•聚焦国家重点研发计划•

DOI:10.12454/j.jsuese.202400800

本刊网刊

面向暗网抑制的普适性安全理论研究构想和成果展望

黄　诚[1], 丁建伟[2], 赵佳鹏[3], 陈周国[2], 时金桥[3]

(1.四川大学 网络空间安全学院, 四川 成都 610065; 2.中国电子科技集团公司第三十研究所, 四川 成都 610093;
3.北京邮电大学 网络空间安全学院, 北京 100876)

摘　要: 近年来, 匿名网络及其架构上的“暗网”因其强隐蔽、高匿名、抗追溯的特性, 成为传递敏感信息、实施网络攻击及开展网络犯罪的重要工具, 给国家安全和社会稳定带来严重威胁。为应对暗网治理中通信行为隐蔽难识别、网络拓扑跳变难绘制、陷阱节点部署难伪装等挑战, 本文旨在研究面向暗网抑制的普适性安全理论。本研究的关键科学问题凝练为: 强对抗机制下结构信息缺失的动态时变网络行为刻画与推理问题。为突破以上问题, 拟从基础理论、应用技术和示范系统3个层面开展研究, 实现1个框架、3个方法、1个系统等五大研究内容。具体为: 一是, 建立面向暗网流量差异性与行为共性的协同量化理论框架, 提出异构暗网普适性特征与差异化要素表征、统一安全量化、生态脆弱图构建及推理理论, 解决网络结构复杂多样、通信行为动态多变的暗网可抑制性量化评估问题; 二是, 提出基于凸优化问题求解的流量实时轻量化识别方法, 通过构建基于自身相似性关联的小流抽样模型与基于高斯核函数和多模态优化的暗网流量识别与业务分类模型, 实现对暗网流量的实时、轻量化精准识别与分类; 三是, 提出基于行为不变性的多网络全时域连接预测与通连关系绘制方法, 在统一安全量化理论的基础上, 对跨位点连接进行表示, 在动态网络中过滤无关连接后进行多网络全时域连接预测, 并绘制通连关系, 实现局部观测条件下暗网通连的多点全局关联; 四是, 提出基于局部观测暗网通连最优化的陷阱节点部署与溯源方法, 实现部分可控节点条件下的暗网追踪溯源; 五是, 研发面向真实暗网场景的实时流量检测与溯源示范应用系统, 并在相关执法单位进行落地应用, 实现对暗网犯罪的精准治理。并且, 详细阐述了协同量化理论构建、轻量化暗网流量识别、连接预测与通连关系绘制、陷阱部署与溯源机理、示范应用系统等五大任务的技术路线。通过本文的基础理论研究、技术应用和系统示范验证, 推动暗网治理的理论发展, 提升抑制暗网的效率, 具有重要的社会与经济效益。

关键词: 暗网治理; 流量检测; 行为识别; 安全量化; 陷阱节点部署

中图分类号: TP309.1　　**文献标志码:** A　　**文章编号:** 2096-3246(2025)01-0001-10

当前互联网主要分为表网、深网。暗网是一张附着于互联网, “看不见、摸不着”的网络, 属于深网的一部分。近年来, 由于普通用户访问暗网的门槛大幅降低, 导致了一系列影响社会安全和稳定的问题, 给网络监管者和执法机构带来了更复杂和严峻的考验。尽管执法机构不断更新和完善监管技术手段, 但是暗网依然能够借助其强隐蔽、高匿名、抗追溯的特性被越来越多地用于传递军事情报、发布政治敏感信息、实施网络攻击, 其承载了大量的网络犯罪市场、暴恐分裂宣传阵地[1], 给国家安全和社会稳定造成了严峻威胁。因此, 对暗网的流量进行相关检测分析及研究, 对网络监管者和执法机构及时发现暗网节点及用户违法行为具有重要意义, 有助于维护国家安全、社会稳定和保护个人隐私。

目前, 典型暗网架构主要包含Tor、I2P、ZeroNet、FreeNet等, 其中Tor网络的应用最广泛。暗网实现原理中涉及的技术包括: 洋葱路由技术[2−3]、大蒜路由技术[4]、协议伪装与流量混淆技术(如obfs4协议等)[5]、数据加密技术、匿名身份验证技术、分布式网络技术和P2P技术[6−8]等。其中: 洋葱路由技术是指先将用户

收稿日期:2024 − 10 − 07　　**修回日期:**2024 − 12 − 16　　**网络出版日期:**2024 − 12 − 25

基金项目:国家重点研发计划项目(2023YFB3106600)

