基于Tor的匿名网络技术研究综述

朱俞翡[1]，胡宇翔[1,2,3]，陈博[1,2,3]，申涓[1,2,3]，崔鹏帅[1,2,3]，袁征[1,2,3]，田乐[1,2,3]
（1.信息工程大学信息技术研究所，河南 郑州 450002；2.先进通信网全国重点实验室，河南 郑州 450002；
3.网络空间安全教育部重点实验室，河南 郑州 450002）

摘　要：近年来，随着网络攻击技术的不断发展，以Tor为代表的匿名网络技术面临着性能瓶颈和安全挑战。为此，围绕Tor网络发送者匿名性，系统梳理了Tor匿名通信机制及其性能与安全问题。首先，在分析Tor网络目录协议、路径选择及电路构建等核心机制的基础上，总结了当前研究中存在的关键问题，并归纳了相应的优化方法与改进方向。其次，针对主动攻击与被动攻击，系统归纳了典型的去匿名化攻击方法，并分析了其防御策略的效果。最后，探讨了Tor网络在匿名性、安全性与性能方面的局限性，总结了优化思路，并展望了未来匿名网络技术的研究方向。

关键词：Tor网络；匿名网络；网络安全；安全技术；性能优化
中图分类号：TP393.08
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2025077

Survey of research on Tor-based anonymous networking technologies

ZHU Yufei[1], HU Yuxiang[1,2,3], CHEN Bo[1,2,3], SHEN Juan[1,2,3], CUI Pengshuai[1,2,3], YUAN Zheng[1,2,3], TIAN Le[1,2,3]
1. Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China
2. National Key Laboratory of Advanced Communication Networks, Zhengzhou 450002, China
3. Key Laboratory of Cyberspace Security, Ministry of Education of China, Zhengzhou 450002, China

Abstract: In recent years, with the continuous development of network attack techniques, anonymous network technologies represented by Tor have faced performance bottlenecks and security challenges. To this end, a systematic review of the Tor anonymity communication mechanism, as well as its performance and security issues, has been conducted with a focus on the sender anonymity in the Tor network. First, key mechanisms, including the directory protocol, path selection, and circuit construction were analyzed to identify major issues in existing research, and corresponding optimization methods and improvement directions were summarized. Next, typical de-anonymization attacks, including both active and passive methods, were systematically reviewed, and the effectiveness of defense strategies against these attacks were analyzed. Finally, Tor's limitations in terms of anonymity, security and performance were thoroughly examined, optimization strategies were summarized, and future research directions in the development of anonymous network technologies were prospected.

Keywords: Tor network, anonymous network, network security, security technology, performance optimization

收稿日期：2025−02−10；**修回日期：**2025−03−31
通信作者：田乐，xxgctianle@163.com
基金项目：国家重点研发计划基金资助项目（No.2022YFB2901500, No.2023YFB2903900）；中原科技创新领军人才基金资助项目（No.244200510038）；先进通信网全国重点实验室基金一般项目（No.FFX24641X028）
Foundation Items: The National Key Research and Development Program of China (No.2022YFB2901500, No.2023YFB2903900), Zhongyuan Science and Technology Innovation Leading Researcher Project (No.244200510038), The General Project of the National Key Laboratory of Advanced Communication Networks (No.FFX24641X028)

0　引言

在信息传播和交互频繁的数字时代，用户的通信数据和个人信息成为攻击者的目标，隐私泄露事件层出不穷[1]，这些问题的出现催生了匿名网络技术。与传统的端到端加密技术不同，匿名网络重点在于隐藏通信双方的身份、位置、时间以及其他能够追踪用户的元数据信息，在保护用户隐私和保障网络安全方面发挥了不可替代的作用。匿名网络的起源可追溯至由 Chaum[2]提出的 Mix 网络。随着互联网技术的进步和用户隐私保护需求的提升，各种匿名网络技术相继出现，如第二代洋葱路由（Tor）[3]、隐形互联网计划（I2P）[4]、自由网络（Freenet）[5]等，它们在不同程度上实现了用户通信的匿名保护。根据不同的性能需求和隐私保护特性，可以将匿名网络分类为低时延匿名网络和高时延匿名网络[6]。低时延匿名网络注重低时延和高可用性，适用于如匿名浏览、即时通信、匿名发布等实时通信场景，Tor、I2P、Freenet 等属于低时延匿名网络。高时延匿名网络通过引入时延来混淆流量模式，增强匿名性，适用于电子邮件匿名发送等非实时通信，Mix 网络便是典型的高时延匿名网络。

虽然 I2P、Freenet 等匿名网络在特定领域发挥了重要作用，但 Tor 网络因兼顾匿名性与低时延的特性而成为广泛研究的焦点[7]。然而，随着网络攻击技术的不断进步，Tor 网络面临着诸多挑战，例如，网络性能瓶颈[8]、安全漏洞[9]以及流量分析攻击带来的去匿名化威胁[10]等。这些挑战不仅成为研究者关注的重点，也推动了匿名网络技术的不断发展和创新。近年来，大量学术研究集中于如何优化 Tor 网络性能和提升其抗攻击能力，通过对 Tor 网络机制的深入分析，提出了许多针对性能优化[11]和安全性提升[12]等的解决方案。然而，针对这些研究进展进行系统总结的综述文献仍然较为匮乏。基于这一背景，本文从 Tor 网络核心运行机制出发，聚焦相关领域的重要研究进展，系统分析 Tor 网络在匿名性、安全性和性能[13]方面的优势与不足，并总结针对性的改进技术。本文组织框架如图 1 所示。

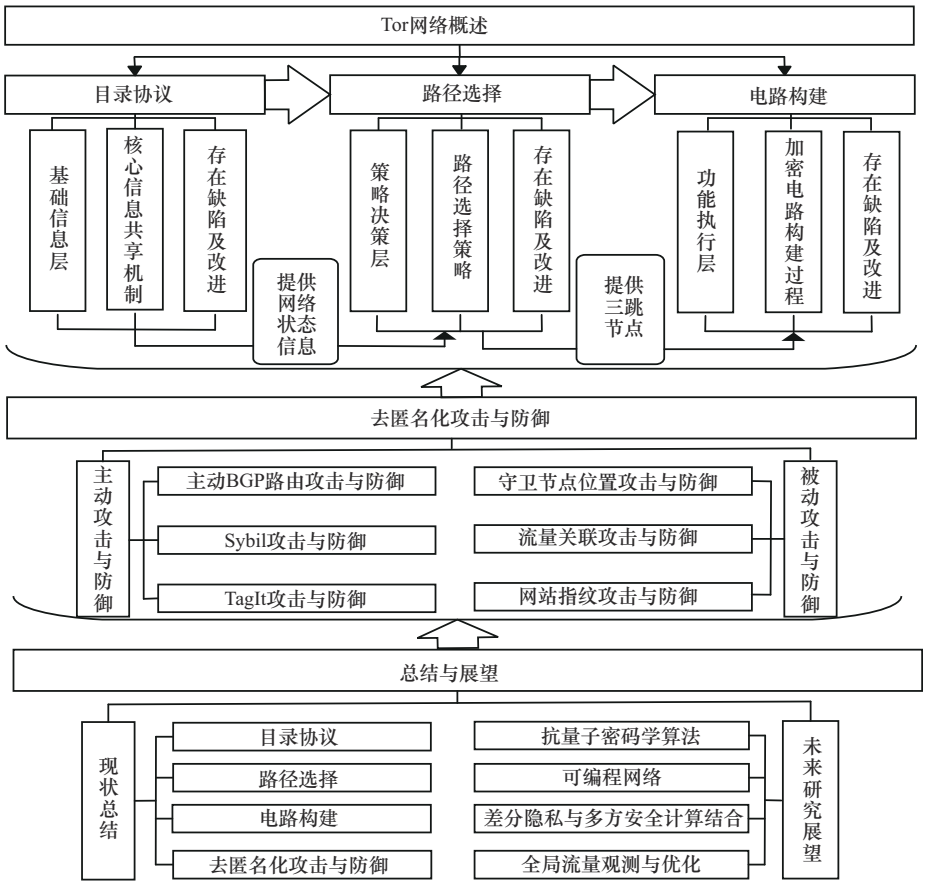


图 1　本文组织框架

1　Tor网络研究架构

1.1　Tor网络概述

Tor网络是一种匿名化低时延的分布式网络[14]，基于洋葱路由技术，通过多层加密和中继节点隐藏通信源头和目的地，从而保护用户隐私。Tor网络改进了原始的洋葱路由系统[15]，显著提升了匿名性和实用性。Tor网络的匿名性包括发送者匿名性和接收者匿名性[3]，发送者匿名性指隐藏和保护通信发送方的身份，而接收者匿名性则涉及隐藏接收方的身份信息。Tor网络通过洋葱路由技术有效实现了发送者匿名性，而隐藏服务[16]则弥补了原始洋葱路由不具备接收者匿名性的不足。本文重点探讨Tor网络发送者匿名性的实现机制及相关技术。

Tor网络由全球志愿者运营的中继节点组成，其中，客户端是用户接入口，目标服务器是用户访问的实际目标。守卫节点是客户端连接到Tor网络的第一跳中继节点，中间节点仅负责转发加密数据，出口节点是流量离开Tor网络连接外部服务端所经过的最后一跳中继节点。此外，目录权威服务器（DA, directory authority）负责管理网络拓扑信息，维护一个实时更新的Tor网络节点列表，为客户端提供最新的网络状态信息。

图2展示了Tor网络工作流程，包括目录协议、路径选择和电路构建3个核心过程。客户端首先下载最新的共识文件并查询DA获取节点信息。根据共识文件，客户端按照“出口节点—守卫节点—中间节点”的顺序选择中继节点，构建匿名通信路径。基于此路径，客户端与各节点依次协商对称加密密钥，形成一个三层加密的匿名电路。电路建立完成后，客户端将消息进行分段并封装，按照从外到内的顺序使用密钥加密。消息经过每个节点逐层解密，最终在出口节点解密，并以明文形式传递至目标服务器。

1.2　技术研究分类

在Tor网络的研究领域，针对Tor发送者匿名性的实现，以及其核心功能模块[17]的设计缺陷和去匿名化攻击带来的安全威胁[13]，研究方向可以分为目录协议、路径选择、电路构建及去匿名化攻击与防御，每一类又根据解决的具体问题进一步细分为子问题，如图3所示。前3类研究方向聚焦于改进Tor网络的核心功能模块，旨在弥补设计缺陷以提升安全性与性能；第4类研究则专注于分析Tor网络面临的去匿名化攻击，并提出相应的防御策略。

