流量分类方法所取得的结果更加准确，这主要是因为数据集中的数据都是有标签的，可更好地指导模型进行训练，不过无法对未知加密流量进行有效预测。而基于无监督学习的加密流量分类方法虽然结果稍差，但是2个指标也能达到87%以上，同时还能处理未知流量，可自动发现数据间的关系，不过很难对结果进行验证和解释。此外，基于半监督学习的加密流量分类方法则结合了两者的优势，其性能也大多处于两者之间，图8也能体现这一特点，但是该方法容易过拟合。对于强化学习而言，其可以做出最优决策，不过训练时间较长。因此，基于传统机器学习的加密流量分类研究未来应着眼于多种学习范式相结合以增强方法的鲁棒性和普适性，弥补其存在的缺点。

3.1.2　基于深度学习的加密流量分类模型

传统机器学习方法虽然取得了不错的分类性能，但其依赖于人工提取方法，耗时长且要求的知识储备较高，同时网络威胁愈加复杂。因此近年来深度学习已成为一种更强大的解决方案，其利用神经网络从海量加密流量数据中自动处理复杂的模式，从而提高分类的准确性和有效性。与传统机器学习的划分方式类似，基于深度学习的加密流量分类方法也可分为有监督学习、半监督学习、无监督学习3种学习范式[97]，具体分类如图9所示。

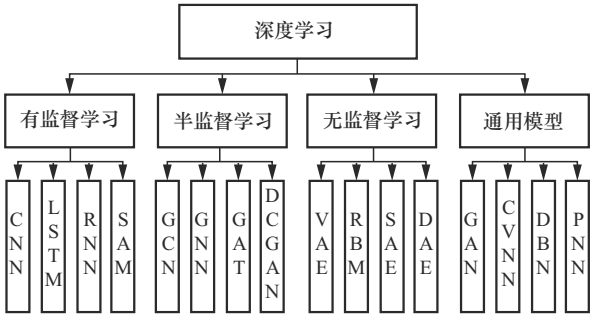

图9　深度学习分类

WANG等[36]首次将端到端的深度学习技术引入加密流量分类领域，该方法使用1DCNN自动从原始流量数据中提取特征并学习其非线性关系，以更好地刻画加密流量的一维序列特性。通过在ISCX VPN-nonVPN数据集上的实验结果可知，所提方法在性能上得到较大提升，更容易收敛到全局最优解，为后续研究打下了坚实的基础。Xie等[110]提出一种结合自注意机制的深度学习方法SAM，该方法对数据包分类只需2 ms，突破了在线分类所面临的限制。同时，所提模型可根据不同的分类任务来调整注意力。具体来说，其首先利用嵌入来丰富数据包级输入的表征，然后通过自注意力机制为输入的每部分分配不同的权重以表示其重要程度，最后应用1DCNN进行分类，该方法在WIDE、UNIBS、ISCX这3个公共数据集上的实验结果表明，SAM在协议、应用和流量类型分类任务上都具有较好的性能。Lin等[111]针对工业物联网中的海量流量提出一种结合CNN和LSTM的加密流量识别方案，该方案首先通过CNN提取抽象的空间特征，然后引入堆叠的双向LSTM学习时间特征，最后在ISCX Tor-nonTor数据集上进行实验并取得了较高的准确率。该方案在没有任何特殊设置的情况下仅使用少量数据包便可实现流量的早期识别，同时不局限于特定的场景，具备较好的泛化性。不过上述方法只能处理单模态输入，未能考虑到加密流量的多种表征形式。Dai等[112]提出一种跨模态融合模型，旨在捕捉不同模态之间的关系，通过融合数据包、上下文和流级别的模态以获得更好的性能，同时模型中引入了许多轻量级神经网络以避免物联网设备上硬件资源有效的问题，并采用知识蒸馏（KD, knowledge distillation）来提高模型的推理速度。该方法在ISCX-VPN-2016、ISCX-Tor-2016等数据集上都优于目前的SOTA方法。此外，由于有效负载可提取和利用的特征非常有限，并且攻击者能够通过修改关键特征逃避检测，为此基于相关性特征的研究为当前加密恶意流量检测分类领域提供一条新思路。Hong等[47]巧妙地利用加密会话作为节点，根据图像特征的相似性构建KNN图，并将向量化后的特征作为对应节点的属性，最后利用GraphSAGE模型学习相关节点信息以丰富各节点的嵌入，在恶意流量数据集上可取得99.9%左右的准确率。该方法通过将加密恶意流量检测问题转化为图节点分类问题，突破了加密流量相关性使用和挖掘的难题，有效结合多视图特征提升了模型性能。

随着各种强大加密协议的出现，对加密流量数据进行捕获和标注愈加困难，已成为当前研究人员面临的一大挑战，而半监督学习恰好能解决该问题。Aouedi等[113]则提出一种半监督深度学习方法，首先基于无监督算法堆叠稀疏自编码器（SSAE, stacked sparse auto-encoder）进行预训练以

提取鲁棒特征，然后利用有监督分类算法进行微调并丢弃SAE的解码层，最后在真实加密流量数据集上进行实验并取得了较好的分类性能。该方法不仅能保持整个过程的自动化，还能同时考虑有标签和无标签数据。Jin等[114]结合半监督学习和对比学习对加密流量进行分类，具体来说，首先提出一个基于均值教师的半监督学习框架SSCMT，其次将对比约束集成到框架中以便挖掘更典型的流量数据分布，最后在ISCX VPN-nonVPN数据集上验证了其可行性，该框架有效提升了对未知流量的分类能力。Chen等[115]开发了基于开放集半监督学习的未知网络流量检测框架，利用少量的有标签数据和大量的无标签数据来训练模型，从而在准确识别已知类流量的同时分类出未知类流量，在USTC-TFC2016和ISCX VPN-nonVPN这2个数据集上取得了较好的性能，优于当前大多数先进方法，并消除了深度学习方法具有封闭世界的假设。同时随着生成式学习的发展，研究人员逐渐开始利用其进行加密流量分类任务，Iliyasu等[116]使用深度卷积生成对抗网络（DCGAN, deep convolution generative adversarial network）生成的样本和未标签的数据在几个有标签样本上训练模型，该模型在自收集的QUIC协议数据集和ISCX VPN-nonVPN数据集上使用极少量有标签样本便分别实现了89%和78%的准确率，极大缓解了大型数据集中数据收集烦琐、标记困难等问题。Wang等[117]基于GAN提出一种用于软件自定义网络边缘网关的半监督加密流量分类方法，该方法通过半监督学习修改常规GAN鉴别器网络的结构和损失函数，不仅能够在ISCX VPN-nonVPN数据集上实现良好的分类效果，而且模型属于轻量级设计，只消耗较少的计算资源。