作者简介:黄　诚(1987—), 男, 副教授, 博士. 研究方向: 网络空间安全. E-mail: codesec@scu.edu.cn

想发送的内容包装成多层加密的数据包，类似于一个洋葱；再通过一系列称为洋葱路由器的网络节点传输，每经过一个洋葱路由器，就会解密一个加密层，直至到达目的地；最后一层解密后，目的地的用户便能够获取原始数据[2–3]。大蒜路由技术是洋葱路由技术的一种变体[4]；大蒜路由技术中，原始待发送的数据被拆分成多个加密数据包，并通过多条交叉的隧道传输；这种方式使得攻击者或监管者难以进行流量检测分析，因为在大蒜路由技术中，上传和下载的加密数据流通常使用不同的隧道，而且每个方向可能有多条不同隧道。

国内外众多学者针对匿名网络开展了多方位研究。例如：调研Tor使用情况[9]、隐形互联网理论建模[10]、匿名网络的安全性[11]、比特币匿名网络安全[12]、分布式匿名存储系统[13]、匿名通信协议[14]等。以上研究可以在一定程度上解决暗网的去匿名化或者态势感知问题，但是为了更全面、更体系化地开展暗网抑制工作，需要结合暗网的整体架构与治理需要，从暗网特征构建与量化、暗网流量识别、暗网连接预测、暗网溯源4个领域对国内外研究现状及发展趋势进行综述。

针对暗网特征构建领域，研究逐渐从基础共性特征向普适性特征演进。早期的研究更多关注加密流量的基础共性特征，对于暗网流量的差异性特征研究较少且形式化程度不高。例如：Soykan等[15]基于时间特征表征Tor流量，包括源、目标IP地址、端口和流详细信息等29个特征；Wails等[16]提出Tempes度量方法，展示多维特征随时间变化对Tor匿名性的影响；Jansen等[17]构建基于差分隐私的严格形式化特征，量化Tor的匿名性服务；陈子涵等[18]在互联网加密流量研究中，分别从检测、分类和识别3个阶段多粒度、多角度进行系统性归纳。目前，暗网特征构建的研究重点是基于扩展的共性特征结合差异性度量，构建普适性的暗网流量分析模型[19]。

在暗网流量识别领域，研究从表层逐渐深入到深层。早期的识别方法多针对小规模、低占比的明文流量，例如：Ding等[20]提出的暗网威胁监测系统，侧重于暗网内容的采集与深度分析；Wang等[21]提出一种基于深度学习的前域流量识别方法，能够仅根据数据包序列对流量进行分类；Guan等[22]针对加密流量的细粒度识别与快速识别进行研究。随着研究的深入，识别对象逐渐转向大规模的加密流量。例如，Sarkar等[23]提出基于深度神经网络的加密流量识别系统，杜捷等[24]针对Tor的obfs4流量提出基于样本维度权重的SVM算法。目前，如何过滤、筛选并深度解析暗网加密流量中的协议是该领域的主要研究方向[25]。

在暗网网络刻画与绘制领域，研究从静态分析逐渐转向动态分析。早期的研究主要是对暗网用户、隐藏服务等主体进行刻画和分析。随着暗网节点多变性和路径选择随机性的增加，研究逐渐转向分析暗网网络的动态特性，例如：Li[26]和Oh[27]等在流关联中引入多头注意力机制及深度学习技术，能够以较低的资源消耗来刻画暗网流量。然而，如何实现多网络全时变的暗网网络刻画仍是下一步研究的重点[28]。

在暗网感知领域，研究逐渐从被动检测转向主动嗅探。被动检测主要通过流量的搜集和分析来实现感知，例如，Sun等[29]提出的基于流量频域指纹的溯源方法，但存在覆盖率低等问题。主动嗅探则通过部署陷阱节点等手段，主动操控暗网流量以实现感知。相较于被动检测，主动嗅探在内存消耗、实时性和准确率等方面更具优势。然而，由于主动感知容易被检测到并暴露陷阱节点，当前的研究趋势是将主动感知与被动感知结合，例如，Xia等[30]利用被动感知的结果来精准部署陷阱节点，从而降低主动探测的暴露风险，但仍然无法实现较大范围内的规模化部署。