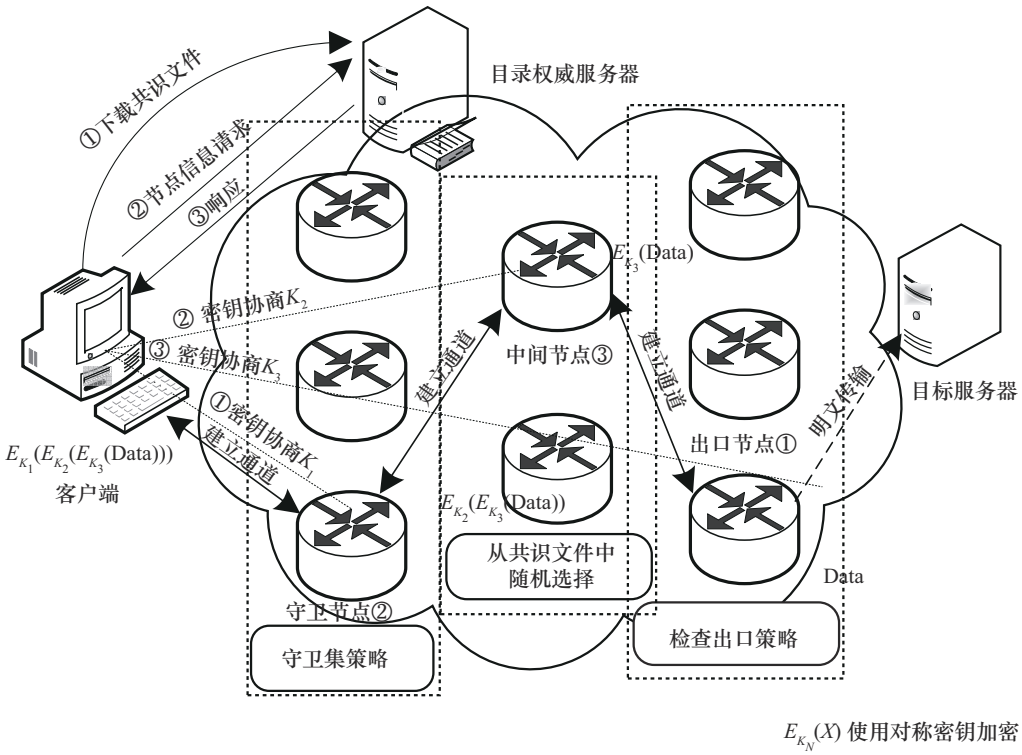


图2　Tor网络工作流程

目录协议是Tor网络的基础，负责维护网络节点信息，并决定中继节点的选择。然而，它存在多个安全隐患，包括：恶意节点带宽虚报以占据更大流量份额；带宽测量漏洞和偏差，攻击者可操控测量结果影响流量分配；共识协议攻击，攻击者通过干扰DA生成不同的共识文件，引导客户端下载被篡改的共识文件。路径选择决定匿名路径的构建，是影响匿名性和安全性的核心，主要研究方向包括：优化路径选择算法来防御流量分析和关联攻击；性能与匿名性平衡，在减少网络时延，提升性能的同时保持匿名性；防护守卫节点和中间节点，避免这些节点对匿名性构成威胁。

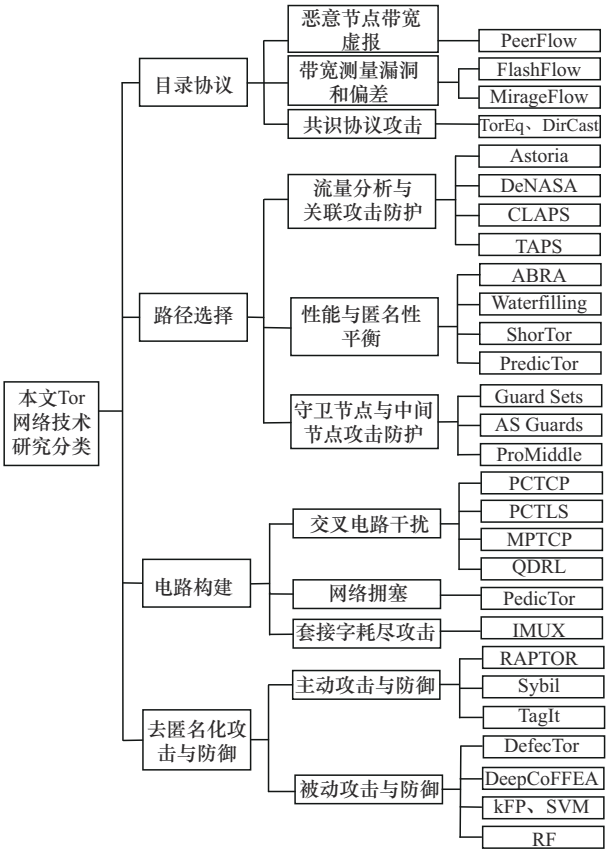


图3　本文Tor网络技术研究分类

电路构建涉及加密电路的构建过程，影响通信的安全性和稳定性。主要研究方向包括：交叉电路干扰，多个流共享同一电路导致相互干扰；网络拥塞，电路与连接共享拥塞窗口，可能影响通信质量；套接字耗尽攻击，恶意连接请求占用Tor节点的资源，降低服务质量。Tor网络面临的去匿名化攻击可以分为主动攻击和被动攻击：主动攻击指攻击者直接干预网络通信，如流量注入、节点渗透、流量劫持等，试图破坏匿名性；被动攻击指攻击者通过长期流量分析、统计特征学习等方式，尝试从流量模式中提取用户身份信息。

1.3　技术评估指标

Tor网络的核心目标在于保障用户隐私安全，然而，随着网络规模的不断扩大，去匿名化攻击、性能瓶颈等问题日益突出。因此，定量化地评估Tor网络的各项指标至关重要。本节将总结关键评估指标，以衡量Tor网络的匿名性、安全性和性能。

1) 匿名性指标

匿名性是Tor网络的核心目标之一，它主要通过衡量用户的身份泄露风险来评估Tor网络的匿名保护能力。常见的匿名性指标包括：匿名集、信息熵、不可追踪性等[1]。

匿名集是指攻击者无法区分的所有潜在通信对象的集合。在Tor网络中，较大的匿名集意味着更强的匿名性，因为攻击者需要区分的可能路径更多。

信息熵是衡量Tor网络匿名性的一个重要指标，它表示系统的随机性和不确定性。在匿名通信中，熵值越高，系统的匿名性越强。香农熵的计算式为

$$H(X)=-\sum_{i=1}^{n}p\left(x_i\right)\mathrm{lb}p\left(x_i\right) \tag{1}$$

其中，$p\left(x_i\right)$是第i个事件的概率，X是离散随机变量，表示系统中可能的状态。

不可追踪性衡量系统是否能够防止关联分析，即攻击者无法通过流量模式或其他特征将发送者与接收者关联起来。

2) 安全性指标

安全性是Tor网络的首要目标之一，尤其是防御去匿名化攻击方面。为量化Tor网络在这些方面的表现，总结了以下安全性相关的评估指标。

攻击成功率是衡量攻击者识别用户真实身份的成功概率，反映了Tor防御去匿名化攻击的有效性[18]，计算式为

$$P_{\text{success}}=\frac{s}{n} \tag{2}$$

其中，s是成功攻击的次数，n是总的攻击尝试次数。

真阳性率（TPR, true positive rate）衡量防御系统正确识别攻击的能力，若TPR高，说明防御系统能有效检测并阻止攻击，攻击成功率会降低；若

TPR低，攻击更容易绕过检测，成功率上升。

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

其中，真阳性（TP, true positive）表示真正的攻击被正确检测为攻击；假阴性（FN, false negative）表示真实攻击未被检测为攻击。

假阳性率（FPR, false positive rate）衡量的是非攻击行为被误判为攻击的概率，反映了系统在防御中的误报率。FPR越低，表示系统的误报率越低，正常的流量不会被错误地当作攻击流量处理[19]。

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

其中，假阳性（FP, false positive）表示正常行为被误判为攻击，真阴性（TN, true negative）表示正常行为被正确判断为正常。

3) 性能指标

性能是Tor网络在实际应用中的重要考量，尤其在处理带宽、时延和吞吐量时[19]。以下是用于评估Tor网络性能的主要指标。

带宽表示网络中每个节点的传输能力，影响用户的上传和下载速度。在Tor网络中，总带宽是由电路中最慢节点的带宽决定，计算式为

$$B_{\mathrm{total}}=\min\left(B_1,B_2,\cdots,B_n\right) \tag{5}$$

其中，B_i为每个中继节点的带宽，B_{total}为电路的总带宽。

时延表示数据从源节点到目标节点的传输时间，时延越低，用户的体验越好，计算式为

$$T_{\mathrm{latency}}=\sum_{i=1}^{n}T_i \tag{6}$$

其中，T_i为每个中继节点的时延，n为电路中的节点数。

吞吐量衡量网络在单位时间内成功传输的数据量，是网络性能的重要指标，特别是在评估Tor网络的效率时，计算式为

$$T=\frac{D}{t} \tag{7}$$

其中，D表示在指定时间段内成功传输的数据量，t表示总时间。

2 目录协议

目录协议是Tor网络的基础，通过提供节点状态和网络拓扑信息，确保客户端能够基于实时更新的共识文件构建匿名通信路径。本节将介绍DA定期收集中继节点描述符生成投票文件以及通过共识过程生成共识文件的过程。此外，还将分析现有目录协议存在的缺陷，并结合相关研究成果，总结现有优化方案。

2.1 运行机制

当一个中继节点上线或更新其状态时，它会向DA上传自己的路由器描述符，DA检查描述符的格式是否正确、签名是否有效。然后依据收集的节点信息对每个节点进行评估，根据评估结果生成每个节点的视图，并将节点视图记录在投票文件中。DA互相交换投票文件，确保各DA对网络状态的视图保持一致。一旦所有DA交换了投票文件并收集了所有节点的状态信息，便会进入共识过程。在共识过程中，DA通过共识算法整合投票文件，生成最终的共识文件。共识文件是Tor网络运行的核心，包含对中继节点状态和属性的统一视图。

2.2 相关研究

Tor网络目录协议在保障网络可信性方面起到重要作用，但也面临带宽欺骗、测量机制安全性不足和共识文件生成不一致等问题。针对这些挑战，研究者提出了一系列改进方案，包括优化中继带宽测量系统、增强带宽测量的安全性和精度，以及设计更鲁棒的共识协议等。本节将详细讨论这些改进方法及其在提升Tor网络性能和安全性方面的作用，表1对现有典型目录协议改进技术[20-23]进行总结。

2.2.1 恶意节点带宽虚报

在Tor网络中，带宽信息是决定客户端流量在中继节点间分布的重要数据。然而，由于Tor网络中继节点由全球志愿者运行，节点报告带宽无法完全信任，恶意节点可能通过虚报高带宽吸引更多流量，从而监控更多通信并提高流量分析攻击的成功率。

为减少恶意节点虚报带宽的影响，研究者提出了一些优化方案。Johnson等[20]提出PeerFlow，旨在通过多种机制显著降低恶意节点虚报带宽的风险。PeerFlow采用对等测量机制，节点之间相互评估实际带宽能力，从而减少对节点自我报告带宽的依赖；同时，在计算总带宽时裁剪掉最大值和最小值，限制恶意节点通过极端值操控流量分配的可能性。此外，PeerFlow引入可信节点的测量数据作为

