加密隧道审查规避技术及流量分析研究综述

吕梦达[1],胡晓艳[1,2,3*],卢俊羲[1],李清昀[1],吴 桦[1],袁亚丽[1],张 帆[4]
(1. 东南大学网络空间安全学院,江苏南京 211189;2. 网络通信与安全紫金山实验室,江苏南京 211189;
3. 区块链应用监管教育部工程研究中心(东南大学),江苏南京 211189;
4. 浙江大学计算机科学与技术学院,浙江杭州 310027)

摘 要: 网络通信的加密化已成为不可逆转的趋势,在提升用户隐私安全基线的同时,也为恶意活动与审查规避提供了可乘之机。加密隧道技术因其独特的双重用途特性,成为网络攻防博弈的焦点。本文将虚拟专用网络(Virtual Private Network, VPN)和加密代理技术作为加密隧道的代表性技术,系统阐释其核心通信机理、典型协议形态与主流规避策略,并构建了涵盖被动流量监听与主动探针探测能力的现实威胁模型,明确了审查方在连接级识别、行为级分类及端到端关联等维度的能力边界。在此基础上,本文从数据集构建、特征提取方法、分析算法和研究动态四个维度,分别对VPN和加密代理的流量分析研究现状进行了深入梳理与对比。首先,本文分析了数据集构建现状,将其分为公开数据集与自采数据集,指出公开数据集存在时效性滞后与协议覆盖不足的问题,而自采数据集虽具有针对性,但其面临采集环境单一与复现困难的挑战。其次,本文从包级别、流级别、主机级别以及深度学习维度展开介绍了特征提取方法,系统归纳了从微观序列指纹到宏观行为图谱的多层次特征工程技术。然后,本文梳理了分析算法的演进路径,展示了从依赖专家知识的规则匹配,到基于统计规律的机器学习,再到具备强大端到端表征能力的深度学习算法的发展脉络,并总结了流量检测、业务分类、指纹识别及生态审计等主要研究动态。最后,本文提炼了当前研究在面对协议伪装等高级规避技术时所面临的核心挑战,包括规避协议快速迭代引发的概念漂移、多路复用与快速UDP互联网连接(Quick UDP Internet Connections,QUIC)协议连接迁移导致的流定义失效、实验室环境与现网威胁模型的差异、深度学习模型的可解释性缺失以及大规模背景流量下的基本比率谬误,并据此展望了协议无关检测、在线部署模型设计、自动化基准数据集构建及生成式隐写技术探索等未来研究方向。

关键词: 加密隧道;VPN;加密代理;审查规避;流量分析
基金项目: 国家重点研发计划(No.2023YFB3106801);国家自然科学基金(No.62472087);江苏省自然科学基金(No.BK20231413);中央高校基本科研业务费(No.2242025K30025)
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112(2026)04-1393-32
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20251052

A Review of Techniques for Bypassing Censorship in Encrypted Tunnels and Traffic Analysis

LÜ Mengda[1], HU Xiaoyan[1,2,3*], LU Junxi[1], LI Qingyun[1], WU Hua[1], YUAN Yali[1], ZHANG Fan[4]
(1. *School of Cyber Science and Engineering*, *Southeast University*, *Nanjing*, *Jiangsu* 211189, *China*;
2. *Purple Mountain Laboratories for Network and Communication Security*, *Nanjing*, *Jiangsu* 211189, *China*;
3. *Engineering Research Center of Blockchain Application*, *Supervision and Management* (*Southeast University*), *Ministry of Education*, *Nanjing*, *Jiangsu* 211189, *China*;
4. *College of Computer Science and Technology*, *Zhejiang University*, *Hangzhou*, *Zhejiang* 310027, *China*)

Abstract: The encryption of network traffic has become an irreversible trend. While enhancing the baseline for user privacy and security, it also creates opportunities for malicious activities and censorship evasion. Encrypted tunneling technology, owing to its unique dual-use nature, has emerged as a focal point in the adversarial network landscape. This paper regards virtual private networks (VPNs) and encrypted proxies as representative encrypted tunneling technologies. It systematically elucidates their core communication mechanisms, typical protocol morphologies, and mainstream evasion strategies. Furthermore, a realistic threat model encompassing passive traffic monitoring and active probing capabilities is constructed to delineate the censor's capability boundaries in connection-level identification, behavioral classification, and end-to-end correlation. Building upon this foundation, this paper presents an in-depth review and comparative analysis of the

收稿日期:2026-01-12;录用日期:2026-02-03;责任编委:沈蒙
*通信作者:胡晓艳

current research landscape regarding traffic analysis for VPNs and encrypted proxies. This analysis is structured across four dimensions: dataset construction, feature extraction methodologies, analytical algorithms, and research dynamics. First, the status of dataset construction is analyzed by categorizing datasets into public and self-collected types. The paper points out that public datasets suffer from issues such as timeliness lag and insufficient protocol coverage, whereas self-collected datasets, despite their targeted nature, face challenges related to singular collection environments and difficulties in reproducibility. Second, feature extraction methodologies are detailed across packet-level, flow-level, and host-level dimensions, and, in the deep learning domain, systematically summarized, ranging from microscopic sequence fingerprints to macroscopic behavioral graphs. Third, the evolutionary path of analytical algorithms is outlined, demonstrating the development trajectory from rule-based matching reliant on expert knowledge, to machine learning based on statistical laws, and finally to deep learning algorithms possessing powerful end-to-end representation capabilities. Additionally, major research dynamics, including traffic detection, service classification, fingerprint identification, and ecosystem auditing, are summarized. Finally, this paper distills the core challenges currently faced in confronting advanced evasion techniques such as protocol imitation. These challenges include concept drift triggered by rapid iteration of evasion protocols, flow-definition failures caused by multiplexing and quick UDP Internet connections (QUIC) connection migration, discrepancies between laboratory environments and real-world threat models, the lack of interpretability in deep learning models, and the base-rate fallacy under large-scale background traffic. Based on these challenges, future research directions include protocol-agnostic detection, the design of online deployment models, automated construction of benchmark datasets, and the exploration of generative steganography techniques.

Keywords: encrypted tunnel; VPN; encrypted proxy; censorship evasion; traffic analysis

Foundation Item(s): National Key Research and Development Program of China (No.2023YFB3106801); National Natural Science Foundation of China (No. 62472087); Jiangsu Province Natural Science Foundation (No. BK20231413); Fundamental Research Funds for the Central Universities (No.2242025K30025)

0 引言

随着传输层安全(Transport Layer Security,TLS)协议的广泛部署和HTTPS的强制推行,网络通信的加密化已成为不可逆转的趋势。谷歌透明度报告[1]指出,截至2025年5月,Chrome浏览器中已有超过90%的网页被加密。这一趋势极大地提升了通信隐私的安全基线,构成了现代网络信任体系的基石。然而,通信的全面加密化在保护合法用户隐私的同时,也为恶意活动提供以可乘之机。传统的网络安全监管与分析工具,尤其是依赖明文内容匹配的深度包检测(Deep Packet Inspection,DPI)技术,在加密流量面前大规模失效。这一根本性转变,迫使网络管理者、安全研究人员和审查系统必须从内容分析转向包的大小、时序、方向等侧信道信息分析,从而构成加密流量分析这一研究领域的核心驱动力[2]。

在海量加密流量中,加密隧道(encrypted tunneling)技术因其独特的双重用途特性,成为网络攻防博弈的焦点。加密隧道技术通过在不可信的公共网络上构建一个逻辑的加密数据通道,为通信双方提供端到端的机密性保护。本文关注的加密隧道主要包含虚拟专用网络(Virtual Private Network,VPN)和加密代理(encrypted proxy)两大类。一方面,VPN作为成熟的标准技术,是企业实现远程安全办公、构建站点到站点安全连接的基石。另一方面,VPN固有的流量加密与隧道封装特性,使其能有效隐藏通信的真实端点与内容,因此也常被用于规避网络审查,或被恶意行为者滥用以隐藏其网络活动。此外,随着审查技术的不断进步,以Shadowsocks[3]为代表的加密代理及相关混淆规避技术层出不穷,并进一步催生了审查方与规避方之间一场持续的技术军备竞赛。本文的核心即系统性地梳理这场军备竞赛中,加密隧道审查规避技术与流量分析技术相互博弈、共同演进的发展脉络。

军备竞赛的早期阶段围绕着固定协议指纹的隐藏与识别展开。规避方的初步策略是使用自定义的加密协议(如早期的Tor[4])来封装流量,以绕过基于明文关键词的审查。然而,审查方通过匹配协议握手包、特定的包长序列或TLS密码套件列表等独特的协议指纹,能轻易识别并封锁这些自定义协议[5]。

为应对基于固定指纹的DPI检测,攻防博弈进入第二阶段,其核心对抗聚焦于协议模糊与主动探测。规避方开发了可插拔传输层并分化出协议模糊策略,即通过完全加密和随机化,使协议流量不具备任何固定指纹。这一策略催生了obfs3、Shadowsocks、VMess[6]等一系列完全加密代理,使得基于固定指纹的DPI技术大规模失效,迫使审查方利用主动探测方法来检测代理服务器[7]。审查方首先被动嗅探

可疑流量,随后伪装成代理客户端主动连接可疑服务器,并根据其响应来确认代理身份。主动探测的威胁催生了新一代抗探测代理,如obfs4[8]和ShadowsocksR[9]。这些协议的核心机制是引入了带外共享密钥。代理服务器只有在客户端能提供正确的会话密钥时才会响应。然而,审查方很快发现这种沉默本身就是一种反常的指纹[10],并最终在2021年底升级了基于白名单的启发式阻断规则[11],该规则结合传输协议、明文内容、字节熵等信息豁免已知流量并封锁其余所有流量,从而直接命中了协议模糊策略加密代理的根本特征。

审查方的白名单策略迫使攻防博弈进入第三阶段,规避方转向协议伪装策略,即伪装成审查方不敢轻易封锁的常见协议。规避方开发出了Trojan[12]等具有标准化协议伪装能力的加密代理协议。Trojan将其流量承载于TLS协议上并运行在443端口,成功将自身隐藏在数以亿计的合法TLS流量之中。这给审查方制造了一个两难困境,即若要封锁Trojan,审查系统必须具备封锁所有TLS流量的能力,但这会导致巨大的附带损害。因此,审查方转向寻找更根本的协议无关指纹。近期的研究揭示了一种极具威胁的协议嵌套指纹[13]。当用户通过加密代理访问HTTPS网站时,其TLS握手阶段的流量结构呈现应用层与代理层的嵌套状态,并且包大小、时序和方向序列特征即使在外部加密后依然清晰可见。面对这一指纹,规避方也迅速作出回应,提出XTLS-Vision[14]等混淆技术来消除协议嵌套的冗余加密,同时还辅以握手包随机填充,以对抗基于握手包长的指纹。之后,研究发现的跨层往返时延(Round-Trip Time, RTT)指纹[15]为审查方指出了新的方向。该指纹利用了代理架构的固有拓扑属性,即传输层RTT显著小于应用层RTT,从而高置信度判定代理存在。

如图1所示,当前加密隧道审查规避与流量分析领域正处于一场由审查方和规避方主导的、侧信道分析与流量混淆技术驱动的攻防军备竞赛之中。然而,目前已有的相关综述工作尚存局限,部分综述侧重于某一特定匿名系统的流量分析[16-18];另一些工作或聚焦于广义的加密流量分类[2],或侧重于审查规避技术的演进[19]。本文以攻防演进为核心主线,系统性地串联起加密隧道审查规避技术及其流量分析技术的相关研究进展。首先,本文介绍了当前主流的加密隧道审查规避技术;其次,梳理了VPN和加密代理两大主流隧道的分析方法;之后基于攻防视角辨析了当前主流流量分析范式在面对高级规避技术时的核心困境;最后基于上述挑战,展望了未来研究方向。

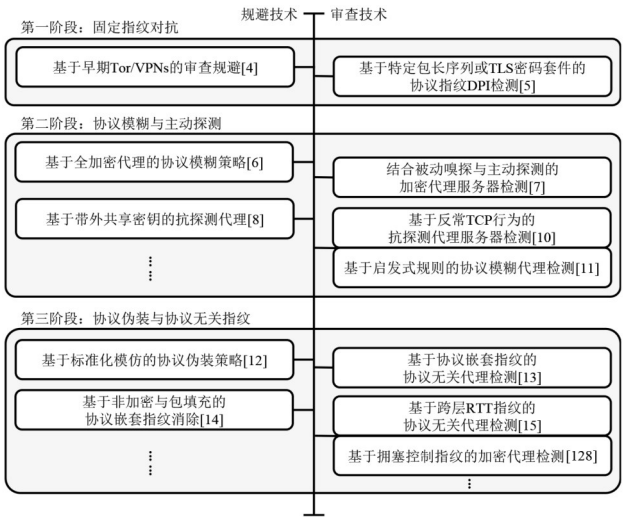

图1　加密隧道审查规避与流量分析对抗发展

Figure 1　Adversarial evolution of encrypted tunneling censorship evasion and traffic analysis

1　加密隧道技术概述

加密隧道技术通过在不可信公共网络上构建逻辑加密通道,保障通信的机密性、完整性与认证性。随着网络对抗升级,该技术已从传统的企业互联(VPN)演进为专注于审查规避的复杂代理体系(加密代理)。本节将概述其核心通信机制、规避策略及本文面临的威胁模型。

1.1　加密隧道通信技术

加密隧道通信技术在两个网络端点之间建立一个虚拟的点对点连接,并对通过该连接的所有数据进行加密封装,从而使得数据在穿越公共网络时免受中间节点的窃听和篡改。本文所研究的加密隧道通信技术按照工作层级不同主要分为VPN和加密代理两大类。

1.1.1　VPN通信技术

VPN作为一项成熟的网络安全技术,其核心在于实现隧道协议。隧道协议负责将原始数据包封装在新的数据包头中,并通过加密算法对整个封装后的数据包进行保护。当前主流VPN协议主要包括互联网协议安全(Internet Protocol security, IPsec)、OpenVPN和WireGuard等。表1展示对比了上述三种VPN协议的特性。

(1)IPsec。作为网络层安全标准套件,IPsec通过认证头(Authentication Header, AH)和封装安全载荷(Encapsulating Security Payload, ESP)提供机密性与完整性保护,通过互联网密钥交换(Internet Key Exchange, IKE)动态协商安全关联和管理加密密钥。此外,IPsec支持传输和隧道两种模式。其通常在内核空间实现,处理效率高,是站点间VPN的标准,但在

表1 主流VPN协议技术对比

Table 1 Comparison of mainstream VPN protocols

VPN类型	工作层级	核心协议	隧道机制	加密原语	性能特点	主要场景
IPsec	网络层(L3) 内核空间	ESP/AH; IKE	隧道模式/ 传输模式	复杂套件 (如AES, 3DES, SHA)	性能中等,配置复杂,硬件加速支持广泛	企业站点到站点 (Site-to-Site),远程访问
OpenVPN	应用层(L7)封装 用户空间	SSL/TLS (v1.2/1.3)	SSL/TLS隧道	依赖OpenSSL库	性能较低,灵活性高,易于配置,但有用户态开销	远程访问,个人用户
WireGuard	网络层(L3) 内核空间	自定义协议 (基于UDP)	封装于UDP	现代加密原语(ChaCha20-Poly1305,Curve25519)	性能高,延迟低,代码精简,配置简单,安全性高	高性能VPN接入,移动设备,物联网(IoT)

配置复杂性上较高。

(2)OpenVPN。OpenVPN基于SSL/TLS协议在用户空间运行,具有极高的跨平台性与灵活性。它支持TCP和UDP传输,其中TCP模式由于在端口层面看起来像HTTPS从而能更好地穿透防火墙,但可能因TCP-over-TCP所导致的隧道内外TCP协议栈相互干扰而性能下降。由于涉及用户态与内核态切换,其性能通常略逊于IPsec。

(3)WireGuard。WireGuard是一种精简、高性能的新兴VPN协议,运行于内核空间。它摒弃了复杂的密钥协商,采用ChaCha20-Poly1305等现代固定加密原语,在吞吐量与延迟方面表现优异,且代码库精简,易于审计与配置。图2展示了使用WireGuard远程访问某台服务器上HTTP服务的通信流程。

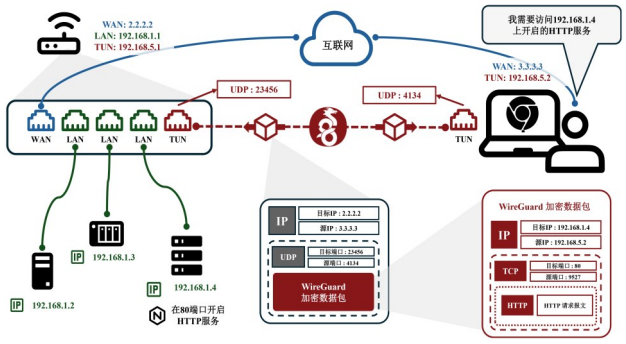

图2 WireGuard通信流程示意

Figure 2 Communication workflow of WireGuard

1.1.2 加密代理通信技术

与VPN旨在创建私有网络不同,加密代理的核心目标是转发特定应用程序的流量。其技术演进路径与审查规避的需求紧密相连,逐步从提供基础的代理功能演变为实现高级的流量混淆和伪装。图3展示了主流加密代理协议所用技术及其所处网络层级。

(1)从SOCKS5到Shadowsocks。SOCKS5协议是一个成熟的代理协议,允许客户端通过代理服务器转发TCP和UDP流量。然而,SOCKS5协议本身不包含任何加密机制,极易受到基于内容的审查。针对SOCKS5协议明文传输的缺陷,Shadowsocks引入预共享密钥(Pre-Shared Key,PSK)加密层,将流量混淆为随机数据流,解决了特征识别问题,是早期主流的规避工具。

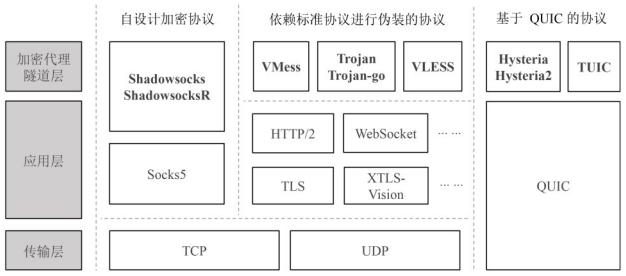

图3 主流加密代理协议审查规避技术

Figure 3 Censorship evasion techniques of mainstream encrypted proxy protocols

(2)VMess。VMess针对Shadowsocks功能单一和易受重放攻击的问题进行了改进。作为V2Ray的核心协议,VMess引入通用唯一标识码(Universally Unique IDentifier,UUID)作为用户标识,支持动态加密与多路复用。其完善的抗重放机制与并发传输能力,使其能更好地应对复杂的网络环境与主动探测。图4展示了通过VMess绕过国家防火墙实现对特定网站访问的通信流程。

