基于机器学习的加密流量分析方法综述

仝鑫[1]，杨莹[2*]，索奇伟[1]，王志宏[2]，
[1]（中国人民公安大学，北京 100038）
[2]（公安部第三研究所，上海 200120）

摘要：随着互联网技术的快速发展，网络安全问题日益突出，其中加密流量的识别与分类成为了一个重要的研究方向。本文对当前基于机器学习的加密流量分类技术进行了全面的综述。首先，按分层的视角简要介绍了常见的加密协议及特点。接着，对该领域的数据集和评估指标进行了概览。在此基础上，对基于传统机器学习的加密流量分析方法和基于深度学习的方法进行了讨论，对其中的特征工程、分类器模型等关键技术进行了分析。最后，总结了目前该领域面临的可解释性不足、对抗样本风险等挑战，并对未来的可解释性加强、自动化特征和模型结构优化等研究方向进行了展望。

关键词 加密流量；机器学习；深度学习；特征工程
中图分类号：TP393.08 **文献标志码** A doi：10.12146/j.issn.2095-3135.20240130001

A Survey of Machine Learning-Based Encrypted Traffic Analysis Methods

TONG Xin[1], YANG Ying[2*], SUO Qiwei[1], WANG Zhihong[2]

[1] (People's Public Security University of China, Beijing, 100038, China)
[2](The Third Research Institute of the Ministry of Public Security, Shanghai, 200120, China)
Corresponding Author: yangying@mcst.org.cn

Abstract: With the rapid development of Internet technology, network security issues have become increasingly prominent. Among these, the identification and classification of encrypted traffic have emerged as significant research directions. This paper provides a comprehensive review of current machine learning-based techniques for encrypted traffic classification. First, it briefly introduces common encryption protocols and their characteristics from a layered perspective. Then, it provides an overview of the datasets and evaluation metrics used in this field. Based on this foundation, it discusses both traditional machine learning methods and deep learning methods for encrypted traffic analysis, with a focus on key techniques such as feature engineering and classifier models. Finally, it summarizes the challenges currently faced in this field, including the lack of interpretability and the risk of adversarial examples, and looks ahead to future research directions aimed at enhancing interpretability, automating feature extraction, and optimizing model structures.

Key words: encrypted traffic; machine learning; deep learning; feature engineering
Funding: This study is supported by the General Project for Research in Humanities and Social Sciences in Universities of Henan Province (2024-ZZJH-290), Basic Research Program for Science and Technology Strengthening Police Force of the Ministry of Public Security

来稿日期：2024-01-30 修回日期：2024-06-21
基金项目：河南省高校人文社会科学一般项目(2024-ZZJH-290)，公安部科技强警基础工作计划(2023JC21)，河南警察学院科研项目(HNJY-2023-42)
作者简介：仝鑫，博士研究生，研究方向为网络空间安全；杨莹（通讯作者），副研究员，研究方向为网络流量分析，E-mail：yangying@mcst.org.cn；索奇伟，讲师，研究方向为英语；王志宏，助理研究员，研究方向为网络空间安全。

(2023JC21), and Research Project of Henan Police College (HNJY-2023-42).

1 引言

随着数字化时代的来临，数据传输的安全性和隐私保护变得越来越重要，网络通信中的流量加密技术已成为用户隐私和数据安全的重要保护手段。在社交媒体互、在线购物以及金融交易场景中，用户的个人信息和敏感数据都以加密的形式在互联网上传输。然而，加密流量技术的发展也为网络安全领域带来了前所未有的挑战。越来越多的黑客和恶意用户正利用加密通信来掩盖其恶意活动，导致传统的基于特定的特征或规则的技术以及基于人工的分析方法难以应对复杂多变的网络环境。因此，探索面向加密流量的智能化和自动化分析方法的研究和应用变得至关重要。

近年来，机器学习和深度学习方法的兴起为加密流量分析提供了新的解决方案。因此，为帮助相关领域研究人员了解这些机器学习方法，本文对基于机器学习的加密流量分析技术进行了综述。具体来说，本文的贡献包括：

（1）对包括 HTTPS、TLS、SSH 和 Tor 等在内的常见加密流量协议和工具进行了概述，同时对数据集和评估指标进行了总结，为读者提供了一个全面的背景知识。

（2）本文详细探讨了基于统计机器学习和深度学习的加密流量检测方法，为读者提供了多种可参考的技术来处理不同类型和不同任务场景的加密流量。

（3）讨论加密流量分析领域的挑战，如可解释性不足、对抗样本攻击等问题。同时，对未来可能的研究方向进行展望，便于后续进一步开展研究工作。

2 常见加密协议概述

在网络通信中，加密协议广泛应用于不同的网络层，以确保数据的保密性和完整性。本节以 TCP/IP 协议的分层体系为分类依据，讨论了常见的加密协议，主要涵盖了网络层加密、传输层加密和应用层的加密技术，如图 1 所示。

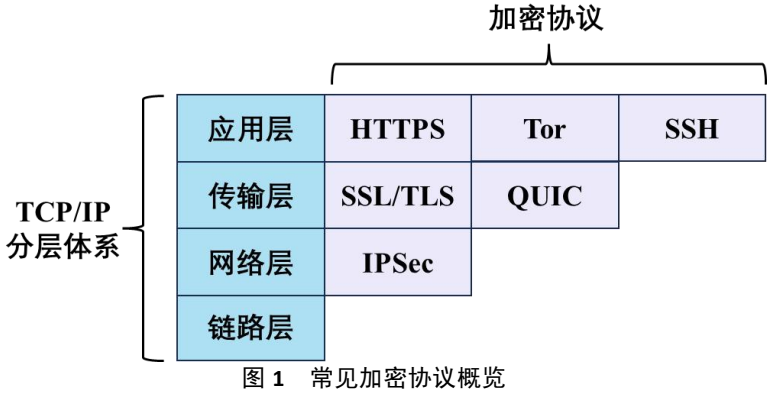

图 1　常见加密协议概览

Fig. 1　Overview of Common Encryption Protocols.

2.1 网络层加密协议

IPSec（Internet Protocol Security）是一种网络层安全协议，用于在 IP 网络上进行安全通信。它提供了一套完整的、集成的安全解决方案，包括加密和认证机制，以保护数据在传输过程中的机密性和完整性。IPSec 主要通过两种协议实现其功能：AH（Authentication Header）和 ESP（Encapsulating Security Payload）。通过这两个协议，IPSec 可实现以传输模式和隧道模式的封装形式两种在两个设备之间建立一条传输隧道，数据通过 IPSec 隧道进行传输，最终实现保护数据的安全性。

AH 协议提供无连接的数据源认证和完整性保护，而不提供具体的加密功能。该协议会在数据包中添加一个 AH 头，用于在接收方对数据包进行验证。AH 报文的结构如图 2 所示。其中，“下一头部”字段用于标识 AH 报文中载荷的类型。传输模式下，用于指明被保护

的上层协议类型（TCP 或 UDP）或 ESP 协议的编号；在隧道模式下，具体指定是否为 IP 协议或 ESP 协议的编号。“安全参数索引”用于唯一标识 IPSec 安全关联（Security Association，SA），以描述对等实体间如何利用安全服务进行通信。“认证数据”为数据完整性验证提供支持，该字段包含数据完整性校验值 ICV（Integrity Check Value），用于接收方进行完整性校验。

图 2　AH 协议的报文结构

Fig. 2　The packet structure of the AH protocol.