表1　　**目录协议研究现状总结**

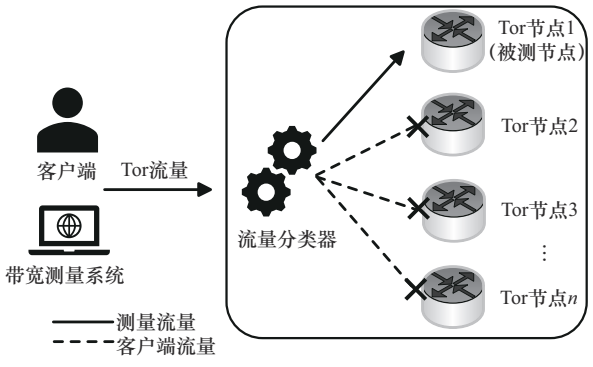
研究问题	解决思路	代表工作	方法	效果	特点
恶意节点带宽虚报	多维度带宽评估	PeerFlow[20]	对等测量、裁剪极值、可信节点数据校正	恶意节点带宽膨胀因子≤4.6倍，误差率0.428，网络利用率中位数49%	减少虚假带宽报告对流量分配的影响，在提升安全性的同时保持良好的网络性能
带宽测量漏洞与偏差	主动流量生成	FlashFlow[21]	主动生成测试流量，多节点协作测量	5 h内完成全网测量，误差≤11%	精确评估中继带宽，减少流量分配误差，提高安全性和精确性
	三跳测量机制	MirageFlow[22]	基于用户流量进行三跳测量电路	10台服务器（每台100 MB/s）部署109个中继，即可控制Tor网络50%流量	攻击者集中资源膨胀带宽，但随节点增加效果减弱
共识协议攻击	将共识问题转化为交互一致性问题	TorEq、DirCast[23]	TorEq检测矛盾攻击，DirCast优化拜占庭协议流程	5 min内完成检测，通信开销约140 MB，无攻击时120 s生成共识，恶意攻击下216 s生成共识，支持500次/h生成	确保存在恶意节点情况下的安全共识，提升协议效率和安全性

参考，用于修正其他节点的带宽估计值，从而确保带宽值更加可靠。基于Shadow的大规模模拟实验显示，PeerFlow的恶意节点带宽膨胀因子低于4.6倍（TorFlow为177倍），流量分配与实际带宽的误差率（0.428）显著低于TorFlow（1.02），下载时间与TorFlow相当，但网络利用率更高（中位数利用率49%，TorFlow的为43%），且测量开销较低。

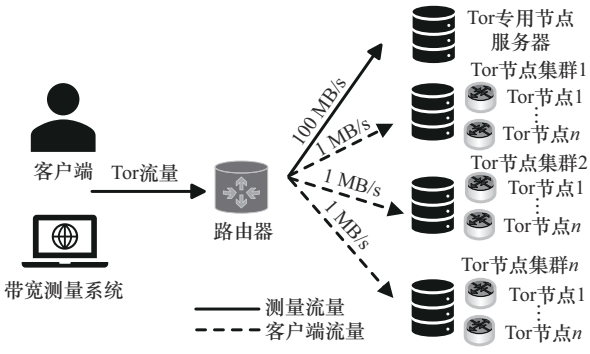
2.2.2　带宽测量漏洞和偏差

带宽测量机制是Tor网络负载均衡和性能优化的核心，但当前方法存在显著的安全问题和测量偏差。Tor网络使用一种称为TorFlow的测量系统，通过探测器与受测节点间的双跳路由评估中继的转发能力。然而，这种双跳测量电路容易被攻击者识别并操控以导致高带宽测量结果，吸引更多客户端流量。针对这一问题，Traudt等[21]提出了一种带宽测量系统FlashFlow，通过主动生成测试流量验证中继的实际处理能力，并利用多个测量节点协作覆盖高带宽中继，降低被操控的可能性。实验表明，FlashFlow使用3个1 Gbit/s的测量节点，可在5 h内完成全网测量，且对真实Tor中继的测量误差在11%以内。

Sendner等[22]提出一种新型带宽膨胀攻击MirageFlow，攻击者首先区别Tor网络中的客户端流量与测量流量，通过共享网络资源或专用服务器动态分配流量，引导测量流量集中于被测节点，从而夸大带宽估算值。如图4(a)所示，多个Tor节点共享一个高带宽服务器，当检测到测量流量时，将其重路由至该服务器，模拟节点具有超高带宽。如图4(b)所示，结合一个主服务器和多个弱服务器，分散流量以规避检测，进一步提升带宽膨胀位数。实验表明，攻击者仅需10台服务器（每台100 MB/s）部署109个中继，即可控制Tor网络50%流量，严重破坏负载均衡并增强去匿名化能力。为防御带宽膨胀攻击，文献[22]提出一些潜在的改进方向：采用更复杂的三跳测量电路，增加攻击者识别测量流量的难度。



(a) C-MirageFlow（基于共驻节点）



(b) D-MirageFlow（基于专用服务器）

图4　MirageFlow攻击原理示意

2.2.3 共识协议攻击

共识协议是Tor网络维持一致性和安全性的关键，但现有协议难以有效应对信息矛盾攻击。这种攻击发生在DA被攻破的情况下，攻击者向不同的DA发送不一致的投票信息，导致各DA生成不同的共识文件。这种不一致可能诱导客户端下载并使用被篡改的共识文件，将流量路由至攻击者控制的中继节点，进一步进行窃听、数据篡改或流量分析等恶意行为。为解决这一问题，Luo等[23]提出了应对方案：首先，设计一个监控工具TorEq，专门用于检测信息矛盾攻击。在亚马逊云服务（AWS）实例上测试，TorEq在5 min内完成检测，通信开销约为140 MB，虽高于原系统但实际可行。其次，文献[23]将Tor的共识生成问题转化为“交互一致性”问题，设计了一种优化的拜占庭广播协议DirCast。实验表明，DirCast无攻击时120 s生成共识，恶意攻击下216 s生成共识，满足Tor每小时一次的频率需求；支持每小时500次共识生成，远超实际需求。

3 路径选择

路径选择是Tor网络中确保安全性和性能的核心步骤，在目录协议提供的共识文件的基础上，通过动态且随机的节点选择策略，构建通信路径。本节将介绍Tor网络路径选择算法，同时，分析现有路径选择算法存在的问题与不足、面临的挑战，并结合相关研究成果进行总结。

3.1 运行机制

已知目标IP地址，客户端可以查看Tor网络中出口节点的出口策略，检查它是否允许连接至该IP地址，从而根据出口策略来选择出口节点。中间节点的选择则更侧重随机性，依据带宽及其权重进行加权选择。守卫节点的选择严格遵循“高带宽优先、逐步确认和过滤”的策略，通过分组管理和优先使用主守卫节点，减少了守卫节点更换的频率。

3.2 相关研究

现有路径选择算法虽然在提供安全性和隐私性方面发挥了重要作用，但仍面临全球性流量分析与流量关联（FC, flow correlation）攻击以及性能与安全性平衡等问题。研究者提出了一系列改进方案，包括位置感知和信任感知路径选择策略、提升路径选择性能，以及优化守卫节点选择和中间节点防护机制等。本节将分类讨论这些改进技术的核心思路及其在提升Tor网络匿名性、安全性和性能中的作用，表2对现有典型路径选择改进技术进行总结。

3.2.1 流量分析与关联攻击防护

Tor网络易受流量分析与关联攻击的影响，尤其是在攻击者能够观察到Tor路径两端流量的情况下。为了减轻自治系统（AS, autonomous system）级别的流量分析攻击，Nithyanand等[24]构建了Astoria，一种AS感知的Tor客户端，通过路径预测和智能中继选择，能够显著降低电路的脆弱性。Astoria将AS级攻击威胁从40%降至2%，合谋AS威胁从42%降至5%，国家级威胁从85%降至25%。然而，Astoria等AS感知路径选择算法需要根据目的地址实时构建安全电路，这限制了路径预构建能力，影响性能。针对这个问题，Barton等[25]提出了DeNASA，实现了目标无关的AS感知路径选择。DeNASA在无须预知用户访问目标的情况下，将Tor流量的AS级攻击漏洞降低74%。其目标无关特性允许预建电路，使首字节时间（TTFB）接近原生Tor，末字节时间（TTLB）亦无显著差异，实现了安全性与性能的高效平衡。

尽管位置感知路径选择算法在减少AS级攻击方面表现出色，但也存在客户端位置信息泄露风险，易受守卫节点位置攻击。Rochet等[26]开发了改进的客户端位置感知路径选择（CLAPS, client-location-aware path selection）框架，使用纯线性规划优化中继节点权重，并引入位置掩码技术，限制路径选择过程中泄露的位置信息。将CLAPS应用于DeNASA，可疑AS数量减少至原生Tor的$\frac{1}{2.3}$，守卫节点位置攻击成功率限制为原生Tor的2倍，而DeNASA可达40倍。此外，传统位置感知路径选择算法在多连接场景下去匿名化风险较大。为此，Johnson等[27]提出基于信任的路径选择（TAPS, trust-aware path selection）算法，通过灵活建模攻击者在网络中的位置分布和用户对攻击者的信任策略，有效抵御了多连接下的流量关联攻击，在The Man模型中攻击成功率降低43%，且性能与原生Tor接近。

3.2.2 性能与匿名性平衡

Tor网络在路径选择中面临性能与匿名性的平衡难题。为了降低时延和提升性能，Tor客户端通常倾向于选择高带宽节点构建电路，但这一策略会

表2　路径选择改进技术总结

研究问题	解决思路	代表工作	方法	效果	特点
流量分析与关联攻击防护	位置感知	Astoria[24]	网络位置优化路径	AS级攻击威胁降至2%，合谋AS威胁降至5%，国家级威胁降至25%	降低脆弱性，但需实时分析路径，可能泄露位置信息
		DeNASA[25]		AS级攻击漏洞降低74%，TTFB接近原生Tor，TTLB无显著差异	目标无关，但依赖可疑AS列表，可能泄露位置信息
		CLAPS[26]		可疑AS减少至原生Tor的$\frac{1}{2.3}$，攻击成功率为原生Tor的2倍	线性规划优化路径选择，位置掩码技术限制信息泄露
	信任感知	TAPS[27]	攻击者分布与信任策略建模	攻击成功率降低43%，性能与原生Tor接近	提升全球性攻击防御能力，适应多连接场景
性能与匿名性平衡	平衡网络负载	ABRA[28]	时延加权带宽，选择未瓶颈化路径	带宽利用率提升14%，隐私无显著影响	提升网络利用率
		Waterfilling[29]	动态调整带宽权重	攻击成功率降至2%，轻负载下性能与原生Tor相当，重负载下约3%电路性能下降	均衡负载分配，降低流量关联攻击风险
	降低网络时延	ShorTor[30]	使用中转节点，选择低时延路径	降低时延，改善用户体验	降低时延，同时保持匿名性
		PredicTor[31]	基于机器学习预测路径性能	中位数TTLB提升23%，90%分位数提升28%，负载更均衡	提升性能，维持匿名性
守卫节点与中间节点攻击防护	改进守卫集设计	Guard Sets[32]	选择高性能守卫节点构成守卫集	抵御攻击，性能与带宽利用率无显著降低	提高匿名性和负载分布效率，但是存在安全漏洞
		AS Guards[33]	基于AS关系的守卫集设计	低资源攻击者条件下用户被攻击比例从0.076%降至0.044%，高资源攻击者渗透率从53%降至10%，目标攻击成功率从98%降至44%	利用互联网拓扑的稳定性减少攻击渗透
	中间节点攻击防护	ProMiddle[34]	基于机器学习分析中间节点流量指纹	检测电路用途准确率92.41%，节点位置准确率98.48%	提高对中间节点攻击的防护