此外，当前也存在较多基于无监督学习的加密流量分类方法来解决数据难收集的问题。王攀等[118]提出一种基于SAE模型的加密流量识别方法，通过SAE的堆叠逐层提取高维特征，对流量进行重构，同时利用SMOTE解决数据集类不平衡问题。该方法克服了传统机器学习方法准确率偏低、特征提取和选择费时费力等问题，在ISCX VPN-nonVPN数据集上的准确率稳定在99%左右。Lin等[119]设计了一种新型的多模态深度学习框架，其使用原始字节和长度序列作为输入，并利用自注意力机制来学习双流中网络数据包之间的深层关系，同时引入无监督的预训练方式来增强网络流量字节间的相关性，从而提升模型随数据包的表示能力，最后在真实流量数据集中取得了较好的性能。该框架不依赖于其他领域知识，具有较好的泛化性和并行推理能力。Jang等[120]采用变分自编码器（VAE, variational auto-encoder）对软件自定义网络中的加密流量进行分类，同时该方法不只局限于软件自定义网络环境，在传统的网络架构中也可进行使用，例如收集和监控网络流量信息。具体来说，其提取前n个数据包中的6个统计特征作为输入，然后VAE学习其内在分布，并且在收集的流量数据集上实现了89%的平均准确率。Boppana等[121]则结合GAN和AE提出一种用于物联网中MQTT协议的无监督方法，该方法使用GAN进行对抗性训练，并将自动编码器作为生成器，同时，GAN-AE可直接处理通过聚合数据包信息生成的流记录，而无须将流量进行转换，其在MQTT-IoT-IDS2020数据集上的性能均优于其他无监督模型，不仅具有良好的稳定性，而且还满足流量实时检测的需求。Carvalho等[122]介绍了一种针对异构网络流量检测泛化问题的堆叠无监督联邦学习方法，其包含一个深度自编码器和一个能量流分类器，可将流量分类任务推广到不同的网络系统，并在不同网络上下文之间实现了最佳的泛化性能，最后在基于流特征组成的TON-IoT、Bot-IoT等4个加密流量数据集上能较好地检测出攻击流量，同时所提模型不需要将数据移动到中央服务器上便可保护系统用户的隐私。

加密流量分类深度学习方法对比如表8所示，同时图10展示了上述方法在准确率和F1分数方面的对比，图10中的指标值仍是相关方法所能达到的最优水准。总体而言，当前基于深度学习的方法避免了传统ML方法中人工特征提取耗时长、不完备等问题，不过有监督方法受限于无标签数据，无监督方法和半监督方法虽然在一定程度上能处理无标签数据，但是存在应用场景单一、泛化能力弱、对噪声数据敏感等问题，因此，未来基于深度学习的加密流量分类方法应着眼于如何更好地处理无标签数据以实现未知加密流量的精准分类。

3.2 加密流量分类性能评估

为了能直观地评估加密流量分类方法的有效性，大多研究工作的实验结果都会采取评价指标进行对比分析，以体现方法的性能优势。

表8　加密流量分类深度学习方法对比

学习范式	文献	分类模型	数据集	优点	缺点
有监督学习	文献[36]	1DCNN	ISCX VPN-nonVPN	复杂度较低	容易陷入局部最优
	文献[47]	GraphSAGE	CTU-13、MCFP	提高了分类效率	过于依赖图连通性
	文献[110]	SAM	WIDE、UNIBS、ISCX	可捕捉全局信息	复杂度较高
	文献[111]	CNN+LSTM	ISCX Tor-nonTor	兼顾空间和时间特征	参数较多
	文献[112]	Knowledge Distillation	ISCX-VPN-2016、ISCX-Tor-2016 等	能挖掘不同模态之间的关系	不能处理零日流量
半监督学习	文献[113]	SSAE	自建数据集	泛化性较强	对异常识别不敏感
	文献[114]	SSCMT	ISCX VPN-nonVPN	能有效降低过拟合	过于依赖有标签数据的质量
	文献[115]	DivinEye	USTC-TFC2016、ISCX VPN-nonVPN	消除了封闭世界的假设	缺乏可解释性
	文献[116]	DCGAN	ISCX VPN-nonVPN、自建数据集	可扩展性强	计算成本较高
	文献[117]	ByteSGAN	ISCX VPN-nonVPN	能学习到复杂的数据分布	难以处理模式崩溃问题
无监督学习	文献[118]	SAE	ISCX VPN-nonVPN	具备良好的泛化性能	计算成本较高
	文献[119]	PEAN	自建数据集	有助于增强模型对数据包的表示能力	纯密文流量的分类效果不佳
	文献[120]	VAE	自建数据集	能学习到输入的潜在分布	难以处理模式崩溃问题
	文献[121]	GAN+AE	MQTT-IoT-IDS2020	不易被噪声数据影响	生成样本可能无意义
	文献[122]	DAE+FL	TON-IoT、Bot-IoT 等	能提取输入的本质特征	鲁棒性不高

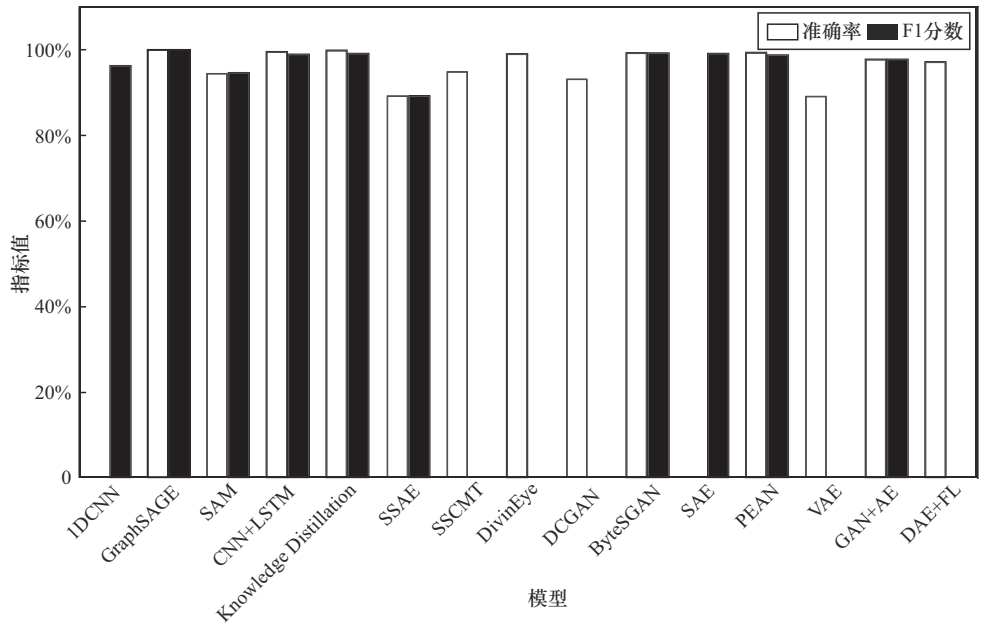

图10　加密流量分类深度学习方法性能对比

现有的研究工作大都集中采用准确率（Acc, Accuracy）、精确率（Pre, Precision）、召回率（Rec, Recall）、误报率（FPR）以及F1分数（F1）这5个评价指标进行性能评估。其中，准确率是用来衡量总体的有效性，但由于其对所有类别都一视同仁，因此该指标不适合类不平衡数据集，这时准