ESP 协议则提供机密性和可选的源认证，它通过在数据包中添加一个 ESP 头来实现加密，同时也可以在接收方进行验证。ESP 协议的报文结构如图 3 所示。其中，“载荷数据”即为通过 IPSec 进行加密来安全传输的报文主体部分。

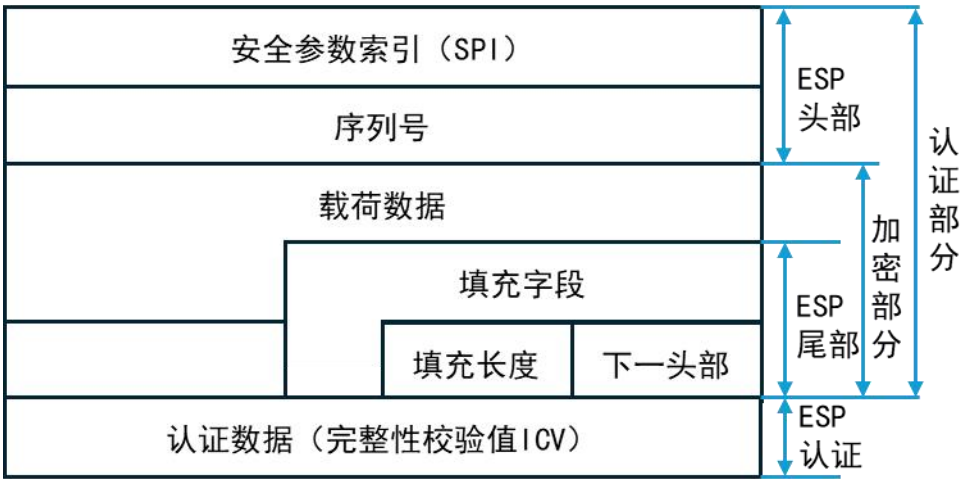

图 3　ESP 协议的报文结构

Fig. 3　The packet structure of the ESP protocol.

IPSec 可以在 IP 网络的任何地方进行配置，无论是端点、网关还是拨接隧道。它支持各种不同的加密算法，如 DES、3DES 和 AES 等，并提供了灵活的配置选项，以满足不同用户和环境的需求。得益于 IPSec 的安全性，通过解密数据的方式来对 IPSec 报文进行分析很难实现，如何在不解密传输报文的前提下对 IPSec 的功能、恶意性进行分析成为该领域的研究重点。

2.2 传输层加密协议

SSL（Secure Sockets Layer）和其继任者 TLS（Transport Layer Security）是最常见的传输层加密协议，用于在客户端和服务器之间建立安全的通信通道。SSL/TLS 提供了数据机密性、完整性和身份验证，使通信流量在传输过程中变得不可读以防止中间人攻击和窃听。从细节来看，SSL/TLS 协议内部也是基于分层架构设计。上层协议包含 4 种子协议，分别是：握手协议（Handshake Protocal）、警报协议（Alert Protocol）、应用数据协议（Application Protocol）及改变密码规范协议(Change cipher spec protocol)。

其中握手协议是该层最核心的协议，主要用于实现在进行安全传输之前必要的身份鉴别和安全参数协商。下层为记录协议（TLS Record Layer），为 TLS 上层子协议为传送提供分片、消息加密及加密后传输等功能，同时对接收到的数据进行验证、解密、重新组装，然后提交给高层的应用层。整个 SSL/TLS 协议栈的报文结构如图 4 所示，两层组合起来实现完整的协议功能。当前，SSL/TLS 广泛用于保护网页、电子邮件、即时消息和其他互联网通信。因此，针对 SSL/TLS 协议的有效分析对于后续研究基于该协议的 HTTPS 等上层网络协议具有积极意义。

图 4　SSL/TLS 协议栈的报文结构

Fig.4　The packet structure of the SSL/TLS protocol stack.

QUIC（Quick UDP Internet Connections）[1]是一种传输层加密协议，旨在提供更快的互联网连接。QUIC 融合了包括 TCP、TLS、HTTP/2.0 等协议的特性，但是基于 UDP 传输。该协议具有低延迟和高度安全性，避免 HTTP/2.0 的线头阻塞（Head-of-Line Blocking）问题。它采用 TLS 1.3 进行加密，支持前向错误纠正，以确保在网络不稳定的情况下仍能保持连接。QUIC 已经在许多大型互联网公司的服务中得到广泛采用，以提供更好的性能和隐私保护。QUIC 协议的报文结构如图 5 所示，头部数据以明文方式传输，主要描述了基本的协议版本和传输标记信息。数据部以加密形式传输，并提供了分片传输服务。当前，Google 超过 50%的请求基于 QUIC 协议，Youtube 也有 20%的流量来自 QUIC，微博移动端全面支持 QUIC 协议。因此，针对 QUIC 协议的自动化分析方法对于研判用户在此类平台上的行为等任务能够提供高效的技术支撑

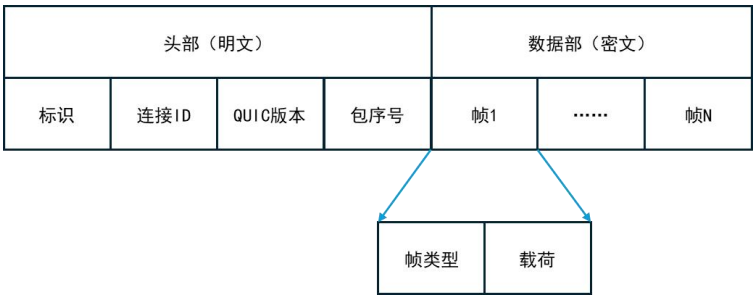

图 5　QUIC 协议的报文结构

Fig.5　The packet structure of the QUIC protocol.

2.3 应用层加密协议

Tor（The Onion Router）[2]是一种用于保护网络用户隐私和匿名性的开放源代码协议和软件，常被应用于访问“暗网”等场景中。它通过将网络通信路由通过多个随机选择的中间节点来隐藏用户的真实 IP 地址和身份，从而保护用户免受网络监视和追踪，其报文传输流程如图 6 所示。具体来说，每个通过 Tor 网络的访问流量在传输时都会被三个 Tor 节点处理：入口节点、中继节点和出口节点，数据在传输过程中会被进行加密和混淆，每

个节点只能解开一层加密以提升数据的匿名性。同时每个中继都只知道前一个和后一个中继，而不知道通信的起始点和目的地。这种模式可以防止中间节点嗅探数据，有效避免用户的真实网络地址和身份信息被追踪。由于当前基于 Tor 的“暗网”已经成为了滋生各类违法犯罪行为的温床，如何针对 Tor 数据进行有效分析对正成为维护网络安全和公共安全的重中之重。

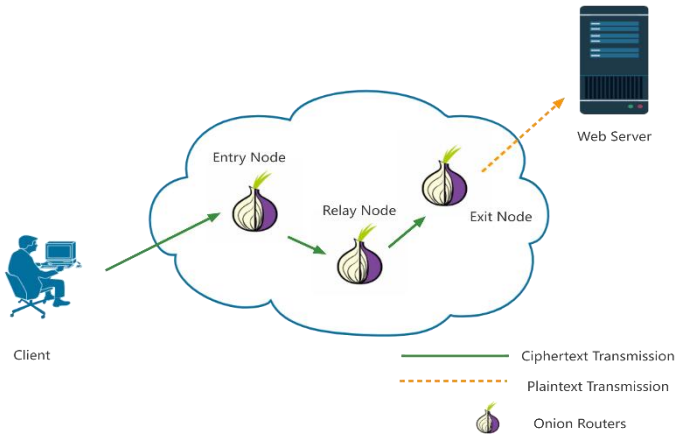

图 6　基于 Tor 协议的网络加密流量传输过程

Fig. 6　Network Encryption Traffic Transmission Process Based on the Tor Protocol.