导致负载失衡、高带宽节点过载以及路径选择的单一化，从而引发匿名性削弱等问题，不仅影响了Tor网络的整体效率，还增加了流量分析攻击的成功率。

Geddes等[28]提出了避免瓶颈中继ABRA算法，通过允许客户端和中继之间共享部分状态信息，优化路径选择，避免使用带宽瓶颈的中继节点。中继节点根据自身带宽使用情况计算瓶颈权重，并定期将权重信息发送给客户端，客户端根据权重优先选择未被瓶颈化的路径。相比原生Tor，在不显著影响隐私的前提下，网络带宽利用率提升14%。此外，Rochet等[29]提出了一种名为注水法Waterfilling的路径选择算法，通过动态调整每个中继节点的带宽权重来平衡流量分配，以确保高带宽节点主要承担电路中间段的流量传输，而低带宽节点则用于处理终端的流量。实验结果表明，Waterfilling将攻击成功率从24%降至2%，显著延长了攻击时间。轻负载下与原生Tor性能相当，重负载下约3%的电路性能下降。

Hogan等[30]提出了短路径Tor协议ShorTor，用于降低Tor网络时延。如图5所示，ShorTor借鉴内容分发网络的多跳覆盖路由技术，在Tor电路的相邻节点之间引入中转节点，动态优化路径，减少时延。ShorTor核心机制包括：分布式时延测量，通过全网节点间的周期性RTT测量生成候选Via Relays列表；数据竞赛路径选择，通过实时并行探测确定最优转发路径，避免网络动态变化导致的次优

决策；无状态转发，Via Relays仅转发流量而不参与洋葱加密，确保与Tor核心协议的兼容性。实验表明，99.9%分位数的时延从487 ms降至125 ms，99%分位数的电路时延减少122 ms，并且验证了其不影响Tor的匿名性。

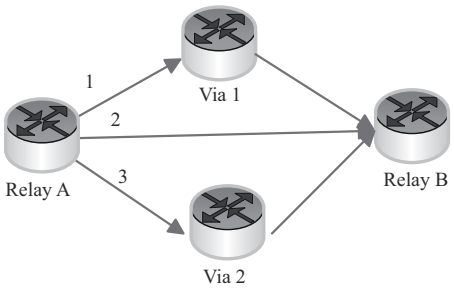


图5　ShorTor示意

同样地，Barton等[31]提出了预测式Tor路径选择算法PredicTor，一种基于机器学习的路径选择算法，利用随机森林和k近邻（kNN）分类器预测路径性能，选择较快、低拥堵的路径，目的在于保证匿名性的同时，显著提升Tor网络的性能。使用Shadow模拟实验表明，PredicTor比原生Tor中位数TTLB提升23%，90%分位数提升28%。且PredicTor使用85%（原生Tor仅55%）的节点，负载更均衡。

3.2.3　守卫节点和中间节点攻击防护

在Tor网络中，守卫节点和中间节点均可能成为攻击目标，对匿名性构成严重威胁。守卫节点一旦被恶意控制，用户的IP地址可能被直接暴露。尽管传统观点认为中间节点的威胁较小，但研究表明，中间节点同样可以通过流量指纹分析推测电路用途或目标网站，对用户的匿名性构成重大隐患。

Hayes等[32]提出了基于共享守卫集的设计，通过分组守卫节点形成共享集合，以提升匿名性和负载分布效率。然而，Imani等[33]发现了守卫集方案仍存在漏洞，攻击者可以通过调整恶意节点的带宽，渗透到多个守卫节点集合中。此外，网络波动导致的守卫集合分裂或重新分组，进一步增加了攻击者的渗透机会。为此，研究者提出了基于网络位置的守卫集设计，通过利用AS关系构建守卫层级。实验表明，低资源攻击者条件下，用户被攻击比例从原有方法的0.076%降至0.044%。高资源攻击者条件下，渗透率从53%降至10%，且目标攻击成功率从98%降至44%。Jansen等[34]的研究表明，中间节点同样可以通过流量指纹分析对匿名性构成严重威胁，并设计了一种基于中间节点位置的Tor流量指纹分析方法，利用机器学习技术对流量进行分类，从中间节点预测电路的用途或目标网站。实验表明，检测电路用途（隐藏服务与普通流量）和节点位置，准确率分别达到92.41%和98.48%。

4　电路构建

路径选择为匿名通信路径的构建提供了节点选择策略，而电路构建则是将路径选择的结果转化为实际匿名通信电路的关键步骤。通过多跳加密和密钥协商，实现了路径的匿名性。本节将介绍电路构建过程以及数据传输机制。同时，将分析Tor网络电路构建机制中存在的问题和缺陷，例如交叉电路干扰、网络拥塞等，并结合相关研究成果对改进方案进行综述。

4.1　运行机制

电路构建是Tor网络匿名通信的核心，客户端逐跳与每个中继节点协商对称密钥，建立电路。首先，客户端与守卫节点交换密钥生成材料，协商共享密钥K_1。然后，客户端通过守卫节点与中间节点协商密钥K_2，继续向出口节点扩展，协商密钥K_3。每次扩展，客户端与新节点协商生成新的会话密钥，以确保各跳之间的加密独立性。电路建立后，数据传输采用分段封装和逐跳加密。

图6展示了数据传输过程，客户端将数据分割

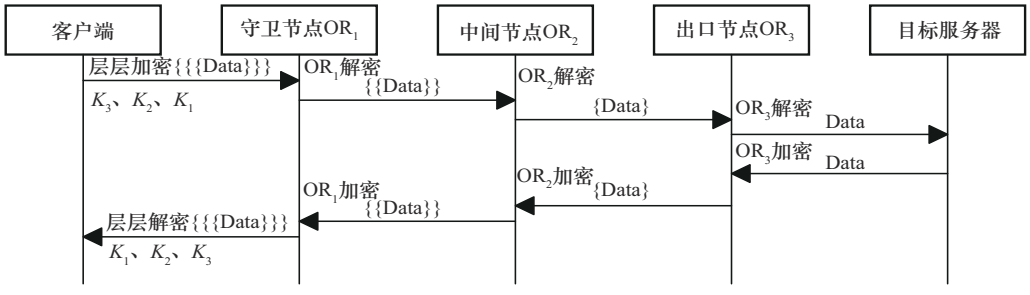


图6　数据传输过程

并封装为固定大小的单元，并按照节点顺序依次加密。每个中继节点解密数据包并转发，直到出口节点。出口节点解密并组合数据包，转发给目标服务器。返回数据也通过电路逐跳传输并加密，最终到达客户端解密。

4.2　相关研究

在面对Tor网络电路构建机制中的交叉电路干扰和拥塞控制局限等问题时，研究者提出了多种改进方案。这些方案包括优化传输协议以提升复用效率、设计公平的资源调度策略以及应用现代控制理论和机器学习技术以缓解拥塞问题。本节将详细探讨这些改进技术的核心思路及其在实际中的应用成效，表3对现有典型电路构建改进技术[11,35-39]进行了总结。

4.2.1　交叉电路干扰

在单一连接中实现多路复用时，Tor网络中的高流量电路与低时延需求电路之间会因带宽竞争，产生交叉电路干扰问题，导致资源分配的不公平性，进而影响匿名性和网络性能。传统传输控制协议（TCP）传输方式在公平性和性能优化方面存在显著挑战。

Alsabah等[35]提出基于IPsec的逐电路TCP——PCTCP，为每个Tor电路分配一个独立的内核级TCP连接，同时使用互联网安全协议IPsec保护通信。实验表明，高带宽场景下，Web客户端下载时间中位数从3.6 s降至1.6 s。高负载下，PCTCP仍能保持Web客户端的响应时间优势。Pahl等[11]提出了基于TLS的逐电路TCP——PCTLS，为每个电路提供独立的TCP连接，并独立管理拥塞窗口，避免丢包或拥塞对其他电路的影响。在25%规模网络中，PCTLS使99%的5 MB文件传输时间从约12 s降至5 s，而传统Tor因共享链路时延显著。PCTLS在无丢包时平均快703 ms，有丢包时快5 696 ms，但电路建立时间增加约725 ms。Cadena等[36]提出使用MPTCP作为Tor的传输协议，通过多路径通信提高资源利用率，并减少带宽分配的不公平性。实验表明，MPTCP可显著提升Tor性能（平均15%）。与其他多连接传输设计相比，MPTCP具备易于部署、内核级调度和更好的抗攻击能力，但需解决隐私风险。

Basyoni等[37]提出了用于Tor电路调度的服务质量（QoS, quality of service）感知深度强化学习方法（QDRL, QoS-aware deep reinforcement learning），结合深度强化学习技术，综合考虑公平性与QoS，根据应用类型（交互式、流媒体、批量传输）动态分配权重，优化公平性与效率的权衡。具体而言，研究提出了3种调度方法：基于深度确定性策略梯度的强化学习方法，适应动态环境；基于凸优化的资源分配，最大化系统吞吐量；启发式平均速率比例公平算法，结合历史速率动态调整。图7展示了QDRL系统模型，其输入源于Tor的应用层和内核层，调度器融合了3种调度算法，依据

表3　　**电路构建改进技术总结**

研究问题	解决思路	代表工作	方法	效果	特点
交叉电路干扰	改进传输层协议	PCTCP[35]	为每条电路分配独立TCP连接	高带宽场景下载时间中位数从3.6 s降至1.6 s，高负载下保持响应时间优势	使用IPsec隐藏TCP/IP头部信息，避免交叉电路干扰，增加匿名性
		PCTLS[11]		25%规模网络中，PCTLS使文件传输时延降低8%，且在丢包场景下优势更显著	独立拥塞控制，增加电路建立时间和内存占用
		MPTCP[36]	使用MPTCP替代Tor的传输协议	平均性能提升15%，易于部署，内核级调度，抗攻击能力强	多路径传输，减少带宽分配不公平，但存在去匿名化风险
	QoS感知电路调度	QDRL[37]	基于深度强化学习动态化资源分配	显著提升系统公平性与用户满意度	智能化动态资源分配，需复杂训练和计算资源
网络拥塞	建模为优化问题	PredicTor[38]	引入现代控制理论，分布式模型预测控制	显著降低时延，高负载下时延稳定，但吞吐量较传统Tor降低约20%，增加计算开销	实现接近最大-最小公平性，但吞吐量降低，计算开销增加
套接字耗尽攻击	动态连接管理	IMUX[39]	动态调整中继节点间的传输层安全协议（TLS）连接数量	吞吐量在攻击中保持稳定，但攻击者可伪造活动电路扰乱分配机制	基于PCTCP的扩展，动态连接管理，需提高电路活跃度判定门槛或引入复杂分类器