(3)Trojan。随着审查技术升级为基于熵值和主动探测的方式,随机化全加密的协议模糊策略逐渐失

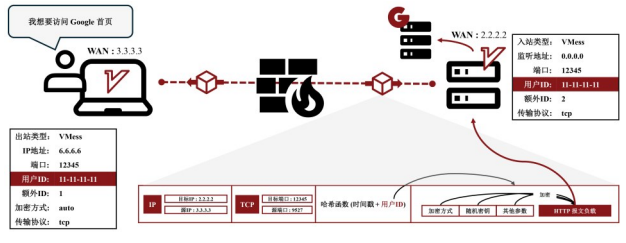

图4 VMess通信流程示意

Figure 4 Communication workflow of VMess

效。为了应对这一威胁,Trojan直接利用标准TLS协议封装流量,并在443端口模拟HTTPS服务器。当代理用户认证失败时,服务器会把流量回落到本地的一个真实Web服务器。这种机制使得Trojan服务器在面对主动探测时表现得与正常的HTTPS网站近乎一致,极大地提高了抗探测能力。

(4)VLESS。VLESS协议可以视为VMess的轻量化演进,与Trojan类似,VLESS的设计理念反映了审查规避技术策略的重要转向。VLESS协议拥有比Trojan更为强大和灵活的回落机制。它不仅可以像Trojan一样在认证失败时回落到指定的Web端口,还可以根据TLS握手阶段的ALPN字段或HTTP请求的路径进行精细化分流。这种高度可配置性使其能够构建极其复杂的网络拓扑,进一步混淆审查者的视线。

(5)Hysteria。随着HTTP/3标准的推进,Hysteria、TUIC等基于UDP的规避技术逐渐成为新的研究热点。早期的Hysteria协议基于定制化的快速UDP互联网连接(Quick UDP Internet Connections, QUIC)协议构建。它采用侧重于吞吐量的自定义拥塞控制算法,通过激进的带宽抢占策略维持极高的传输速率,但其非标准的协议实现导致其流量特征明显。针对早期版本在协议标准化与抗封锁能力上的局限,Hysteria2进行了重大的架构演进。在协议设计上,其完全遵循标准HTTP/3协议。在伪装能力方面,引入了端口跳跃机制,允许客户端在会话保持状态下动态切换目标端口,有效对抗了审查者针对单一UDP端口的持续性阻断与服务质量限速。

1.2　加密隧道审查规避技术

现代审查规避技术的核心已转变为流量伪装,即通过一系列技术手段,使加密隧道的流量在网络上变得不可见或不可区分,从而对抗基于主被动分析的高级审查手段。本节将分别探讨VPN和加密代理所采用的主流规避技术,以及其他重要的辅助规避策略。

1.2.1　VPN审查规避技术

标准VPN协议的设计初衷主要侧重于通信的机密性与完整性,而非对抗网络审查的隐蔽性。因此,这些协议在握手阶段的报文结构、加密协商过程以及数据传输时的头部特征往往呈现出相对固定且明显的统计指纹,使得它们极易被审查系统识别并阻断。为此,学术界和工业界开发了多种针对性的规避技术,旨在通过消除协议指纹、混淆流量行为等手段,提升VPN流量的生存能力。

最简单的规避手段是基于端口的伪装。审查者可能会封锁VPN的默认端口,因此VPN规避的第一步是将服务运行在常见的、不易被封锁的端口上,例如TCP 443端口、TCP 80端口或UDP 53端口。然而,这种方法只能规避基于端口的简单封锁。对于能够执行DPI的审查者,即使流量运行在443端口,其数据包的协议指纹依然清晰可见,DPI仍能识别并阻断它。

更高级的规避技术是基于协议封装的规避,通常被称为Stealth VPNs。为了对抗DPI,Stealth VPNs技术将VPN流量封装在另一层协议中。例如,使用stunnel等工具将OpenVPN流量封装在TLS隧道内。对于被动观测者而言,这种流量的外层是一个标准的TLS握手和加密数据流,与正常的HTTPS访问流量几乎没有区别,从而使其能够混入海量的Web流量中实现规避。然而,这种方法虽然能有效对抗被动指纹识别,但可能无法抵御主动探测。如果审查者主动连接到该443端口,并尝试发送OpenVPN的握手包,服务器如果配置不当,依然可能会响应OpenVPN的特征从而暴露其身份。

1.2.2　加密代理审查规避技术

现代加密代理从设计之初就内置了多样化强大的审查规避策略考量,其规避技术与协议设计本身高度耦合。

具体来说,Shadowsocks和VMess采用协议层混淆。它们采用自定义的加密格式,协议头部经过精心设计,以消除明文的协议特征。通过使用AEAD加密,它们还能在一定程度上抵抗基于重放和篡改的主动探测攻击。其目标是使流量看起来尽可能像无特征的随机数据。

相比之下,VLESS、Trojan等采用传输层伪装,这是当前最高效的规避策略。VLESS协议放弃了伪装成随机数据的思路,转而选择伪装成标准TLS流量。通过将VLESS承载于TCP与TLS之上,其流量在网络上与数以亿计的HTTPS网站访问在协议层面完全同构。这种策略给审查者制造了一个两难困境,即如果放行TLS流量,就必须放行VLESS;而如果封锁VLESS,就必须封锁所有TLS流量,但这将会导致互联网上绝大多数合法网站无法访问,造成不可接受的附带损害。

1.2.3　其他加密隧道审查规避技术

除了隧道协议本身的流量混淆与伪装设计外,确保隧道连接建立过程的隐蔽性同样是规避审查的关键环节。在实际网络环境中,审查者往往通过监控DNS查询记录或深度检测TLS握手阶段的服务器名称指示(Server Name Indication, SNI)等元数据,在加密隧道正式构建之前即实施精准阻断。为此,学术界和工业界发展了多种针对连接建立阶段的辅助规避

技术，旨在通过保护握手阶段的敏感信息或利用网络架构层面的欺骗手段来绕过封锁。

（1）域前置。域前置（domain fronting）是一种利用大型云服务提供商（如内容分发网络，Content Delivery Network，CDN）架构的欺骗技术。其核心是利用了 TLS 握手阶段中 SNI 和 Host 目标地址的分离。首先客户端在 TLS 握手的 SNI 字段中，填入一个允许访问的大型服务域名。由于 SNI 在加密服务器名称指示（Encrypted SNI，ESNI）与加密客户端问候（Encrypted Client Hello，ECH）技术出现前是明文的，审查者看到的是一个对合法域名的请求，因此予以放行。在 TLS 隧道建立之后，客户端在加密的 HTTP Host 头部中，填入真正的、被封锁的服务器域名。之后，大型 CDN 平台的边缘节点会解密 TLS，读取内层的 Host 头，并根据该头部将流量路由给被封锁的后端服务。图 5 展示了基于域前置的加密代理通信流程。由于该技术被广泛应用，Google 和 Amazon AWS 等主要云服务商已修改其 CDN 策略，开始强制校验 TLS SNI 和 HTTP Host 头的一致性，导致该技术在很大程度上已经失效。

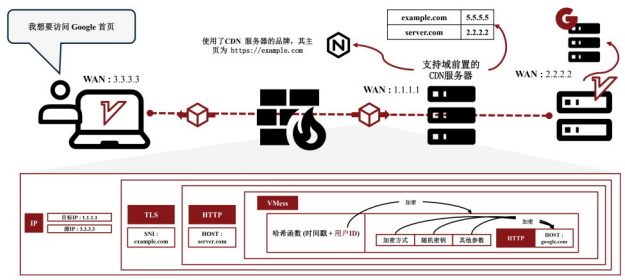

图 5 基于域前置的加密代理通信示意

Figure 5 Encrypted proxy communication based on domain fronting

（2）ESNI 与 ECH。域前置是一种欺骗策略，而 ESNI 与 ECH 则旨在从根本上解决 SNI 明文泄露这一导致 SNI 过滤的根本问题。ESNI 是 TLS 1.3 的一个实验性扩展。它允许客户端通过 DNS 获取服务器的公钥，并使用该公钥加密 SNI 字段，使得无法通过 SNI 明文获知具体访问网站。ECH 的目标更进一步，它不仅加密 SNI，而是加密整个 TLS 客户端问候消息。这使得审查者几乎无法从握手包中获取任何有意义的明文信息。尽管 ESNI/ECH 在技术上是先进的，但其也面临着审查者的反制。由于 ESNI 在早期采用率极低，审查者采取了直接封禁策略。这一反制手段的有效性反向依赖于规避技术的普及率。随着 ECH 的广泛部署，审查者再采取直接封锁策略的附带损害将变得无法承受。

1.3 威胁模型

为确保后续章节中关于加密隧道流量分析的研究综述具有清晰一致的上下文，本节将严格定义本文所采用的威胁模型，从而明确攻击者的假定位置、能力和目标，并提出后续所有分析的通用假设。图 6 是本文构建的威胁模型，直观展示攻击者在网络中的位置和能力。

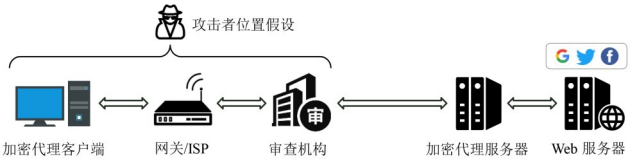

图 6 威胁模型示意

Figure 6 Threat model

1.3.1 攻击者位置

攻击者在网络中所处的位置决定了其可以观测到的流量范围。在本文所构建的威胁模型中一共存在三种不同的角色。首先是本地攻击者。攻击者控制客户端的本地网络环境，例如，客户端所连接的无线接入点、寝室路由器、企业网关或校园网交换机。本地攻击者可以观测到单个或少量用户的出站流量。其次是网络攻击者。攻击者是互联网服务提供商（Internet Service Provider，ISP）、骨干网运营商，或是能够实施网络审查的国家级行为体，这同时是本文所关注的核心威胁模型。该攻击者能够观测到其管辖范围内所有用户的流量，并拥有实施大规模、自动化分析和阻断的计算资源。最后是全局被动观测者。一个理论上的、可以观测全球所有网络流量的超级攻击者。该模型通常用于 Tor 等强匿名系统的最坏情况分析，但在本文的 VPN 和加密代理分析中采用更实际、能力稍弱的网络攻击模型。

1.3.2 攻击者能力

本文依据攻击者是否对传输中的网络流量进行实质性的交互或干预，将其能力划分为以下两类。首先是被动攻击者，其能力仅限于被动地监听、截获和分析网络流量，无法修改、注入或删除数据包。对于加密隧道，他们无法访问加密内容，但可以观测到所有元数据，包括 IP 头、数据包时间戳、数据包大小、数据包方向等信息。这种能力是被动流量分析的基础，支撑着本综述后续章节将讨论的协议识别、流量分类和网站指纹等任务。其次是主动攻击者，他们具备被动攻击者的所有能力，并且还能主动地注入、修改、重放和丢弃数据包。这种能力主要用于实现审查与阻断（例如通过注入 TCP RST 包、伪造 DNS 响应或直接丢包来阻断连接）、主动探测，或是进行协议降级或篡改。

1.3.3 攻击者目标

基于上述攻击者的位置与能力,流量分析不再是单一维度的技术行为,而是服务于从阻断干扰到精准画像等不同监管需求的体系化过程。据此,本文所综述的流量分析研究将攻击者目标归纳为以下三类,其难度和威胁性呈现逐层递进的特征。第一类是连接级识别,其目标是回答“是”或“不是”的问题,即判断一条加密流量是否属于某种特定的隧道协议。实现方法包括被动的协议指纹匹配或主动探测,这是实施审查阻断的第一步。第二类是行为级分类,其目标是在确认流量为加密隧道后,进一步回答“在做什么”的问题,可细分为粗粒度分类(识别用户在隧道内的应用类型,例如网页浏览、视频流、P2P或即时通信)和细粒度分类(网站指纹或其他细粒度行为)。实现方法主要是利用机器学习或深度学习算法,对被动观测到的数据包大小、时序、方向等元数据序列进行模式识别。第三类是端到端关联,其目标是回答“谁在和谁通信”的问题。这需要一个更强大的威胁模型,假设攻击者能同时观测到隧道的入口端和出口端。实现方法是通过分析入口流和出口流在时间、包计数、包大小等统计特征上的相关性,将两条流匹配起来,从而实现对匿名性的破解,这在Tor流量分析中称为流关联。

2 VPN流量分析研究进展

本节旨在系统性地综述VPN流量分析领域的研究进展,将重点从数据集构建、特征提取方法、分类模型算法、主要研究动态四个方面展开论述。表2对比了VPN流量分析的主要研究工作[20-35]。

2.1 VPN数据集构建

公开数据集为VPN流量分析研究提供了便利的可复现基准。研究者可以直接使用这些数据集来训练和评估模型,便于将自己的工作与先前研究进行对比。然而,公开数据集也存在局限性,例如数据集中可能包含陈旧的数据,采集环境与真实网络存在偏差,特定VPN协议覆盖不足,甚至存在标注错误等严重问题。例如,Kotak等人[36]在分析时就指出数据集中可能存在采集偏差或标注问题。

相比之下,自采数据集具有更高的灵活性和针对性。研究者可以根据特定的研究目标(如评估特定VPN协议[27,37]、分析特定应用[34,38-39]、测量移动端生态[20,30,40]或评估特定网络环境[31-33,41-42])来设计采集方案、控制变量并获取最新的流量数据。自采数据集的主要弊端在于采集成本高、周期长、标注困难,且由于采集环境和方法的异质性,其复现性相对较低,除非研究者将其公开发布。表3汇总了VPN流量分析研究中使用的部分数据集及采集方法[21,23,30,34,37,41,43-44]。

2.1.1 公开数据集

Draper-Gil等人[21]提出的ISCXVPN2016数据集包含了OpenVPN隧道流量以及对应的非VPN流量,覆盖了网页浏览、电子邮件、聊天、流媒体、文件传输、VoIP和P2P七类应用。由于其标注清晰,同时包含VPN与非VPN的对比,该数据集被大量用于VPN检测[28,45-51]和VPN业务分类[25,36,52-55]任务的基准测试。然而,Kotak等人[36]在研究中指出,该数据集中的部分流量并非真实的VPN加密流量,且存在采集偏差和标注问题。Lv等人[56]也发现该数据集存在缺陷,例如并未真正包含OpenVPN的数据包。

为了克服ISCXVPN2016在协议多样性上的不足,Naas和Fesl[37]构建并发布了USBVPN2022数据集。该数据集在受控环境中采集了包括PPTP、L2TP、L2TP-IPSEC、SSTP、WireGuard和OpenVPN在内的六种VPN协议流量并覆盖五类应用,为多协议VPN指纹研究提供了重要基准。Fesl和Naas[44]随后利用此数据集对多种机器学习模型及流量混淆方法进行了评估。

此外,还有若干常用于广义加密流量分析的数据集被应用于VPN流量分析的相关工作中。具体来说,ISCX-Tor2016数据集[57]主要用于Tor流量与非Tor流量的识别,但也常被许多工作[25,58-61]用于评估对包括VPN在内的多种加密流量的分类能力;CIC-Darknet2020[62]整合了ISCXVPN2016和ISCXTor2016,并加入了其他暗网流量,Aswad等人[63]使用此数据集在Apache Spark平台上训练ANN模型;Datacon21数据集[64]是一个包含100个网站与应用类别的数据集,Xu等人[65]利用此数据集构建流量图来识别VPN加密流量;Razooqi等人[48]使用VNAT数据集[66]对10个应用和5类业务的VPN与非VPN流量进行了分类。

2.1.2 自采数据集与采集方法

为了克服公开数据集的局限性,许多研究者选择自行采集数据。一类重要的自采数据集专注于扩展VPN协议的覆盖范围。Gao等人[27]采集了包括ExpressVPN、OpenVPN、FreeLAN在内的多种VPN实现。此外,针对VPN和加密代理,Wu等人[42]采集了包含VPN及V2Ray加密代理客户端在不同应用场景下的流量。

另一类自采数据集专注于特定应用场景或设备类型。例如,为研究移动端VPN流量,Oh等人[30]采集了100~150个Android应用在4种VPN下的流量;Liu等人[41]则构建了跨平台、跨地点的数据集,专门用于分析CloudflareWARP流量。针对物联网和智能

表2 VPN流量分析主要研究工作对比

Table 2 Comparison of representative studies on VPN traffic analysis

文献	年份	特征	分析算法	数据集	分析任务
文献[20]	2016	主机级别 (Android权限,追踪器)	规则算法(客户端审计)	自采数据 (Android VPN应用)	VPN生态实证研究
文献[21]	2016	流级别 (时间相关特征)	机器学习(C4.5,KNN)	公开数据集 (ISCXVPN2016)	VPN流量检测
文献[22]	2016	包级别 (上行包时序信息)	机器学习(DTW)	自采数据	VPN流量指纹细粒度识别
文献[23]	2018	主机级别 (客户端行为,泄露)	规则算法(自动化审计框架)	自采数据 (60余种商业VPN)	VPN生态实证研究
文献[24]	2019	主机级别 (DNS,SNI,元数据)	规则算法(元数据不一致性)	自采数据	VPN流量检测
文献[25]	2019	深度学习 (流转2D直方图)	深度学习(CNN)	公开数据集 (ISCXVPN2016)	VPN流量业务分类
文献[26]	2019	深度学习(自动学习)	深度学习 (多任务,联邦学习)	自采数据(隐私保护)	VPN流量业务分类
文献[27]	2020	包级别 (有效载荷长度序列)	机器学习(随机森林)	自采数据 (6种VPN实现)	VPN流量指纹细粒度识别
文献[28]	2020	深度学习 (会话字节转图像)	深度学习(卷积自编码器)	公开数据集 (ISCXVPN2016)	VPN流量检测
文献[29]	2023	流级别 (高速采样鲁棒特征)	机器学习(高速处理算法)	自采数据(高速采样)	VPN流量业务分类
文献[30]	2023	包级别(包长序列)	机器学习(堆叠集成模型)	自采数据 (100余种Android应用)	VPN流量指纹细粒度识别
文献[31]	2024	主机级别 (主动探测RTT)	规则算法(RTT不一致性)	自采数据(主动探测)	VPN流量检测
文献[32]	2024	包级别(握手包Opcode)	规则算法(协议指纹)	自采数据(OpenVPN)	VPN流量指纹细粒度识别
文献[33]	2024	主机级别 (探测响应,拓扑图)	深度学习(GNN)	自采数据 (全网扫描,ISP日志)	VPN生态实证研究
文献[34]	2025	流级别 (流量速率时间序列)	深度学习(LSTM)	自采数据(VoiceAttack)	VPN流量指纹细粒度识别
文献[35]	2026	包级别(DPI) 主机级别(DNS分析)	规则算法 (基于域名匹配、配置审计)	自采数据 (281款安卓VPN应用)	VPN生态实证研究

家居隐私,Li等人[39]采集了包含22台IoT设备、长达105天的真实家庭VPN聚合流量。Guo等人[34,67]则构建了VoiceAttack数据集,专门采集VPN加密保护下对智能音箱进行语音指令的流量。针对特定业务,Xu等人[38]采集了VPN封装下的Twitter和Dailymotion视频流数据。

第三类自采数据来源于大规模真实世界的网络测量与生态审计。这类研究通常不以发布标准化的分类数据集为目标,而是通过主动探测或被动监测来构建数据集以分析VPN生态。例如,Maghsoudlou等人[68]和Wang等人[33]通过全网主动探测并结合ISP流量数据来构建VPN服务器数据集。Khan等人[23]和Ramesh等人[43]则开发了vpn_tests和VPNalyzer等自动化审计框架,通过在终端运行并执行包括DNS/IPv6泄露、隧道失效测试在内的一系列测试来系统性地收集60~80家商业VPN提供商的客户端行为数据。Farnan等人[69]则利用DNS缓存嗅探技术,通过查询VPN内部DNS服务器来收集聚合的用户访问域名数据。