确率的意义不大；精确率从预测结果出发，表示在所有预测为正样本的数量中实际为正样本的概率，主要用来最小化分类错误的正样本数量；召回率则是针对原样本而言，也称检测率，主要用来最小化分类错误的负样本数量；误报率即虚警率，可用于评估类不平衡数据集；F1分数则是由精确率和召回率计算而成的，既考虑了识别异常样本的能力，又兼顾了捕获所有实际异常样本的能力，同样适用于类不平衡数据集。5个指标的具体计算方式如下所示。

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

$$\mathrm{Pre}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}} \tag{2}$$

$$\mathrm{Rec}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{3}$$

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{4}$$

$$\mathrm{F1}=\frac{2\times\mathrm{Pre}\times\mathrm{Rec}}{\mathrm{Pre}+\mathrm{Rec}} \tag{5}$$

其中，TP、TN、FP和FN分别表示真阳性、真阴性、假阳性及假阴性，即攻击样本预测正确的数量、正常样本预测正确的数量、攻击样本预测错误的数量、正常样本预测错误的数量。TP、TN、FP和FN均来自混淆矩阵，其通常被认为是最直观、最基本的评估模型性能的方法，因此本文通过热力图、色差和亮度等方式来体现不同类别数据之间的差异性。当混淆矩阵的对角线上数据最大且最暗时，说明已预测出大部分数据样本，具体如图11所示。

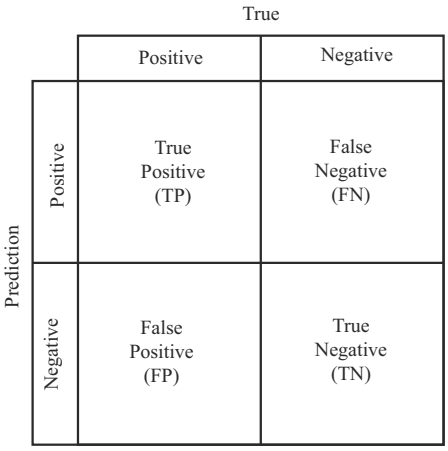

图11 二分类混淆矩阵

此外，除上述5个评价指标外，研究人员还使用ROC、AUC、MAE、MSE及RMSE进行性能评估。其中，ROC是指接收者操作特征曲线，该曲线的横坐标为假正率，即FPR，纵坐标为真正率，即TPR，也就是召回率，曲线越陡说明模型性能越优，而且ROC曲线能无视类不平衡问题，无论样本之间的比例如何变化对其都不会产生影响。AUC则表示ROC曲线下的面积，用来衡量模型的整体表现，其值越大则模型性能越好，一般介于0.5和1之间。MAE为预测值和真实值之间平均绝对误差，用来衡量数据集残差的平均值。MSE是均方误差，也是用来衡量预测值和真实值之间的差距。RMSE是均方根误差，表示预测值与真实值之差的标准偏差。

上述指标在模型性能评估中出现的频率最高，虽然还存在其他评价指标，但其出现频率较低，在此不再赘述。总体而言，加密流量分类模型性能评估需要构建综合的指标体系才能进行全面的对比分析，因此，未来在选取评价指标时应更加注重指标间的关系，做到互为补充、相互融合。

4 挑战与未来研究展望

目前研究人员在加密流量分类领域中做了大量的工作并取得了实质性的突破。然而随着时间的推移，一方面，计算机技术不断地向前迭代发展，网络安全形势也不断地更新变化，这将给加密流量分类工作带来不小的挑战。另一方面，互联网加密技术持续更新发展，现有的技术方法已难以满足日益增长的加密流量分类需求，主要体现在以下几个方面。首先，现有的加密流量数据集种类繁多且侧重点各不相同，通常可从样本质量、数据形式、采集日期及样本分布等方面来评估。例如，USTC-TFC2016数据集中的原始流量文件质量较低，经过数据处理后进一步降低了数据质量。UNSW-NB15、NSL-KDD及CICIDS2017等数据集以已提取的特征形式提供，并不包含原始流量文件，限制了提取新特征的灵活性。此外，从数据采集日期和样本分布上比较，ISCX VPN-nonVPN、ISCX Tor-nonTor以及Ariel（BOA2016）等多个数据集的年份都较久远，难以反映当前流量模式。同时样本分布也都不平衡，这些问题一直都影响着分类性能。其次，当前所提取的特征在新型网络协议（如QUIC、TLS）下信息表示能力不足，尤其是传统的流统计特征和时序特征难以表征新型网络流量之

间的关系且易受噪声干扰。而且特征选择过程费时费力，由文献[123]可知，特征选择后数据集的训练时间比未经过特征选择时快一倍，但6种算法特征选择过程的耗时却是训练时间的7~8倍，这使得快速分类需求难以满足。再次，现有的分类器会消耗大量的计算资源，且在开放世界的场景下会失效，泛化性不足。此外，当前不断有分类方法被提出，但缺乏全面系统的指标体系进行评价。最后，机器学习方法缺乏可解释性，安全性不高。针对上述所提出的基于机器学习的加密流量分类工作中存在的问题，在此对下一阶段值得探索且有价值的研究方向进行分析与展望。

1) 构造真实且动态多样的加密流量数据集

一个高质量的加密流量数据集可在训练中发挥巨大作用。然而现有加密流量数据集普遍存在以下问题：首先缺乏真实性，现有数据集中的部分数据只是通过工具在虚拟环境中生成或者简单复制流量样本，不能代表真实的流量环境，同时流量特征也随着时间不断变化，无法准确描述其特性；其次缺乏动态多样性，当前加密流量数据集通常为一次性采集或构建而成，随着网络流量特征的不断演变，其已无法反映流量特征随时间变化的动态特性，泛化性不足。此外，加密流量数据集还存在类不平衡问题，这种不平衡会导致少数类样本直接被淹没，不利于模型分类，而现有类不平衡方法只能在一定程度上缓解，并不能从根本上彻底消除该问题。这主要是因为数据级方法生成流量数据在样本分布上与原有样本并无区别，无法与真实环境中采集的样本相比较，而算法级方法并不能保证分类器的结果最优。因此，为突破加密流量数据集所面临的窘境，未来研究工作应构造真实且动态多样的加密流量数据集，重点关注自动标注工具的使用，通过其实现加密流量数据的持续更新，并且在动态更新中不断调整样本分布以解决类不平衡问题。