HTTPS（Hypertext Transfer Protocol Secure）是一种用于在互联网上安全传输数据的通信协议。它是 HTTP 的安全版本，通过加密通信来保护数据的完整性和机密性。一方面，它使用 TLS/SSL 对数据进行加密。另一方面，HTTPS 通过数字证书验证服务器的身份。服务器拥有一个数字证书，由受信任的证书颁发机构（Certificate Authority，CA）签发。当客户端连接到服务器时，服务器会向客户端提供证书，客户端会基于非对称加密技术来验证证书的有效性和完整性。然后，进一步利用非对称加密方法来协商后续传输所用的对称密钥。最后，客户端和服务器后续传输的数据都通过对称密钥加密解密。此外，HTTPS 协议还使用消息认证码机制来验证数据的完整性。这意味着如果数据在传输过程中被篡改，接收方会检测到并拒绝接受已损坏的数据。

SSH（Secure Shell）是一种用于安全远程访问和数据传输的协议，旨在保护计算机网络中的数据传输的机密性和完整性。SSH 协议允许用户远程登录到远程计算机系统，并执行命令、传输文件以及管理远程系统，同时提供了强大的身份验证和加密机制。由于该协议的安全性和身份验证功能，SSH 被广泛用于企业、云计算环境以及个人用户之间的远程通信。为实现 SSH 的安全连接，服务器和客户端需要经历如图 7 所示的五个阶段，其中前三个阶段以明文传输方式实现，后两个阶段基于密文传输方式实现。

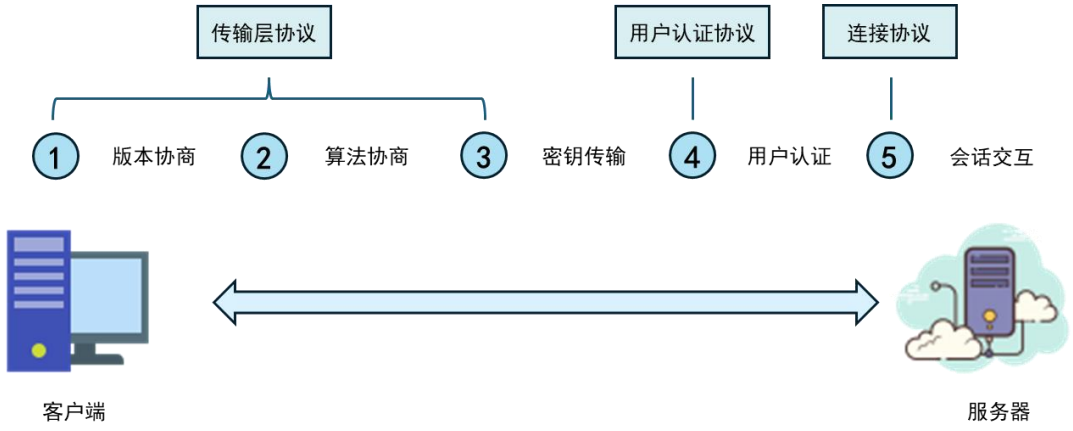

图 7　服务器和客户端使用 SSH 建立链接时的主要步骤

Fig.7 The main steps involved in establishing a connection between the server and the client using SSH.

分析上述协议可以发现，这些加密协议和工具能够在不同 TCP/IP 层为网络传输数据提供加密服务，使用户能够在互联网上进行安全的通信和数据传输。但同时各个协议的加密流程、报文格式也存在较大的差异，使得传统基于规则和人工的分析方法难以实时、精准地处理海量的网络流量，亟需探索智能化、自动化的解决方案。

3 数据集和评估指标

3.1 公开数据集

构建基于机器学习的加密流量分析系统时，需要高质量的标注数据做支撑，表 1 对目前该领域常用的代表性公开数据集进行了汇总。当前加密流量分析领域的数据集一部分针对 HTTPS、IPSec 等特定协议进行构建，以评估各类算法模型在分析相关协议的加密流量时的表现。另一部分则涵盖了多种类型的加密流量，用于评估模型在加密流量分析领域的通用性和泛化性。

表 1 加密流量分析领域常用公开数据集

Table 1 Common publicly available datasets in the field of encrypted traffic analysis.

名称	发布时间	规模/样本量	类别数量	简介
CICIDS2017[3]	2017	283K	7	用于恶意流量分析的数据集，包括基于 HTTP、HTTPS、FTP、SSH 和电子邮件协议在内的多种类型的流量数据。
ISCXTor2016[4]	2016	20GB	7	用于 Tor 流量分析。数据集包含来自超过 18 种代表性应用程序（例如 facebook，skype，spotify，gmail 等）的 8 种类型的流量。
ISCXVPN2016[5]	2016	28GB	14	用于对基于 IPSec 协议的 VPN 流量进行分析，该数据集有 14 种原始流量数据，7 种常规的加密流量和 7 种 VPN 协议封装的流量。
CIRA-CIC-DoHBrw-2020[6]	2020	1167K	3	用于分析基于 HTTPS 协议的 DoH 流量的数据集，包含 3 个类型，分别是良性 DoH 流量、恶意 DoH 流量和非 DoH 流量，各类别样本分布不均匀。
CIC-Darknet2020[7]	2020	158K	8	包含了常规流量和暗网流量，暗网流量包含了基于 Tor 和 VPN 的流量，同时每种流量包含了 8 种类型的应用。
QUIC dataset[8]	2018	6672	5	用于流量应用分类的 QUIC 流量数据集，主要包含 Google Drive、Youtube、Google Docs、Google Search 和 Google Music 在内 5 种类别的流量，并且在流量搜集时使用了 windows、ubuntu 等多个版本的系统。
CESNET-QUIC22[9]	2022	89GB	102	该数据集包含在 ISP 骨干网络中收集的一个月的 QUIC 流量，该网络连接了 500 个大型机构，为大约五十万人提供服务。数据涵盖了各种 Web 浏览器、操作系统、移动设备和台式计算机的网络流量的真实特征
SJTU-AN21[10]	2021	36K	10	用于匿名网络流量分析的数据集，包含了 3 种类型的流量，分别是 Tor、I2P 和 JonDonym。每种类型中又涵盖了多种应用传输的流量，共有 10 种应用类型。

其中，CICIDS2017、ISCXTor2016、ISCXVPN2016 和 CIRA-CIC-DoHBrw-2020 都是由加拿大网络安全研究所发布的经典的公开流量数据集，CIC-Darknet2020 则是该机构将 ISCXTor2016 和 ISCXVPN2016 数据集进行过滤和混合后得到的数据。这些数据集同时提供了原始流量数据包（PCAP 文件）以及处理好的结构化特征文件（CSV 文件），具备良好的易用性，可被应用于特征工程、分类模型等多种研究场景，因此吸引了大量研究人员基于这些数据开展加密流量分析研究。目前，最先进的方法在 CICIDS2017、ISCXTor2016、

ISCXVPN2016、CIRA-CIC-DoHBrw-2020 和 CIC-Darknet2020 这五个数据集上的多分类准确率分别达到了 99.99%[11]、99.90%[12]、99.96%[13]、100%[14]和 99.06%[15]。

QUIC dataset 和 CESNET-QUIC22 是用于分析 QUIC 数据包的常用公开数据集。前者由加州大学戴维斯分校的研究人员构建，数据量和类别数量都比较有限。当前在该数据集上的最优方法的准确率可以达到 99.40%[16]。CESNET-QUIC22 是由 CESNET 协会搜集并构建的大规模 QUIC 数据集，除了更大的规模和更多的类别标签外，该数据集还具有较长的时间跨度，可用于支持研究数据分布漂移等任务。尽管数据规模较大，但目前基于机器学习的方法已经能够在该数据集上达到了 99.95%的分类准确率[17]。

SJTU-AN21 是由上海交通大学开源的匿名网络流量数据集，除了 Chat、FTP、Streaming 等常见应用的流量，该数据集还涵盖了 BitTorrent、Eepsites 等服务的流量，可用于支持粗粒度和细粒度的网络流量分类研究。出于安全和隐私考虑，该数据集仅提供了处理后的特征文件，而不开放原始流量 PCAP 文件。该数据集相比上述数据集的分类难度更加困难，目前最优方法的分类准确率为 94.76%[13]。

目前，主流的研究通常用分类模型完成加密流量分析任务，因此，一些用于评估分类效果的指标常被用于评估该领域方法的有效性。具体来说，常见的评估指标有：

（1）准确率（Accuracy）：模型正确预测的样本数量与总样本数量之比，通常用于衡量模型整体性能。但对于不平衡数据集，准确率可能会失效。原理如公式（1）所示。

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

（2）查准率（Precision）：模型预测为正类别的样本中，实际为正类别的比例。它用于衡量模型的精确性，即模型不会错误地将负类别样本预测为正类别。原理如公式（2）所示。

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

（3）查全率（Recall）：查全率是指模型正确预测为正类别的样本数量与实际正类别样本数量之比。它衡量了模型识别正类别样本的能力，即模型不会遗漏正类别。原理如公式（3）所示。