综上所述,当前VPN数据集构建主要面临公开数据集缺乏真实性与自采数据集难以复现的矛盾。一方面,以ISCXVPN2016为代表的公开数据集虽然为算法性能评估提供了统一基准,但由于采集环境较为理想化且协议版本相对滞后,导致其难以真实反映

表3　VPN流量部分数据集及采集方法

Table 3　Selected VPN traffic datasets and their collection methods

数据集名称	年份	流量类型	规模/内容	采集方法
ISCXVPN2016[21]	2016	OpenVPN、PPTP、L2TP、SSH等	28 GB流量; 7种VPN协议与非VPN流量; 包含Web、Email、P2P等业务	模拟Alice-Bob通信架构, 使用自动化脚本 生成背景流与VPN流
Commercial VPN Ecosystem[23]	2018	OpenVPN	62家商业VPN服务商; 包含网络配置、流量特征及DNS泄露测试数据	在虚拟机中对主流商业VPN客户端进行自动化与人工测试
VPNalyzer[43]	2022	OpenVPN、WireGuard等	80家桌面端VPN服务商; 230次实验测量数据; 含隧道失效、DNS/IPv6泄露数据	开发跨平台测量工具,在用户终端及受控环境中进行大规模生态测试
AppSniffer[30]	2023	移动应用流量 (OpenVPN, WireGuard, IPsec)	主流移动App在VPN下的流量; 包含报文长度序列特征	使用脚本驱动移动设备与多款VPN客户端交互采集
USBVPN2022[37,44]	2023 2025	OpenVPN, WireGuard, IPsec, PPTP, L2TP, SSTP	约300 GB流量; 6种主流VPN的包/流级数据	基于MikroTik路由器搭建采集环境,自动化生成多协议加密流量
VoiceAttack[34]	2024	智能音箱语音指令 (VPN加密)	多类语音指令在VPN下的流量;含噪声场景	使用TTS合成语音激励智能音箱,采集经商业VPN加密的流量
Cross-Platform VPN[41]	2024	WireGuard	跨平台(PC/移动端); 校园网、家庭网等异构网络环境	使用Selenium与ADB工具在不同设备和网络位置自动触发业务流量

现网中复杂的背景噪声与动态协议演进。另一方面,自采数据集虽然通过主动探测或受控环境提升了数据的时效性与针对性,但由于缺乏统一的采集规范与标注标准,导致研究成果难以在不同研究间进行横向对比与复现。综合来看,单一、静态的离线数据集已难以满足当前高对抗性研究的需求,未来的数据集构建将向着涵盖多协议版本、跨异构网络环境以及包含对抗性混淆流量的动态、大规模方向发展,以解决模型在真实部署中的泛化难题。

2.2　VPN流量特征提取

由于VPN流量的有效载荷被加密,研究工作转向利用流量的侧信道信息。对于VPN流量分析,所使用的特征按其粒度和抽象级别,可分为包级别特征、流级别特征、主机级别特征以及深度学习自动提取的特征。不同的研究根据其所面向的具体问题选择不同粒度或方法的特征。

2.2.1　包级别特征

包级别特征是从单个数据包中直接提取的信息,构成了最细粒度的分析基础。这类特征通常被用作序列输入到时间序列分析模型或深度学习网络中,其中最核心的包级别特征是包长。Gao等人[27]提出的有效载荷长度序列即利用会话前N个数据包的载荷长度作为指纹来区分不同的VPN实现。Oh等人[30]同样使用了带方向的报文长度序列来构建对抗VPN的移动应用指纹。Shapira和Shavitt[25]将包大小与到达时间结合,构建了二维直方图。此外,包长也被用于计算熵[37,53]或作为原始序列输入[23,26]。

其次是包时间与包方向信息。包到达时间戳或包间到达间隔反映了流量的突发和时序特性。突发通常定义为连续的单向数据包序列,常用于刻画用户与应用之间的交互行为。Feghhi和Leith[22]的研究表明,仅利用上行包的时间戳信息,通过导数动态时间规整算法,即可实现对VPN和Tor流量的网站指纹攻击。Kotak等人[36]也利用逐秒的时间序列滑动窗口来构造特征。总的来说,包时间、包方向常与包长信息结合,用于区分上下行流量并形成时空特征,从而构建能反映交互模式的序列[70]。

再次是原始包字节信息,其被许多深度学习方法直接用作输入。例如,Telikani等人[71]使用前1 480字节,Zhang等人[72-73]使用前1 456字节。这种方法依赖于深度学习模型自动从原始字节序列中学习模式,这些模式可能来源于加密协议的握手字段、头部结构或非理想的加密随机性[58,60-61]。

最后,协议头部字段也提供了重要信息[74]。例如,Wu等人[29,42]利用TCP头部中的接收窗口字段作为在高速采样数据中识别V2Ray的鲁棒特征。Xue等人[32]则利用OpenVPN控制包中的Opcode序列作为被动指纹。周益旻等人[75]则利用IP头部的协议字段与UDP端口特征作为识别IPSec流量的指纹。

2.2.2　流级别特征

流级别特征是通过对一个流(通常由源IP、目的IP、源端口、目的端口和协议五元组定义)中的所有数据包进行统计聚合而生成的特征。这是传统机器学

习方法中最常用的一类特征，因为它们具有较强的概括能力与稳定性，且数据维度较低。这些特征主要包括以下几类。

首先是时间相关统计[21,45,47,49]，如流持续时间、区分前后方向的包间到达间隔的均值、最小标准差、最大标准差等。Meng 等人[76]提出了将转向包间隔作为一种新颖的时间特征，即方向相反的相邻数据包之间的时间间隔。其次是长度和计数相关统计[44,50-51,54-55,63]，如流中的总包数、总字节数以及包长度的均值、最小标准差、最大标准差等。然后是速率相关统计[21,45,47]，如每秒包数和每秒字节数。再次是 TCP 头部统计[45,47,49]，如 TCP 标志位的计数等。最后是流活跃性统计[21,44]，如流的活跃和空闲时间的均值、最小标准差、最大标准差等。

此外，一些研究[77]利用更高级的信号处理技术来构造流级别特征。例如，Razooqi 和 Pekar[48]应用离散小波变换到包大小序列上，提取了不同分解尺度上的相对能量、均值、标准差和香农熵作为特征。流级别特征的优势在于其高度概括性、对个别包丢失的鲁棒性以及较低的计算开销。Wu 等人[29,42]专门设计了一套在高速网络流量采样后仍能保持稳定性的流级别特征，以实现实时识别。

2.2.3 主机级别特征

主机级别特征的分析粒度超越了单个数据流，转而关注一个端点的整体行为、属性或其在网络中的拓扑关系。这类特征对于识别 VPN 服务器或进行大规模生态系统分析至关重要。

主动探测是获取主机级别特征的主要手段。研究者主动向目标 IP 发送特制的探测包，并根据响应来判断其身份。Wang 等人[33]通过主动探测获取服务器对 SSTP、IPsec、OpenVPN 等协议的响应类型、响应时间、响应长度以及 TCP 终止行为等，并将其作为图神经网络的节点特征。Xue 等人[32]使用主动探测来确认 OpenVPN 服务器。Tian 等人[31]和 Schwartz 等人[70]也通过主动探测目标主机和可信地标的往返时延，利用 RTT 的不一致性来检测 VPN 使用。Ling 等人[78]则通过主动调制 TCP 通告窗口来嵌入水印，实现对匿名网络的主动追踪。

网络与应用层元数据也是重要主机级别特征之一。Maghsoudlou 等人[68]通过全网扫描收集 TLS 证书、rDNS、SNI 和开放端口信息来构建 VPN hitlist。Zain Ul Abideen 等人[24]也利用 DNS 查询、SNI 和证书信息来检测封装在 SSL/TLS 中的 VPN。Wang 等人[33]发现隐形端口（即在被动流量中观测到但在主动探测中无响应的端口）是识别 VPN 服务器的有效特征。

生态与行为特征提供了更宏观的视角。Ramesh 等人[43]、Khan 等人[23]以及 Ikram 等人[20]通过自动化审计框架在终端运行 VPN 应用，收集包括 DNS/IPv6 泄露、隧道失效行为、第三方 DNS 使用情况以及安装的追踪器等特征。Mixon-Baca 等人[40]则通过分析 APK、共享基础设施和硬编码的 Shadowsocks 凭据来识别隐秘家族。

图拓扑特征是一种新兴的主机级别特征。研究者将网络通信信息构建为图。Xu 等人[65]基于时间窗口内的流交互构建行为图，并输入图注意力网络进行分类。Wang 等人[33]则构建了基于端口相似性的探测图和基于 ISP 日志的通信图，并提取节点的度、中心性等图度量作为特征。

2.2.4 深度学习特征

深度学习特征指由深度神经网络从未经人工设计的数据中自动学习到的抽象表示。这类方法的关键在于输入数据的表征方式以及网络学习到的中间嵌入。输入表征是深度学习特征工程的核心。对于原始字节的处理策略主要是将数据包的前 N 个字节视为一维向量或重塑为二维图像。例如，Guo 等人[28]将 1 521 字节转换为 39 × 39 的灰度图；Shapira 和 Shavitt[25]提出的 FlowPic 将流映射为 2D 直方图；Liu 等人[60]则将每个包的前 m 字节转换为一个小图像，再将 n 个包的图像堆叠起来。针对序列数据主要是使用包长度、包长加方向或包长与包间隔的序列作为循环神经网络或 Transformer 的输入。Fu 等人[49]则使用了 NetFlow 记录的序列。而对于图数据则是将通信关系图或字节共现图作为图神经网络的输入。

学习到的特征表示则是指模型内部的抽象嵌入，当前主要包含以下三种表示方法。首先是自编码器。Gudla 等人[54]使用自动编码器对流特征进行降维；Guo 等人[28]使用卷积自编码器进行无监督预训练；Lv 等人[56]则使用对抗自编码器来学习数据分布。其次是预训练模型。Lin 等人[59]提出的 ET-BERT 是该领域的代表性工作，它借鉴自然语言处理（Natural Language Processing，NLP）中的 BERT 模型，在海量的流量突发上进行掩码语言模型的预训练，学习通用的数据报上下文表示。最后是中间层激活。在监督学习中，模型在全连接层之前所学到的高维向量即自动提取的深度特征。Zhang 等人[73]提取了分类器内部密集层的特征图，并将其用于后续的聚类分析。

综上所述，VPN 流量特征提取呈现出从包级和流级统计特征向主机级行为特征，进而向深度学习自动提取特征演进的趋势。包级别与流级别特征凭借低计算开销与高可解释性的优势，长期被作为轻量级检测的首选，然而在面对流量整形与填充等现代对抗措

施时,基于统计规律的特征往往因流量模式被扰动而失效。相比之下,主机级别特征通过引入主动探测与图拓扑结构等方法,突破了单流分析的局限,提升了对VPN服务器识别的鲁棒性,但其获取成本较高且易被防火墙阻断。深度学习特征虽然通过端到端学习解决了人工特征工程的繁琐问题,并能捕捉复杂的非线性时空模式,但其黑盒特性导致的可解释性不足,限制了其在安全敏感场景中的实际应用。未来的特征工程研究需要在特征的抗混淆鲁棒性、计算实时性与语义可解释性之间寻求平衡。

2.3 VPN流量分析算法

现有VPN流量分析工作中所采用的算法可分为基于规则的算法、传统机器学习算法和深度学习算法三种类型。基于规则的算法高度依赖专家知识和明确的模式,传统机器学习算法利用手工提取的特征进行学习,而深度学习算法则倾向于从数据中自动学习特征和分类边界。

2.3.1 规则算法

基于规则的算法依赖网络协议规范和专家经验来定义一组明确的指纹或启发式规则,以匹配特定的流量行为。这类算法可解释性强,计算开销低,并且在规则设计精确时能达到极低的误报率。在VPN流量分析中,规则算法主要应用于协议指纹识别和主机行为分析。Xue等人[32]和Rajore等人[79]的工作是利用协议指纹的典型代表。他们通过分析OpenVPN和WireGuard等协议的握手包,发现了控制消息中的明文字段(如OpenVPN的Opcode)或固定的字节模式(如WireGuard的保留字段),并以此构建了精确的指纹规则。Zain Ul Abideen等人[24]也利用TLS握手中的SNI、证书信息和DNS查询之间的不一致性来制定规则,识别封装在SSL/TLS中的VPN。

另一类规则算法基于主动探测或行为启发式。Almutairi等人[80]利用家用路由器固件,通过简单的包计数和会话时长阈值来指纹化,将所有流量汇聚到单一IP的VPN设备上。Tian等人[31]和Schwartz等人[70]则通过主动探测目标主机和可信地标的RTT,利用两者RTT的显著差异来判断VPN的使用。基于规则的算法优势在于其透明度高、计算资源消耗小,尤其适用于需要低误报率的在线阻断或审计系统。

2.3.2 机器学习算法

传统机器学习算法通过引入统计学习范式,弥补了基于规则的方法在泛化能力上的固有缺陷。在众多机器学习算法中,集成学习模型因其高准确性和鲁棒性而备受青睐。随机森林(Random Forest,RF)是应用最广泛的集成算法之一。例如,Razooqi和Pekar[48]证明了RF在基于小波特征的VPN检测中表现最稳健;Gao等人[27]也发现RF在基于包级别特征的VPN实现分类上效果最佳。梯度提升(gradient boosting)及其变体,如XGBoost、LightGBM和CatBoost,也是性能卓越的集成算法。Huang等人[51]使用CatBoost进行特征筛选,并结合LightGBM等模型进行堆叠,从而将多个异构的基学习器的预测结果作为元学习器的输入,以期获得比单一模型更优的性能。决策树因其模型结构直观、可解释性强而被用于VPN流量分类,尤其是在需要理解QoS标记依据的场景中[55]。K近邻(K-Nearest Neighbors,KNN)尤其适用于基于相似度度量的指纹识别任务,例如Feghhi和Leith[22]将其用于时间序列的网站指纹攻击。在流特征分类中,KNN也常被用作基准模型之一。此外,一些研究探索了其他模型。例如,Li等人[39]和Guo等人[34,67]使用隐马尔可夫模型及其变体阶乘隐马尔可夫模型[39]来对VPN加密下的聚合流量进行反聚合,从而将混合流量分离为单个设备的流量。

2.3.3 深度学习算法

深度学习算法通过构建深层神经网络,极大地突破了传统机器学习在特征表达能力上的瓶颈。卷积神经网络(Convolutional Neural Networks,CNN)是应用最广泛的深度学习模型。研究者通常将流量数据表征为一维序列或二维图像。例如,将数据包的原始字节或包长序列视为一维信号,使用一维卷积来捕捉局部的序列模式。或者,将流量转换为二维图像,如Guo等人[28]将784字节重塑为39 × 39的灰度图;Shapira和Shavitt[25]提出的FlowPic将流映射为2D直方图;Liu等人[60]则将每个包转换为小图像再堆叠。此外,Peng等人[61]还探索了多尺度CNN以捕获不同粒度的特征。

循环神经网络(Recurrent Neural Networks,RNN)及其变体长短期记忆网络(Long Short-Term Memory,LSTM)天然适用于处理包序列或NetFlow序列等具有时序依赖的数据。Yao等人[81]和Fu等人[49]引入注意力机制来动态加权LSTM在不同时间步上的输出,以突出关键数据包。混合模型,特别是CNN-LSTM,被广泛用于同时提取空间或局部特征和时序特征。例如,Tang等人[52]提出的Caps-LSTM结合了胶囊网络和LSTM来进行层次化特征学习。

图神经网络(Graph Neural Networks,GNN)是处理图结构数据的重要方法。在VPN流量分析中,GNN被用于学习主机间的拓扑关系或字节间的共现模式。例如,Xu等人[65]将时间窗口内的流交互构建为行为图,并应用图注意力网络进行分类。Wang等人[33]也使用GraphSAGE来建模VPN服务器的探测图和通信图。Li等人[58]则将每个数据包的字节视为节

点构图，并使用GNN进行分类。

Transformer模型同样可以应用于流量分析[82]。Lin等人[59]提出的ET-BERT是该方向的代表，它通过在大量无标签突发上进行预训练，学习通用的流量上下文表示，在下游任务中表现出色。Liu等人[60]也将Vision Transformer用于包图像序列的全局特征提取。

此外，研究者还探索了不同的学习范式来解决特定挑战。例如，为应对数据不平衡，Telikani等人[71]和Nascita等人[83]引入了代价敏感学习。为提高模型效率和泛化性，Zhao等人[26]采用了多任务学习，并将其与联邦学习相结合以保护数据隐私。为应对网络环境的动态变化，Zhang等人[72-73]和Cai等人[84]研究了增量学习和在线更新机制。

综上所述，VPN流量分析算法经历了从基于规则的匹配方法向传统机器学习，再到深度学习算法的演进过程。基于规则的算法虽然在特定协议指纹识别上具有高准确率，但其静态特性使其在面对协议变体时较为脆弱，需要频繁更新特征库。传统机器学习算法利用统计规律提升了泛化能力，在大规模流分类中实现了性能与开销的平衡，但其性能上限受制于手工特征的表达能力。深度学习算法凭借强大的表征学习能力，在细粒度分类与复杂混淆场景下表现优异，然而，其对大规模标注数据的依赖以及较高的训练推理成本，限制了其在边缘设备或高速骨干网中的实时部署。当前技术路线需要在检测性能、计算效率与模型可解释性之间进行权衡，未来的突破口可能在于轻量化模型设计与融合专家知识的混合学习方法。

2.4 VPN主要研究动态

VPN流量分析领域的研究动态活跃，涵盖了从基础检测到精细化指纹识别，再到宏观生态系统审计的多个层面。现有针对VPN流量分析的主要研究动态可以归纳为流量检测、业务分类、指纹识别、生态实证研究四大类。接下来分别进行详细介绍。

2.4.1 VPN流量检测研究

VPN流量检测是加密隧道流量分析体系中的基础任务，其目标是构建二分类模型，以在混杂流量中区分VPN流量与非VPN流量。早期及经典方法主要依赖于手工提取的流级别统计特征与传统机器学习算法。Draper-Gil等人[21]利用包时间和流活跃度等时间相关特征，结合C4.5和KNN算法进行分类。受此启发，大量研究致力于优化特征集和算法。例如，Abbas等人[47]和Huang等人[51]均通过特征工程和集成学习显著提升了检测性能。Gudla等人[54]引入自动编码器对特征进行降维，以实现时间受限的分类。Razooqi和Pekar[48]则另辟蹊径，应用离散小波变换提取包大小序列的时频域特征，并发现RF对此表现稳健。Meng等人[76]提出了转向包间隔这一新颖的时间特征，并将其概率分布作为输入，取得了良好的效果。Fesl和Naas[44]则在一个包含六种VPN协议的新数据集上对比了RF、XGBoost等多种模型。