输入状态，动态确定各连接和电路的资源分配比例。通过整合深度强化学习与传统优化方法，QoS感知调度机制实现了动态资源分配的智能化，显著提升了系统的公平性与用户满意度。

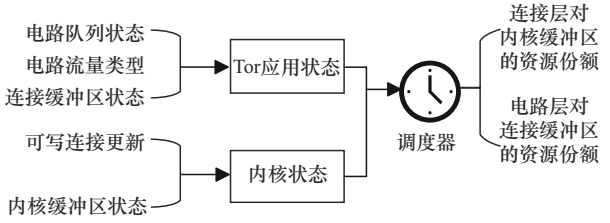


图7　QDRL系统模型

4.2.2　网络拥塞

在Tor网络中，电路与连接共享拥塞窗口的设计导致了一个关键问题：当某个电路的数据包因时延或丢失而触发拥塞窗口调整时，整个连接的拥塞窗口都会受到影响，从而波及所有电路。为解决上述问题，Döpmann等[38]提出了一种名为预测式Tor拥塞控制PredicTor的新方法，基于分布式模型预测控制的思想，通过优化算法来最小化时延并实现最大-最小公平性，即优化保障低速率电路的带宽。PredicTor将Tor网络中的每个中继节点视为一个独立的控制实体，每个节点通过局部优化决定自身的传输速率和流量分配，并通过与其相邻节点交换预测结果，实现跨节点的网络级协同。实验结果表明，PredicTor将平均时延从553 ms降至94 ms，在复杂网络场景中，PredicTor的时延在高负载下保持稳定，而Tor和PCTCP的时延随电路数量增加显著上升。但是，吞吐量较传统Tor网络降低约20%，且模型预测和优化带来了额外的计算开销。

4.2.3　套接字耗尽攻击

在Tor网络中，套接字耗尽攻击是一种常见的资源消耗型攻击。攻击者通过创建大量虚假连接来消耗中继资源，导致中继性能下降甚至引发拒绝服务攻击。为应对这一问题，Geddes等[39]在PCTCP的基础上，提出了一种名为具有自适应通道大小的反向复用Tor协议IMUX的解决方案，旨在通过动态调整中继间的传输层安全协议TLS连接数量，优化连接管理，并有效防御套接字耗尽攻击，实验显示其吞吐量在攻击中保持稳定。但IMUX仍存在一些局限，攻击者可通过伪造活动电路扰乱IMUX的连接分配机制，文献[39]建议提高电路活跃度的判定门槛或引入更复杂的分类器以增加攻击的难度。

5　去匿名化攻击与防御

在匿名网络研究领域，除了探索如何提升隐私保护技术之外，对去匿名化攻击的研究同样重要。可以将去匿名化攻击分类为主动攻击和被动攻击[40]，主动攻击通过注入流量或操控中继节点等直接影响网络运行，被动攻击则通过被动监听与分析现有通信，推测用户身份及通信关系。本节将围绕这两类去匿名化攻击的研究进展展开讨论，重点研究去匿名化攻击如何影响Tor等匿名网络的匿名性，以及如何抵抗去匿名化攻击造成的安全威胁。

5.1　Tor网络威胁模型

Tor网络威胁模型假定存在一个本地的主动攻击者[41]，该攻击者能够监控或控制网络的某部分，并且可能劫持或设置部分中继节点为恶意节点[42]。图8展示了攻击者可能实施的攻击活动，其中，攻击者可能会劫持或部署恶意中继节点，通过控制恶

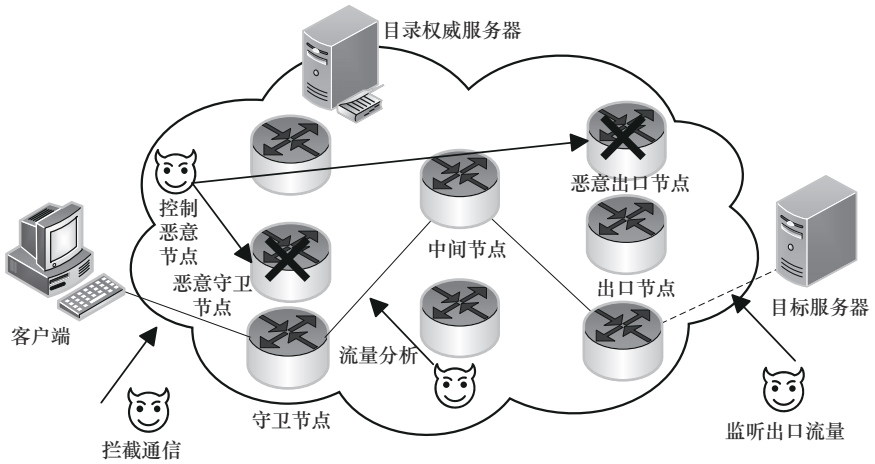


图8　Tor网络威胁模型示意

意中继节点，攻击者可以监控通过这些节点的数据流，并篡改、注入或删除数据包。攻击者还可能隐藏在网络中各个位置，以拦截客户端与守卫节点之间的通信，监控中继节点之间的流量以进行流量分析攻击，或监听未加密的出口流量，试图推测通信内容。通过观察数据包的大小、时间戳以及流量模式，攻击者能够识别通信内容、关联通信双方，或建立流量指纹来识别通信的具体目标网站。

5.2　典型主动攻击与防御

主动攻击是指攻击者通过直接干预匿名网络的运行或通信内容来实施攻击，有以下几种攻击方式：1) 主动路由攻击通过操控边界网关协议（BGP）劫持和拦截手段破坏匿名性；2) 女巫（Sybil）攻击通过构建多个虚拟节点，占据Tor网络的入口、出口或中继节点位置；3) TagIt攻击对网络流量的时间模式进行精细调整，并嵌入标记信息，以便关联入口和出口流量。表4对以上几种主动攻击[43-46]依据攻击方式、威胁、相应防御措施与防御措施的局限性进行总结。

5.2.1　主动BGP路由攻击与防御

Sun等[43]提出了Tor网络隐私路由攻击RAPTOR，利用互联网路由的不对称性，攻击者能够监控单向流量的时间和大小，从而破坏匿名性。实验表明，攻击者通过观察TCP序列号和确认号，关联客户端与服务器的流量方向，准确率达95%。网络路径变化使同一AS逐渐覆盖更多客户端与服务器路径，攻击成功率随时间增加50%~100%。攻击者通过伪造BGP路由，劫持Tor中继前缀或拦截流量路径，直接监控特定客户端或服务器的通信，实验中成功对实时Tor中继实施拦截攻击。

针对RAPTOR攻击，Sun等[44]提出了防御措施对抗Tor网络隐私路由攻击Counter-RAPTOR。首先，文献[44]通过适配的AS弹性指标，量化Tor网络抵御BGP劫持和拦截攻击的能力，并开发了一种结合AS弹性的守卫节点选择的算法，以增强Tor网络对BGP劫持的抵抗力。此外，研究团队还构建了实时BGP路由监测系统，用于检测并分析可疑的路由异常。尽管Counter-RAPTOR能够有效减少特定AS攻击的风险，但仍存在以下局限性：算法依赖于AS拓扑和实时BGP数据的准确性，而第三方数据源的更新频率可能不足以应对快速或短暂的攻击。

5.2.2　Sybil攻击与防御

Sybil攻击是指攻击者通过控制大量虚拟节点以获得不成比例的影响力。在Tor网络中，Sybil攻击可以通过以下方式威胁匿名性：控制多个虚拟节点，干预共识过程；通过控制网络的守卫和出口节点，将用户的身份与其活动关联起来；在出口节点篡改未加密的内容或执行中间人攻击。Winter等[45]开发了名为“Sybilhunter”的工具，通过检测和分类Tor网络中的Sybil节点来对抗Sybil攻击。

图9为Sybilhunter内部结构，其核心流程为：首先输入历史共识文件、服务器描述符，经可选过滤后，数据分流至4个分析模块——网络流量变化分析识别节点异常加入/离开模式、正常运行时间矩阵可视化节点在线/离线同步行为、指纹分析追踪频繁更换身份的节点、最近邻排名基于配置相似性生成潜在关联列表。各模块独立运行并共享数据，最终输出逗号分隔值（CSV）报告或可视化图像（如运行时间矩阵图），辅助人工或自动化识别Sybil群组。尽管Sybilhunter提供了一种有效手段，但当前针对Sybil攻击的防御措施在Tor网络中的效果有限，攻击者可以通过增加资源或更复杂的手段绕过检测，并且攻击模式不断变化，现有的检测方法需要持续更新和改进。

表4　主动去匿名化攻击与防御措施总结

攻击类型	方式	威胁	防御措施	防御措施局限性
RAPTOR攻击[43-44]	利用BGP路由不对称性进行路由劫持或拦截	流量方向关联准确率高达95%，攻击成功率随时间增加50%~100%，严重破坏匿名性	定义AS弹性指标量化抵抗能力，优化守卫节点选择提高抗劫持性，实时BGP监测分析路由异常	存在位置泄露和负载不均衡问题
Sybil攻击[45]	创建大量虚拟节点占据入口、中继或出口位置	破坏共识，关联身份，实施中间人攻击	检测和分类可疑Sybil节点	资源密集型攻击可能绕过现有检测
TagIt攻击[46]	注入隐蔽指纹实现流量关联	高效隐蔽的去匿名化	丰富伪装流量特征，减少被标记的可能	可能造成额外计算开销和网络时延

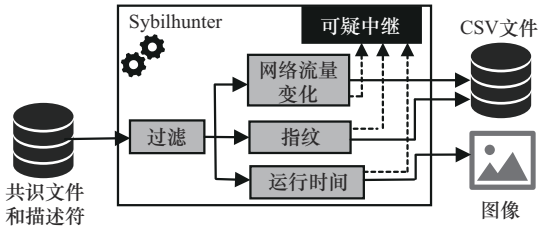


图9　Sybilhunter内部结构

5.2.3　TagIt攻击与防御

Rezaei等[46]提出了一种名为TagIt的盲流指纹系统，旨在克服非盲指纹系统的通信和扩展性限制，同时确保指纹的隐蔽性和鲁棒性。TagIt通过在数据包的时间戳中引入轻微时延嵌入指纹，这种时延对合法提取方可检测，但对不知密钥的攻击者而言无法察觉。文献[46]指出，TagIt可用于攻击匿名通信系统，例如对Tor流量中的守卫和出口节点流量进行打标，实现更大规模的去匿名化。针对TagIt带来的流量指纹攻击威胁，本文认为，可以通过以下措施进行防御：在Tor网络中设置监控机制，检测数据包异常时延，并及时调整路径选择策略；通过引入随机时延和填充包来干扰指纹嵌入，使攻击者难以提取有效信息。