2) 探究更鲁棒稳定的加密流量特征

近年来，互联网通信技术和加密技术快速发展，由此许多复杂新型的加密网络通信协议不断地涌现，例如QUIC协议、TLS-1.3协议等。这些新型协议导致网络环境中的未知流量比例急剧上升，所提取特征的有效性不断地降低。而当前机器学习方法高度依赖于所提取的特征，所以在构造有效的特征形式时需要考虑以下几点问题：首先应提取鲁棒性强的特征以抵抗新型协议下不断变化的加密流量环境，而统计特征在动态环境中变化较大，相比之下流特征鲁棒性较强，因为其是从原始数据包流中提取的，不易受变化影响[17]；其次应考虑特征的辨别性，通过缩小相同流量样本的类内距离和放大不同流量样本的类间距离来增强特征的表达能力；最后应注意特征的有效性，当前大部分侧信道特征为浅层特征，在面向新型网络协议的未知流量时其有效性不高。所以在探究新型加密协议下的加密流量特征时应深入研究加密流量的信息分布特性，构造出可反映加密流量固有属性的强有力特征，进而为新型加密网络协议下的流量分类模型与方法提供支撑。

此外，大多数加密流量特征选择技术都是从大量的待选特征中进行多次尝试以寻找出具备显著区分度的特征。整个过程所消耗的时间较长，并且其效果并不明显，可能仍然存在冗余或不相干特征，无法实现快速分类。这种做法显然未能考虑到数据集与特征之间的关系，若能确定数据集中的加密流量样本是通过加密应用程序产生的，那么可以从数据包长度中寻找关键特征，因为加密应用程序包含唯一的信息交换协议且反映在数据包长度信息中[124]。另一方面，特征选择技术对流量数据较敏感，稳定性不足，而现实世界中的网络流量环境呈动态复杂趋势变化，一个细微的差异便可使通过同一个特征选择算法筛选出来的特征子集不同，影响后续的分类性能。因此，未来应着眼于加密流量数据集和特征之间的关系，探究数据集中流量的生成方式及组成内容，深入分析特征选择技术的基本原理，从而研究出更快速、准确、稳定及具有普适性的加密流量特征选择技术。

3) 构建轻量型加密流量分类模型与评价体系

当前大多数加密流量分类工作都是在封闭世界假设下评估模型，受制于在分类阶段所出现的类别也必须在模型训练阶段出现的条件，即只能在预定义的静态数据集中对加密流量进行分类，这与真实世界的动态开放环境并不相符。在开放世界假设中，流量数量呈复杂波动性，加密流量可以从比封闭世界目标源数量大得多的非目标源中生成。这些非目标源产生的加密流量对于分类模型而言是未知的，但是这些分类模型必须能够检测出非目标源，以支持网络测量和管理。同时真实世界中的加密流量数据可能会随着时间的推移而发生突发或渐进变

化，称为概念漂移现象[125]，从而使得训练好的分类模型在经过一段时间后性能有所下降。另一方面，加密流量因其不透明性导致在分类过程中需要消耗更多的计算资源，这种情况在加密流量激增的情况下更严重。而基于深度学习的加密流量分类方法是通过牺牲效率来提升分类结果，需要研究人员在计算、内存和功率方面提供丰富的设备资源供其训练使用，这与他们打算在资源受限设备上部署人工智能和深度学习技术的想法相矛盾[126-127]。因此，未来应更加考虑开放世界场景，着眼于联邦学习等多点协同分布式训练方法以减少资源消耗，从而构建突破封闭世界假设的轻量型加密流量分类模型。

当前加密流量分类方法层出不穷，并且基本采用准确率、精确率等评价指标来衡量方法的优劣，很少会采用带宽、时延及丢包率等评价指标，所以这种评价方式比较片面，不够全面系统。尤其是在海量数据背景下，由于系统复杂、专家知识储备有限等因素的影响更是难以在众多加密流量分类方法中确定相对客观可靠的方法。然而目前对于加密流量分类方法评价体系的研究乏善可陈，并无合理有效的综合评价模型。所以，刻画全面系统的加密流量分类方法评价体系也是未来加密流量分类领域一个较重要的研究方向。

4) 建立可解释性深度学习的加密流量分类安全机制

当前深度学习方法已广泛运用于加密流量分类领域并取得了不错的性能，但是大部分互联网服务提供商在通过深度学习方法得到准确预测的同时更想知道某些性能为什么好或者为什么差。整个过程并不透明，无法为互联网服务提供商进行解释说明，这也是深度学习被研究人员称作“黑盒”的原因。尽管目前已有部分工作针对计算机视觉等领域的模型可解性进行研究，但其发展还不成熟，存在较多问题，同时也难以直接迁移到模糊抽象的加密流量数据上[128]。另一方面，统计特征相较流特征而言其可解释性较强，因为统计特征可直接用于推理模型的预测，而流特征作为自动提取的抽象特征无法进行解释，所以良好的特征可解释性可提升模型性能，帮助研究人员更好地理解深度学习模型行为[129-130]。因此，未来应着眼于可解释性深度学习的工作研究，通过数据可视化、规则法等可解释性方法建立加密流量分类安全机制。

5 结束语

近年来，互联网流量加密呈常态化趋势，在此背景下，加密流量分类已成为当前网络空间安全领域最具挑战性的问题之一。针对该问题，本文从特征流动角度将加密流量分类工作抽象为加密流量数据采集与处理、加密流量特征提取与选择及加密流量分类过程与性能评估3个部分。然后细分为流量采集、数据集构建、数据预处理、特征提取、特征选择、分类模型及性能评估7个工作流程。最后分别对这7个阶段进行系统性的综述。

本文在加密流量数据采集与处理阶段首先对当前典型的流量采集工具和数据集进行归纳，并且从数据级、算法级两方面总结现有的类不平衡方法；其次对于加密流量特征提取的研究则从网络流元数据特征、明文特征、侧信道特征和原始流量特征4类特征进行回顾，目前基于明文特征和侧信道特征的研究工作较多，此外，随着深度学习技术和算力的发展，原始流量特征逐渐占据主导地位；接着在加密流量特征选择阶段，综述了过滤式、封装式和嵌入式3种方法的研究，有助于消除冗余特征和不相关特征的干扰，不过该领域的相关研究工作较少；然后从传统机器学习和深度学习两方面入手，围绕有监督、半监督、无监督等学习范式开展详细的综述，并对当前研究工作中所采用的评价指标进行归纳分析；最后，通过分析当前加密流量分类方法中所面临的问题，提出了未来的研究方向，并为机器学习赋能的加密流量分类工作提供新的思路。综上所述，加密流量分类仍是目前研究的热点之一，希望本文研究可为后续工作提供一定的参考价值。

参考文献：

[1] 陈子涵, 程光, 徐子恒, 等. 互联网加密流量检测、分类与识别研究综述[J]. 计算机学报, 2023, 46(5): 1060-1085.
CHEN Z H, CHENG G, XU Z H, et al. A survey on Internet encrypted traffic detection, classification and identification[J]. Chinese Journal of Computers, 2023, 46(5): 1060-1085.