随着深度学习的发展，研究者开始探索利用神经网络进行VPN检测。Guo等人[28]将会话字节转换为39 × 39的图像，使用卷积自编码器进行无监督预训练，在二分类任务上取得了极高性能。Fu等人[49]则构建了NSA-Net，利用NetFlow序列作为输入，结合双向LSTM和注意力机制进行检测。Lv等人[56]针对开放世界中背景流量难以穷尽的问题，提出了一种基于对抗自编码器和深度SVDD的单类分类模型，仅使用VPN正样本流量进行训练。

另一类重要的方法是基于规则、启发式或主动探测。这类方法不依赖复杂的模型训练，而是寻找VPN协议或行为的确定性指纹。Zain Ul Abideen等人[24]利用DNS查询、TLS SNI和证书之间的元数据不一致性来识别基于SSL/TLS封装的VPN。Almutairi等人[80]提出了一种新颖的威胁模型，利用被篡改的家用路由器固件，通过简单的包计数和会话时长阈值即可在NAT前指纹化VPN设备。更进一步，主动探测技术被用于确认VPN服务器或客户端，Tian等人[31]和Schwartz等人[70]均利用了服务器端主动探测RTT与客户端RTT之间的不一致性来检测VPN使用。

2.4.2 VPN流量业务分类研究

在成功检测出VPN流量的基础上，进一步识别隧道内部封装的具体业务类型是实现精细化管控的关键。传统方法同样依赖流级别统计特征。Caicedo-Muñoz等人[55]将7类应用映射为DiffServ中的每跳行为类别，并使用Bagging算法进行QoS分类。Aswad和Sonuç[63]则利用Apache Spark平台处理大规模流量的时间相关特征来进行业务分类。

深度学习已成为该领域的主流方法，尤其是处理原始数据或序列数据的能力使其具有显著优势。在基于图像的表征方面，Shapira和Shavitt[25]提出的FlowPic将流映射为2D直方图，使用标准CNN即可对VPN内的业务类型进行分类。在基于时序的模型方面，Kotak等人[36]采用逐秒滑动窗口提取时序特征，并输入模型进行分类。Tang等人[52]结合胶囊网络和LSTM进行层次化识别。Yao等人[81]将注意力机制引入LSTM。Liu等人[60]则融合了Transformer、CNN和LSTM的多模态输入。Peng等人[61]设计了多尺度CNN并使用精英策略蜣螂优化算法搜索超参数。

为解决高速网络的实时性挑战，Kattadige等人[85]提出了流采样技术结合期望最大算法恢复流分布，并使用XGBoost分类。Wu等人[29]则设计了在采样数据

下依然鲁棒的流特征,并利用Counting Bloom Filter和链式哈希表实现高速处理。此外,为解决真实网络环境中的复杂问题,研究者引入了多种先进范式。Telikani等人[71]和Nascita等人[83]采用代价敏感学习和可解释性分析来处理类别不平衡和模型不可信问题。Zhao等人[26]将多任务学习与联邦学习结合,实现隐私保护下的多维分析。Zhang等人[72-73]和Cai等人[84]则专注于开放世界问题,研究了模型的自治更新和增量学习。Gao等人[86]探索了无监督域自适应方法,以解决多源数据分布对齐的问题。Liu等人[41]则在跨平台和跨地点的数据集上评估了模型泛化能力。

2.4.3　VPN流量指纹研究

VPN流量指纹研究旨在实现比业务分类更细粒度的识别,其目标包括区分不同的VPN协议实现,识别用户访问的具体网站、正在使用的移动App,甚至推断视频标题或语音指令。VPN协议指纹研究关注VPN协议本身的侧信道。Gao等人[27]利用包有效载荷长度序列和随机森林,成功地区分了6种不同类型的VPN。Xue等人[32]和Rajore等人[79]则深入分析了OpenVPN和WireGuard的协议握手过程,发现了如明文Opcode、静态HMAC密钥、WireGuard的保留字段等可用于高精度被动指纹和主动探测的特征。

网站指纹(website fingerprinting)攻击旨在识别用户通过VPN访问的具体网站。该类攻击最早主要在Tor匿名网络场景下被系统化提出与研究[87-91],随后其威胁模型与技术路线逐步扩展到VPN以及加密代理环境中。Feghhi和Leith[22]的研究表明,仅利用上行数据包的时序信息并结合DTW算法,即可在VPN和Tor环境中实现网站指纹攻击。Kamal和Almuhammadi[92]复现了经典的网站指纹攻击方法,并评估了五种常见VPN服务对网站指纹的脆弱性。Perdices等人[93]则证明,即使在VPN和加密DNS保护下,仅凭观测到的目标IP地址序列并结合深度学习,依然可以高精度地识别热门网站。

移动App指纹研究随着移动VPN的普及而成为热点。Oh等人[30]提出了AppSniffer框架,他们发现现有的App指纹方法(如FlowPrint)在开启了多路复用的VPN下会失效。因此,提出了基于包长序列的堆叠集成模型,用于识别VPN隧道内的移动App并取得了较高准确率。

IoT、语音及视频指纹研究关注特定应用场景下的高价值信息泄露。Li等人[39]使用阶乘隐马尔可夫模型,成功从VPN加密的智能家居聚合流量中反推出单个设备的活动状态。Guo等人[34,67]进一步证明,仅通过分析VPN流量速率的时间序列,即可利用LSTM模型指纹识别出用户对智能音箱下达的具体语音指令类别甚至句子。Xu等人[38]则针对VPN封装的视频流,通过识别客户端请求点来切分视频片段,并利用CNN-LSTM模型对片段序列进行分类,实现对Twitter和Dailymotion视频标题的指纹识别。

高级模型应用方面,为应对VPN带来的流量形态同质化和one-flow挑战,研究者也应用了GNN和Transformer等高级模型。Xu等人[65]将流交互构建为图,使用图注意力网络来识别VPN下的应用指纹。Lin等人[59]和Li等人[58]分别使用基于Transformer的预训练模型和基于GNN的字节共现图模型,对包括VPN在内的多种加密流量进行了细粒度分类。

2.4.4　VPN生态实证研究

VPN生态实证研究通过大规模测量、客户端与服务器审计和安全分析,揭示了VPN生态系统的宏观特性、安全漏洞和隐私风险。客户端审计旨在评估VPN客户端软件的实际行为。Khan等人[23]和Ramesh等人[43]对桌面VPN客户端进行了深入审计。他们开发了自动化框架并发现了普遍存在的问题,如隧道失效时的流量泄露、DNS泄露、流量篡改、IP泄露以及对主动探测的脆弱性。针对移动端(特别是Android),Ikram等人[20]和Wang等人[35]的研究揭示了更严重的问题,包括大量应用嵌入第三方追踪器、请求过多敏感权限、明文传输VPN配置文件、硬编码凭据,以及主动进行TLS拦截等。Mixon-Baca等人[40]还揭露了共享基础设施和硬编码Shadowsocks凭据的隐秘家族。

服务器端探测与识别专注于从全网视角识别和分析VPN服务器。Maghsoudlou等人[68]和Wang等人[33]均通过大规模主动探测来构建VPN服务器数据集。其中,Maghsoudlou[68]等人的工作还引入图神经网络,结合服务器的探测响应特征和ISP日志中的通信拓扑特征,实现了对隐形端口和无响应服务器的识别。

特定攻击与漏洞分析揭示了VPN生态中存在的具体攻击向量。Tolley等人[94]提出了盲路径攻击,该攻击利用流量分析配合精心构造的包注入,在无法解密的情况下推断出VPN隧道内部的TCP序列号(SEQ/ACK)或DNS事务ID,从而实现连接劫持或DNS投毒。Farnan等人[69]利用DNS缓存嗅探技术,通过查询VPN提供商的内部DNS解析器,被动地推断出该VPN用户群体聚合访问的域名。Ling等人[78]则展示了利用SDN的能力,通过主动调制TCP通告窗口在匿名通道中嵌入水印,从而实现对恶意流量的主动追踪。此外,Fu等人[95]通过观测包长序列,并结合CNN表征包长模式之间的强相关性,从而检测加密隧道中的洪泛攻击。

综上所述，当前研究动态主要集中在对特定业务与行为的精细化识别以及对VPN生态系统的宏观安全审计。在精细化识别方面，研究目标已从粗粒度的协议检测与业务分类，深化至细粒度的指纹识别。在生态审计方面，研究视角从单点的流量识别扩展至整个VPN生态系统的安全性分析，通过大规模主动测量揭示了生态中普遍存在隐私合规风险与安全漏洞。然而，现有研究大多仍基于封闭世界或半开放世界的理想假设，针对多路复用、动态IP等复杂现网场景的分析仍显不足。随着审查规避技术的进一步完善，未来的研究重心将转向如何在进行审查规避对抗的前提下，实现对混淆VPN流量的精准治理与监管。

3 加密代理流量分析研究进展

本节将延续前一节的分析框架，系统性地梳理加密代理流量分析的研究进展，包括数据集构建、特征提取、算法模型、主要研究动态四个方面。表4对比了加密代理流量分析的主要研究工作。

表4 加密代理流量分析主要研究工作对比

Table 4 Comparison of representative studies on encrypted proxy traffic analysis

文献	年份	特征	分析算法	数据集	分析任务
文献[96]	2017	包级别(包长与方向序列)	机器学习(Profile HMM)	自采数据(Shadowsocks)	细粒度识别
文献[97]	2019	主机级别 (流上下文、主机DNS行为)	机器学习(RF)	自采数据(真实校园网)	加密代理检测
文献[7]	2020	主机级别(TCP层响应特征)	规则算法(逆向分析国家防火墙的主动探测逻辑)	自采数据(国家防火墙-SS-Probes,5.1万探针)	审查技术测量
文献[10]	2020	主机级别 (TCP响应、连接关闭阈值)	规则算法 (主动探测决策树)	自采数据(多种抗探测代理)	审查技术测量
文献[98]	2020	主机级别(主动探测的响应特征)	机器学习(XGBoost)	自采数据(Shadowsocks)	加密代理检测
文献[99-100]	2021、2023	流级别 (RF模型提取的叶节点索引)	机器学习(RF+KNN)	自采数据	网站指纹识别
文献[101]	2022	主机级别 (网站文本语义、DNS、API)	机器学习(RF、NLP)	自采数据(China-RESIP,908万IP)	代理生态测量
文献[102]	2022	流级别(滑动窗口JS散度)	机器学习(RF)	自采数据(Shadowsocks)	应用指纹识别
文献[103]	2022	深度学习 (包长、方向、IAT序列)	深度学习(LSTM+Viterbi)	自采数据	细粒度识别
文献[11]	2023	包级别 (首包字节熵、ASCII比例)	规则算法(逆向分析国家防火墙的被动豁免规则)	自采数据(GFW-Passive-Rules,1.7亿连接)	审查技术测量
文献[104]	2024	深度学习(原始字节序列)	深度学习 (packet-bytes textCNN)	自采数据(Abnormal-Proxy-Dataset)	细粒度识别
文献[15]	2025	包级别(跨层RTT差异)	规则算法(序贯假设检验)	自采数据	加密代理检测
文献[105]	2025	主机级别(异构信息网络拓扑);流级别(统计特征)	深度学习(GNN)	自采数据(HTPA,132万流)	加密代理检测
文献[106]	2025	包级别 (TCP ACK序号差值序列)	深度学习(1D-CNN)	自采数据(VMess视频流)	视频标题识别
文献[107]	2025	深度学习(包大小与方向序列)	深度学习 (Siamese Net,对抗损失)	自采数据(多种隧道)	应用指纹识别
文献[108]	2025	深度学习 (时序状态序列、二维空间轨迹)	深度学习(Transformer)	自采数据(Proxy-Corr-Dataset)	细粒度识别

3.1 加密代理数据集构建

与VPN相比，加密代理领域的高质量公开数据集极为匮乏。这种匮乏现状主要源于加密代理的协议快速迭代、对抗性采集环境等内在特性。表5汇总了加密代理流量分析研究中使用的部分数据集及采集方法[7,11,101,104-105,108-110]。

3.1.1 公开数据集

目前，学术界仍缺乏一个像ISCX-VPN-2016那样被广泛接受和引用的加密代理基准数据集。研究者通常利用现有的通用网络流量数据集作为背景流量或非代理流量[103,106]。部分研究在分析网站指纹攻击等特定场景时，会基于已有的公开数据集通过仿真

表5　加密代理流量部分数据集及采集方法

Table 5　Selected encrypted proxy traffic datasets and their collection methods

数据集名称	年份	流量类型	规模/内容	采集方法
Proxy-Torrent-Dataset[109]	2018	免费HTTPS代理	39 143个可用代理,2 TB流量	多阶段漏斗式:爬虫+主动探测+Chrome插件被动收集
GFW-SS-Probes[7]	2020	Shadowsocks、GFW Probes	51 837个探针,12 300个源IP	跨国VPS部署代理,诱捕国家防火墙主动探测
China-RESIP[101]	2022	住宅代理(RESIP)	908万RESIP IP,399个服务	NLP爬虫+API抓取+被动DNS+渗透
GFW-Passive-Rules[11]	2023	TCP(Random、TLS、HTTP)	1.7亿连接日志,10% IPv4扫描	跨国VPS主动构造流量;CU Boulder 40 Gbps tap被动监测
Abnormal-Proxy-Dataset[104]	2024	Shadowsocks(正常/异常)	8.75 GB,37 796会话,5类行为	受控环境,设置SS加密为none模拟异常,覆盖5类应用
HTPA[105]	2025	HTTPS隧道(VPN/Proxy)	132万条流,8种隧道	客户端爬虫(Alexa)+真实校园流量,标注隧道与非隧道
Proxy-Corr-Dataset[108]	2025	V2Ray、SSH、Tor	多协议,多种混淆/稀疏度设置	受控单跳代理环境,爬虫(Alexa 10k)+代理日志关联
CE-450x6[110]	2025	Shadowsocks、V2Ray	6个环境×450个网站×50样本	受控环境,Selenium自动化,覆盖不同浏览器与代理组合

手段生成代理封装后的流量[111],但这限制了对真实代理协议特征的捕捉。

AnonProxy2023[112]是一个较新的公开数据集,其明确标注并包含了匿名、代理和VPN流量,为相关研究提供了宝贵的资源。CSTNET-TLS 1.3数据集[59]虽然主要针对TLS 1.3服务,但鉴于VLESS等先进代理技术高度依赖TLS 1.3,该数据集可作为研究标准TLS与VLESS伪装TLS之间基线特征差异的参照。此外,由国内机构发布的加密应用识别与公害行为发现流量数据集[113],明确包含了VPN类工具和IM工具等加密流量,其数据采集环境更贴近国内网络,具有特定的研究价值。

3.1.2　自采数据与采集方法

根据核心研究目标与采集视角的差异,自采数据的采集方法可归纳为审查测量与对抗、检测与指纹识别以及生态实证分析三类。首先是审查测量与对抗,此类研究旨在逆向分析审查系统的行为。研究者通常在目标审查国家与境外部署代理客户端与服务器,通过主动发起连接以触发审查者的被动检测或主动探测,并在两端抓包以记录探测报文与审查行为[7,10-11,114]。其次是检测与指纹识别,此类研究需要大量标注清晰的加密代理流量,或细粒度的应用与网站标签。研究者通常在受控的实验室环境或真实网络中搭建代理服务器和客户端,使用自动化脚本模拟用户访问,同时使用tcpdump或TShark等工具在客户端、代理服务器或中间节点抓取流量,并结合代理日志或客户端行为进行精确标注[110,115-119]。最后是生态实证分析,此类研究旨在刻画加密代理的宏观生态。研究者会使用大规模网络爬虫、API抓取、被动DNS分析、ZMap/Nmap主动扫描和轻量级渗透测试等手段,从互联网上大规模发现代理服务提供商及其IP池,构建庞大的代理数据集[101,109,120]。

综上所述,加密代理数据集的构建面临着比VPN更为严峻的挑战,主要源于协议的快速迭代与采集环境的对抗性。公开数据集极其匮乏,且往往无法覆盖VLESS、Hysteria等新兴协议,导致基于此的研究成果难以适应现网环境。自采数据集虽然填补了针对特定协议的研究空白,但受限于采集视角(通常为实验室受控环境),难以真实复现ISP级别的背景噪声与大规模流量的统计分布,且在混合网络流量中缺乏可靠的自动化标注手段。当前数据集构建工作在真实性与规模化之间存在明显短板,未来的发展趋势需要转向构建包含真实网络干扰、涵盖多种混淆策略以及能够动态更新的高质量基准数据集,以支撑模型在对抗环境下的鲁棒性验证。

3.2　加密代理流量特征提取

本文同样将加密代理流量分析中使用的特征分为四个主要类别,包括包级别特征、流级别特征、主机级别特征以及深度学习自动提取特征。接下来进行详细介绍。

3.2.1　包级别特征

与VPN流量研究思路类似,许多研究将其构成序列,并重点分析流的前N个包[121-122]。此外,部分研究利用载荷熵来区分高度随机的加密数据与结构化的明文数据[117,123]。

(1)包长与方向序列。包长度和包方向的组合序

列是加密代理网站和应用指纹识别最核心的输入。研究者通常将五元组流中数据包的长度与方向序列作为后续模型的输入。Zhuo 等人[96]将包方向与包长结合进行符号化,作为 Profile HMM 模型的输入,以建模包含超链接跳转的网站访问。Gu 等人[107]和 Hartl 等人[103]也将包方向与包长序列作为其深度学习模型输入序列的关键维度,用于应用指纹识别或多路复用下流分离。Zhou 等人[117]则直接使用流的前 30 个包的长度序列作为特征。

(2)包时间信息。Hartl 等人[103]在分离加密隧道中的复用流时,将包间到达间隔和定向包间隔的对数值作为 LSTM 模型的关键特征。Beckerle 等人[111]在其 Maturesc 攻击中也发现,使用包到达间隔作为输入比使用时间戳更稳健。此外,包时间信息也被用于构建更抽象的特征,并结合深度学习模型[107,124-126]。Liu 等人[108]在其 ProxyCorr 模型中将流时序状态序列输入 Transformer 模型。Zhang[118]则将包间到达间隔作为图神经网络中的节点特征。

另一类重要的包时间特征来源于主动探测或 RTT 测量。Cheng 等人[98]和 Frolov 等人[10]通过主动探测,利用服务器的响应时间、连接关闭时间或超时行为来指纹化代理。Xue 等人[15]和 Mühle 等人[120]则利用了代理架构固有的延迟特性,通过测量数据包的往返时延来提取跨层 RTT 差异或多视角延迟差异作为协议无关的指纹。

最后,时间信息还被用于其他形式的序列特征。Janbeglou 和 Brownlee[127]计算了比特率的时间序列曲线。Wang 等人[128]利用了发送速率随时间的轨迹来检测自定义拥塞控制算法。Spreitzer 等人[129]则通过在 Android 客户端高频采样数据使用量,构建了近似的字节数时间序列。

(3)包载荷特征。尽管加密代理旨在隐藏应用层载荷,但载荷本身的字节级特征仍是极其重要的信息源。研究者通过提取载荷的统计信息来量化其随机性,以区分高度随机的加密数据与结构化的明文协议。Wu 等人[11]对 GFW 的逆向分析发现,其被动检测系统利用首包的字节熵、字节位计数和可打印 ASCII 字符比例来构建规则。受此启发,部分研究[122-123,130-131]使用首 16 字节负载熵、分片信息熵、字节级与二进制香农熵、置位比等基于载荷的统计信息来检测加密代理流量。