5.3　典型被动攻击与防御

被动攻击是指攻击者不主动干预网络，而是通过监视和收集匿名网络中的流量和行为特征来推断用户的身份或通信关系，有以下几种攻击方式：1) 守卫节点位置攻击通过部署特定位置的守卫节点，提高被选中的概率；2) 流量关联攻击结合域名系统（DNS）流量和TCP流量进行关联分析；3) 网站指纹（WF, website fingerprinting）攻击通过分析网络流量特征来推测用户访问目标网站。表5对以上几种被动攻击[47-53]依据攻击方式、威胁与防御措施进行总结。

5.3.1　守卫节点位置攻击与防御

为了增强安全性，研究者提出了基于位置的路径选择算法，通过考虑中继节点的地理或网络位置来减少特定攻击的威胁。但是，攻击者可以通过优化守卫节点的部署策略，显著提高被选概率，对这类算法进行去匿名化攻击。Wan等[47]定义了守卫节点位置攻击的威胁模型，并对3种典型的基于位置的路径选择算法（对抗Tor网络隐私路由攻击Counter-RAPTOR[44]、DeNASA[25]和LASTor[48]）进行了攻击模拟。实验表明，对于Counter-RAPTOR，攻击者贡献0.216%带宽时，平均选择概率达18.22%，是当前Tor网络的84倍。对于DeNASA，单个低带宽节点可使特定客户端选择概率提升964倍，多节点部署可进一步提高成功率。对于LASTor，通过地理聚类算法，攻击者可使概率提升103倍，多节点部署效果显著。因此，基于位置的路径选择算法在设计时需平衡位置考虑与对抗位置攻击的能力。为缓解守卫位置攻击的威胁，文献[47]提出了一种通用的防御机制，可适用于任何路径选择算法，核心思想是限制守卫节点选择概率，使其相对于节点的贡献成本（如带宽、地理位置、运行时间等）保持合理的比例。

表5　　**被动攻击与防御措施总结**

攻击类型		代表工作	方式	威胁	防御措施
守卫节点位置攻击		RAPTOR[47]	部署特定守卫节点实施流量分析攻击	对位置感知的路径选择算法去匿名化，控制部分节点影响整体匿名性	限制守卫节点选择概率，增强路径选择算法鲁棒性
流量关联攻击		DefecTor[49]	结合DNS和TCP流量关联	提高不受欢迎网站指纹识别精度	加密与伪装DNS流量，优化DNS解析机制
		DeepCoFFEA[50]	特征嵌入技术、时间窗口投票机制	降低攻击方式的计算复杂度至$O(N)$并保持高攻击准确率（在10 000条流量规模下，真阳性率TPR达93%）	强化流量伪装，扰乱深度学习模型的特征提取能力
网站指纹攻击	传统机器学习	kFP、SVM[51-52]	SVM、kNN等统计特征分类	实验环境下识别成功率高	加强流量加密和伪装，降低特征提取效果
	深度学习	RF[53]	自动提取流量特征	复杂场景下识别网站模式，挑战现有防御	开发对抗性防御，改进流量伪装算法

5.3.2　流量关联攻击与防御

流量关联攻击是匿名通信系统中的一种主要威胁，攻击者通过关联入口和出口流量的特征，识别用户通信路径，进而破坏匿名性。Greschbach 等[49]提出了一种新型攻击方式，称为基于 Tor 的 DNS 增强指纹识别与出口流量关联攻击 DefecTor，通过结合 DNS 流量和 TCP 流量，DefecTor 对不常访问的网站可实现几乎完美的指纹识别，大幅提高了流量关联攻击的成功率。为了抵抗这种针对 DNS 流量的攻击，可以加强 DNS 流量的加密和伪装，防止其被攻击者利用，或改进 Tor 的 DNS 解析方式以减少暴露。

Oh 等[50]提出了深度相关流特征提取与增强攻击 DeepCoFFEA，通过改进深度学习方法，使流量关联攻击更高效、更精准。DeepCoFFEA 使用改进的三元组网络结构，分别处理 Tor 入口流量和出口流量，生成低维嵌入向量，将计算复杂度降至 $O(N)$。并将流量分割为多个时间窗口，每个窗口独立判断关联性，通过多数投票机制降低误报率。实验表明，在 10 000 条流量规模下，相较于 DeepCorr[51]，DeepCoFFEA 攻击成功率达 93%（DeepCorr 仅为 13%），计算速度提升 2 个数量级。

5.3.3　网站指纹攻击与防御

网站指纹攻击通过提取和学习网络流量的特征（如数据包大小、时间间隔和方向），以推断用户正在访问的具体网站[51-52]。早期的网站指纹攻击主要依赖简单分类器，如使用 k-指纹（kFP，k-fingerprinting）、SVM 等，依赖于基础的流量特征提取。传统的网站指纹攻击虽然在实验环境下表现良好，但在应对复杂流量和高级防御机制时存在局限性。深度学习的引入为网站指纹攻击提供了更强大的特征提取能力和适应性，Shen 等[53]提出了一种攻击方法稳健指纹（RF, robust fingerprinting）识别，引入了流量聚合矩阵，捕捉网络流量中未被防御措施显著干扰的关键信息，并使用基于卷积神经网络的分类器自动从矩阵中提取有效特征。封闭世界场景下，RF 识别在 WTF-PAD、FRONT 等防御下准确率均显著高于现有攻击，平均提升 8.9%。在 Trafficsliver-BWR 防御下，RF 准确率为 79.68%，远超其他攻击。开放世界场景下，RF 的整体表现优于现有攻击，尤其在高召回率下仍保持高精度。

随着网站指纹攻击技术的不断演进，相应的防御策略也在持续发展。例如，通过流量填充和混淆技术来隐藏流量特征、将具有相似特征的数据流进行分组以掩盖个别流量的独特性，以及通过调整通信模式来改变流量的传输模式和特征。表 6 对以上几种网站指纹攻击防御方法[54-61]依据实现方法、特点等进行了总结。

1)流量填充与混淆。Gong 等[54]提出了 2 种零时延轻量级防御方法：FRONT 通过在流量前段添加伪装数据包，并随机化数据包的数量和分布，混淆流量特征，使每次访问相同页面的流量特征差异显著。GLUE 在实际流量间插入伪装数据，使其看起来像是用户连续访问多个页面。并应用新的分割框架，防止攻击者有效区分实际流量与伪装流量。实验表明，FRONT 带来的数据开销约 33%，与 WTF-PAD 相当，但性能更优。FRONT 显著降低深度指纹（DF, deep fingerprinting）识别、kFP 等攻击的精度，尤其对 kNN 攻击效果突出。在高难度攻击场景下，GLUE 可将攻击的真阳性率 TPR 和精度降至 1% 以下，性能超过传统重量级防御。

Holland 等[55]提出了洪流相关流量分析防御系统 DeTorrent，一种基于生成对抗网络的抗流量分析防御策略。利用长短期记忆（LSTM, long short-term memory）网络生成器和卷积神经网络判别器（CNN, convolutional neural network）的对抗训练，生成器学习插入虚拟数据包以混淆流量特征，判别器尝试识别真实流量。实验表明，在足够大（BE, bigenough）数据集上，DeTorrent 将 Tik-Tok 准确率从 93.4% 降至 31.9%，比 FRONT（42.4%）和 WTF-PAD（62.3%）更优。信息泄露显著降低，关键特征泄露减少 50% 以上。对于 FC 防御，在深度相关流嵌入攻击（DCF, deepcoffea）数据集上，DeTorrent 将 DeepCoFFEA 的 TPR 在 FPR = 10^{-5} 时降至 0.12，远低于 Decaf[50]（0.29）和 FRONT（0.34）。但是 DeTorrent 也存在一定的局限性，对于更复杂的网络流量模式可能需要额外调整。在某些情况下，生成伪流量的开销仍可能较高。

2)流量聚类。Nithyanand 等[56]提出一种高效防御方法 Glove，通过流量聚类和伪装流量生成对抗 WF 攻击。Glove 将具有相似网络特征的网页分组，为每组生成一个超级轨迹，覆盖组内所有网页的流量特征。实验表明，Glove 在相同安全级别下，带宽开销仅为 CS-BuFLO[57] 的 $\frac{1}{3}$。Shen 等[58]提出了一

表6 网站指纹攻击防御方法总结

解决思路	代表工作	方法	防御目标	数据集	效果	特点
流量填充与混淆	FRONT、GLUE[54]	伪装数据包和随机化分布混淆流量	DF、kFP	DS-19、DS-14	FRONT显著降低DF识别、kFP的TPR和精度，GLUE将其降至1%以下	高效解决高开销与时延问题
	DeTorrent[55]	利用GAN生成伪流量干扰攻击模型	Tik-Tok、DF、DeepCoFFEA	BE、DF、DCF	在BE数据集上，将Tik-Tok准确率从93.4%降至31.9%。在DCF数据集上，将DeepCoFFEA的TPR在FPR = 10^{-5}时降至0.12	提供抗流量分析攻击的新思路，但需优化生成器和判别器性能
流量聚类	Glove[56]	生成超级轨迹以隐藏特征，分组相似网页流量	Panchenko、DL-SVM	收集Alexa前500网站	带宽开销为CS-BuFLO的$\frac{1}{3}$，远低于BuFLO	高效安全，但动态网页内容可能失效
	Palette[58]	构建超级轨迹，隐藏单个网站特征	DF、Tik-Tok、Var-CNN、RF	封闭世界：95个网站；开放世界：40 716个未监控网站	封闭世界，将RF攻击准确率从98.40%降至36.43%；开放世界，召回率降至0.1以下	平衡高匿名性和开销，但需适应动态流量与复杂网络环境
通信模式调整	Walkie-Talkie（WT）[59]	半双工通信，分段突发交替传输数据	SVM、kNN、CUMUL	封闭世界：Alexa前100网站；开放世界：Alexa前10 000网站	封闭世界，将kNN攻击准确率从95%降至28%，SVM从81%降至44%；开放世界，攻击的FPR显著增加，带宽开销31%，时间开销34%	高效抵御WF攻击，但需适配动态内容
	TrafficSliver[61]	多路径分散流量或分片HTTP请求	kNN、CUMUL、kFP、DF	封闭世界：Alexa前100网站；开放世界：Alexa前11 307网站	攻击准确率降至16%以下，带宽开销低于1%，时延开销低于传统防御	轻量级、低开销、易部署，适应多路径传输

种新型防御方法Palette，针对现有深度学习模型提升WF攻击准确性的挑战，通过流量聚类匿名化减少攻击成功率。Palette使用流量聚合矩阵对流量特征进行多维信息聚合，以隐藏单个网站的特性。封闭世界场景下，Palette将RF攻击准确率从98.4%降至36.43%，信息泄露量显著低于其他防御，关键特征泄露减少50%以上。开放世界场景下，Palette将攻击的召回率降至0.1以下（高精度设置），显著优于现有方法。