[2] CHEN Z H, CHENG G, NIU D D, et al. WFF-EGNN: encrypted traffic classification based on weaved flow fragment via ensemble graph neural networks[J]. IEEE Transactions on Machine Learning in Communications and Networking, 2023, 1: 389-411.

[3] WU D M, DENG Y, LI M Y. FL-MGVN: Federated learning for anomaly detection using mixed Gaussian variational self-encoding network[J]. Information Processing & Management, 2022, 59(2): 102839.

[4] AN P, WANG Z Y, ZHANG C J. Ensemble unsupervised autoencoders

and Gaussian mixture model for cyberattack detection[J]. Information Processing & Management, 2022, 59(2): 102844.

[5] D'ANGELO G, CASTIGLIONE A, PALMIERI F. DNS tunnels detection via DNS-images[J]. Information Processing & Management, 2022, 59(3): 102930.

[6] WANG W L, WANG Y J, DUAN P Y, et al. A triple real-time trajectory privacy protection mechanism based on edge computing and blockchain in mobile crowdsourcing[J]. IEEE Transactions on Mobile Computing, 2023, 22(10): 5625-5642.

[7] HUANG Y, LI W, WANG J B, et al. Privacy protection among three antithetic-parties for context-aware services[J]. Journal of Network and Computer Applications, 2021, 191: 103115.

[8] Google. Google transparency report[R]. 2022.

[9] ENCRYPT L. Percentage of web pages loaded by firefox using HTTPS [R]. 2023.

[10] R&S. Protocol and application classification with metadata extraction (PACE2)[R]. 2017.

[11] Cisco. Network based application recognition(MBAR)[R]. 2017.

[12] Ntop. Open and extensible LGPLv3 deep packet inspection library (nDPI)[R]. 2017.

[13] L7-filter. L7-filter sourcecode (17-filter)[R]. 2017.

[14] MARTIN R. Network intrusion detection & prevention system (Snort) [R]. 2017.

[15] 侯剑, 鲁辉, 刘方爱, 等. 加密恶意流量检测及对抗综述[J]. 软件学报, 2024, 35(1): 333-355.
HOU J, LU H, LIU F A, et al. Detection and countermeasure of encrypted malicious traffic: a survey[J]. Journal of Software, 2024, 35 (1): 333-355.

[16] VELAN P, ČERMÁK M, ČELEDA P, et al. A survey of methods for encrypted traffic classification and analysis[J]. International Journal of Network Management, 2015, 25(5): 355-374.

[17] SHEN M, YE K, LIU X T, et al. Machine learning-powered encrypted network traffic analysis: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 791-824.

[18] 于治平, 刘彩霞, 刘树新, 等. 基于机器学习的网络流量分类综述[J]. 信息工程大学学报, 2023, 24(4): 447-453, 483.
YU Z P, LIU C X, LIU S X, et al. Overview of network traffic classification based on machine learning[J]. Journal of Information Engineering University, 2023, 24(4): 447-453, 483.

[19] REZAEI S, LIU X. Deep learning for encrypted traffic classification: an overview[J]. IEEE Communications Magazine, 2019, 57(5): 76-81.

[20] 郭宇斌, 李航, 丁建伟. 基于深度学习的加密流量识别研究综述及展望[J]. 通信技术, 2021, 54(9): 2074-2079.
GUO Y B, LI H, DING J W. Review and perspective on encrypted traffic identification using deep learning[J]. Communications Technology, 2021, 54(9): 2074-2079.

[21] HENDAOUI F, FERCHICHI A, TRABELSI L, et al. Advances in deep learning intrusion detection over encrypted data with privacy preservation: a systematic review[J]. Cluster Computing, 2024, 27(7): 8683-8724.

[22] RESCORLA E. SSL and TLS: designing and building secure systems [R]. 2001.

[23] BHIOGADE M S. Secure socket layer[C]//Proceedings of the Computer Science and Information Technology Education Conference. Piscataway: IEEE Press, 2002: 85-90.

[24] LANGLEY A, RIDDOCH A, WILK A, et al. The QUIC transport protocol[C]//Proceedings of the Conference of the ACM Special Interest Group on Data Communication. New York: ACM Press, 2017: 183-196.

[25] YLONEN T, LONVICK C. The secure shell (SSH) protocol architecture[R]. 2006.

[26] FRANKEL S. Demystifying the IPsec puzzle[M]. Boston: Artech House, 2001.

[27] 付钰, 王坤, 段雪源, 等. 面向软件定义网络的异常流量检测研究综述[J]. 通信学报, 2024, 45(3): 208-226.
FU Y, WANG K, DUAN X Y, et al. Survey of research on abnormal traffic detection for software defined networks[J]. Journal on Communications, 2024, 45(3): 208-226.

[28] WANG K, FU Y, DUAN X Y, et al. Abnormal traffic detection system in SDN based on deep learning hybrid models[J]. Computer Communications, 2024, 216: 183-194.

[29] CHAPPELL L. Wireshark network analysis[M]. Laura: Laura Chappell University, 2012.

[30] TIWARI A, SARASWAT S, DIXIT U, et al. Refinements in Zeek intrusion detection system[C]//Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS). Piscataway: IEEE Press, 2022: 974-979.

[31] BONELLI N, GIORDANO S, PROCISSI G. Enabling packet fan-out in the Libpcap library for parallel traffic processing[C]//Proceedings of the 2017 Network Traffic Measurement and Analysis Conference (TMA). Piscataway: IEEE Press, 2017: 1-9.

[32] GOYAL P, GOYAL A. Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark[C]//Proceedings of the 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN). Piscataway: IEEE Press, 2017: 77-81.

[33] HOFSTEDE R, ČELEDA P, TRAMMELL B, et al. Flow monitoring explained: from packet capture to data analysis with Netflow and IPFIX[J]. IEEE Communications Surveys & Tutorials, 2014, 16(4): 2037-2064.

[34] UJJAN R M A, PERVEZ Z, DAHAL K, et al. Towards Sflow and adaptive polling sampling for deep learning based DDoS detection in SDN[J]. Future Generation Computer Systems, 2020, 111: 763-779.

[35] 王伟. 基于深度学习的网络流量分类及异常检测方法研究[D]. 合肥: 中国科学技术大学, 2018.
WANG W. Research on network traffic classification and anomaly detection method based on deep learning[D]. Hefei: University of Science and Technology of China, 2018.

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

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

[38] BADER O, LICHY A, HAJAJ C, et al. MalDIST: from encrypted traffic classification to malware traffic detection and classification[C]//Proceedings of the 2022 IEEE 19th Annual Consumer Communications &

Networking Conference (CCNC). Piscataway: IEEE Press, 2022: 527-533.