3.2.2 流级别特征

首先是基本统计特征。这是最基础的流级别特征,涵盖了对包长、时间、方向的全局统计。具体包括计数与时长,如流的总包数、总字节数、总持续时间,以及上行和下行各自的包数、字节数和方向比率等[119,121,123,131-132]。同时还有包长统计,如上行、下行及双向包长度的均值、中位数、标准差、方差、最大值、最小值、百分位数等[115-116,121]。还包括时间统计,如包间到达间隔的均值、中位数、标准差、最大值、最小值等[133-136]。Miller 等人[135]还额外统计了流的活跃和空闲时间的统计量。

其次是分布特征。Aceto 等人[115]和 Cui 等人[116]构建了包长和包到达间隔的频率分布直方图。Engelberg 和 Wool[137]则证明,使用完整的包长分布在对抗 IoT 流量填充时具有极强的鲁棒性。Hu 等人[138]也构建了包长和包间到达间隔的累积分布函数,并使用 K-S 检验进行对比。

再次是突发与子序列特征。Rahman 等人[139]通过迭代地增加数据包来修改突发的大小,从而将原突发模式扭曲变形以实现网站指纹防御。Aceto 等人[115]提出了服务突发,即基于时间阈值切分的子流,对每个服务突发提取统计特征。Ejeta 等人[132]和 Zhao 等人[133]也提取了最大突发长度、平均突发长度和突发数量等特征。

最后是高级构造特征。Wang 等人[102]和 Cui 等人[116]提出了滑动窗口 JS 散度,通过计算流内部相邻窗口间包长/时间分布的相似性,来刻画流量模式的内部变化性。Luo 等人[119]提出了流翻转次数特征,即一个流中非空单向流的方向发生翻转的次数,该特征被证明在使用加密代理前后具有高度不变性。Zhang 等人[106]还提取了基于应用层的派生特征,通过分析客户端请求包的 ACK 序号差值,提取视频流的分段大小序列,作为网站指纹的输入。

3.2.3 主机级别特征

首先是跨流聚合与上下文。此类特征的核心是分析来自同一主机的多个流之间的关联模式。Zeng 等人[97]提出了流上下文特征,通过时间窗口关联,统计当前流与邻近流在源与目的 IP、目的端口上的共享关系。Luo 等人[122]同样利用了主机在短时间窗口内的行为,提取了流聚合、流突发以及目的 IP 分布熵等特征,以刻画代理流量汇聚到单一服务器的模式。

其次是主动探测。Cheng 等人[98]设计了 ACER 框架,主动发送类 Shadowsocks 报文,并提取响应的时间、TCP 标志和包信息特征进行分类。Frolov 等人[10]则通过发送 HTTP、TLS、随机字节等一系列探针,测量服务器的响应数据、连接关闭类型,从而精确指纹化 obfs4、Lampshade、Shadowsocks 等多种抗探测代理。Mühle 等人[120]则通过多视角主动测量,利用代理架构导致的延迟差异来识别比特币 P2P 网络中的代理。

再次是 DNS 与外部情报。此类特征利用 DNS 查询日志或外部数据源来辅助判断。Zeng 等人[97]利用

了主机DNS行为,特别是未关联域名数,即主机在DNS中请求了某域名但在短时间内未产生访问该IP的流量,这通常是DNS泄露导致的。Janbeglou和Brownlee[127]也利用了目标IP从未通过DNS解析这一启发式规则来识别自定义UDP隧道。Yang等人[101]在研究住宅代理生态时,综合运用了被动DNS分析、API抓取、ZMap扫描以及对代理服务商网站的自然语言处理语义分析。

最后是图拓扑特征。其将网络通信建模为图结构[95,140]。Liu等人[105]提出的HINT框架是该方向的代表。该方法构建了一个包含主机、服务和客户端在内的异构信息网络,并将流级别统计量作为图节点的属性。通过在此图上运行图神经网络,HINT能够融合拓扑结构和统计信息,实现对高度混淆HTTPS隧道的鲁棒检测。

3.2.4　深度学习特征

首先是基于原始字节序列的学习。Zhang等人[104]提出了packet-bytes textCNN模型,将一个会话的前784字节视为“句子”,字节视为“词”,用于识别异常代理流量并进行细粒度用户行为分类。Zhao等人[126]在相同任务上对比了多种深度模型,发现LSTM在处理具有强时序依赖的行为(如聊天和VoIP)时表现更优。Xie[125]也将原始流量序列输入1D-CNN中进行自动分类。

其次是基于包序列的学习。Hartl等人[103]使用LSTM从该序列中学习概率分布,以分离复用流。Gu等人[107]在其DecETT框架中,使用双分支Siamese网络从包序列中解耦出协议无关的应用语义表征。Liu等人[108]的ProxyCorr模型则将流量建模为时序状态序列和二维空间轨迹,并输入Transformer编码器学习时空依赖。Beckerle等人[111]也使用xresnet处理时间差和方向序列。

最后是基于手工特征的深度学习。Zhou等人[117]提出的BiAE-MLP模型,使用双自编码器将325维的手工流特征压缩为32维的低维表征,再进行分类。Zhou等人[141]和Zhang[118]则将流级别统计特征输入Transformer或GCN中,以学习特征间的复杂关系。

综上所述,加密代理流量特征提取技术正经历从单一维度的统计特征向多维度、深层次的关联特征演进。VPN特征工程侧重于从标准协议中提取固有指纹,而加密代理特征提取则侧重于在主动伪装中寻找破绽。由于加密代理广泛采用了TLS伪装、填充和流量整形技术,传统VPN分析中有效的流级统计特征(如包长分布、载荷熵)在此场景下迅速失效。因此,研究重心逐渐从单一流特征转向更具穿透力的侧信道与关联特征,例如利用代理架构固有的跨层RTT差异、主机级别的DNS上下文关联以及异构图拓扑结构等。深度学习特征提取在此处的作用不仅是分类,更在于从被混淆的时序中解耦出真实业务模式。未来的特征研究可更加关注那些难以被协议层伪装所消除的物理层或架构层本质属性,以对抗日益完善的审查规避技术。

3.3　加密代理流量分析算法

分析算法是实现从特征向量到具体类别映射的核心。本文同样将加密代理流量分析所采用的算法模型分为三类,包括规则算法、机器学习算法和深度学习算法。

3.3.1　规则算法

首先是主动探测。其核心是利用代理实现在处理非认证或异常请求时,TCP层或应用层响应与真实协议不一致的特性。Alice等人[7]和Frolov等人[10]的研究是该领域的代表性工作,他们系统性地逆向了审查系统用于检测抗探测代理的机制。首先,审查者定义了发送探针的规则,如重放客户端首包或发送HTTP/TLS/随机字节等特定探针。其次,审查者制定了一套决策规则树来判别响应。这些规则不关心应用层数据,而是匹配TCP层的响应行为。Wang等人[114]通过构造损坏的TLS应用数据包,利用ShadowTLS握手后TCP行为与真实TLS服务器不一致的缺陷来识别它。此外,规则算法也被用于生态测量或漏洞发现。Mühle等人[120]在探测比特币P2P网络中的代理时,使用了一条基于多视角RTT测量的启发式规则。Wedwardes等人[142]利用特定规则构造畸形DNS请求,以主动触发GFW注入器的内存泄露漏洞。Perino等人[109]在测量免费代理生态时,也使用了基于内容相似度阈值和TLS证书匹配的规则来判定代理的可用性与恶意行为。

其次是被动指纹匹配。规则算法被用于在流量中寻找由特定协议、实现或伪装行为所固有的静态、可识别模式。最直接的规则是基于协议字段的字典查询。Husák等人[143]的工作展示了通过被动匹配TLS ClientHello包中的明文字段即可构建规则字典,高精度地识别客户端类型。GFW的豁免规则中,有四条即统计规则,例如检查首包的字节位计数是否在特定区间或包中可打印ASCII字符的比例是否超过阈值[11]。Luo等人[130]指出,ShadowsocksR在伪装HTTP/TLS时,其伪造头部中包含了可被规则匹配的固定字段。Wang等人[128]通过比较观测吞吐量与Mathis方程的预期值,来判定代理是否使用非标准拥塞控制。Janbeglou等人[127]还提出了一条启发式规则,即一个端点若产生了大量流量,但其IP从未出现在DNS查询中,且其流量与另一条流高度相关,则可

能为隧道。

最后是统计检验分析。其基于统计检验或距离度量判断流量是否偏离正常基线或符合目标区间。Xue 等人[13,15]利用代理架构固有的协议无关特征，并应用马氏距离度量和序贯假设检验进行在线判定。Hu 等人[138]在检测加密矿工流量时，采用了两样本 K-S 检验，通过比较待测流与已知模板的累计分布来进行判别。Engelberg 和 Wool[137]则使用完整的包长分布向量，通过计算余弦距离来识别 IoT 设备。Spreitzer 等人[129]也利用了 Jaccard 相似度规则来匹配高频采样的客户端字节序列。

3.3.2 机器学习算法

（1）随机森林。Zeng 等人[97]在其加密代理检测工作中利用 RF 模型处理流上下文和主机行为等 12 维异构特征，取得了优于 SVM、逻辑回归等算法的性能。Deng 等人[134]也使用 RF 对 Shadowsocks 流量进行检测。在更具挑战性的网站指纹识别任务中，Zhao 等人[133]通过实证对比发现，RF 在真实 Shadowsocks 流量上的表现优于 SVM、KNN 和朴素贝叶斯。RF 的灵活性使其不仅能作为分类器，还能充当特征提取器。Ma 等人[99-100]在其上下文感知的网站指纹识别框架中利用 RF 训练流分类器，并提取流样本在森林中落入的叶节点索引作为高区分度的流指纹。在跨环境分析中，Li 等人[110]使用 RF 作为核心基础分类器来评估不变特征子集的有效性。在移动端，Wang 等人[102]证明了 RF 在结合滑动窗口 JS 散度特征后，对跨设备应用识别具有很强的鲁棒性。此外，RF 还常被用作基准[117]或作为主动学习框架的基础分类器[136]。

（2）梯度提升决策树。Cui 等人[116]在 Shadowsocks 应用识别中，对比了 RF、XGBoost 和 LightGBM 三种模型。Cheng 等人[98]在其主动探测框架 ACER 中，使用 XGBoost 处理探测响应特征以识别 Shadowsocks 服务器。Ji 等人[121]和 Litvinov[131]也分别应用 XGBoost 识别 ShadowsocksR 的 HTTP 伪装流量和 V2Ray 流量。为应对 SSR 更复杂的协议伪装，Ji 等人[123]和 Luo 等人[130]进一步采用了 XGBoost 的变体 DART 和 GOSS，以提升模型的泛化能力。

（3）支持向量机。Ejeta 等人[132]在分析 Psiphon 流量时发现，SVM 在检测 Psiphon 流量方面表现最佳。Song 等人[144]则利用 SVM 对 Tor-over-Proxy 流量的包长分布特征进行分类，取得了高精度。然而，在网站指纹和移动应用识别等多分类任务中，SVM 的性能通常不及 RF。

（4）K 近邻。Ejeta 等人[132]发现 KNN 适用于 Psiphon 代理下封闭世界的网站指纹识别。Ma 等人[99-100]也使用 KNN 对其 RF 提取的流指纹进行最终的网站分类。Rahman 等人[139]在评估其 Mockingbird 防御时，也将 KNN 和 k-FP 作为基线攻击模型。

朴素贝叶斯及其变体和决策树因其简单高效，同样被用作基准模型[97,102,122,131,133]。Aceto 等人[115]在移动应用分类研究中，深入探索了多种分类器融合方法，以结合多个异构分类器的优势。

3.3.3 深度学习算法

（1）卷积神经网络。CNN 及其变体擅长捕捉流量序列中的局部模式或空间特征。Zhang 等人[104]利用一维卷积捕捉字节序列中的局部 n-gram 模式，用于识别 Shadowsocks 加密失效异常并进行细粒度用户行为分类。Zhao 等人[126]在相同任务上对比了 1D-CNN、2D-CNN 和 LSTM，发现 CNN 在二分类任务上表现优异。Zliang 等人[124]和 Xie[125]均使用 1D-CNN 处理包序列以识别 Shadowsocks。Zhang 等人[106]提出的 SCEP-TI 则使用 1D-CNN 处理从 ACK 差值中提取的视频分段大小序列，以实现对 VMess 代理下视频标题的指纹识别。Beckerle 等人[111]提出的 Maturesc 攻击则使用了 ResNet 处理包时间差和方向序列，以实现在流量分裂防御下进行网站指纹攻击。

（2）循环神经网络。RNN 及其变体被广泛用于建模流量的强时序依赖性。Zhao 等人[126]在对比实验中发现，LSTM 在处理原始字节序列时，对聊天和 VoIP 等具有强时序交互模式的细粒度行为分类效果最佳。Hartl 等人[103]则利用 LSTM 学习包序列的条件概率分布，并结合 Viterbi-like 搜索算法，成功地从加密隧道中分离出被复用的多个原始流。Gu 等人[107]提出的 DecETT 框架利用双分支 Siamese 网络处理包大小与方向序列，通过解耦协议特征和应用语义，显著提升了在多种隧道下的应用指纹识别能力。Zhou 等人[141]也采用了双向状态空间模型这一 RNN 的演进变体来建模分段的包长序列。

（3）图神经网络。GNN 适用于对流量中蕴含的拓扑关系和复杂交互进行建模，尤其在主机级别分析中表现突出。Liu 等人[105]提出的 HINT 框架是该方向的代表性工作。该方法将 HTTPS 隧道检测问题建模为异构信息网络中的节点分类，网络中包含了主机、服务、客户端和指纹等多类节点。HINT 利用双层注意力 GNN 聚合元路径上的邻居信息，从而融合了网络拓扑、主机行为统计和流指纹等多模态信息，在对抗流量填充和整形时表现出极高的鲁棒性。Zhang[118]在分析 Tor-over-Socks5 流量时，也利用图卷积网络来建模包与包之间的时空关系。

（4）Transformer。Transformer 模型利用自注意力机制来捕捉序列内的长程依赖关系，克服了传统

RNN的局限性。Liu等人[108]提出的ProxyCorr模型是Transformer在流关联任务上的典型应用。该模型将流量抽象为时序状态序列和二维空间轨迹,并分别输入Transformer编码器。Xie[125]将自注意力模块嵌入1D-CNN中以强化关键特征。Zhang[118]和Zhou等人[141]则使用Transformer的多头注意力模块来处理高维的流级别统计特征,以捕捉不同特征组之间的非线性关系。

(5)自编码器。自编码器作为一种无监督的表征学习模型,主要用于特征降维和异常检测。Zhou等人[117]提出了BiAE-MLP模型,使用双自编码器分别学习正常流量和代理流量的高维手工特征,并将其压缩为32维的低维表征,以此提升跨平台检测的泛化能力。Litvinov[131]在对比V2Ray识别模型时也测试了自编码器,但发现在面对未见配置时其泛化能力较差。

综上所述,加密代理流量分析算法的演进主要围绕检测与生存的攻防博弈展开。基于规则的算法从早期的静态特征匹配演变为针对代理协议实现逻辑缺陷的验证手段。其深层动因在于,虽然加密代理在流量形态上能高度拟态标准加密协议(如HTTPS),但其轻量化的服务端实现在异常处理、重放抵抗或TLS握手支持上,往往难以复刻成熟Web服务器的完整逻辑。机器学习算法在VPN分析中表现稳健,但在加密代理场景下,受限于人工特征在强伪装流量中的表达能力瓶颈,难以在海量背景流量中有效区分高度拟态的代理流量,从而陷入高误报的困境。未来的算法研究需要在模型的抗混淆鲁棒性与计算资源消耗之间寻找平衡,并重点解决实验室环境下高精度模型在现网大规模部署中的适应性难题。

3.4　加密代理主要研究动态

加密代理流量分析的主要研究动态集中体现了审查与规避博弈中的最新进展。本节将加密代理流量主要研究动态归纳为三个方向,包括加密代理审查技术研究、加密代理检测技术研究以及加密代理流量指纹研究。

3.4.1　加密代理审查技术研究

加密代理审查技术研究关注审查系统工作机制及代理生态特征。该领域首先关注庞杂的代理生态。Perino等人[109]利用ProxyTorrent平台对全球免费HTTPS代理生态进行了长期监测,发现其可用性极低且约10%存在可疑行为,揭示了该生态的不可靠性。随后,研究转向逆向分析国家级审查系统的检测机制。Alice等人[7]系统测量发现,GFW采用被动监测标记与主动探测确认相结合的策略,即根据服务器对探针的TCP层响应最终确认Shadowsocks身份。Frolov等人[10]进一步泛化该思想,证明多种抗探测代理在实现沉默策略时的TCP连接关闭阈值存在可被利用的实现指纹。

在理解审查机制的同时,对代理生态的测量也在深化。Mühle等人[120]利用多视角RTT测量发现,比特币P2P网络中代理使用率极低。Yang等人[101]则针对中国住宅代理生态构建了大规模数据集,利用NLP与被动DNS分析揭示了该生态的高流失率及与恶意活动高度共现的特征。

随着代理技术转向协议模仿,审查技术也随之演进。Wu等人[11]揭示了GFW针对完全加密流量的新型被动检测系统。该系统采用了一套高效的豁免规则,即流量默认可疑,除非其首包匹配特定统计规则或已知协议指纹,否则将被概率性阻断。Wang等人[114]则发现ShadowTLS虽模拟了握手,但其握手后TCP行为与真实TLS服务器的不一致性仍可被主动探测识别。

审查基础设施本身也成为研究对象。Sakamoto等人[142]利用GFW DNS注入器的越界读取漏洞,成功诱导其泄露内存数据,揭示了设备安全缺陷及DDoS放大风险。Lange等人[145]则揭示了伊朗审查系统在HTTP/DNS解析上的实现缺陷(如大小写敏感),为规避提供了新思路。

3.4.2　加密代理检测技术研究

加密代理检测旨在解决代理与非代理的二分类问题。由于现代代理协议常伪装成TLS且缺乏固定指纹,研究重点已从端口和DPI转向基于侧信道与行为模式的分析。与VPN相比,加密代理伪装更灵活,检测框架已演进为综合运用主动探测、主机上下文、协议无关侧信道及深度学习的多模态、高鲁棒性分析体系。

早期研究主要依赖启发式规则与经典机器学习。Janbeglou和Brownlee[127]通过寻找目标IP DNS解析缺失及流量时序相关性来识别自定义隧道。Husák等人[143]利用ClientHello中的密码套件构建被动TLS指纹库,实现了客户端的高精度识别。Deng等人[134]较早利用随机森林检测Shadowsocks,准确率超85%。Ejeta等人[132]利用SVM检测Psiphon。Perino等人[109]则结合爬虫、主动探测与相似度匹配,实现了对免费HTTPS代理生态的大规模检测。

随着技术发展,复杂特征与主动探测被引入。Zeng等人[97]引入主机流行为与DNS等上下文特征,在校园网中实现了Shadowsocks的高精度识别。Cheng等人[98]提出的ACER框架则结合主动探针与XGBoost来识别代理服务器。此后,检测方法进一步多样化。Miller等人[135]利用TCP头与流统计特征训练多层感知器检测匿名代理。Mühle等人[120]通过多