本研究拟建立一套面向暗网抑制的流量差异性与行为共性的协同量化理论框架；并针对真实暗网场景研发一套实时流量检测与溯源示范应用系统，推动暗网治理领域的基础理论发展；取得一批具有国际影响力、能落地应用的研究成果，有效应对暗网通信行为隐蔽难识别、网络拓扑跳变难绘制、陷阱节点部署难伪装等难题，大幅提升暗网抑制治理效率，产生显著的社会和经济效益。

1 关键科学问题

暗网通信呈现复杂、隐蔽等特征，导致暗网网络治理存在诸多难题，通过对暗网通信机理进行深度剖析及对暗网网络治理诸多难题分解归因，将本研究的关键科学问题凝练为：强对抗机制下结构信息缺失的动态时变网络行为刻画与推理问题。该问题的重要性和合理性体现在以下几个方面：

1）暗网的复杂异构特性使得特征表征和度量极为困难。暗网通信协议繁多，通信行为在时域、频域和空域等多个维度表现出多样性。这种复杂异构性导致难以提取普适性的网络特征，从而无法准确识别缺陷节点。暗网通信节点多跳变、流量强加密，更增加了关键要素的抽取难度，阻碍了统一安全量化模型的构建。这些问题都表明了动态时变网络行为刻画的难度。

2）暗网流量的强对抗特性加剧了流量筛选和行为识别的难度。嵌套加密、协议伪装和流量混淆等行

为使得暗网流量难以与正常流量进行区分。暗网网络中的目录服务器与节点隐蔽性极高，在高速网络环境中，暗网流量占比极低，实时分析难度大。这表明在强对抗机制下要精准刻画和推理暗网的行为特征，面临极大的挑战。

3）时空差异特性导致暗网连接预测和拓扑绘制困难。暗网通信协议的复杂性、流量伪装性、链路选择的随机性等固有特性，造成节点信息、拓扑结构和服务信息严重缺失，无法实现局部观测下的全局网络连通性。这凸显了在动态时变条件下理解和推理暗网行为的必要性和复杂性。

4）暗网的动态时变特性使得陷阱节点的部署和追踪溯源变得困难。由于暗网通信链路和路由选择随时间不断变化，在现有节点共识机制下，陷阱节点难以存活且难以优化部署位置，无法实现对暗网网络的有效监控。因此，刻画和推理这种动态时变网络行为，尤其是在缺乏结构信息的情况下，显得尤为重要。

通过以上剖析可以看出，研究在强对抗机制下结构信息缺失的动态时变网络行为的刻画与推理问题，具有重要的理论价值和实际意义。这不仅是破解暗网治理难题的关键所在，也是提升网络安全防护能力的基础。

2　主要研究内容

针对上述关键科学问题，重点从基础理论、应用技术和示范系统3个层面，实现1个框架、3个方法、1个系统共五大研究内容，如图1所示。

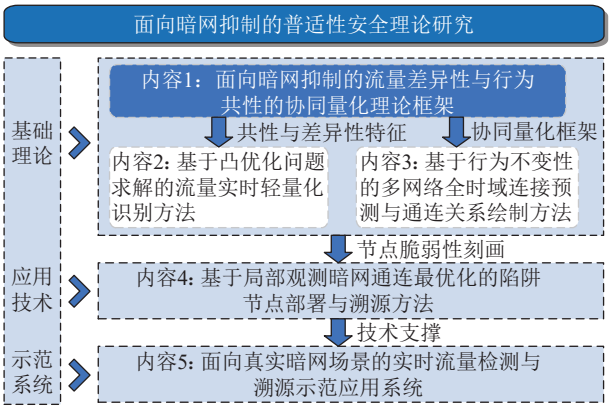

图 1　主要研究内容

Fig. 1　Main research contents

由图1可见：在基础理论层面，主要研究，一是，提出面向暗网抑制的流量差异性与行为共性的协同量化理论框架，解决暗网流量表征难、统一量化难、缺陷节点挖掘难的问题；二是，提出基于凸优化问题求解的流量实时轻量化识别方法，解决暗网流量筛选难、行为识别难的问题；三是，提出基于行为不变性的多网络全时域连接预测与通连关系绘制方法，解决暗网拓扑构建难、连接预测难的问题。在应用技术层面，主要提出基于局部观测暗网通连最优化的陷阱节点部署与溯源方法，解决暗网陷阱部署难、暗网通信追踪溯源难的问题。在示范系统层面，重点研发面向真实暗网场景的实时流量检测与溯源示范应用系统，以验证所提理论和方法的有效性，为后续发展提供方向。