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

（4）F1 度量（F1 Score）：F1 度量是查准率和查全率的调和平均值，它综合考虑了模型的精确性和召回率。它在不平衡数据集中通常比准确率更有意义。原理如公式（4）所示。

$$\text{F1} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \tag{4}$$

（5）特异度 Specificity：也被称作真负率，指正确预测为负类占所有真实负类的比例，常用于以识别负类为核心的评估任务，如恶意加密流量识别。原理如公式（5）所示。

$$\text{Specificity} = \frac{TN}{TN + FP} \tag{5}$$

（6）阴性预测值（Negative Predictive Value，NPV）：指正确预测为负类的样本数占所有预测为负类的样本数的比例。原理如公式（6）所示。

$$\mathrm{NPV}=\frac{TN}{TN+FN} \quad (5)$$

除了上述的评估指标外，一些图和表能够以动态的形式更加直观地呈现模型的分类效果，包括混淆矩阵、ROC 曲线（Receiver Operating Characteristic Curve）和 PR 曲线（Precision-Recall Curve）等。

4 基于统计机器学习的分析方法

4.1 特征工程

通常从互联网中捕获的原始流量都是以 PCAP 或 PCAPNG 格式进行存储，这些文件复杂化、非结构化和变长化等特点，无法直接被输入到机器学习模型中进行训练和预测，因此需要特征工程处理。特征工程是机器学习中至关重要的一步，它涉及到从原始流量包中提取、选择和构建特征，并转化为数值或分类特征等过程，以便让机器学习算法能够更好地理解和分辨不同的加密流量。目前，主流特征工程主要分为两类方法：一类是与网络协议无关的特征工程方法，另一类是面向特定协议的特征提取技术。

4.1.1 协议无关的特征工程

对于网络协议无关的特征工程方法，旨在通过提取通用特征来实现流量分类而不受具体协议专有特征的限制。早期的研究主要关注孤立的流量数据包的分析。代表性的工作是 Alshammari[18]提出的一种基于机器学习的加密流量分析方法，该方法仅使用简单的数据包标头特征集和统计流特征集，而不使用任何和 IP 地址、源/目标端口和有效负载相关的特征作为输入，能够针对 SSH 等协议的加密流量实现较高精度的流量分类，证明了协议无关特征用于加密流量分析的可行性。考虑到网络数据包具有变长特性，并不是所有的字段都对分析任务具有贡献，一些冗余特征还可能会对分类任务的效果和效率带来负面影响。Al-Fayoumi[19]针对基于时间的流量特征进行了优化，利用皮尔逊相关和遗传算法进行特征筛选，最终使得每个数据包的检测时间缩短至一微秒，而准确率则仅下降了 2.37%，在实时的 VPN 加密流量分析任务中具备良好的应用价值。但这类基于相关系数或智能算法的方法主要用于已有特征间的相关性筛选，难以在原始流量包到特征向量转化的特征生成阶段发现新的特征间关联性。针对这一局限，后续的工作[20]提出了一种轻量化的加密流量特征工程。首先，使用滑动窗口来搜索 IP 数据包的头部关键特征，并通过优化算法动态地确定窗口大小。然后构建了一种名为“BITization”的特征编码方法实现字节数组的重采样，过程如图 8 所示。具体来说，BITization 包含四种不同的特征转换方法：BIT-1，BIT-2，BIT-4 和 BIT-8，这些方法能够将字节数组的每个元素转换为二进制，并将这些二进制特征编码为整数和按原始排列顺序进行组合。实验证明，通过该特征工程方法，后续机器学习分类模型在包含 VPN 在内的多种加密流量数据集上的准确率提升了约 14%的准确率。上述的工作主要聚焦于如何从原始流量中抽取有效的特征，但 Wei 等[21]研究发现在经过加密后，正常流量和恶意流量经过目前主流的特征工程处理后的特征差异性较小，导致各类机器学习模型在小规模、不平衡数据集上的检测率较低。为此他们提出了一种基于特征增强的恶意流量检测模型 FE-MTDM。该方法包括了特征分组和特征增强生成两个主要步骤：首先，根据高斯特征将包括偏度系数、平均值和标准差等在内原始特征划分为几个特征子组。然后，使用 k-means 算法对特征子组进行处理以得到聚类特征，最终实现了放大 CICIDS2017 等数据中正常流量与异常流量之间的差异，有效提高分类模型的性能。

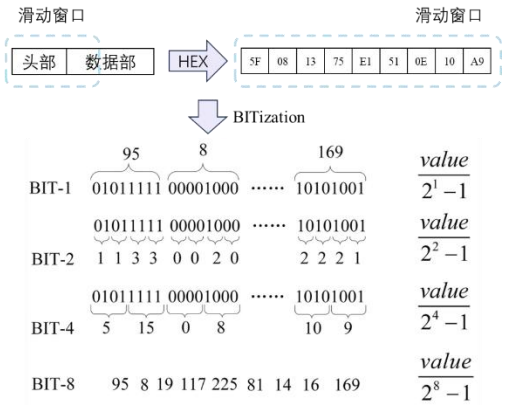

图 8　基于“BITization”的特征编码方法

Fig.8　Feature Encoding Method Based on “BITization”.

对于大多数建立连接的流量协议，综合分析发送和接收方的报文特征相比分析孤立的单独流量数据能够获取更丰富的特征。因此，一系列研究聚焦于分析由多个流量包组成的会话，例如将双向加密流量中数据包大小的平均值、方差、最大值、最小值等统计性特征作为机器学习模型的输入[22]。为了更有效地提取双向加密流量的宏观和微观特征，Satrabhandhu[23]针对有监督的传统机器学习提出了一种双向流非零有效载荷流数据提取方案和双向流有效载荷比特征抽取方法，能够有效兼顾加密流量的局部特征和整个传输过程中的全局特征，最终在 ISCX VPN-NonVPN 数据集上取得了良好的实验效果。考虑到在一次会话中，用户和服务器之间通常存在多轮的交互流量，上述仅基于单轮往返流量的特征工程无法提供充分的交互信息，Xu[24]提出了一种具有路径签名的新型加密流量分类方法 ETC-PS。该方法首先使用会话数据包长度序列构造流量路径，以表示客户端和服务器之间的交互。然后，进行路径变换以抽取不同视角的特征。最终计算出多尺度路径签名作为训练机器学习分类器的输入特征，实现了高鲁棒的准确性和低训练开销，在检测 HTTPS、QUIC 和 IPSec 协议时均有良好的效果。

4.1.2 协议相关的特征工程

考虑到不同协议的加密流量往往展现出类型相关的独特特征，这些特征对构建机器学习模型至关重要。因此，针对特定协议的特征提取技术应运而生，这些技术深入挖掘协议的详细信息，以捕捉更精细的流量特征。例如，针对 TLS 协议，Weng[25]提出了 TLSmell 特征框架，利用“源 IP、目标 IP、目标端口和协议”四元组作为索引，从开源工具 Zeek 生成的 flowmeter.log、conn.log、ssl.log 和 X509.log 文件中进行特征聚合，然后手动提取了连接、TSL 和认证相关的 33 种特征作为分类依据，从而提高恶意加密流量检测的整体性能。另一方面，考虑到 HTTPS 是在 TLS 协议基础上建立的，Chen[26]引入了应用数据单元作为输入，并针对性地提出了应用层特征工程和特征筛选方法，结果证明能够有效提升后端机器学习或深度学习分类器的表现，并且所提出的 ADU 特征在统计和长度序列特征上均优于仅使用 TLS 层的分段粒度特征，在与数据包粒度特征的比较中也具备优势。

4.2 分类模型

统计机器学习模型是面向加密流量分析的关键工具之一，这些分类模型的任务是将网络流量数据划分为不同的类别或标签，以帮助检测恶意活动、优化网络性能和提供安全保障。

4.2.1 基于独立模型的方法

早期的探索主要关注利用贝叶斯、支持向量机（Support Vector Machine,SVM）等单一机器学习模型来完成加密流量的分析，代表性研究包括：Tao[27]提出了一种基于权值朴素贝叶斯的恶意软件加密流量检测方法，该方法分为两个关键步骤：首先，利用基于特征泛化方法的指纹检测技术来识别恶意流量。其次，对于无法区分的指纹，利用目标主机信