视角 RTT 测量检测比特币网络中的代理节点。Luo 等人[122]针对 V2Ray 设计了结合主机行为与首包载荷的实时检测方法。针对 ShadowsocksR，Ji 等人[123]与 Luo 等人[130]分别利用 XGBoost 和 LightGBM 等集成模型，结合包熵与协议头特征实现了有效检测。

近年来，研究转向高级被动分析与深度学习。Yang 等人[101]利用 NLP 分析网站语义并结合被动 DNS 研究住宅代理生态。Zhao 等人[126]和 Zhang 等人[104]利用深度学习处理原始字节序列以检测 Shadowsocks 异常。针对高级伪装，Wang 等人[114]发现 ShadowTLS 虽模拟握手，但握手后 TCP 行为与真实服务器不一致，仍可被探测。Song 等人[144]指出 Tor 即使被加密代理二次封装，其固定 Cell 长度仍可通过 SVM 识别。

最新研究正朝协议无关与强鲁棒性方向发展。Xue 等人[13]利用统计检验识别协议嵌套特征，随后进一步发现跨层 RTT 差异指纹并通过序贯假设检验实现检测[15]。Wang 等人[128]指出自定义拥塞控制会暴露独特模式。Liu 等人[105]提出 HINT 框架，利用 GNN 融合拓扑与统计特征对抗流量整形。Xie[125]和 Litvinov[131]则分别应用 1D-CNN 与新兴 KAN 模型识别 VMess 等最新代理。

3.4.3 加密代理流量指纹研究

与 VPN 相比，加密代理流量指纹分析面临独特挑战。一方面，代理为每个应用连接建立独立连接，带来训练-测试不对称和跨环境泛化难题。另一方面，代理协议及其混淆插件对流量进行重封装、填充或整形，旨在对抗统计分析。

早期研究集中在验证网站指纹在加密代理上的可行性。Spreitzer 等人[129]利用 Android 高频采样构建流量签名，并用 Jaccard 相似度匹配，在封闭世界及 Tor 代理下均有效。Ejeta 等人[132]对 Psiphon 进行网站指纹攻击，利用包长、方向等特征结合 SVM 和 KNN，实现了流量检测和有限的指纹识别。

随后研究关注更复杂的真实场景。Aceto 等人[115]证明组合多个异构分类器能显著提升移动应用指纹识别性能。Zhuo 等人[96]针对真实浏览中的超链接跳转噪声，应用 Profile HMM 模型建模网页跳转，在 Shadowsocks 数据集上准确率远超传统方法。Zhao 等人[133]首次评估真实 Shadowsocks 流量，发现其指纹比受控环境下的 Tor 更难识别，并提出了基于效率的特征选择方法。

之后，研究焦点转向解决真实环境中的训练-测试不对称挑战。Ma 等人[99-100]提出上下文感知的攻击框架，放弃依赖完整访问样本，转而分析独立流。该方法利用 RF 叶节点索引作为流指纹，结合流的网站指示度与时间相关性，在开放世界中实现了高准确率。

同时，网站指纹攻防对抗持续升级。Huang 等人[146]针对 Shadowsocks 提出了 PadS 和 PadI 防御，分别基于真实包长和 IAT 分布进行填充与插包。Rahman 等人[139]提出 Mockingbird 防御，利用对抗样本思想迭代添加填充以混淆流量轨迹，大幅降低了深度学习攻击器的准确率。

2022 年，指纹识别粒度与鲁棒性进一步提升。Wang 等人[102]提出 SSAPPIDENTIFY，利用滑动窗口 JS 散度特征刻画流量局部变化，提升了跨设备识别鲁棒性。Beckerle 等人[111]使用 Maturesc 攻击流量分裂防御，证明仅需观测数百个包即可削弱防御效果。同年，Zhao 等人[126]利用 LSTM 处理原始字节序列，实现了 Shadowsocks 下异常及用户行为的细粒度分类。Hartl 等人[103]解决了流复用难题，利用 LSTM 和 Viterbi-like 算法成功分离交错包序列。

随后，研究关注更具挑战性的场景。Hu 等人[138]针对加密代理下的挖矿流量，通过对比包长和 IAT 分布，在数据极端不平衡下实现了零误报。Cui 等人[116]解决了单向流可见下的 Shadowsocks 应用识别难题，利用 JS 散度等特征和集成树模型达到约 67% 准确率。Ding 等人[147]则提取多维指纹，识别加密隧道下的非同质化代币应用。

近期研究向更精细粒度与复杂模型演进。Zhang 等人[104]使用 packet-bytes textCNN 提升了异常及行为识别性能。Zhou 等人[141]提出多模态框架 CNPT-BiSSM，融合统计特征与包长序列识别混淆行为。Zhang 等[106]提出 SCEP-TI，分析 VMess 下 TCP ACK 差值提取视频分段序列，利用 1D-CNN 识别视频标题。Gu 等人[107]提出 DecETT，利用 TLS 流作语义锚点解耦协议与应用特征，提升了指纹识别能力。Li 等人[110]提出 X-EPRINT，通过生成跨环境不变特征解决泛化难题。Liu 等人[108]提出 ProxyCorr，利用 Transformer 建模时空轨迹实现流鲁棒关联。Zhang[118]结合 GCN 与 Transformer 识别 Tor-over-Socks5 下的细粒度服务。

综上所述，加密代理流量分析的研究动态主要集中在主动探索审查系统的检测规则与深度挖掘细粒度的应用行为特征这两个方向。在审查机制研究方面，工作重心已从单纯的被动测量转向对审查系统主动探测逻辑与检测规则的深度逆向，从而揭示审查者利用协议实现差异识别的机制。在指纹识别方面，研究已突破简单的应用分类，向着更具挑战性的网站指纹防御、复用流分离以及特定恶意行为识别方向发展。然而，现有研究在对抗鲁棒性、模型可解释性及跨环境泛化能力等方面仍显不足，未来的研究将致力

于挖掘难以被伪装消除的协议无关本质特征,并向着低误报、可解释的实战化分析方向演进。

4　研究挑战与未来展望

本节将聚焦于当前对抗场景下的加密隧道流量分析难题提出挑战与展望。挑战包括概念漂移、流定义失效、威胁模型差异、可解释性缺失以及基本比率谬误五个方面。之后,本节从四个维度展望了未来的研究方向。

4.1　研究挑战

4.1.1　概念漂移

概念漂移是指目标预测变量的统计特性随时间发生变化,从而导致已训练模型的性能下降。在加密隧道流量分析领域,这种漂移并非源于良性的网络变化,而是由加密隧道协议不断进化而主动驱动的。具体而言,无论是VPN协议还是加密代理,其协议规范、加密原语、握手模式和包长分布都在对抗场景下快速迭代。此外,流量混淆插件和ESNI/ECH等技术更是主动地随机化或消除可辨识的特征。这些因素共同导致了流量分析模型所依赖的特征分布的快速漂移。尽管2.3.3节综述了部分应对概念漂移的先进研究,例如采用增量学习和在线更新机制来动态调整模型。然而,这些方法大多假设特征空间是相对稳定的,它们旨在更新模型以适应流量统计分布的渐变。但加密代理协议更新带来的并非渐变而是突变,其从根本上消除了之前的协议指纹特征,转而采用协议伪装策略。传统的增量学习难以应对这种由规避策略范式转变引起的特征空间坍塌,从而最终导致模型失效。

4.1.2　流定义失效

随着多路复用技术的应用以及QUIC协议的普及,基于五元组的传统流定义正面临严峻挑战。加密流量分析依赖的静态五元组映射假设在现代加密隧道中逐渐不再成立,主要体现在以下维度的物理流与逻辑流映射错位。

(1)多逻辑流对应单一物理流(多路复用)。部分VPN与现代加密代理常采用长会话复用与多路复用等机制,将并发的多个应用层逻辑连接映射到单一的物理隧道连接(即One-flow现象)中。这种聚合行为导致被动观测到的单条五元组流特征不再反映单一应用的特征,而是多个异构应用流量的统计混合体,从而使基于单流特征的细粒度业务识别方法效果降低甚至失效。

(2)一逻辑流对应多物理流(连接迁移)。QUIC协议的连接迁移特性允许客户端在网络环境变化或NAT重绑定时,通过连接ID维持会话,导致一个逻辑连接在网络层分裂为多个具有不同五元组的碎片流。一方面,迁移后的新五元组流往往缺乏握手阶段的关键指纹,极易被模型误判为背景噪声;另一方面,由于QUIC连接ID本身的加密与更新机制,被动观测者难以在缺乏明文标识的情况下,将散落在不同时间、不同IP的碎片流重新关联回同一个逻辑实体。

综上所述,多路复用导致流多合一聚合,而连接迁移导致流一分多碎片化。其意味着基于五元组的特征工程正在失效。未来的研究亟须探索不依赖五元组的、基于时空相关性或行为语义的流定义与关联新范式。

4.1.3　威胁模型差异

当前学术界构建的理想实验环境与审查者所处的现实威胁模型之间存在较大差异。这种差异贯穿于数据获取、模型训练到最终部署的整个流程。其主要表现为数据采集失真与部署环境异构两个维度。

首先是数据集采集。如第2.1.1节所述,在VPN流量分析领域中,即便是应用最广泛的ISCXVPN2016数据集,也被后续研究指出存在严重的采集偏差和标注问题。另一方面,如3.1节所言,在加密代理分析领域,高质量的公开数据集极为匮乏。这种匮乏的根源来源于加密规避技术本身的成功。这一困境迫使绝大多数研究转向在受控的实验室环境中构建自采数据集,并反过来加剧了数据集的失真和匮乏。此外,真实网络环境的网络噪声同样会对分析造成不良影响。实验室中表现优异的细粒度指纹在开放世界中经历丢包、重传、乱序等复杂网络环境后是否依然具备鲁棒性需要进一步验证。

其次是模型部署环境。真实网络是典型的开放世界场景,充斥着海量未知背景流量。由于模型在训练阶段无法覆盖所有非目标负样本,当其面对这些未见流量时可能错误归纳为目标正样本。这种由“未见即误判”引发的高误报率在网站指纹识别等细粒度分类任务中尤为严重,成为实验室高精度模型难以在实战中落地的主要障碍。另一方面,ISP级分析需要满足线速检测。前文提到的复杂特征或重型模型虽然在离线测试中表现优异,但其高昂的计算复杂度可能难以满足实时线速检测的需求。

4.1.4　可解释性缺失

可解释性缺失是当前深度学习流量分析模型面临的共同挑战。如第2.3.3节和第3.3.3节所述,本领域已涌现出大量复杂的黑盒模型。这些模型虽然在特定数据集上取得了极高的分类精度,但其决策过程并不透明。

可解释性不仅仅是一个学术追求,更是关乎技术能否从实验室走向现实部署的关键障碍。在网络攻

击者的真实操作环境中，任何网络干预都具有严肃的法律和商业后果。如果某条流为非法隧道的判定由一个基于深度学习的黑盒模型做出，则运营者无法追溯该判决的具体依据。这导致了两个致命问题。第一，运营者无法信任模型的判决，因为其可能受到数据污染、对抗性攻击或模型偏见的影响；第二，运营者无法在法律上为其决策辩护，尤其是在面对因附带损害而引起的投诉时。

4.1.5 基本比率谬误

基本比率谬误是指在评估概率时过度关注分类器高精度等特定信息，而忽略了基础比率的统计学陷阱。具体而言，设事件C表示某条流为加密代理流量，事件A表示检测系统发出告警。进一步的，$P(\mathrm{C})$为网络环境中加密代理流量的基础比率（prior probability），$P(\mathrm{A}|\mathrm{C})$为检测模型的真阳性率（True Positive Rate，TPR），$P(\mathrm{A}|\neg\mathrm{C})$为假阳性率（False Positive Rate，FPR）。根据贝叶斯公式，当检测系统发出告警时，该流量确为加密代理的后验概率$P(\mathrm{C}|\mathrm{A})$表示为

$$P(\mathrm{C}|\mathrm{A})=\frac{P(\mathrm{A}|\mathrm{C})\cdot P(\mathrm{C})}{P(\mathrm{A}|\mathrm{C})\cdot P(\mathrm{C})+P(\mathrm{A}|\neg\mathrm{C})\cdot P(\neg\mathrm{C})} \tag{1}$$

协议伪装策略协议的核心目标是混入数以亿计的合法TLS流量之中，导致基础比率$P(\mathrm{C})$极低。假设在开放世界场景中，加密代理流量的基础比率仅为万分之一（即$P(\mathrm{C})=10^{-4}$），而绝大多数流量为合法的背景流量（$P(\neg C)\approx 1$）。同时，假设攻击者部署了一个在实验室表现优异的分类器，其TPR高达99.9%，FPR低至0.1%，将上述数值代入公式：

$$\begin{aligned}P(\mathrm{C}|\mathrm{A})&=\frac{0.999\times 0.0001}{0.999\times 0.0001+0.001\times 0.9999}\\&\approx\frac{0.0001}{0.0001+0.001}\approx 9.08\%\end{aligned} \tag{2}$$

计算结果表明，即便模型拥有99.9%的检测能力，在真实环境中，每收到100次阻断告警，其中仍有超过90次是对合法流量的误报（Precision小于10%）。这种极高的FPR会导致审查系统面临不可接受的附带损害。标准化伪装策略协议正是利用这一统计学屏障，迫使审查者若要有效封锁代理，就必须承担大规模阻断正常业务的风险，从而在不对称的攻防博弈中占据天然优势。

4.2 未来展望

4.2.1 协议无关代理检测

当前的加密代理检测技术多依赖于特定的协议指纹或流统计特征，然而由于协议以及伪装策略的快速迭代，这种依赖静态特征的方法正面临严峻的概念漂移（4.1.1节）挑战。同时，QUIC连接迁移与多路复用机制也打破了传统五元组的流定义（4.1.2节）假设，导致基于单流特征的分析失效。因此，未来的分析技术可转向挖掘那些难以被规避者混淆的、与特定协议无关的底层侧信道信息。

首先，跨层RTT指纹[15]仍然具有极高的检测效力。其利用的传输层RTT与应用层RTT之间的固有差异源于代理架构的本质，因此具有协议无关性，现有加密代理协议难以对其进行伪装。其次，数据包长度序列及其统计特征仍是研究热点。尽管填充和流量整形可以对抗简单的包长指纹，但引入的额外开销和延迟迫使规避者在隐蔽性与性能之间做出权衡，这种权衡本身可能暴露新的统计特征。基础协议产生的行为指纹也不容忽视。例如，部分规避工具采用的激进拥塞控制算法会产生区别于标准Cubic或BBR的可识别指纹[128]。

此外，IPv6环境下的特有分析视角值得高度关注。随着IPv6的普及，其协议栈的固有特性为流量分析提供了新的侧信道。例如，IPv6的流标签字段本应具有高熵值以支持负载均衡，但部分加密代理使用的用户态网络栈实现可能将其置零或呈现固定模式，与现代浏览器的高熵随机化行为形成显著统计差异[148]。同时，IPv6的扩展头链式结构和源端分片机制也暴露了新的指纹。隧道封装引入的固定头部开销（如WireGuard的80字节开销）会导致特定的MTU截断，进而产生区别于正常HTTPS流的分片模式。并且，用户态网络栈在处理ICMPv6消息或双栈并发时的时序与逻辑差异，也极易在IPv6环境下暴露代理工具的实现指纹。

另一方面，针对流定义失效与映射错位的挑战，未来的分析范式需突破单流统计的局限，转向基于时空关联的分析视角[107]。面对QUIC连接迁移导致的流碎片化，可探索基于时序相关性与行为模式相似性的跨流关联技术[108]，利用深度学习模型挖掘散落在不同五元组中的碎片流之间的隐式联系，重构完整的逻辑会话。面对多路复用导致的流聚合，可引入异构图神经网络[105]，将流量实体建模为图节点，利用图拓扑结构中的关联信息辅助从混合流量中分离出特定的业务行为。

4.2.2 在线部署模型设计

当前的加密隧道流量细粒度识别研究中，出于对识别准确率的追求，前沿研究中使用了较多深度学习模型。这些模型虽然在实验室环境下有较好的效果，但是距离在真实网络中部署还存在效率较低（4.1.3节）以及可解释性缺失（4.1.4节）等问题。因此，未来的研究可以从以下两个维度进行改进与优化。

首先，轻量化与实时性是部署于ISP级真实网络环境的刚需。深度学习模型的高计算复杂度使其在

一些情况下能够取得较高准确率,但却与骨干网Tbps级线速检测需求之间存在巨大差异。未来的研究需要转向模型轻量化与软硬协同架构。一方面,可以采用硬件感知的结构化剪枝和低位宽量化技术,在保持精度的同时大幅降低Transformer、GNN等模型的参数量与计算开销。另一方面,探索利用P4可编程交换机或FPGA智能网卡进行硬件卸载。例如,利用P4交换机通过查找表蒸馏[149]或Brain-on-switch技术[150]在数据平面直接过滤大部分背景流量;或采用异构架构,利用ASIC进行特征提取并将复杂流调度至FPGA加速器进行深度推理,从而实现实时高效的在线流量分析。

其次,深度学习模型的黑盒特性是其落地部署的主要障碍。未来的模型设计可引入可解释人工智能技术,利用SHAP、LIME或积分梯度等方法,将模型的预测归因可视化,明确模型是关注于特定的时序模式、载荷统计还是潜在的协议指纹。这不仅有助于建立运营者的信任,满足合规性审计要求,还能反向辅助研究人员理解加密流量在深层特征空间的分布规律,从而设计出更具抗干扰能力的鲁棒特征。

4.2.3　基准数据集构建

现有的加密隧道数据集多构建于受控的实验室环境或静态的采集脚本,缺乏真实网络环境中的复杂背景噪声与动态干扰,导致训练出的模型难以克服数据集困境(4.1.3节)并在真实部署中陷入基本比率谬误(4.1.5节)。因此,未来的数据集构建需要向主动的自动化仿真生成转变,致力于构建涵盖高背景噪声、包含对抗性混淆流量以及具备动态分布特性的下一代基准数据集。

首先,亟须构建基于网络仿真与容器化技术的自动化流量生成框架。现有的采集工作多局限于实验室理想环境或特定的自动化测试脚本,难以复现现网复杂的背景噪声。未来的研究可利用NS-3、Mininet等高保真网络模拟器或Docker容器编排技术,构建可定义的自动化靶场,按需注入不同分布的丢包、延迟、抖动及背景流噪声,从而批量生成带有精确标注的样本。

其次,利用生成式人工智能(Generative Artificial Intelligence,GAI)技术解决数据不平衡问题。在被动采集难以获得足够的正样本时,未来的研究可探索利用生成对抗网络、变分自编码器或扩散模型等来学习加密隧道流量的隐空间特征。通过构造高保真的、统计特性与真实流量一致的合成流量,可以有效扩充少数类样本,人为平衡训练集的类别分布,从而抑制模型对目标流量的过拟合倾向。

最后,构建包含对抗性扰动流量的多样性数据集。鉴于Mockingbird[139]、PadS/PadI[146]等流量变形与防御技术以及XTLS-Vision、Reality等新型协议伪装技术的出现,仅包含未混淆流量的数据集已无法反映真实的攻防现状。新一代数据集需要包含对抗样本以及多种代理协议,即利用自动化框架生成经过填充、整形、伪造时序等混淆处理的对抗性流量,并包含V2Ray、Xray、QUIC-based等类型的现代加密代理协议。

4.2.4　生成式隐写技术探索

随着生成式人工智能的快速发展,利用大语言模型、扩散模型等实现生成式隐写可能成为审查规避技术一个理论上的未来演进方向。以Trojan、VLESS等为代表的现代加密代理转向协议伪装策略,直接借助TLS等主流协议作为封装,使代理连接在外观上更接近常规HTTPS流量。而生成式隐写则强调无载体或自生成载体的思路,即利用生成模型实时构造具有合法语义的载体流量,例如逻辑连贯的聊天文本、音视频片段或其他交互式业务流,并在此基础上承载隧道通信,从而实现原始数据层面上的行为级伪装。理论上,这种方法使载体在语义、交互节奏与统计分布上都能逼近真实应用,极大增加了审查者进行细粒度识别(如网站指纹分析或特定应用识别)的难度。

然而,将GAI应用于加密隧道中在实际落地上仍面临严峻挑战。首先,实时性与算力开销是主要瓶颈。大模型的推理延迟以及对隐写内容的编解码可能难以满足即时通讯或流媒体传输的实时性要求,可能导致严重的用户体验下降甚至服务中断。其次,生成式隐写主要掩盖的是应用层特征及其衍生特征,对于基于网络架构或基础协议固有属性的检测手段[13,15,128],其规避效果可能较为有限。

因此,生成式隐写技术在加密隧道流量对抗中的实际效能尚待验证。未来的研究可以积极探索GAI在规避与检测两端的应用潜力,例如研究轻量化生成模型以解决计算瓶颈,或探索针对生成流量的时序侧信道检测技术,以期在这一新兴领域形成更完善的攻防理论体系。

5　结束语

加密隧道固有的机密性与封装特性使其在规避网络审查方面被广泛应用,催生了审查方与规避方之间持续升级的技术军备竞赛。本文梳理了加密隧道审查规避技术及流量分析领域的相关研究成果,首先从加密隧道基本原理出发,阐述了VPN和加密代理的核心机制,探讨了主流审查规避技术的演进脉络,并为后续分析构建了威胁模型。在此基础上,本文按照技术类别将研究分为VPN流量分析和加密代理流

量分析两大主要进展。针对这两类技术,本文均遵循统一的分析框架,从数据集构建、特征提取、分析算法、研究动态四个维度,系统地梳理了相关研究现状。最后,本文提炼了当前研究面临的核心挑战,并展望了未来研究方向。希望本文能为相关领域的研究人员提供有益的参考,并推动加密隧道流量分析技术的研究与发展。

参考文献

[1] Google. HTTPS encryption on the web[R/OL]. (2025-06-01) [2025-11-14]. https://transparencyreport. google. com/https/overview.