3)通信模式调整。Wang等[59]提出了一种防御方法WT，通过半双工通信模式，客户端和服务器之间的通信不再同时进行，而是以分段突发的形式交替发送和接收数据。WT是在有效性、效率和实用性之间取得了良好平衡。封闭世界场景下，WT将kNN攻击准确率从95%降至28%，SVM从81%降至44%。关键特征（如突发大小、序列长度）的泄露量显著降低。开放世界场景下，攻击的FPR显著增加（如kNN的FPR从0.09升至0.62），导致攻击者的精度大幅下降。WT的带宽开销为31%，时间开销为34%，远低于现有防御（如Tamaraw[60]的带宽开销103%、时间开销140%）。然而，WT主要针对静态网页，对动态内容的防御效果有限。

Cadena等[61]提出轻量级网站指纹攻击防御机制流量切片TrafficSliver，在Tor网络层（Traffic-Sliver-Net）和应用层（TrafficSliver-App）分别实现流量分割，将流量分散到多个不同的守卫节点，无须引入人工时延或伪造流量。如图10所示，对于网络层防御，用户通过Tor网络建立多条子电路，初始电路为三跳结构，后续通过Cookie认证机制快速创建额外的两跳子电路（守卫−中间），所有子电路共享同一中间节点和出口节点，实现流量分散。流量分割采用批量加权随机（BWR）策略，将Tor单元按批次动态分配到不同子电路，中间节点缓存时延单元以确保正确处理。实验表明，封闭世界场景下，TrafficSliver-Net将攻击准确率从98%以上降至16%以下。TrafficSliver-App将DF准确率从98.75%降至57.34%，显著优于WTF-PAD等现有防御。开放世界场景下，攻击的ROC曲线下面积值接近随机猜测（0.5），表明防御有效破坏了攻击的识别能力。带宽开销可忽略（<1%），时延开

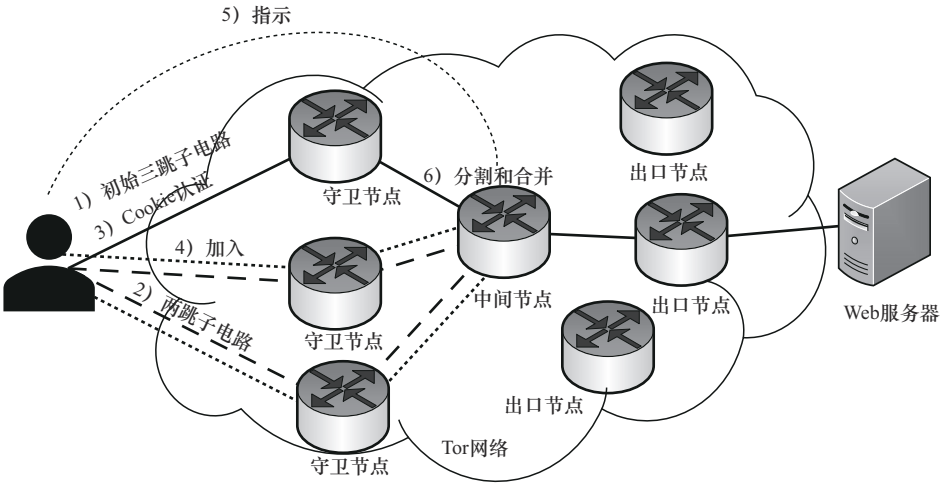


图10　TrafficSliver-Net防御设计概述

销较低（TrafficSliver-Net为34%，TrafficSliver-App为24%），远低于传统防御。

6　总结与展望

本文从Tor网络发送者匿名性相关的核心功能模块出发，介绍了Tor的目录协议、路径选择、电路构建等关键机制，分析了其设计缺陷，并探讨了针对Tor网络的去匿名化攻击手段及其防御策略。在此基础上，本文对近年来Tor网络领域的典型研究进展进行了系统的梳理与分类。针对每个研究分类，本文都列举了若干具有代表性的研究工作，对其优缺点进行了分析，评估不同研究方案的有效性和适用性。

基于上述4个研究领域，表7从研究方向、存在缺陷与解决思路3个方面，对当前相关研究现状进行总结。目录协议方面，针对恶意节点伪造带宽欺骗问题，可以结合强化学习方法来动态监测和绕过潜在恶意节点，优化路径选择。通过降低单节点的流量上限并引入基于机器学习的带宽预测算法，提高带宽测量的准确性和抗攻击性。此外，探索更高效的目录更新机制，提升协议的安全性并减少时延和网络负载。路径选择方面，为平衡匿名性、安全性和性能，可以开发基于人工智能的智能路径选择算法，根据实时的网络状况和用户行为动态调整路径。同时，引入流量分割机制，通过分割流量增加流量关联难度。并结合流量填充和流量整形技术，有效混淆流量模式。针对守卫节点和中间节点选择，采用安全评分机制来动态评估节点，改进节点的选择策略，从而减少恶意节点的渗透。

表7　Tor研究工作总结

研究方向	存在缺陷	解决思路
目录协议	恶意节点伪造带宽欺骗； 带宽测量机制存在安全漏洞与测量偏差； 共识文件生成的不一致性	优化流量分配； 改进带宽测量机制，提高测量抗攻击性； 增强目录协议的抗攻击能力
路径选择	对流量分析与关联攻击的防御不足； 性能与匿名性平衡的难题； 守卫节点选择策略的易受攻击性； 中间节点被忽视的潜在威胁	综合考虑带宽、AS路径、互联网交换（IX, Internet exchange）中心威胁等多因素进行路径选择； 平衡网络负载，降低网络时延； 开发动态守卫集管理机制，根据网络波动情况动态调整守卫集； 引入中间节点的安全性评估机制，避免选择高风险节点
电路构建	交叉电路干扰； 网络拥塞问题； 套接字耗尽攻击	根据实时电路需求动态调整带宽分配； 改进或替代传统的TCP； 动态管理套接字
去匿名化攻击与防御	攻击范围扩大化； 攻击技术智能化； 协同攻击日益增强； 节点渗透与内部攻击增强	动态防御与实时监测； 流量混淆与特征伪装； 加强协议安全性； 改进路径选择与节点验证机制

电路构建方面，为应对网络拥塞和流量管理问题，研发自适应拥塞控制算法，根据实时需求动态调整带宽，避免高流量任务占用过多资源，提升整体性能。针对套接字耗尽攻击，通过动态管理套接字来限制连接占用资源，并根据需求调整系统资源。针对去匿名化攻击的挑战，随着攻击手段的智能化、协同化和复合化，Tor网络需不断加强防御。未来的防御技术应重点开发针对联合攻击和多维攻击的增强型匿名性机制，并结合智能化检测技术提升对去匿名化攻击的应对能力，确保用户隐私安全。

此外，随着技术和网络环境的快速发展，传统隐私保护技术面临以下挑战：量子计算的威胁、网络复杂性的增加，以及高性能与高隐私的平衡等。未来匿名网络的研究发展可以关注以下内容。

1)抗量子密码学算法：研究抗量子密码学算法（如基于格的密码协议）以应对量子计算对传统加密算法的威胁。结合量子密钥分发技术，增强高安全需求场景下的隐私保护。比如，用抗量子密码学算法替代Tor网络中的RSA（Rivest-Shamir-Adleman）加密，提升目录协议安全性；引入量子抗性密钥交换协议，增强路径选择中的通信安全，抵御量子计算的流量分析攻击。

2) 可编程网络：通过可编程网络技术，设计支持动态流量混淆与实时攻击防御的匿名通信协议，提升灵活性和可扩展性。例如，基于实时网络状况和攻击情况，动态调整路径选择，平衡匿名性与性能；通过动态流量控制，解决网络拥塞，提高传输效率，并增强Tor对复杂网络环境的适应能力。

3) 差分隐私与多方安全计算结合：引入差分隐私技术保护流量数据，防止敏感信息泄露，确保即便攻击者能够访问部分数据，也无法精确获取用户的身份信息。此外，结合零知识证明和多方安全计算，可以使得多个节点之间在不暴露个人数据的情况下进行协作，进一步增强防御能力，避免协同攻击，同时提高计算效率和通信性能。

4) 全局流量观测与优化：结合边缘计算和云计算，设计跨区域匿名网络的流量调度与优化方案，实现全局范围内的高效资源分配，提升网络性能，减少时延，并平衡流量负载。全局流量观测可以优化守卫节点的选择策略，动态评估节点风险，避免网络中存在的潜在威胁，提高路径选择的安全性。

7 结束语

尽管Tor网络在保障匿名性与隐私性方面具有重要价值，但其面临的性能优化、安全威胁等问题仍亟待解决。当前的研究进展揭示，增强匿名网络的鲁棒性、提升其效率以及增强其抵御去匿名化攻击的能力，已经成为该领域研究的核心焦点。尤其是随着量子计算、人工智能等前沿技术的迅猛发展，匿名网络的安全性将遭遇更为严峻的挑战，同时也提供了更多的机遇和可能性。本文通过对Tor网络的匿名通信基本原理、现存问题与改进技术的梳理，以及对去匿名化攻击方式与防御方法的系统分析，揭示了匿名网络领域的复杂性与多样性。最后，本文总结了Tor等匿名网络安全技术研究现状，并对未来研究方向进行了展望。

参考文献：

[1] 赵蕙, 王良民, 申屠浩, 等. 网络匿名度量研究综述[J]. 软件学报, 2021, 32(1): 218-245.
ZHAO H, WANG L M, SHENTU H, et al. Survey on anonymity metrics in communication network[J]. Journal of Software, 2021, 32(1): 218-245.

[2] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[3] 马传旺, 张宇, 方滨兴, 等. 匿名网络综述[J]. 软件学报, 2023, 34(1): 404-420.
MA C W, ZHANG Y, FANG B X, et al. Survey on anonymous networks[J]. Journal of Software, 2023, 34(1): 404-420.

[4] 杨云, 李凌燕, 魏庆征. 匿名网络Tor与I2P的比较研究[J]. 网络与信息安全学报, 2019, 5(1): 66-77.
YANG Y, LI L Y, WEI Q Z. Comparative study of anonymous network tor and I2P[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 66-77.

[5] XU Y H, YANG M, LING Z, et al. A de-anonymization attack against downloaders in freenet[C]//Proceedings of the IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2024: 1-10.

[6] EDMAN M, YENER B. On anonymity in an electronic society: a survey of anonymous communication systems[J]. ACM Computing Surveys, 2010, 42(1):1-35.

[7] CHEN Z C, JARDINE E, LIU X F, et al. Seeking anonymity on the Internet: the knowledge accumulation process and global usage of the tor

network[J]. New Media & Society, 2024, 26(2): 1074-1095.

[8] CANGIALOSI F, LEVIN D, SPRING N. Ting: measuring and exploiting latencies between all tor nodes[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM Press, 2015: 289-302.

[9] TAN Q F, WANG X B, SHI W, et al. An anonymity vulnerability in tor[J]. IEEE/ACM Transactions on Networking, 2022, 30(6): 2574-2587.

[10] TIPPE P, TIPPE A. Onion services in the wild: a study of deanonymization attacks[J]. Proceedings on Privacy Enhancing Technologies, 2024(4): 291-310.

[11] PAHL S, ADAMSKY F, KAISER D, et al. Examining the hydra: simultaneously shared links in tor and the effects on its performance[J]. Proceedings on Privacy Enhancing Technologies, 2023(3): 268-285.