息特征，结合加权贝叶斯来进一步判断流量的类别。Sun[28]提出了基于 SVM 的加密流量检测方法，并引入了增量训练技术，有效克服了传统流量识别方法需要反复从零训练的缺点。Zhioua [29] 提出了一种基于隐马尔可夫模型（Hidden Markov Model，HMM）的 Tor 流量分析模型，该模型可以检测目标 Tor 客户端与第一个 Tor 中继节点之间的本地网络流量。实验分析表明，该方法具有较高的精度（平均 93%）和 F1 分数（平均 75%）。这种方法也可以用来攻击 Tor 网络的隐私[30]。

4.2.2 基于集成学习的方法

集成学习是近年来统计机器学习领域的热点，这一类方法通过构建并组合多个学习器来解决单一预测问题的方法，可以有效提高整体的预测准确性和避免过拟合风险，因此在针对结构化的加密流量数据进行分析时具有优势。Gupta [31]构建了一个基于极端梯度提升算法的加密流量分类模型，在 VPN、Tor 和常规流量的三分类任务中具有较好的准确率，且能够有效处理样本类型分布不均衡的任务场景。后续的研究[12]构建了基于深度森林[32]的加密流量分析方法，并通过与信息增益和重排序特征优化方法相结合，不仅能够以较高的精度检测 Tor 流量，同时具备良好的识别速度。Afuwape 等人 [33]使用随机森林和梯度提升机构建了一个集成学习分类器，在区分 VPN 流量和非 VPN 流量的任务中实现了 93.80% 的分类准确率，优于 KNN、多层感知器和决策树等单一分类器。随后的研究[34]基于这项工作增加了一个决策树模型，将 VPN 流量的分类准确率提高了 0.6%。然而在集成学习中，通过人工经验决策融合多个学习器往往存在局限性，针对此，Isingizwe[35]引入了基于 AutoML 技术的加密流量分析方法，该方法能够有效融合 7 个具有代表性的模型，并实现了自动超参数调整和模型组装。此外，还能对特征贡献和模型贡献提供直观的解释。

此外，与上述基于分类模型的研究不同，Rao 等人[36]提出了一种用于 Tor 网络流量分析的引力聚类算法，该算法可以利用引力和相似度样本进行聚类，并且对数据标注的依赖远小于分类模型。实验表明，该方法的平均准确率和 F1 得分均超过 80%，而在同一数据集上训练的 K 均值算法的准确率仅达到 50%。

5 基于深度学习的分析方法

基于特征工程和传统机器学习的方法已经在许多加密流量分析实际应用中取得了显著的成效。然而，随着互联网流量的日益复杂和加密技术的不断发展，这些基于手工特征提取的方法在处理大量复杂数据时逐渐暴露出了一些局限性。例如，它们往往需要大量的领域知识进行特征工程，且在面对动态变化的网络环境时，模型的鲁棒性和适应性相对较弱。为了克服这些挑战，近年来深度学习技术得到了该领域的广泛关注和应用。深度学习模型通过自动提取特征，能够处理大量复杂的数据并从中挖掘深层次的模式，为加密流量分类提供了新的解决方案。目前，利用深度学习模型来分析加密流量的主流技术可划分为：基于图像特征和视觉模型的方法、基于序列特征和时序模型的方法、基于图特征和图神经网络的方法、基于生成对抗网络的方法和基于预训练模型的方法。

5.1 基于图像特征和视觉模型的方法

深度学习技术最早在计算机视觉领域被证明具备超越统计机器学习技术和媲美人类的性能，因此一些研究者尝试将加密流量转化为图像风格的特征，并基于此使用计算机视觉领域的相关模型进行处理。工作[37]提出了基于卷积神经网络（Convolutional Neural Networks，CNN）的加密流量分类模型。在该实验中，将原始的 VPN 和 Tor 加密流量数据直接转换为灰度图，其中每组字节对应一个像素，然后使用一维或二维卷积层来学习流量灰度图中的特定模式。最后，使用全连接层对从卷积层中提取的特征进行分类。这些方法的实验结果表明优于主流的浅层分类器。上述方法当遇到新类别的流量时，往往需要进行重新。为了克服这个问题，Ma[38]提出了一种基于 ResNet[39]的增量学习方法以实现扩展加密

流量分类算法。该方法能够在进行部分训练的情况下向模型中添加新类的特征，在检测 VPN 加密流量时取得了较好的效果。

5.2 基于序列特征和时序模型的方法

加密流量数据本质是一种数据流，因此具备时序特征，部分研究者尝试将自然语言处理和时间序列分析领域常用的长短期记忆网络（Long Short-Term Memory，LSTM）[40]和门控循环单元（Gated Recurrent Unit，GRU）[41]等时序模型应用于该领域。Liu[42]提出了 BGRUA 方法，该方法融合了双向 GRU 网络和注意力机制，在包含 HTTPS 加密流量在内的 3 个公开数据集的实验中准确性、精确度、召回率和 F1 分数方面均优于对比方法。Zhao[43]等研究发现现有的加密流量分析方法会受链路数据包丢失、重传和无序等现象的影响而导致误报，因此提出了 ERNN 模型，该模型在 LSTM 模型的基础上额外增加了“会话状态门”，如图 9 所示，使得模型能够更好地处理异常流量而降低误报。实验证明，当利用 ERNN 处理包含 16%的异常数据包序列时，仍然能够以 98.63%的准确率识别加密入侵流量。可解释性弱是目前制约深度学习模型在加密流量领域落地应用的主要难题，针对此，Song[44]提出了用于加密流量分类的增量可解释递归神经网络 I_2RNN。I_2 RNN 中引入了一种新的传播过程，能够从加密流量中更好提取序列指纹。同时，还提供了包括时间序列特征归因和类间相似性画像在内的可解释性分析机制。此外，与研究[38]类似，I_2 RNN 也能够以增量训练的方式处理新增类别样本。

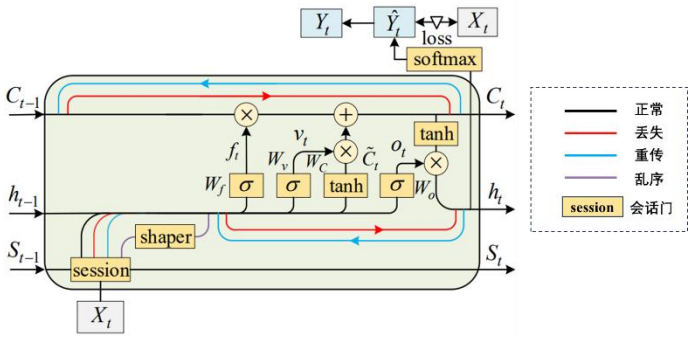

图 9　ERNN 模型在 LSTM 模型的基础上引入了“会话门”组件

Fig. 9　The ERNN model introduces a 'session gate' component based on the LSTM model.

5.3 基于图特征和图神经网络的方法

图神经网络（Graph Neural Networks，GNN）是一种专为处理图结构数据设计的神经网络模型。不同于传统的 CNN 等主要应用于规则的欧氏空间数据，图神经网络能够有效处理不规则的图结构数据，如社交网络、知识图谱等。由于加密流量的复杂性，传统的基于欧氏空间的特征提取方法可能无法有效揭示流量的本质属性。而通过图神经网络，能够将网络流建模为图，例如节点代表数据包或会话，边代表它们之间的关系，进而通过节点间的消息传递机制，学习到节点的高阶邻近信息和全局结构特征。Zhang[45]提出了一种基于逐点互信息的字节级流量图构建方法，基于此，构建了一种使用图神经网络进行特征提取的时间融合编码器模型 TFE-GNN，该模型同时接收 VPN、Tor 等流量头部和载荷部数据的图结构作为输入，并利用双塔 GraphSAGE[46]作为主干网络进行特征关联性计算和特征融合，最终使用多种分类模型进行特征分析，总体流程如图 10 所示，最终有效地提升了检测精度。为了保证构建的图结构具备稳定性和可迁移性，Diao[47]提出了一种基于多尺度图卷积神经网络的加密流量分析方法 EC-GCN，并利用元数据作为输入，可被用于多种网络协议的加密流量分析任务。

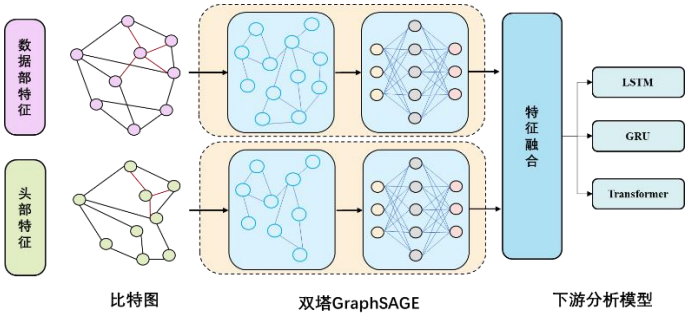

图 10　TFE-GNN 同时使用流量头部和载荷部作为模型输入并进行特征融合

Fig. 10　TFE-GNN simultaneously utilizes both traffic headers and payloads as model inputs and performs feature fusion.