[39] 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. Piscataway: IEEE Press, 2016: 407-414.

[40] ZHANG H Z, YU L, XIAO X, et al. TFE-GNN: a temporal fusion encoder using graph neural networks for fine-grained encrypted traffic classification[C]//Proceedings of the ACM Web Conference 2023. New York: ACM Press, 2023: 2066-2075.

[41] ACETO G, CIUONZO D, MONTIERI A, et al. DISTILLER: encrypted traffic classification via multimodal multitask deep learning[J]. Journal of Network and Computer Applications, 2021, 183: 102985.

[42] ZHANG H Z, XIAO X, YU L, et al. One train for two tasks: an encrypted traffic classification framework using supervised contrastive learning[J]. arXiv Preprint, arXiv: 2402.07501, 2024.

[43] LASHKARI A H, GIL G D, MAMUN M S I, et al. Characterization of tor traffic using time based features[C]//Proceedings of the 3rd International Conference on Information Systems Security and Privacy. Piscataway: IEEE Press, 2017: 253-262.

[44] HAN X B, XU G Z, ZHANG M, et al. DE-GNN: dual embedding with graph neural network for fine-grained encrypted traffic classification [J]. Computer Networks, 2024, 245: 110372.

[45] LI Y, CHEN X S, TANG W Y, et al. Interaction matters: encrypted traffic classification via status-based interactive behavior graph[J]. Applied Soft Computing, 2024, 155: 111423.

[46] GARCÍA S, GRILL M, STIBOREK J, et al. An empirical comparison of botnet detection methods[J]. Computers & Security, 2014, 45: 100-123.

[47] HONG Y P, LI Q, YANG Y Q, et al. Graph based encrypted malicious traffic detection with hybrid analysis of multi-view features[J]. Information Sciences, 2023, 644: 119229.

[48] SHEKHAWAT A S, DI TROIA F, STAMP M. Feature analysis of encrypted malicious traffic[J]. Expert Systems with Applications, 2019, 125: 130-141.

[49] MUEHLSTEIN J, ZION Y, BAHUMI M, et al. Analyzing HTTPS encrypted traffic to identify user's operating system, browser and application[C]//Proceedings of the 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC). Piscataway: IEEE Press, 2017: 1-6.

[50] YANG Z J, LIN W. Unknown traffic identification based on deep adaptation networks[C]//Proceedings of the 2020 IEEE 45th LCN Symposium on Emerging Topics in Networking (LCN Symposium). Piscataway: IEEE Press, 2020: 10-18.

[51] REZAEI S, LIU X. How to achieve high classification accuracy with just a few labels: a semi-supervised approach using sampled packets[J]. arXiv Preprint, arXiv: 1812.09761, 2018.

[52] MOUSTAFA N, SLAY J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) [C]// Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS). Piscataway: IEEE Press, 2015: 1-6.

[53] SONG J M, WANG X J, HE M S, et al. CSK-CNN: network intrusion detection model based on two-layer convolution neural network for handling imbalanced dataset[J]. Information, 2023, 14(2): 130.

[54] DING Z X, ZHONG G Q, QIN X P, et al. MF-Net: multi-frequency intrusion detection network for Internet traffic data[J]. Pattern Recognition, 2024, 146: 109999.

[55] DHANABAL L, SHANTHARAJAH S P. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms[J]. International Journal of Advanced Research in Computer and Communication Engineering, 2015, 4(6): 446-452.

[56] LIU T T, FU Y, WANG K, et al. A multiscale approach for network intrusion detection based on variance–covariance subspace distance and EQL v2[J]. Computers & Security, 2025, 148: 104173.

[57] SHARAFALDIN I, HABIBI LASHKARI A, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Piscataway: IEEE Press, 2018: 108-116.

[58] WANG Z D, LI Z Y, HE D J, et al. A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning[J]. Expert Systems with Applications, 2022, 206: 117671.

[59] DIAO Z L, XIE G G, WANG X, et al. EC-GCN: a encrypted traffic classification framework based on multi-scale graph convolution networks[J]. Computer Networks, 2023, 224: 109614.

[60] YUN X C, WANG Y P, ZHANG Y Z, et al. Encrypted TLS traffic classification on cloud platforms[J]. IEEE/ACM Transactions on Networking, 2023, 31(1): 164-177.

[61] 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.

[62] HASIBI R, SHOKRI M, DEHGHAN M. Augmentation scheme for dealing with imbalanced network traffic classification using deep learning[J]. arXiv Preprint, arXiv: 1901.00204, 2019.

[63] WANG P, LI S H, YE F, et al. PacketCGAN: exploratory study of class imbalance for encrypted traffic classification using CGAN[C]//Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-7.

[64] VU L, BUI C T, NGUYEN Q U, et al. A deep learning based method for handling imbalanced problem in network traffic classification[C]// Proceedings of the 8th International Symposium on Information and Communication Technology. New York: ACM Press, 2017: 333-339.

[65] ZHU S Z, XU X L, GAO H H, et al. CMTSNN: a deep learning model for multiclassification of abnormal and encrypted traffic of Internet of Things[J]. IEEE Internet of Things Journal, 2023, 10(13): 11773-11791.

[66] TELIKANI A, GANDOMI A H, CHOO K R, et al. A cost-sensitive deep learning-based approach for network traffic classification[J]. IEEE Transactions on Network and Service Management, 2022, 19(1): 661-670.

[67] ZHOU N, WANG Q, ZHOU J X. IoT unbalanced traffic classification system based on Focal_Attention_LSTM[C]//Proceedings of the 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Piscataway: IEEE Press, 2021: 899-903.

[68] XU L Y, ZHOU X, LIN X F, et al. A new loss function for traffic classification task on dramatic imbalanced datasets[C]//Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications

(ICC). Piscataway: IEEE Press, 2020: 1-7.

[69] MCGREW D, ANDERSON B. Enhanced telemetry for encrypted threat analytics[C]//Proceedings of the 2016 IEEE 24th International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2016: 1-6.

[70] 秦鸣乐. 基于TLS的恶意加密流量识别研究[D]. 乌鲁木齐: 新疆师范大学, 2022.
QIN M L. Research on identification of malicious encrypted traffic based on TLS[D]. Urumqi: Xinjiang Normal University, 2022.

[71] 姜鹏. APT攻击下的C&C加密信道网络行为分析与检测[D]. 上海: 上海师范大学, 2018.
JIANG P. Analysis and detection of network behavior of C&C encrypted channel under APT attack[D]. Shanghai: Shanghai Normal University, 2018.

[72] 霍跃华, 吴文昊, 赵法起, 等. 结合协同训练的多视图加密恶意流量检测方法[J]. 西安电子科技大学学报, 2023, 50(4): 139-147.
HUO Y H, WU W H, ZHAO F Q, et al. Multi-view encryption malicious traffic detection method combined with co-training[J]. Journal of Xidian University, 2023, 50(4): 139-147.