[12] ARORA A, GARMAN C. Improving the performance and security of Tor's onion services[J]. Proceedings on Privacy Enhancing Technologies, 2025(1): 531-552.

[13] KARUNANAYAKE I, AHMED N, MALANEY R, et al. Deanonymisation attacks on Tor: a survey[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2324-2350.

[14] DINGLEDINE R, MATHEWSON N, SYVERSON P F. Tor: the second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004: 303-320.

[15] SYVERSON P F, GOLDSCHLAG D M, REED M G. Anonymous connections and onion routing[C]//Proceedings of 1997 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 1997: 44-54.

[16] 罗军舟, 杨明, 凌振, 等. 匿名通信与暗网研究综述[J]. 计算机研究与发展, 2019, 56(1): 103-130.
LUO J Z, YANG M, LING Z, et al. Anonymous communication and darknet: a survey[J]. Journal of Computer Research and Development, 2019, 56(1): 103-130.

[17] JANSEN R, TRAUDT M, GEDDES J, et al. KIST: kernel-informed socket transport for Tor[J]. ACM Transactions on Privacy and Security, 2019, 22(1): 1-37.

[18] MATHEWS N, HOLLAND J K, OH S E, et al. SoK: a critical evaluation of efficient website fingerprinting defenses[C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2023: 969-986.

[19] XIAO X, ZHOU X, YANG Z Y, et al. A comprehensive analysis of website fingerprinting defenses on Tor[J]. Computers & Security, 2024, 136: 103577.

[20] JOHNSON A, JANSEN R, HOPPER N, et al. PeerFlow: secure load balancing in tor[J]. Proceedings on Privacy Enhancing Technologies, 2017(2): 74-94.

[21] TRAUDT M, JANSEN R, JOHNSON A. FlashFlow: a secure speed test for tor[C]//Proceedings of the 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS). Piscataway: IEEE Press, 2021: 381-391.

[22] SENDNER C, STANG J, DMITRIENKO A, et al. MirageFlow: a new bandwidth inflation attack on Tor[C]//Proceedings of the 31st Annual Network and Distrib uted System Security Symposium. Virginia: Internet Society, 2024: 1-16.

[23] LUO Z T, BHAT A, NAYAK K, et al. Attacking and improving the tor directory protocol[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 3221-3237.

[24] NITHYANAND R, STAROV O, ZAIR A, et al. Measuring and mitigating AS-level adversaries against Tor[C]//Proceedings of the 2016 Network and Distributed System Security Symposium. Virginia: Internet Society, 2016: 1-15.

[25] BARTON A, WRIGHT M. DeNASA: destination-naive AS-awareness in anonymous communications[J]. Proceedings on Privacy Enhancing Technologies, 2016(4): 356-372.

[26] ROCHET F, WAILS R, JOHNSON A, et al. CLAPS: client-location-aware path selection in Tor[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 17-34.

[27] JOHNSON A, JANSEN R, JAGGARD A D, et al. Avoiding the man on the wire: improving Tor's security with trust-aware path selection[C]//Proceedings of the 2017 Network and Distributed System Security Symposium. Virginia: Internet Society, 2017: 1-79.

[28] GEDDES J, SCHLIEP M, HOPPER N. ABRA CADABRA: magically increasing network utilization in Tor by avoiding bottlenecks[C]//Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. New York: ACM Press, 2016: 165-176.

[29] ROCHET F, PEREIRA O. Waterfilling: Balancing the Tor network with maximum diversity[J]. Proceedings on Privacy Enhancing Technologies, 2017(2): 4-22.

[30] HOGAN K, SERVAN-SCHREIBER S, NEWMAN Z, et al. ShorTor: improving tor network latency via multi-hop overlay routing[C]//Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1933-1952.

[31] BARTON A, WRIGHT M, MING J, et al. Towards predicting efficient and anonymous Tor circuits[C]//Proceedings of the 27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 429-444.

[32] HAYES J, DANEZIS G. Guard sets for onion routing[J]. Proceedings on Privacy Enhancing Technologies, 2015(2): 65-80.

[33] IMANI M, BARTON A, WRIGHT M. Guard sets in Tor using AS relationships[J]. Proceedings on Privacy Enhancing Technologies, 2018(1): 145-165.

[34] JANSEN R, JUAREZ M, GALVEZ R, et al. Inside job: applying traffic analysis to measure Tor from within[C]//Proceedings of the 2018 Network and Distributed System Security Symposium. Virginia: Internet Society, 2018: 1-15.

[35] ALSABAH M, GOLDBERG I. PCTCP: per-circuit TCP-over-IPsec transport for anonymous communication overlay networks[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Com-

munications Security - CCS'13. New York: ACM Press, 2013: 349-360.

[36] CADENA W D L, KAISER D, PANCHENKO A, et al. Out-of-the-box multipath TCP as a tor transport protocol: performance and privacy implications[C]//Proceedings of the 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). Piscataway: IEEE Press, 2020: 1-6.

[37] BASYONI L, ERBAD A, MOHAMED A, et al. QDRL: QoS-aware deep reinforcement learning approach for Tor's circuit scheduling[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(5): 3396-3410.

[38] DÖPMANN C, FIEDLER F, LUCIA S, et al. Optimization-based predictive congestion control for the Tor network: opportunities and challenges[J]. ACM Transactions on Internet Technology, 2022, 22(4): 1-30.

[39] GEDDES J, JANSEN R, HOPPER N. IMUX: managing tor connections from two to infinity, and beyond[C]//Proceedings of the 13th Workshop on Privacy in the Electronic Society. New York: ACM Press, 2014: 181-190.

[40] CHAO D C, XU D W, GAO F, et al. A systematic survey on security in anonymity networks: vulnerabilities, attacks, defenses, and formalization[J]. IEEE Communications Surveys & Tutorials, 2024, 26(3): 1775-1829.

[41] ALSABAH M, GOLDBERG I. Performance and security improvements for Tor[J]. ACM Computing Surveys, 2017, 49(2): 1-36.

[42] KOMLO C, MATHEWSON N, GOLDBERG I. Walking onions: scaling anonymity networks while protecting users[C]//Proceedings of the 29th USENIX Security Symposium. Berkeley: USENIX Association, 2020: 1003-1020.

[43] SUN Y, EDMUNDSON A, VANBEVER L, et al. RAPTOR: routing attacks on privacy in Tor[C]//Proceedings of the 24th USENIX Security Symposium. Berkeley: USENIX Association, 2015: 271-286.

[44] SUN Y X, EDMUNDSON A, FEAMSTER N, et al. Counter-RAPTOR: safeguarding Tor against active routing attacks[C]//Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2017: 977-992.

[45] WINTER P, ENSAFI R, LOESING K, et al. Identifying and characterizing sybils in the Tor network[C]//Proceedings of the 25th USENIX Security Symposium. Berkeley: USENIX Association, 2016: 1169-1185.

[46] REZAEI F, HOUMANSADR A. TagIt: tagging network flows using blind fingerprints[J]. Proceedings on Privacy Enhancing Technologies, 2017(4): 290-307.

[47] WAN G, JOHNSON A, WAILS R, et al. Guard placement attacks on path selection algorithms for Tor[J]. Proceedings on Privacy Enhancing Technologies, 2019(4): 272-291.

[48] AKHOONDI M, YU C, MADHYASTHA H V. LASTor: a low-latency AS-aware tor client[C]//Proceedings of the 2012 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2012: 476-490.

[49] GRESCHBACH B, PULLS T, ROBERTS L M, et al. The effect of DNS on Tor's anonymity[C]//Proceedings of the 2017 Network and Distributed System Security Symposium. Virginia: Internet Society, 2017: 1.

[50] OH S E, YANG T J, MATHEWS N, et al. DeepCoFFEA: improved flow correlation attacks on Tor via metric learning and amplification[C]//Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2022: 1915-1932.

[51] NASR M, BAHRAMALI A, HOUMANSADR A. DeepCorr: strong flow correlation attacks on Tor using deep learning[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 1962-1976.

[52] 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 H C, SU J S, WEI Z L, et al. A review of the research of website fingerprinting identification and defense[J]. Chinese Journal of Computers, 2022, 45(10): 2243-2278.

[53] SHEN M, JI K, GAO Z, et al. Subverting website fingerprinting defenses with robust traffic representation[C]//Proceedings of the 32nd USENIX Security Symposium. Berkeley: USENIX Association, 2023: 607-624.

[54] GONG J, WANG T. Zero-delay lightweight defenses against website fingerprinting[C]//Proceedings of the 29th USENIX Security Symposium. Berkeley: USENIX Association, 2020: 717-734.

[55] HOLLAND J K, CARPENTER J, OH S E, et al. DeTorrent: an adversarial padding-only traffic analysis defense[J]. Proceedings on Privacy Enhancing Technologies, 2024(1): 98-115.

[56] NITHYANAND R, CAI X, JOHNSON R. Glove: a bespoke website fingerprinting defense[C]//Proceedings of the 13th Workshop on Privacy in the Electronic Society. New York: ACM Press, 2014: 131-134.

[57] CAI X, NITHYANAND R, JOHNSON R. CS-BuFLO: a congestion sensitive website fingerprinting defense[C]//Proceedings of the 13th Workshop on Privacy in the Electronic Society. New York: ACM Press, 2014: 121-130.

[58] SHEN M, JI K X, WU J H, et al. Real-time website fingerprinting defense via traffic cluster anonymization[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 3238-3256.

[59] WANG T, GOLDBERG I. Walkie-talkie: an efficient defense against passive website fingerprinting attacks[C]//Proceedings of the 26th USENIX Security Symposium. Berkeley: USENIX Association, 2017: 1375-1390.

[60] CAI X, NITHYANAND R, WANG T, et al. A systematic approach to developing and evaluating website fingerprinting defenses[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and

Communications Security. New York: ACM Press, 2014: 227-238.

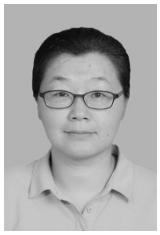
[61] CADENA W D L, MITSEVA A, HILLER J, et al. TrafficSliver: fighting website fingerprinting attacks with traffic splitting[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2020: 1971-1985.

[作者简介]

朱俞翡（2002– ），女，河南商丘人，信息工程大学博士生，主要研究方向为网络空间安全、隐私保护。

胡宇翔（1982– ），男，河南周口人，博士，信息工程大学教授、博士生导师，主要研究方向为网络空间安全、新型网络架构。

陈博（1989– ），男，河南商丘人，博士，信息工程大学助理研究员，主要研究方向为网络空间安全、软件定义网络。



申涓（1976– ），女，河南郑州人，信息工程大学副教授，主要研究方向为网络空间安全、新型网络架构。

崔鹏帅（1990– ），男，河南安阳人，博士，信息工程大学副研究员，主要研究方向为网络空间安全、新型网络架构。

袁征（1982– ），女，河南驻马店人，信息工程大学助理研究员，主要研究方向为新型网络架构、内生安全。

田乐（1987– ），男，陕西咸阳人，博士，信息工程大学副研究员，主要研究方向为网络空间安全、软件定义网络。