5.4 基于生成对抗网络的方法

数据规模小和数据标注困难时训练加密流量分析模型的主要困难。而生成对抗网络（Generative Adversarial Nets，GAN）由两个相互竞争的神经网络组成：生成器（Generator）和判别器（Discriminator），它们在训练过程中相互博弈，以提升各自的性能。这种独特的结构使得 GAN 在生成逼真的数据样本方面表现出色，因此，一些研究尝试利用 GAN 以更好地理解加密流量的分布特性，并生成高质量的合成流量数据，从而用于训练更高效的检测模型。ByteSGAN[48]模型采用交替训练判别器和生成器的方式进行优化，能够在只能使用少量标注流量样本和大量无标记样本的前提下以半监督学习的方式进行训练，进而缓解数据不足难题，可有效分析 HTTPS、SSL、SSH 等多种类型的流量。PacketCGAN[49]利用条件 GAN 网络（Conditional Generative Adversarial Nets，CGAN）[50]的优势，实现了以应用程序类型的作为输入为条件生成网络层、传输层和应用层指定类别的流量样本，从而构建更加均衡的训练数据集，并且效果显著由于随机过采样和合成少数过采样技术等方法。

5.5 基于预训练模型的方法

在探讨了 GAN 的加密流量分析方法之后，本节将转向另一种高效利用现有资源的技术——基于预训练模型的方法。预训练模型是指在大量数据上预先训练好的深度学习模型，这些模型通常在大规模任务中取得了优异的性能，并且可以迁移到相关但不同的任务中。在加密流量分析领域，预训练模型提供了一种快速有效的方式来利用已有的知识和特征，从而避免了从零开始训练模型所需的大量计算资源和标注数据。通过微调（Fine-tuning）等技术，预训练模型可以被适配到特定的加密流量分析任务中，以提高模型的性能和泛化能力。文献[51]和文献[52]分别提出了 BFCN 和 TSFN 模型，在 BERT[53]预训练模型的基础上通过增加 CNN 网络和 LSTM 网络来更好地适配加密流量分析任务，实验效果均优于从零开始训练的对比方法。Kenton[54]提出了 PERT 方法，该方法参考了 BERT 模型的预训练过程，如图 11 所示，利用无标注的海量加密流量样本进行预训练，然后在 Android HTTPS 加密流量等下游分类任务中进行微调，相比直接加载文本预训练模型权重的方法有了更进一步的准确率提升。但上述方法的模型具有较大规模的参数量，使得模型很难被应用于实时性要求较高的场景中。Shin [55]等利用基于知识蒸馏的 DistilBERT[56]模型进行加密流量数据分析，并且对冗余特征进行了过滤，有效提升了检测效率。为了进一步提高加密流量分类的准确性，Wang[57]提出了一种基于深度学习的加密流量分类方法，将 CNN 和预训练的 Swin Transformer[58]的核心模块与加密流量分类模型相结合，实现加密流量应用类型的识别。该方法中，CNN 模块能够捕捉加密交通数据的局部空间信息特征。Swin-Transformer 的多头注意力机制可以捕获关于数据属性之间关联的全局信息。最终在 ISCX VPN non-VPN 加密数据集上取得了 96.7%的准确率。以 GPT 为代表的大语言模型（Large Language Models，

LLMs）得益于其海量的训练数据和庞大的模型参数，具备了良好的逻辑推理能力和世界知识，在多种下游任务中取得了良好的表现。基于 LLMs 微调得到的 NetGPT[59]、Lens[60]等模型不仅在在多个加密流量分析数据集上都取得了超越 BERT 等预训练模型的效果，而且可以用于流量数据生成等场景中，有效缓解了数据标注难题。

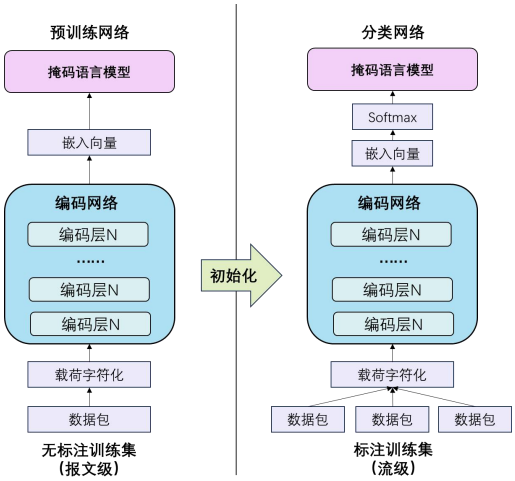

图 11　PERT 模型的预训练和下游微调流程

Fig. 11　The pre-training and downstream fine-tuning process of the PERT model.

此外，一些基于训练方式和特征的优化方法也被证明能够进一步提升加密流量分析的效果。基于多模态-多任务训练方法[61,62]能够帮助深度学习模型从不同的视角提取特征，进而缓解信息损失等问题。基于元学习的方法[63]能够降低模型对标记数据的依赖和实现自动化参数调优，在少样本场景中取得更高的准确率。

6 局限与展望

近年来，基于机器学习和深度学习的模型在加密流量分析领域取得了显著的进展，并展现出各自的独特性和优势。例如，传统机器学习模型以其高效的训练和推理能力、低资源消耗以及易于工程化实现的特点，在低资源和边缘计算设备上具有广泛的应用前景。相比之下，深度学习模型则凭借其强大的表征能力和卓越的分析效果，在高性能算力设备的支持下，适用于对实时性要求较低且精确度要求较高的流量分析任务。然而，将这些技术应用于实际场景仍然面临着诸多挑战。尽管部分问题已经找到了初步的解决方案和研究方向，但仍有关键难题受到算法和数据等因素的限制，难以在短期内得到有效解决。

6.1 部分解决的问题

高维数据问题在加密流量分析中尤为突出。高维数据容易引起过拟合、计算复杂度增加以及“维度灾难”等问题，导致许多传统机器学习算法的性能会显著下降。在面对高维数据时，目前主流的解决方案需要依赖复杂的特征选择和降维技术。特征选择是一种通过选择对模型性能最有贡献的特征来减少特征数量的方法。常见的特征选择方法包括过滤法（如卡方检验、互信息）、包裹法（如递归特征消除）和嵌入法（如 L1 正则化）。这些方法可以有效地降低数据维度，从而减少计算复杂度并提高模型的泛化能力。但特征选择过程本身需要额外的计算资源，而且有时会因为误判特征的重要性而导致信息丢失，影响模型的预测性能。降维技术通过将高维数据映射到低维空间来降低特征维度，代表性方法包括主成分分析、线性判别分析等。这些方法可以在保持数据结构的同时显著减少特征维度，但也存在局限性。例如主成分分析假设数据是线性可分的，这可能与复杂的流量数据并不完全契合。此外，降维过程中的信息压缩可能导致丢失信息，从而影响模型的精度。因此，这些技术虽然可以在一定程度上缓解维度问题，但仍存在不可忽视的缺陷。

深度学习模型在加密流量分析中表现出了强大的能力，但其高昂的硬件成本和运行效

率问题仍然是一个重要的挑战。近年来，研究人员提出了一系列解决方案来缓解这些问题。包括通过模型量化和剪枝技术、知识蒸馏等减少模型参数量和计算量，从而降低硬件需求。同时，迁移学习和少样本学习技术的应用也使得在数据有限的情况下能够训练出性能良好的模型。这些精简后的模型虽然在一定程度上降低了硬件需求，但其效率仍显著低于基于传统机器学习的方法，在实时处理和在线检测场景中的表现仍不尽如人意。