[2] Shen Meng, Ye Ke, Liu Xingtong, et al. Machine learning-powered encrypted network traffic analysis: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(1): 791-824.

[3] Shadowsocks. Shadowsocks | A fast tunnel proxy that helps you bypass firewalls[EB/OL]. (2025-03-07)[2025-11-14]. https://shadowsocks.org/.

[4] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium (USENIX Security 04). San Diego: USENIX Association, 2004: 21.

[5] Ensafi R, Fifield D, Winter P, et al. Examining how the great firewall discovers hidden circumvention servers[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM, 2015: 445-458.

[6] V2Fly. VMess protocol | V2Fly.org[EB/OL]. (2022-01-01)[2025-11-14]. https://www.v2fly.org/en_US/developer/protocols/vmess.html.

[7] Alice, Bob, Carol, et al. How China detects and blocks shadowsocks[C]//Proceedings of the ACM Internet Measurement Conference. New York: ACM, 2020: 111-124.

[8] Yawning. Obfs4 - the obfourscator[EB/OL]. (2022-09-04)[2025-11-14]. https://github.com/yawning/obfs4.

[9] shadowsocksrr. ShadowsocksR: Python port of ShadowsocksR[EB/OL]. (2023-01-03)[2025-11-14]. https://github.com/shadowsocksrr/shadowsocksr.

[10] Frolov S, Wampler J, Wustrow E. Detecting probe-resistant proxies[C]//Proceedings of 2020 Network and Distributed System Security Symposium. San Diego: NDSS Symposium, 2020.

[11] Wu Mingshi, Sippe J, Sivakumar D, et al. How the great firewall of China detects and blocks fully encrypted traffic[C]//Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23). Anaheim: USENIX Association, 2023: 149.

[12] Trojan-GFW. Trojan documentation[EB/OL]. (2024-08-21)[2025-11-14]. https://trojan-gfw.github.io/trojan/.

[13] Xue Diwen, Kallitsis M, Houmansadr A, et al. Fingerprinting obfuscated proxy traffic with encapsulated TLS handshakes[C]//Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24). Philadelphia: USENIX Association, 2024: 2689-2706.

[14] XTLS. XTLS vision, fixes TLS in TLS, to the star and beyond XTLS/Xray-core discussion #1295[EB/OL]. (2022-10-31) [2025-11-14]. https://github. com/XTLS/Xray-core/discussions/1295.

[15] Xue Diwen, Stanley R, Kumar P, et al. The discriminative power of cross-layer RTTs in fingerprinting proxy traffic[C]//Proceedings of the 32nd Network and Distributed System Security Symposium. San Diego: NDSS Symposium, 2025.

[16] 梅汉涛, 程光, 朱怡霖, 等. Tor被动流量分析综述[J]. 软件学报, 2025, 36(1): 253-288.
Mei Hantao, Cheng Guang, Zhu Yilin, et al. Survey on Tor passive traffic analysis[J]. Journal of Software, 2025, 36(1): 253-288. (in Chinese)

[17] 邹鸿程, 苏金树, 魏子令, 等. 网站指纹识别与防御研究综述[J]. 计算机学报, 2022, 45(10): 2243-2278.
Zou Hongcheng, Su Jinshu, Wei Ziling, et al. A review of the research of website fingerprinting identification and defense[J]. Chinese Journal of Computers, 2022, 45(10): 2243-2278. (in Chinese)

[18] 姚忠将, 葛敬国, 张潇丹, 等. 流量混淆技术及相应识别、追踪技术研究综述[J]. 软件学报, 2018, 29(10): 3205-3222.
Yao Zhongjiang, Ge Jingguo, Zhang Xiaodan, et al. Research review on traffic obfuscation and its corresponding identification and tracking technologies[J]. Journal of Software, 2018, 29(10): 3205-3222. (in Chinese)

[19] 史鑫, 郭云飞, 王亚文, 等. 面向匿名网络的审查规避技术研究综述[J]. 信息工程大学学报, 2024, 25(5): 552-558.
Shi Xin, Guo Yunfei, Wang Yawen, et al. A survey on censorship circumvention technologies for anonymous

networks[J]. Journal of Information Engineering University, 2024, 25(5): 552-558. (in Chinese)

[20] Ikram M, Vallina-Rodriguez N, Seneviratne S, et al. An analysis of the privacy and security risks of Android VPN permission-enabled apps[C]//Proceedings of the 2016 Internet Measurement Conference. New York: ACM, 2016: 349-364.

[21] Draper-Gil G, Lashkari A H, Mamun M S I, et al. Characterization of encrypted and VPN traffic using time-related features[C]//Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP). Rome: SciTePress, 2016: 407-414.

[22] Feghhi S, Leith D J. A web traffic analysis attack using only timing information[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1747-1759.

[23] Khan M T, Deblasio J, Voelker G M, et al. An empirical analysis of the commercial VPN ecosystem[C]//Proceedings of the Internet Measurement Conference 2018. New York: ACM, 2018: 443-456.

[24] Zain Ul Abideen M, Saleem S, Ejaz M. VPN traffic detection in SSL-protected channel[J]. Security and Communication Networks, 2019, 2019: 7924690.

[25] Shapira T, Shavitt Y. FlowPic: Encrypted Internet traffic classification is as easy as image recognition[C]//Proceedings of the IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE, 2019: 680-687.

[26] Zhao Ying, Chen Junjun, Wu Di, et al. Multi-task network anomaly detection using federated learning[C]//Proceedings of the 10th International Symposium on Information and Communication Technology. New York: ACM, 2019: 273-279.

[27] Gao Ping, Li Guangsong, Shi Yanan, et al. VPN traffic classification based on payload length sequence[C]//Proceedings of 2020 International Conference on Networking and Network Applications (NaNA). Piscataway: IEEE, 2020: 241-247.

[28] Guo Lulu, Wu Qianqiong, Liu Shengli, et al. Deep learning-based real-time VPN encrypted traffic identification methods[J]. Journal of Real-Time Image Processing, 2020, 17(1): 103-114.

[29] Wu Hua, Liu Yujie, Cheng Guang, et al. RT-CBCH: Real-time VPN traffic service identification based on sampled data in high-speed networks[J]. IEEE Transactions on Network and Service Management, 2024, 21(1): 88-107.

[30] Oh S, Lee M, Lee H, et al. AppSniffer: Towards robust mobile app fingerprinting against VPN[C]//Proceedings of the ACM Web Conference 2023. New York: ACM, 2023: 2318-2328.

[31] Tian Yuan, Cao Zechun, Huang S H S. Detecting VPN traffic in real-time with active probing[C]//Proceedings of 2024 22nd International Symposium on Network Computing and Applications (NCA). Piscataway: IEEE, 2024: 132-139.

[32] Xue Diwen, Ramesh R, Jain A, et al. OpenVPN is open to VPN fingerprinting[J]. Communications of the ACM, 2025, 68(1): 79-87.

[33] Wang Chenxu, Yin Jiangyi, Li Zhao, et al. Identifying VPN servers through graph-represented behaviors[C]//Proceedings of the ACM Web Conference 2024. New York: ACM, 2024: 1790-1799.

[34] Guo Xiaoguang, Yu Keyang, Li Qi, et al. Fingerprinting voice commands of VPN-protected smart speakers[J]. ACM Transactions on Sensor Networks, 2026, 22(4): 1-31.

[35] Wang W, Ortwein A, Sobrados E, et al. MVPNalyzer: An investigative framework for auditing the security & privacy of mobile VPNs[C]//Proceedings of the 2026 Network and Distributed System Security (NDSS) Symposium. San Diego: The Internet Society, 2026. DOI: 10.14722/ndss.2026.231573.

[36] Kotak J, Yankelev I, Bibi I, et al. VPN-encrypted network traffic classification using a time-series approach[J]. IEEE Transactions on Network and Service Management, 2025, 22(2): 2225-2242.

[37] Naas M, Fesl J. A novel dataset for encrypted virtual private network traffic analysis[J]. Data in Brief, 2023, 47: 108945.

[38] Xu Zhenyu, Ren Xurui, Zhang Yi, et al. Peering through the veil: A segment-based approach for VPN encapsulated video title identification[C]//Proceedings of the IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway: IEEE, 2024: 1500-1505.

[39] Li Qi, Yu Keyang, Chen Dong, et al. TrafficSpy: Disaggregating VPN-encrypted IoT network traffic for user pri-

vacy inference[C]//Proceedings of 2022 IEEE Conference on Communications and Network Security. Piscataway: IEEE, 2022: 145-153.

[40] Mixon-Baca B, Knockel J, Crandall J R. Hidden links: Analyzing secret families of VPN apps[C]//Proceedings of the 15th Workshop on Free and Open Communications on the Internet (FOCI). Washington: The PETS Symposium, 2025: 18-27.

[41] Liu Haotian, Alshammari R, Zincir-Heywood N. Edge-cloud VPN traffic analysis over cross platforms[C]//Proceedings of 2024 IEEE 10th World Forum on Internet of Things (WF-IoT). Piscataway: IEEE, 2024: 10811218.

[42] Wu Hua, Liu Yujie, Cheng Guang, et al. Real-time identification of VPN traffic based on counting bloom filter and chained hash table from sampled data in high-speed networks[C]//Proceedings of ICC 2022-IEEE International Conference on Communications. Piscataway: IEEE, 2022: 5070-5075.

[43] Ramesh R, Evdokimov L, Xue Diwen, et al. VPNInspector: Systematic investigation of the VPN ecosystem[C]// Proceedings of the Network and Distributed System Security (NDSS) Symposium. San Diego: The Internet Society, 2022: 24285.

[44] Fesl J, Naas M. A comprehensive machine learning-based approach for virtual private network traffic detection, classification and hiding[J]. Computer Networks, 2025, 270: 111530.

[45] Almomani A. Classification of virtual private networks encrypted traffic using ensemble learning algorithms[J]. Egyptian Informatics Journal, 2022, 23(4): 57-68.

[46] Gupta A. VPN-nonVPN traffic classification using deep reinforced naive Bayes and fuzzy K-means clustering[C]// Proceedings of 2021 IEEE 41st International Conference on Distributed Computing Systems Workshops (ICDCSW). Piscataway: IEEE, 2021: 00008.

[47] Abbas G, Farooq U, Singh P, et al. Feature engineering and ensemble learning-based classification of VPN and non-VPN-based network traffic over temporal features[J]. SN Computer Science, 2023, 4(5): 546.

[48] Razooqi Y S, Pekar A. Binary VPN traffic detection using wavelet features and machine learning[C]//Proceedings of 2025 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Piscataway: IEEE, 2025: 11197436.

[49] Fu Peipei, Liu Chang, Yang Qingya, et al. NSA-Net: A NetFlow sequence attention network for virtual private network traffic detection[C]//Proceedings of the 21st International Conference on Web Information Systems Engineering (WISE). Heidelberg: Springer, 2020: 430-444.

[50] Miller S, Curran K, Lunney T. Multilayer perceptron neural network for detection of encrypted VPN network traffic[C]//Proceedings of 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). Piscataway: IEEE, 2018: 8551395.

[51] Huang Kai, Zhou Ming, Zhang Peng, et al. Enhancing VPN traffic recognition through CatBoost feature extraction and stacking ensemble learning[C]//Proceedings of ICC 2024 - IEEE International Conference on Communications. Piscataway: IEEE, 2024: 79-84.

[52] Tang Jiyue, Yang Le, Liu Song, et al. Caps-LSTM: A novel hierarchical encrypted VPN network traffic identification using CapsNet and LSTM[C]//Proceedings of the Third International Conference on Science of Cyber Security. Heidelberg: Springer, 2021: 139-153.

[53] Balachandran A, Amritha P P. VPN network traffic classification using entropy estimation and time-related features[M]//IOT with smart systems. Singapore: Springer Nature Singapore, 2022: 509-520.

[54] Gudla R, Vollala S, Srinivasa K G, et al. TCC: Time constrained classification of VPN and Non-VPN traffic using machine learning algorithms[J]. Wireless Networks, 2025, 31(4): 3415-3429.

[55] Caicedo-Muñoz J A, Ledezma Espino A, Corrales J C, et al. QoS-Classifier for VPN and Non-VPN traffic based on time-related features[J]. Computer Networks, 2018, 144: 271-279.

[56] Lv Sicai, Wang Chao, Wang Zibo, et al. AAE-DSVDD: A one-class classification model for VPN traffic identification[J]. Computer Networks, 2023, 236: 109990.

[57] Habibi Lashkari A, Draper Gil G, 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 (ICISSP). Porto: SciTePress, 2017: 253-262.

[58] Li Zhiyuan, Zhao Hongyi, Zhao Jingyu, et al. SAT-Net: A staggered attention network using graph neural net-

works for encrypted traffic classification[J]. Journal of Network and Computer Applications, 2025, 233: 104069.

[59] Lin Xinjie, Xiong Gang, Gou Gaopeng, et al. ET-BERT: A contextualized datagram representation with pre-training transformers for encrypted traffic classification[C]// Proceedings of the ACM Web Conference 2022. New York: ACM, 2022: 633-642.

[60] Liu Ya, Wang Xiao, Qu Bo, et al. ATVITSC: A novel encrypted traffic classification method based on deep learning[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 9374-9389.

[61] Peng Quan, Fu Xingbing, Lin Fei, et al. Multi-scale convolutional neural networks optimized by elite strategy dung beetle optimization algorithm for encrypted traffic classification[J]. Expert Systems with Applications, 2025, 264: 125729.

[62] Habibi L A, Kaur G, Rahali A. DIDarknet: A contemporary approach to detect and characterize the darknet traffic using deep image learning[C]//Proceedings of the 2020 10th International Conference on Communication and Network Security (ICCNS). New York: ACM, 2020: 3442521.

[63] Aswad S A, Sonuç E. Classification of VPN network traffic flow using time related features on Apache Spark[C]// Proceedings of 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). Piscataway: IEEE, 2020: 9254893.

[64] 郑晓峰, 段海新, 陈震宇, 等. DataCon: 面向安全研究的多领域大规模竞赛开放数据[J]. 信息安全学报, 2024, 9(1): 123-136.
Zheng Xiaofeng, Duan Haixin, Chen Zhenyu, et al. DataCon: Open dataset for large-scale multiple fields security research and competitions[J]. Journal of Cyber Security, 2024, 9(1): 123-136. (in Chinese)

[65] Xu Hongbo, Li Shuhao, Cheng Zhenyu, et al. VT-GAT: A novel VPN encrypted traffic classification model based on graph attention neural network[C]//Proceedings of the 18th EAI International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). Heidelberg: Springer, 2022: 437-456.

[66] Jorgensen S, Holodnak J, Dempsey J, et al. Extensible machine learning for encrypted network traffic application labeling via uncertainty quantification[J]. IEEE Transactions on Artificial Intelligence, 2024, 5(1): 420-433.

[67] Guo Xiaoguang, Yu Keyang, Li Qi, et al. VoiceAttack: Fingerprinting voice command on VPN-protected smart home speakers[C]//Proceedings of the 11th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation. New York: ACM, 2024: 55-65.

[68] Maghsoudlou A, Vermeulen L, Poese I, et al. Characterizing the VPN ecosystem in the wild[C]//Proceedings of the 24th International Conference on Passive and Active Measurement. Heidelberg: Springer, 2023: 18-45.

[69] Farnan O, Wright J, Darer A. Analysing censorship circumvention with VPNs via DNS cache snooping[C]//Proceedings of 2019 IEEE Security and Privacy Workshops. Piscataway: IEEE, 2019: 205-211.

[70] Schwartz T, Manor O, Otung A. SNITCH: Leveraging IP geolocation for active VPN detection[C]//Proceedings of 2025 Workshop on Measurements, Attacks, and Defenses for the Web. NDSS Symposium, 2025. DOI: 10.14722/madweb.2025.23008.

[71] Telikani A, Gandomi A H, Choo K 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.

[72] Zhang Jielun, Li Fuhao, Wu Hongyu, et al. Autonomous model update scheme for deep learning based network traffic classifiers[C]//Proceedings of 2019 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE, 2019: 9014036.

[73] Zhang Jielun, Li Fuhao, Ye Feng, et al. Autonomous unknown-application filtering and labeling for DL-based traffic classifier update[C]//Proceedings of IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2020: 397-405.