2.1　面向暗网抑制的流量差异性与行为共性的协同量化理论框架

从全局视角研究暗网的复杂结构和动态通信行为，提出暗网普适性特征与安全要素的表征理论；并且，提出分级透视策略下的统一安全量化理论，以实现异构暗网之间的可比较安全度量；同时，建立暗网生态脆弱图及推理理论，结合时间和空间维度分析脆弱性，预测潜在的脆弱节点。其创新性体现在：

1）针对暗网通信行为动态多变、网络结构复杂多样等现象，研究暗网普适性特征与安全要素表征理论。从行为与内容一致性出发，挖掘暗网流量间的共性与差异性，以暗网体系与实现为基础对暗网安全要素进行有效表征。

2）针对暗网实现机制多样导致的统一度量难问题，采取分级透视策略协同异构网络的表里特性，构建动态网络的统一安全量化方法，以实现异构网络的统一安全量化评估。

3）针对暗网通信协议复杂多样导致的缺陷节点挖掘难问题，构建暗网生态脆弱图及推理理论，融合时间域和空间域上暗网生态脆弱图间的差异性和共性，实现对潜在脆弱节点的预测推理。

2.2　基于凸优化问题求解的流量实时轻量化识别方法

针对高速超点环境中暗网流量的强对抗特性及其低占比导致的识别难题，综合时、空、频3域的特征，提出暗网流量的快速抽样和过滤方法；将流量识别问题转化为凸优化问题，利用高斯核函数和多模态优化技术，深入挖掘高维特征空间中的流量差异；同时，从时间、大小、内容等维度刻画暗网数据包，研究数据集的增强方法，以实现对暗网业务的准确分类。其创新性体现在：

1）针对高速超点网络环境中暗网流量占比低的问题，提出基于自身相似性关联的小流抽样方法，通过规则匹配和邻域聚类对海量超点流量数据进行快速划分，从中筛选可疑暗网流量。

2）针对暗网流量对抗性强的问题，提出基于凸优化求解的流量实时轻量化识别方法，借助高斯核函数在高维特征空间中表征数据集，进一步使用凸

优化求解方案建立超平面，对暗网流量进行精准识别。

3）提出基于高斯贝叶斯算法的暗网业务识别方法，借助多维特征表征数据包，通过线性插值生成类间样本，增强训练数据集；采用迭代的训练方式建立基于贝叶斯算法的轻量级机器学习模型，对暗网业务进行准确识别。

2.3 基于行为不变性的多网络全时域连接预测与通连关系绘制方法

针对暗网节点在跨位点、跨时间和跨链路下加密流量差异性导致的连接预测与通连关系绘制难题，提出一种多网络全时域连接预测与通连关系绘制方法，实现异构网络中不同节点的通用连接行为表示；探讨基于真值发现理论和相似性度量的连接预测方法，实现局部观测下的多点全局关联。其创新点体现在：

1）针对异构网络下连接的多样性和复杂性，提出跨位点连接通用表示方法，并提出基于显式特征和隐式特征相结合的连接表示方法，实现异构网络连接的统一表示。

2）针对观测流量规模庞大，匿名网络连接众多导致的连接预测周期长、代价大的难题，提出动态网络环境下无关连接筛选方法，使用分层过滤策略将大量连接聚合成小连接池，以降低负样本连接数，提高连接预测效率。

3）针对动态网络空间下暗网实现机制多样、通连行为局部观测呈现时空差异性、全局通连关系绘制难等问题，提出基于表征学习和相似性度量连接预测方法，来消减连接在跨位点、跨时间、跨链路下的噪声，提升跨位置连接预测准确率，实现局部观测暗网通连的全局关联。

2.4 基于局部观测暗网通连最优化的陷阱节点部署与溯源方法

针对暗网拓扑信息缺失、链路动态组建复杂及新节点生存困难等问题，提出基于图推理的暗网关键节点发现方法；提出基于成本、生存时间、监控视野和脆弱性利用效果的多目标优化陷阱节点部署模型；同时，提出基于部分受控节点的端到端关联溯源方法，实现局部受控条件下的暗网追踪溯源。其创新点体现在：

1）针对暗网节点连接动态变化、通信行为隐蔽难测的特性，从节点的拓扑属性、关联属性、行为属性等信息出发，并将多时段下的网络通连图转化为带属性的有向传播图，提出基于图推理的暗网关键通信节点预测方法。

2）提出基于多目标优化的陷阱节点部署方法，通过对真实暗网环境下陷阱节点存活率较低问题的研究，并对链路节点生存时间、监控视野、带宽能力进行嗅探，完成局部节点优化部署，实现暗网网络全局监控效能最大化。