[73] 汪洋, 梁丁, 查志成, 等. 一种基于测速行为的VPN服务器节点识别[J]. 网络空间安全科学学报, 2023(3): 59-67.
WANG Y, LIANG D, ZHA Z C, et al. Traffic identification for VPN nodes based on velocity measurement behavior[J]. Journal of Cybersecurity, 2023(3): 59-67.

[74] AKBARI I, SALAHUDDIN M A, VEN L, et al. A look behind the curtain: traffic classification in an increasingly encrypted web[J]. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2021, 5(1): 1-26.

[75] LUXEMBURK J, TOMÁŠ Č. Fine-grained TLS services classification with reject option[J]. Computer Networks, 2023, 220: 109467.

[76] 周益旻, 刘方正, 王勇. 基于混合方法的IPSec VPN加密流量识别[J]. 计算机科学, 2021, 48(4): 295-302.
ZHOU Y M, LIU F Z, WANG Y. IPSec VPN encrypted traffic identification based on hybrid method[J]. Computer Science, 2021, 48(4): 295-302.

[77] CHEN Y G, ZANG T N, ZHANG Y Z, et al. Rethinking encrypted traffic classification: a multi-attribute associated fingerprint approach[C]//Proceedings of the 2019 IEEE 27th International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2019: 1-11.

[78] LIU J Y, ZENG Y Z, SHI J Y, et al. MalDetect: a structure of encrypted malware traffic detection[J]. Computers, Materials & Continua, 2019, 60(2): 721-739.

[79] YAO H P, LIU C, ZHANG P Y, et al. Identification of encrypted traffic through attention mechanism based long short term memory[J]. IEEE Transactions on Big Data, 2022, 8(1): 241-252.

[80] SHEN M, LIU Y T, ZHU L H, et al. Fine-grained webpage fingerprinting using only packet length information of encrypted traffic[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 2046-2059.

[81] 孙云霄, 李军, 王佰玲. 基于侧信道特征的IPSec VPN闭合性检测方法[J]. 计算机科学, 2023, 50(10): 308-314.
SUN Y X, LI J, WANG B L. IPSec VPN closure detection method based on side-channel features[J]. Computer Science, 2023, 50(10): 308-314.

[82] HE H J, LAI Y X, WANG Y P, et al. A data skew-based unknown traffic classification approach for TLS applications[J]. Future Generation Computer Systems, 2023, 138: 1-12.

[83] KOUMAR J, HYNEK K, ČEJKA T. Network traffic classification based on single flow time series analysis[C]//Proceedings of the 2023 19th International Conference on Network and Service Management (CNSM). Piscataway: IEEE Press, 2023: 1-7.

[84] LONG G, ZHANG Z X. Deep encrypted traffic detection: an anomaly detection framework for encryption traffic based on parallel automatic feature extraction[J]. Computational Intelligence and Neuroscience, 2023, 2023(1): 3316642.

[85] 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 the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 397-405.

[86] ZOU Z, GE J G, ZHENG H B, et al. Encrypted traffic classification with a convolutional long short-term memory neural network[C]//Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE Press, 2018: 329-334.

[87] MARÍN G, CAASAS P, CAPDEHOURAT G. Deepmal-deep learning models for malware traffic detection and classification[C]//Proceedings of the 3rd International Data Science Conference. Berlin: Springer, 2021: 105-112.

[88] 李郅琴, 杜建强, 聂斌, 等. 特征选择方法综述[J]. 计算机工程与应用, 2019, 55(24): 10-19.
LI Z Q, DU J Q, NIE B, et al. Summary of feature selection methods [J]. Computer Engineering and Applications, 2019, 55(24): 10-19.

[89] 刘涛涛, 付钰, 王坤, 等. 基于VAE-CWGAN和特征统计重要性融合的网络入侵检测方法[J]. 通信学报, 2024, 45(2): 54-67.
LIU T T, FU Y, WANG K, et al. Network intrusion detection method based on VAE-CWGAN and fusion of statistical importance of feature [J]. Journal on Communications, 2024, 45(2): 54-67.

[90] DONG Y N, CAO R L, ZHANG M. A multi-objective evolutionary algorithm for multimedia traffic classification[C]//Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE Press, 2019: 2804-2810.

[91] MANJU N, HARISH B S, et al. Ensemble feature selection and classification of Internet traffic using XGBoost classifier[J]. International Journal of Computer Network and Information Security, 2019, 11(7): 37-44.

[92] MCGAUGHEY D, SEMENIUK T, SMITH R, et al. A systematic approach of feature selection for encrypted network traffic classification [C]//Proceedings of the 2018 Annual IEEE International Systems Conference (SysCon). Piscataway: IEEE Press, 2018: 1-8.

[93] AL-GARADI M A, MOHAMED A, AL-ALI A K, et al. A survey of machine and deep learning methods for Internet of Things (IoT) security[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1646-1685.

[94] KOTSIOPOULOS T, SARIGIANNIDIS P, IOANNIDIS D, et al. Machine learning and deep learning in smart manufacturing: the smart grid paradigm[J]. Computer Science Review, 2021, 40: 100341.

[95] SHINDE P P, SHAH S. A review of machine learning and deep learning applications[C]//Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). Piscataway: IEEE Press, 2018: 1-6.

[96] XIN Y, KONG L S, LIU Z, et al. Machine learning and deep learning methods for cybersecurity[J]. IEEE Access, 2018, 6: 35365-35381.

[97] HULAYYIL S B, LI S C, XU L D. Machine-learning-based vulnerability detection and classification in Internet of Things device security[J]. Electronics, 2023, 12(18): 3927.

[98] ALSHAMMARI R, ZINCIR-HEYWOOD A N. Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?[J]. Computer Networks, 2011, 55(6): 1326-1350.

[99] ZAKI F, AFIFI F, ABD RAZAK S, et al. GRAIN: Granular multi-label encrypted traffic classification using classifier chain[J]. Computer Networks, 2022, 213: 109084.

[100] HE Y Z, HU L P, GAO R. Detection of tor traffic hiding under Obfs4 protocol based on two-level filtering[C]//Proceedings of the 2019 2nd International Conference on Data Intelligence and Security (ICDIS). Piscataway: IEEE Press, 2019: 195-200.

[101] HAN S B, WU Q H, ZHANG H, et al. Light-weight unsupervised anomaly detection for encrypted malware traffic[C]//Proceedings of the 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2022: 206-213.

[102] GIJÓN C, TORIL M, SOLERA M, et al. Encrypted traffic classification based on unsupervised learning in cellular radio access networks [J]. IEEE Access, 2020, 8: 167252-167263.

[103] YANG L M, FU S J, LUO Y C, et al. A clustering method of encrypted video traffic based on levenshtein distance[C]//Proceedings of the 2021 17th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2021: 1-8.