可靠性和鲁棒性是阻碍相关模型落地的另一大关键因素。研究表明，即使是性能优越的加密流量分析模型也面临着潜在的对抗样本攻击风险[64]，即攻击者通过对加密流量数据添加微小的噪声，就能达到欺骗分析模型的目的，导致模型的存在应用风险。为了提高机器学习和深度学习模型的鲁棒性，研究人员提出了对抗训练、防御性检测等多种防御对策。这些方法在提升模型鲁棒性的同时可能会增加漏报和误报，还可能带来额外的计算开销和复杂性。

6.2 短期内难以解决的问题

传统机器学习方法在加密流量分析中高度依赖手动选择和构造特征。但加密流量数据具有其独特的复杂性和非线性特征，使得研究人员很难通过直觉和经验来选择有效的特征，最终导致难以捕捉到数据中的关键特征。另一方面，手动构造特征往往具有一定的主观性，不同的研究人员可能会得出不同的特征集合，进一步增加了加密流量分析的复杂性并影响方法的泛化性。

传统机器学习模型的参数数量有限，导致其表征能力通常不足并难以充分捕捉加密流量数据中的复杂模式和特征。虽然在小规模数据集上这些模型的收敛速度较快，但大规模数据集包含更多的多样性和复杂性，导致传统模型难以通过有限的参数空间来充分表示这些信息，最终形成学习瓶颈问题。

深度学习模型通常被视为“黑盒”，其决策过程缺乏透明度和解释性，导致用于分析加密流量分析领域时无法为用户提供支持决策的相关说明。当前，尽管已有一些研究致力于提高模型的可解释性，但这些方法大多仍处于理论研究阶段，尚未成熟。同时，现有的可解释性技术在应用场景上存在受限的问题，相关方法主要针对自然语言处理和计算机视觉等具备人类数据可理解性的任务设计，很难被迁移至复杂和用户难以直观理解的加密流量数据上。因此，如何在保证深度学习模型高效性的同时，提高其解释性和透明度仍是亟待解决的问题。

6.3 展望

针对上述挑战，学术界和工业界在关注模型分析效果的同时，聚焦于加密流量分析技术的安全性、效率等指标对于促进该领域的进一步发展和技术落地具有积极意义。具体来说：

特征和模型优化：随着加密流量分析领域对精度要求的增长，未来研究可以探索更为高效的特征处理方法。例如通过自动化特征工程[65]、自动化模型参数和结构搜索[66]等技术发现并组合特征以及优化模型结构，在减少人工介入的前提下提升模型的泛化性。还可引入流形学习为代表的非线性降维方法和基于深度学习的端到端特征降维等技术，实现在不影响模型效果的同时更好地处理复杂的高维加密流量数据。此外，跨域和多模态学习方法[67]将通过整合不同网络层和其他数据源的信息，帮助开发出更全面和准确的加密流量分类系统。

安全和可解释性：加密流量分析模型在应用中的安全性[68]和可解释性[69]将成为研究的重点。通过建立全面的安全性评估指标和基准，研究人员可实现对模型潜在的对抗样本攻击等威胁进行有效地评估，在此基础上可开展针对性的安全加固以增强模型的鲁棒性。同时，利用 LLMs 等前沿技术辅助加密流量分析模型的决策归因对于提升可解释性具有积极意义。

软硬件结合优化：为了应对加密流量分析的高计算需求，工业界可通过设计专门的加密流量分析处理器或采用现有的FPGAs进行定制化优化等方法实现提高模型的处理速度和效率。在软件层面，可采用异步计算和分布式处理技术提高模型在实时环境中的处理速度和效率，使其更适用于实时监控和在线检测等应用场景。

7 总结

本文对基于机器学习和深度学习方法的加密流量分析技术进行了综述，在概览加密协议、数据集和评估指标的基础上，对领域经典和前沿的模型方法进行了分析和讨论。一方面，各类特征工程和分析模型不断发展和完善，在多种类型的加密流量任务中能够取得较高的准确率。另一方面，多数方法但仍面临着鲁棒性不足、可解释性弱和时间复杂度高等痛点。此外，现有研究主要在实验封闭环境中进行测评，相关方法在真实场景中针对丢包、重传等更复杂的网络环境的分析仍有待进一步验证。因此，在今后的研究中，研究者如何兼顾模型的效果、效率和安全性等多个指标，开展更加丰富合理的测评工作将是该领域的研究重点。

参考文献

[1] Langley A , Riddoch A , Wilk A ,et al.The QUIC Transport Protocol: Design and Internet-Scale Deployment[C]//ACM Special Interest Group on Data Communication.ACM, 2017.DOI:10.1145/3098822.3098842.

[2] DINGLEDINE, Roger, et al. Tor: The second-generation onion router. In: USENIX security symposium. 2004. p. 303-320.

[3] Sharafaldin I, Lashkari A H, 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. SCITEPRESS-Science and Technology Publications, 2018.

[4] Lashkari A H, Gil G D, Mamun M S I, et al. Characterization of tor traffic using time based features[C]//International Conference on Information Systems Security and Privacy. SciTePress, 2017, 2: 253-262.

[5] Draper-Gil G, Lashkari A H, Mamun M S I, et al. Characterization of encrypted and vpn traffic using time-related[C]//Proceedings of the 2nd international conference on information systems security and privacy (ICISSP). 2016: 407-414.

[6] MontazeriShatoori M, Davidson L, Kaur G, et al. Detection of doh tunnels using time-series classification of encrypted traffic[C]//2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). IEEE, 2020: 63-70.

[7] Habibi Lashkari A, Kaur G, Rahali A. Didarknet: A contemporary approach to detect and characterize the darknet traffic using deep image learning[C]//2020 the 10th international conference on communication and network security. 2020: 1-13.

[8] 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.

[9] LUXEMBURK, Jan, et al. CESNET-QUIC22: A large one-month QUIC network traffic dataset from backbone lines. Data in Brief, 2023, 46: 108888.

[10] Zhao R, Deng X, Wang Y, et al. Flow sequence-based anonymity network traffic identification with residual graph convolutional networks[C]//2022 IEEE/ACM 30th International Symposium on Quality of Service (IWQoS). IEEE, 2022: 1-10.

[11] HNAMTE, Vanlalruata, et al. A novel two-stage deep learning model for network intrusion detection: LSTM-AE. IEEE Access, 2023.

[12] 魏松杰,李成豪,沈浩桐,等.基于深度森林的网络匿名流量检测方法研究与应用[J].信息网络安全,2022,22(08):64-71.

[13] DENG, Xianwen; WANG, Yijun; XUE, Zhi. AN-Net: an Anti-Noise Network for Anonymous Traffic Classification. In: Proceedings of the ACM on Web Conference 2024. 2024. p. 4417-4428.

[14] ABU AL-HAIJA, Qasem; ALOHALY, Manar; ODEH, Ammar. A lightweight double-stage scheme to identify malicious DNS over HTTPS traffic using a hybrid learning approach. Sensors, 2023, 23.7: 3489.

[15] ZHU, Yuehao, et al. DGNN: Accurate Darknet Application Classification Adopting Attention Graph Neural Network. IEEE Transactions on Network and Service Management, 2023.

[16] ALMUHAMMADI, Sultan; ALNAJIM, Abdullatif; AYUB, Mohammed. QUIC Network traffic classification using ensemble machine learning techniques. Applied Sciences, 2023, 13.8: 4725.

[17] BAI, Lirong; TANG, Zhengzhi. QUIC Traffic Classification Based on Multi-Feature Fusion. In: 2024 7th World Conference on Computing and Communication Technologies (WCCCT). IEEE, 2024. p. 204-209.

[18] 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.

[19] Al-Fayoumi M, Al-Fawa'reh M, Nashwan S. VPN and Non-VPN Network Traffic Classification Using Time-Related Features[J]. Computers, Materials & Continua, 2022, 72(2).

[20] Luo P, Chu J, Yang G. IP packet-level encrypted traffic classification using machine learning with a light weight feature engineering method[J]. Journal of Information Security and Applications, 2023, 75: 103519.

[21] Wei N, Yin L, Zhou X, et al. A feature enhancement-based model for the malicious traffic detection with small-scale imbalanced dataset[J]. Information Sciences, 2023, 647: 119512.