3）提出部分可控节点条件下的暗网追踪溯源方法，从暗网生态脆弱图挖掘出发，分析利用可控节点完成对目标节点的去匿名化，并暴露目标主机的隐私信息；结合已部署陷阱节点，完成暗网节点间通信连接的动态跟踪，为暗网端到端关联溯源提供重要支撑。

2.5 面向真实暗网场景的实时流量检测与溯源示范应用系统

基于提出的暗网流量差异性与行为共性的协同量化理论框架及关键技术，研发节点探测、流量检测、服务发现等核心模块，形成暗网空间的隐藏资源发现、隐蔽行为识别等暗网监测治理能力，设计可扩展平台接口，最终形成一体化的暗网流量检测与溯源示范应用系统。

3 主要技术路线

以“面向暗网抑制的普适性安全理论研究”为目标，采取“基础理论研究—方法技术应用—系统示范验证”的研究思路，实现对暗网的有效监管和精准治理，总体技术路线如图2所示。

由图2可见：第2节的五大研究内容分别对应5个研究任务，即任务1协同量化理论构建、任务2轻量化暗网流量识别、任务3连接预测与通连关系绘制、任务4陷阱阶段部署与溯源、任务5示范应用系统。在基础理论研究方面：首先，分析和提取暗网的普适性特征和安全要素，对暗网进行精准表征；建立统一的安全量化理论；并结合生态脆弱图构建及推理理论，形成协同量化理论（任务1）。然后，基于暗网普适性特征，提出基于自身相似性关联的小流抽样技术，构建基于凸优化求解的实时轻量化流量识别模型，并进一步建立基于高斯贝叶斯算法的暗网业务识别模型，实现对暗网流量的实时、精准、轻量化识别（任务2）。最后，在统一安全量化框架的基础上，对跨位点连接进行表示，在动态网络中过滤无关连接后，进行多网络全时域连接预测并绘制通连关系（任务3）。在方法技术应用方面，根据绘制的通连关系，预测暗网中的关键节点，并通过多目标优化进行陷阱节点的部署，从而在受控环境下推理暗网节点的脆弱性并进行溯源，完成任务4。在系统示范验证方面，以高活跃度暗网网络为具体研究对象，设计并实现示范应用系统，对所提出的理论方法和核心技术进行验证和应用落地，从而完成任务5。