[74] 王琳, 封化民, 刘飚, 等. 基于混合方法的SSL VPN加密流量识别研究[J]. 计算机应用与软件, 2019, 36(2): 315-322.
Wang Lin, Feng Huamin, Liu Biao, et al. SSL VPN encrypted traffic identification based on hybrid method[J]. Computer Applications and Software, 2019, 36(2): 315-322. (in Chinese)

[75] 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 Yimin, Liu Fangzheng, Wang Yong. IPSec VPN en-

crypted traffic identification based on hybrid method[J]. Computer Science, 2021, 48(4): 295-302. (in Chinese)

[76] Meng Yongwei, Qin Tao, Wang Haonian, et al. TPIPD: A robust model for online VPN traffic classification[C]// Proceedings of 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway: IEEE, 2022: 105-110.

[77] 唐舒烨, 程光, 蒋泊淼, 等. 基于分段熵分布的VPN加密流量检测与识别方法[J]. 网络空间安全, 2020, 11(8): 23-27.
Tang Shuye, Cheng Guang, Jiang Bomiao, et al. Detection and recognition of VPN encrypted traffic based on segmented entropy distribution[J]. Cyberspace Security, 2020, 11(8): 23-27. (in Chinese)

[78] Ling Zhen, Luo Junzhou, Xu Danni, et al. Novel and practical SDN-based traceback technique for malicious traffic over anonymous networks[C]//Proceedings of the IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2019: 1180-1188.

[79] Rajore T, Jithin S, Gupta A, et al. VPN or Vpwn How afraid should you be of VPN traffic identification? [C]// Proceedings of 2025 9th Network Traffic Measurement and Analysis Conference (TMA). Piscataway: IEEE, 2025: 11096969.

[80] Almutairi S, Neumann Y, Harfoush K. Fingerprinting VPNs with custom router firmware: A new censorship threat model[C]//Proceedings of 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC). Piscataway: IEEE, 2024: 976-981.

[81] Yao Haipeng, Liu Chong, Zhang Peiying, 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.

[82] Zhou Guangmeng, Guo Xiongwen, Liu Zhuotao, et al. TrafficFormer: An efficient pre-trained model for traffic data[C]//Proceedings of 2025 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2025: 1844-1860.

[83] Nascita A, Montieri A, Aceto G, et al. Improving performance, reliability, and feasibility in multimodal multitask traffic classification with XAI[J]. IEEE Transactions on Network and Service Management, 2023, 20(2): 1267-1289.

[84] Cai Wei, Hou Chengshang, Cui Mingxin, et al. Incremental encrypted traffic classification via contrastive prototype networks[J]. Computer Networks, 2024, 250: 110591.

[85] Kattadige C, Choi K N, Wijesinghe A, et al. SETA++: Real-time scalable encrypted traffic analytics in multi-Gbps networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 3244-3259.

[86] Gao Bowen, Yang Yang, Gao Zhipeng, et al. Unsupervised network traffic classification based on multi-source synergistic distribution alignment[C]//Proceedings of GLOBECOM 2023 - 2023 IEEE Global Communications Conference. Piscataway: IEEE, 2023: 4313-4319.

[87] Shen Meng, Ji Kexin, Wu Jinhe, et al. Real-time website fingerprinting defense via traffic cluster anonymization[C]// Proceedings of the 45th IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2024: 3238-3256.

[88] Shen Meng, Ji Kexin, Gao Zhenbo, et al. Subverting website fingerprinting defenses with robust traffic representation[C]//Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23). Anaheim: USENIX Association, 2023: 607-624.

[89] Shen Meng, Liu Yiting, Zhu Liehuang, et al. Fine-grained webpage fingerprinting using only packet length information of encrypted traffic[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2046-2059.

[90] Zhao Xiyuan, Deng Xinhao, Li Qi, et al. Towards fine-grained webpage fingerprinting at scale[C]//Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS'24). New York: ACM, 2024: 423-436.

[91] Deng Xinhao, Yin Qilei, Liu Zhuotao, et al. Robust multi-tab website fingerprinting attacks in the wild[C]//Proceedings of 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE, 2023: 1005-1022.

[92] Kamal K M A, Almuhammadi S. Vulnerability of virtual private networks to web fingerprinting attack[M]//Advances in security, networks, and internet of things. Cham: Springer International Publishing, 2021: 147-165.

[93] Perdices D, López De Vergara J E, González I, et al. Web browsing privacy in the deep learning era: Beyond VPNs and encryption[J]. Computer Networks, 2023, 220: 109471.

[94] Tolley W J, Kujath B, Khan M T, et al. Blind In/On-Path

attacks and applications to VPNs[C]//Proceedings of the 30th USENIX Security Symposium (USENIX Security 21). Online: USENIX Association, 2021: 3129-3146.

[95] Fu Chuanpu, Li Qi, Shen Meng, et al. Detecting tunneled flooding traffic via deep semantic analysis of packet length patterns[C]//Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2024: 3659-3673.

[96] Zhuo Zhongliu, Zhang Yang, Zhang Zhili, et al. Website fingerprinting attack on anonymity networks based on profile hidden Markov model[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(5): 1081-1095.

[97] Zeng Xuemei, Chen Xingshu, Shao Guolin, et al. Flow context and host behavior based Shadowsocks's traffic identification[J]. IEEE Access, 2019, 7: 41017-41032.

[98] Cheng Jiaxing, Li Ying, Huang Cheng, et al. ACER: Detecting Shadowsocks server based on active probe technology[J]. Journal of Computer Virology and Hacking Techniques, 2020, 16(3): 217-227.

[99] Ma Xiaobo, Qu Jian, Shi Mawei, et al. Website fingerprinting on encrypted proxies: A flow-context-aware approach and countermeasures[J]. IEEE/ACM Transactions on Networking, 2024, 32(3): 1904-1919.

[100] Ma Xiaobo, Shi Mawei, An Bingyu, et al. Context-aware website fingerprinting over encrypted proxies[C]//Proceedings of the IEEE INFOCOM 2021-IEEE Conference on Computer Communications. Piscataway: IEEE, 2021: 9488676.

[101] Yang Mingshuo, Yu Yunnan, Mi Xianghang, et al. An extensive study of residential proxies in China[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 3049-3062.

[102] Wang Suixing, Yang Chao, Guo Gang, et al. SSAPPIDENTIFY: A robust system identifies application over Shadowsocks's traffic[J]. Computer Networks, 2022, 203: 108659.

[103] Hartl A, Fabini J, Zseby T. Separating flows in encrypted tunnel traffic[C]//Proceedings of 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA). Piscataway: IEEE, 2022: 609-616.

[104] Zhang Shunliang, Zhao Hongce, Fan Zuwei. Packet bytes-based abnormal encrypted proxy traffic identification[C]//Proceedings of 2024 IEEE 30th International Conference on Telecommunications (ICT). Piscataway: IEEE, 2024: 10606114.

[105] Liu Mengyan, Gou Gaopeng, Xiong Gang, et al. Enhanced detection of obfuscated HTTPS tunnel traffic using heterogeneous information network[J]. Computer Networks, 2025, 257: 110975.

[106] Zhang Yi, Xu Zhenyu, Ren Xurui, et al. SCEP-TI: A side-channel attack on encrypted proxy video streams for video title identification[J]. Computer Networks, 2025, 271: 111630.

[107] Gu Zheyuan, Liu Chang, Zhang Xiyuan, et al. DecETT: Accurate app fingerprinting under encrypted tunnels via dual decouple-based semantic enhancement[C]//Proceedings of the ACM on Web Conference 2025. New York: ACM, 2025: 2413-2423.

[108] Liu Mengyan, Gou Gaopeng, Xiong Gang, et al. ProxyCorr: Robust traffic correlation attacks via mixed spatio-temporal analysis in encrypted proxy networks[J]. Computer Networks, 2025, 273: 111763.

[109] Perino D, Varvello M, Soriente C. ProxyTorrent: Untangling the free HTTP(S) proxy ecosystem[C]//Proceedings of the 2018 World Wide Web Conference. New York: ACM, 2018: 197-206.

[110] Li Jianfeng, Wang Dongliang, Liu Yixuan, et al. Cross-environmental website fingerprinting[C]//Proceedings of the IEEE INFOCOM 2025 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2025: 11044569.

[111] Beckerle M, Magnusson J, Pulls T. Splitting hairs and network traces: Improved attacks against traffic splitting as a website fingerprinting defense[C]//Proceedings of the 21st Workshop on Privacy in the Electronic Society. New York: ACM, 2022: 15-27.

[112] Xu Hongbo, Cheng Zhenyu, Li Shuhao, et al. ProxyKiller: An anonymous proxy traffic attack model based on traffic behavior graphs[C]//Proceedings of the 29th European Symposium on Research in Computer Security. Heidelberg: Springer, 2024: 162-181.

[113] 苟高鹏 . 加密应用识别与公害行为发现流量数据集[DB/OL]. (2025-03-31)[2025-11-14]. https://cstr.cn/16666.11.nbsdc.jtMB7oBB.
Gou Gaopeng. Encrypted application identification

and public nuisance behavior discovery traffic dataset: V1[DB/OL]. (2025-03-31)[2025-11-14]. https://cstr.cn/16666.11.nbsdc.jtMB7oBB. (in Chinese)

[114] Wang G, Sippe J, Chi Hai, et al. Chasing shadows: A security analysis of the ShadowTLS proxy[C]//Proceedings of the 13th Free and Open Communications on the Internet (FOCI 23). Online: The PETS Symposium, 2023: 8-13.

[115] Aceto G, Ciuonzo D, Montieri A, et al. Multi-classification approaches for classifying mobile app traffic[J]. Journal of Network and Computer Applications, 2018, 103: 131-145.

[116] Cui Simiao, Wang Dinghua, Zhang Xi, et al. Identifying mobile application over Shadowsocks with single-direction traffic[C]//Proceedings of 2023 8th International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE, 2023: 551-558.

[117] Zhou Nanxin, Liu Yiwei, Li Yujun, et al. A generalization-enhanced method for encrypted proxy traffic identification based on autoencoder[C]//Proceedings of 2024 2nd International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS). Piscataway: IEEE, 2024: 221-228.

[118] Zhang Junzhe. Research on Tor over SOCKS5 proxy anonymous communication behavior reconition[C]//Proceedings of 2025 5th International Conference on Sensors and Information Technology (ICSIIT). Piscataway: IEEE, 2025: 307-312.

[119] Luo Yuantu, Tao Jun, Yu Linxiao, et al. Together may be better: A novel framework and high-consistency feature for proxy traffic analysis[J]. Computer Networks, 2025, 272: 111672.

[120] Mühle A, Grüner A, Meinel C. Characterising proxy usage in the bitcoin peer-to-peer network[C]//Proceedings of the 22nd International Conference on Distributed Computing and Networking. New York: ACM, 2021: 176-185.

[121] Ji Qingbing, Deng Xiaoyan, Ni Lulin, et al. Research on ShadowsocksR traffic identification based on XGBoost algorithm[C]//Proceedings of the 5th International Conference on Intelligent and Interactive Systems and Applications. Heidelberg: Springer, 2020: 53-61.

[122] Luo Ping, Wang Fei, Chen Shuhui, et al. Behavior-based method for real-time identification of encrypted proxy traffic[C]//Proceedings of 2021 13th International Conference on Communication Software and Networks (ICCSN). Piscataway: IEEE, 2021: 289-295.

[123] Ji Qingbing, Deng Xiaoyan, Ni Lulin. Research on ShadowsocksR traffic identification based on DART algorithm[C]//Proceedings of 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC). Piscataway: IEEE, 2021: 666-672.

[124] Zliang N, Wu Tiantian, Zhang Yuening, et al. Shadowsocks traffic identification based on convolutional neural network[C]//Proceedings of 2020 International Conference on Information Science and Education (ICISE-IE). Piscataway: IEEE, 2020: 480-485.

[125] Xie Yanfeng. Automated encrypted proxy traffic classification via optimized 1D-CNN and feature attention[C]//Proceedings of 2025 IEEE 5th International Conference on Electronic Technology, Communication and Information (ICETCI). Piscataway: IEEE, 2025: 1406-1410.

[126] Zhao Hongce, Zhang Shunliang, Qiao Zhuang, et al. On the performance of deep learning methods for identifying abnormal encrypted proxy traffic[C]//Proceedings of 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway: IEEE, 2022: 1416-1423.

[127] Janbeglou M, Brownlee N. Identifying tunnelled proxies through passively monitoring network traffic[C]//Proceedings of 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE, 2016: 63-69.

[128] Wang W, Xue Diwen, Kumar P, et al. Is custom congestion control a bad idea for circumvention tools [C]//Proceedings of the 15th Free and Open Communications on the Internet (FOCI 25). Online: The PETS Symposium, 2025: 1-6.

[129] Spreitzer R, Griesmayr S, Korak T, et al. Exploiting data-usage statistics for website fingerprinting attacks on Android[C]//Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York: ACM, 2016: 49-60.

[130] Luo Jie, Bao Liang, Ni Lvlin. A method of Shadowsocks (R) traffic identification based on protocol analysis[C]// Proceedings of 2021 IEEE 21st International Conference on Communication Technology. Piscataway: IEEE, 2021: 6-10.

[131] Litvinov V L. Research of methods for recognizing anonymized traffic[C]//Proceedings of 2025 VI International Conference on Control in Technical Systems (CTS). Piscataway: IEEE, 2025: 127-130.

[132] Ejeta T G, Kim H J. Website fingerprinting attack on Psiphon and its forensic analysis[M]//Digital forensics and watermarking. Cham: Springer International Publishing, 2017: 42-51.

[133] Zhao Yankang, Ma Xiaobo, Li Jianfeng, et al. Revisiting website fingerprinting attacks in real-world scenarios: A case study of Shadowsocks[C]//Proceedings of the 12th International Conference on Network and System Security (NSS). Heidelberg: Springer, 2018: 319-336.

[134] Deng Ziye, Liu Zihan, Chen Zhouguo, et al. The random forest based detection of Shadowsock's traffic[C]//Proceedings of 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC): Vol. 2. Piscataway: IEEE, 2017: 75-78.

[135] Miller S, Curran K, Lunney T. Detection of anonymising proxies using machine learning[J]. International Journal of Digital Crime and Forensics, 2021, 13(6): 1-17.

[136] Zhang Xianlei, Ma Xiaobo, Han Xiao, et al. An uncertainty-based traffic training approach to efficiently identifying encrypted proxies[C]//Proceedings of 2020 12th International Conference on Advanced Infocomm Technology (ICAIT). Piscataway: IEEE, 2020: 95-99.

[137] Engelberg A, Wool A. Classification of encrypted IoT traffic despite padding and shaping[C]//Proceedings of the 21st Workshop on Privacy in the Electronic Society. New York: ACM, 2022: 3563191.

[138] Hu Xiaoyan, Lin Boquan, Cheng Guang, et al. Detecting cryptomining traffic over an encrypted proxy based on K-S test[C]//Proceedings of the ICC 2023-IEEE International Conference on Communications. Piscataway: IEEE, 2023: 3787-3792.

[139] Rahman M S, Imani M, Mathews N, et al. Mockingbird: Defending against deep-learning-based website fingerprinting attacks with adversarial traces[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 1594-1609.

[140] Fu Chuanpu, Li Qi, Xu Ke. Detecting unknown encrypted malicious traffic in real time via flow interaction graph analysis[C]//Proceedings of the Network and Distributed System Security Symposium (NDSS). San Diego: The Internet Society, 2023.

[141] Zhou Yong, Liu Weiwei, Sun Jinsheng. A multi-modal learning-based behavior identification scheme for obfuscated tunneling traffic[C]//Proceedings of the 2024 7th International Conference on Computer Information Science and Artificial Intelligence. New York: ACM, 2024: 581-586.

[142] Sakamoto, Edwards E. Bleeding wall: A hematologic examination on the Great Firewall[C]//Proceedings of the 14th Free and Open Communications on the Internet. Online: The PETS Symposium, 2024: 13-21.

[143] Husák M, Čermák M, Jirsík T, et al. HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting[J]. EURASIP Journal on Information Security, 2016, 2016(1): 6.

[144] Song Yafeng, Yang Ming, Chen Qi, et al. Evaluating the distinguishability of tor traffic over censorship circumvention tools[C]//Proceedings of 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE, 2023: 917-922.

[145] Lange F, Niere N, Von Niessen J, et al. I(ra)nconsistencies: Novel insights into Iran's censorship[C]//Proceedings of the 15th Free and Open Communications on the Internet (FOCI 25). Online: The PETS Symposium, 2025: 7-12.

[146] Huang Shuangshuang, Ma Xiaobo, Bian Huafeng. Effectively and efficiently defending Shadowsocks against website fingerprinting attacks[C]//Proceedings of 2021 8th International Conference on Dependable Systems and Their Applications (DSA). Piscataway: IEEE, 2021: 251-256.

[147] Ding Ke, Hu Xiaoyan, Shu Zhuozhuo, et al. NFT-AF: Multi-dimensional non-fungible token application fingerprinting over encrypted tunnels[J]. IEEE Network, 2025: 1-8.

[148] Kaplan I, Even R, Klein A. You can rand but you can't

hide: A holistic security analysis of Google Fuchsia's (and gVisor's) network stack[C]//Proceedings of the 32nd Annual Network and Distributed System Security Symposium (NDSS). San Diego: The Internet Society, 2025.

[149] Paolini E, De Marinis L, Scano D, et al. In-line any-depth deep neural networks using P4 switches[J]. IEEE Open Journal of the Communications Society, 2024, 5: 3556-3567.

[150] Yan Jinzhu, Xu Haotian, Liu Zhuotao, et al. Brain-on-Switch: Towards advanced intelligent network data plane via NN-driven traffic analysis at line-speed[C]// Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24). Santa Clara: USENIX Association, 2024: 24.

作者简介

吕梦达 男,1998年12月出生于山东省菏泽市。现为东南大学网络空间安全学院博士研究生。主要研究方向为加密流量分析。中国电子学会会员编号:E190202388A。

E-mail: mdlyu@seu.edu.cn

胡晓艳 女,1985年7月出生于江西省抚州市。2012年博士毕业于东南大学,现为东南大学网络空间安全学院副教授。主要研究方向为加密流量分析、网络空间安全、未来网络体系结构。

E-mail: xyhu@seu.edu.cn

卢俊羲 男,1998年3月出生于山东省淄博市。现为东南大学网络空间安全学院博士研究生。主要研究方向为钓鱼网站检测与域名安全。

E-mail: jxlu@seu.edu.cn

李清昀 男,2000年2月出生于陕西省宝鸡市。现为东南大学网络空间安全学院硕士研究生。主要研究方向为加密流量分析。

E-mail: 220235248@seu.edu.cn

吴 桦 女,1973年4月出生于江苏省南京市。2010年博士毕业于东南大学,现为东南大学网络空间安全学院副教授。主要研究方向为加密流量分析、网络空间安全、网络态势感知。

E-mail: hwu@seu.edu.cn

袁亚丽 女,1986年2月出生于河南省周口市。2018年毕业于德国哥廷根大学,现为东南大学网络空间安全学院副教授。主要研究方向为网络流量安全分析、协议逆向、漏洞挖掘、网络攻防、暗网、人工智能安全。中国电子学会会员编号:E190202061M。

E-mail: yaliyuan@seu.edu.cn

张 帆 男,1978年10月出生于浙江省杭州市。2011年博士毕业于美国康涅狄格大学,现为浙江大学计算机科学与技术学院教授。主要研究方向为硬件安全、物联网安全、网络安全、系统安全、密码学等。

E-mail: fanzhang@zju.edu.cn