[22] Zhang Q, Su C J. Application-layer Characterization and Traffic Analysis for Encrypted QUIC Transport Protocol[C]//2023 IEEE Conference on Communications and Network Security (CNS). IEEE, 2023: 1-9.

[23] Satrabhandhu W, Tritilanunt S. Encrypted Traffic characterization using None Zero payload and Payload Ratio Characteristics[C]//2021 25th International Computer Science and Engineering Conference (ICSEC). IEEE, 2021: 63-69.

[24] Xu S J, Geng G G, et al. Seeing traffic paths: encrypted traffic classification with path signature features[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2166-2181.

[25] Weng Z, Chen T, Zhu T, et al. TLSmell: Direct Identification on Malicious HTTPs Encryption Traffic with Simple Connection-Specific Indicators[J]. Comput. Syst. Sci. Eng., 2021, 37(1):

105-119.

[26] Chen Z, Cheng G, Wei Z, et al. Higher Layers, Better Results: Application Layer Feature Engineering in Encrypted Traffic Classification[C]//International Conference on Wireless Algorithms, Systems, and Applications. Cham: Springer Nature Switzerland, 2022: 548-556.

[27] Tao L, Gu L. An improved fingerprint matching algorithm to detect malware encrypted traffic based on weighted Bayes[C]//International Conference on Cryptography, Network Security, and Communication Technology (CNSCT 2022). SPIE, 2022, 12245: 77-81.

[28] Sun G, Chen T, Su Y, et al. Internet traffic classification based on incremental support vector machines[J]. Mobile Networks and Applications, 2018, 23: 789-796..

[29] Zhioua S. Tor traffic analysis using hidden markov models[J]. Security and Communication Networks, 2013, 6(9): 1075-1086.

[30] He G, Yang M, Luo J, et al. A novel application classification attack against Tor[J]. Concurrency and Computation: Practice and Experience, 2015, 27(18): 5640-5661.

[31] Gupta N, Jindal V, Bedi P. Encrypted traffic classification using extreme gradient boosting algorithm[C]//International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 3. Springer Singapore, 2022: 225-232.

[32] Zhou Z H, Feng J. Deep forest: towards an alternative to deep neural networks[C]//Proceedings of the 26th International Joint Conference on Artificial Intelligence. 2017: 3553-3559.

[33] Afuwape A A, Xu Y, Anajemba J H, et al. Performance evaluation of secured network traffic classification using a machine learning approach[J]. Computer Standards & Interfaces, 2021, 78: 103545.

[34] Uğurlu M, Doğru İ A, Arslan R S. A new classification method for encrypted internet traffic using machine learning[J]. Turkish Journal of Electrical Engineering and Computer Sciences, 2021, 29(5): 2450-2468.

[35] Isingizwe D F, Wang M, Liu W, et al. Analyzing learning-based encrypted malware traffic classification with automl[C]//2021 IEEE 21st International Conference on Communication Technology (ICCT). IEEE, 2021: 313-322.

[36] Rao Z, Niu W, Zhang X S, et al. Tor anonymous traffic identification based on gravitational clustering[J]. Peer-to-Peer Networking and Applications, 2018, 11: 592-601.

[37] Shapira T, Shavitt Y. FlowPic: A generic representation for encrypted traffic classification and applications identification[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1218-1232.

[38] Ma X, Zhu W, Wei J, et al. EETC: An extended encrypted traffic classification algorithm based on variant resnet network[J]. Computers & Security, 2023, 128: 103175.

[39] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2016: 770-778.

[40] Hochreiter S, Schmidhuber J. Long short-term memory[J]. Neural computation, 1997, 9(8): 1735-1780.

[41] Cho K, van Merrienboer B, Gulcehre C, et al. Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation[C]//Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP). Association for Computational Linguistics, 2014: 1724.

[42] Liu X, You J, Wu Y, et al. Attention-based bidirectional GRU networks for efficient HTTPS traffic classification[J]. Information Sciences, 2020, 541: 297-315.

[43] Zhao Z, Li Z, Jiang J, et al. ERNN: Error-Resilient RNN for Encrypted Traffic Detection towards Network-Induced Phenomena[J]. IEEE Transactions on Dependable and Secure Computing, 2023.

[44] Song Z, Zhao Z, Zhang F, et al. I_2RNN: An Incremental and Interpretable Recurrent Neural Network for Encrypted Traffic Classification[J]. IEEE Transactions on Dependable and Secure Computing, 2023.

[45] Zhang H, 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. 2023: 2066-2075.

[46] Hamilton W, Ying Z, Leskovec J. Inductive representation learning on large graphs[J]. Advances in neural information processing systems, 2017, 30.

[47] Diao Z, Xie 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.

[48] Wang P, Wang Z, 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.

[49] Wang P, Li S, Ye F, et al. PacketCGAN: Exploratory study of class imbalance for encrypted traffic classification using CGAN[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020: 1-7.

[50] Mirza M, Osindero S. Conditional generative adversarial nets[J]. arXiv preprint arXiv:1411.1784, 2014.

[51] Shi Z, Luktarhan N, Song Y, et al. BFCN: A Novel Classification Method of Encrypted Traffic Based on BERT and CNN[J]. Electronics, 2023, 12(3): 516.

[52] Shi Z, Luktarhan N, Song Y, et al. TSFN: A Novel Malicious Traffic Classification Method Using BERT and LSTM[J]. Entropy, 2023, 25(5): 821.

[53] Kenton J D M W C, Toutanova L K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding[C]//Proceedings of NAACL-HLT. 2019: 4171-4186.

[54] He H Y, Yang Z G, Chen X N. PERT: Payload encoding representation from transformer for encrypted traffic classification[C]//2020 ITU Kaleidoscope: Industry-Driven Digital Transformation (ITU K). IEEE, 2020: 1-8.

[55] Shin C Y, Park J T, Baek U J, et al. A Feasible and Explainable Network Traffic Classifier Utilizing DistilBERT[J]. IEEE Access, 2023.

[56] Sanh V, Debut L, Chaumond J, et al. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter[J]. arXiv preprint arXiv:1910.01108, 2019.

[57] Wang Y, Gao Y, Li X, et al. Encrypted Traffic Classification Model Based on SwinT-CNN[C]//2023 4th International Conference on Computer Engineering and Application (ICCEA). IEEE, 2023: 138-142.

[58] Liu Z, Lin Y, Cao Y, et al. Swin transformer: Hierarchical vision transformer using shifted windows[C]//Proceedings of the IEEE/CVF international conference on computer vision. 2021: 10012-10022.

[59] MENG, Xuying, et al. Netgpt: Generative pretrained transformer for network traffic. arXiv

preprint arXiv:2304.09513, 2023.
[60] MENG, Xuying, et al. Netgpt: Generative pretrained transformer for network traffic. arXiv preprint arXiv:2304.09513, 2023.
[61] Dai J, Xu X, Xiao F. GLADS: A global-local attention data selection model for multimodal multitask encrypted traffic classification of IoT[J]. Computer Networks, 2023, 225: 109652.
[62] 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.
[63] Yang C, Xiong G, Zhang Q, et al. Few-shot encrypted traffic classification via multi-task representation enhanced meta-learning[J]. Computer Networks, 2023, 228: 109731.
[64]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(01):333-355.
[65] Liu K, Fu Y, Wu L, et al. Automated feature selection: A reinforcement learning perspective[J]. IEEE Transactions on Knowledge and Data Engineering, 2021.
[66] Ren P, Xiao Y, Chang X, et al. A comprehensive survey of neural architecture search: Challenges and solutions[J]. ACM Computing Surveys (CSUR), 2021, 54(4): 1-34.
[67] Baltrušaitis T, Ahuja C, Morency L P. Multimodal machine learning: A survey and taxonomy[J]. IEEE transactions on pattern analysis and machine intelligence, 2018, 41(2): 423-443.
[68] Yuan X, He P, Zhu Q, et al. Adversarial examples: Attacks and defenses for deep learning[J]. IEEE transactions on neural networks and learning systems, 2019, 30(9): 2805-2824.
[69] Moraffah R, Karami M, Guo R, et al. Causal interpretability for machine learning-problems, methods and evaluation[J]. ACM SIGKDD Explorations Newsletter, 2020, 22(1): 18-33.