[104] HE G F, YANG M, LUO J Z, et al. A novel application classification attack against Tor[J]. Concurrency and Computation: Practice and Experience, 2015, 27(18): 5640-5661.

[105] FU Y J, XIONG H, LU X J, et al. Service usage classification with encrypted Internet traffic in mobile messaging apps[J]. IEEE Transactions on Mobile Computing, 2016, 15(11): 2851-2864.

[106] NGUYEN A T, PARK M. Detection of DoH tunneling using semi-supervised learning method[C]//Proceedings of the 2022 International Conference on Information Networking (ICOIN). Piscataway: IEEE Press, 2022: 450-453.

[107] DOWLING S, SCHUKAT M, BARRETT E. Improving adaptive honeypot functionality with efficient reinforcement learning parameters for automated malware[J]. Journal of Cyber Security Technology, 2018, 2(2): 75-91.

[108] GUPTA A. VPN-nonVPN traffic classification using deep reinforced naive Bayes and fuzzy K-means clustering[C]//Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems Workshops (ICDCSW). Piscataway: IEEE Press, 2021: 1-6.

[109] ROOKARD C, KHOJANDI A. Applying deep reinforcement learning for detection of Internet-of- things cyber attacks[C]//Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC). Piscataway: IEEE Press, 2023: 389-395.

[110] XIE G R, LI Q, JIANG Y. Self-attentive deep learning method for online traffic classification and its interpretability[J]. Computer Networks, 2021, 196: 108267.

[111] LIN K D, XU X L, GAO H H. TSCRNN: a novel classification scheme of encrypted traffic based on flow spatiotemporal features for efficient management of IIoT[J]. Computer Networks, 2021, 190: 107974.

[112] DAI J B, XU X L, GAO H H, et al. CMFTC: cross modality fusion efficient multitask encrypt traffic classification in IIoT environment [J]. IEEE Transactions on Network Science and Engineering, 2023, 10(6): 3989-4009.

[113] AOUEDI O, PIAMRAT K, BAGADTHEY D. A semi-supervised stacked autoencoder approach for network traffic classification[C]// Proceedings of the 2020 IEEE 28th International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2020: 1-6.

[114] JIN Y L, FANG J, GAO Y. SSCMT-ETC: a semi-supervised contrastive mean teacher model for encrypted traffic classification[C]//Proceedings of the 2023 2nd International Conference on Sensing, Measurement, Communication and Internet of Things Technologies (SMC-IoT). Piscataway: IEEE Press, 2023: 127-133.

[115] CHEN R, LUO L L, WANG X D, et al. Knowing the unknowns: network traffic detection with open-set semi-supervised learning[J]. Computer Networks, 2024, 251: 110630.

[116] ILIYASU A S, DENG H F. Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks[J]. IEEE Access, 2019, 8: 118-126.

[117] WANG P, WANG Z X, YE F, et al. ByteSGAN: a semi-supervised generative adversarial network for encrypted traffic classification in SDN Edge Gateway[J]. Computer Networks, 2021, 200: 108535.

[118] 王攀, 陈雪娇. 基于堆栈式自动编码器的加密流量识别方法[J]. 计算机工程, 2018, 44(11): 140-147, 153.
WANG P, CHEN X J. SAE-based encrypted traffic identification method[J]. Computer Engineering, 2018, 44(11): 140-147, 153.

[119] LIN P, YE K J, HU Y S, et al. A novel multimodal deep learning framework for encrypted traffic classification[J]. IEEE/ACM Transactions on Networking, 2023, 31(3): 1369-1384.

[120] JANG Y, KIM N, LEE B D. Traffic classification using distributions of latent space in software-defined networks: an experimental evaluation[J]. Engineering Applications of Artificial Intelligence, 2023, 119: 105736.

[121] BOPPANA T K, BAGADE P. GAN-AE: an unsupervised intrusion detection system for MQTT networks[J]. Engineering Applications of Artificial Intelligence, 2023, 119: 105805.

[122] DE CARVALHO BERTOLI G, ALVES PEREIRA L Jr, SAOTOME O, et al. Generalizing intrusion detection for heterogeneous networks: a stacked-unsupervised federated learning approach[J]. Computers & Security, 2023, 127: 103106.

[123] 蒋兴翔. 基于流量的Web攻击失陷检测与分类技术研究[D]. 南京: 东南大学, 2023.
JIANG X X. Research on detection and classification of web attacks based on traffic[D]. Nanjing: Southeast University, 2023.

[124] SHEN M, LIU Y T, ZHU L H, et al. Optimizing feature selection for efficient encrypted traffic classification: a systematic approach[J]. IEEE Network, 2020, 34(4): 20-27.

[125] LU J, LIU A J, DONG F, et al. Learning under concept drift: a review [J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(12): 2346-2363.

[126] CHENG J, WU Y L, YUEPENG E, et al. MATEC: a lightweight neural network for online encrypted traffic classification[J]. Computer Networks, 2021, 199: 108472.

[127] ABBASI M, SHAHRAKI A, TAHERKORDI A. Deep learning for network traffic monitoring and analysis (NTMA): a survey[J]. Computer Communications, 2021, 170: 19-41.

[128] 仝鑫, 杨莹, 索奇伟, 等. 基于机器学习的加密流量分析方法综述[J]. 集成技术, 2024, 13(5): 74-92.
TONG X, YANG Y, SUO Q W, et al. A review of encrypted traffic analysis methods based on machine learning[J]. Integrated Technology, 2024, 13(5): 74-92.

[129] 严如强, 周峥, 杨远贵, 等. 可解释人工智能在工业智能诊断中的挑战和机遇:归因解释[J]. 机械工程学报, 2024, 60(12): 21-40.
YAN R Q, ZHOU ZH, YANG Y G, et al. Challenges and opportunities of explainable artificial intelligence in industrial smart diagnosis: attributional explanation[J]. Journal of Mechanical Engineering, 2024, 60(12): 21-40.

[130] 陈彩华, 余程熙, 王庆阳. 可信机器学习综述[J]. 工业工程, 2024, 27(2): 14-26.
CHEN C H, SHE C X, WANG Q Y. A review of trustworthy machine learning[J]. Industrial Engineering Journal, 2024, 27(2): 14-26.

[作者简介]

付钰（1982– ），女，湖北武汉人，博士，海军工程大学教授、博士生导师，主要研究方向为信息安全、人工智能。

刘涛涛（1996– ），男，江西吉安人，海军工程大学博士生，主要研究方向为人工智能、信息处理、网络安全。

王坤（1981– ），女，河南信阳人，海军工程大学博士生，信阳职业技术学院副教授，主要研究方向为信息安全、人工智能。

俞艺涵（1992– ），男，浙江金华人，博士，海军工程大学讲师，主要研究方向为隐私保护、信息安全。