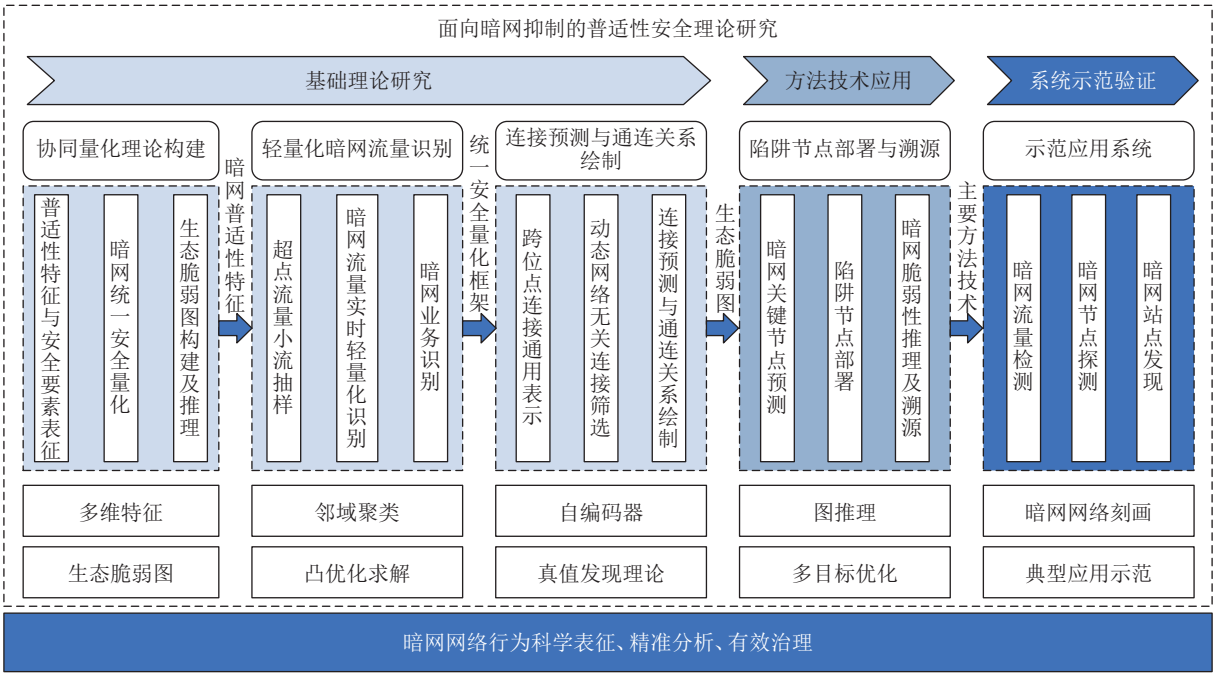

图 2　总体技术路线

Fig. 2　Overall technical roadmap

3.1　任务1协同量化理论构建的技术路线

协同量化理论构建的任务以异构暗网实现机制与专家经验为导向，主要构建暗网流量与行为的协同量化理论框架，详细的技术路线如图3所示。首先，研究全局视角下的暗网网络结构，提出暗网普适性特征与安全要素表征理论；在此基础上，分析异构暗网实现无关的外部特性及内部安全要素，构建分级透视策略下的统一安全量化理论；进一步在时域和空域上挖掘不同暗网生态间的差异性和共性，提出暗网生态脆弱图构建及推理理论。该任务通过表征暗网普适性特征及安全要素，实现异构暗网间可比较度量，并提出生态脆弱图构建及推理方法，为后续研究提供理论支持。

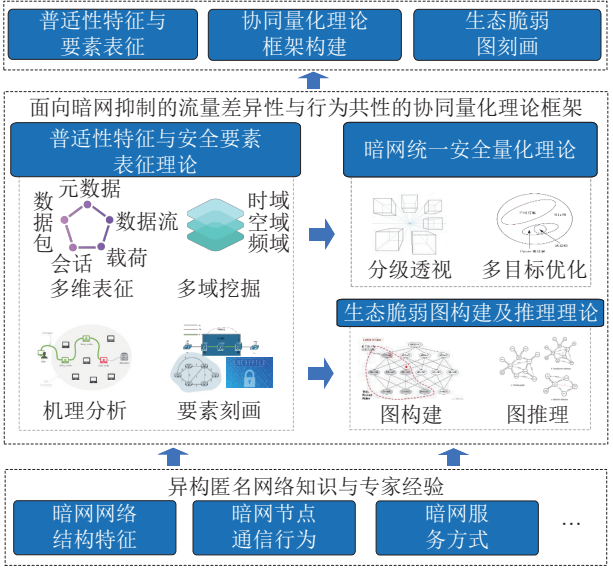

图 3　任务1协同量化理论构建的技术路线

Fig. 3　Technical route of Task One for synergetic quantization theory

3.2　任务2轻量化暗网流量识别的技术路线

针对高速超点网络环境中暗网流量具有强对抗特性且占比极低所导致的识别难问题，提出一系列方法实现对暗网流量的高效精准识别，其技术路线如图4所示。首先，鉴于对全网络、全时域、全流量进行实时分析的资源消耗大、效率低等问题，提出基于自身相似性关联的小流抽样方法，该方法通过结合暗网流量与正常流量的典型差异特性及暗网流量的实现机理，制定筛选规则以快速过滤正常流量。然后，利用信息熵、随机性度量、收发频率等统计特征对数据包进行刻画，并构建以典型暗网流量样本为引导的邻域聚类模型，基于特征相似性对可疑暗网流量进行实时抽样提取。

在此基础上，考虑到暗网流量的高匿名性和强隐蔽性使得现有加密流量检测方法难以满足高速超点网络中对暗网流量的精准识别需求，提出基于凸优化求解的流量实时轻量化识别方法。该方法利用优化的高斯核函数将数据流的统计属性、数据包内容特性和协议指纹等多模态特征映射到高维特征空间，并通过凸优化求解确定决策边界方程，建立超平面，从而实现暗网流量的精确识别。

此外，针对暗网流量通过多层代理、内容加密和

噪声引入等手段提高匿名性和隐蔽性，导致其业务类型难以确定的情况，提出基于高斯贝叶斯算法的暗网业务识别方法。通过时间、大小和内容混乱程度等维度特征对数据包进行描述，并使用契比雪夫距离确定每个流量样本的最近邻，从而基于线性插值生成类间样本，增强不平衡流量之间的分布边界。最终，通过迭代训练基于贝叶斯算法的轻量级机器学习模型，实现对暗网业务类型的精准识别。

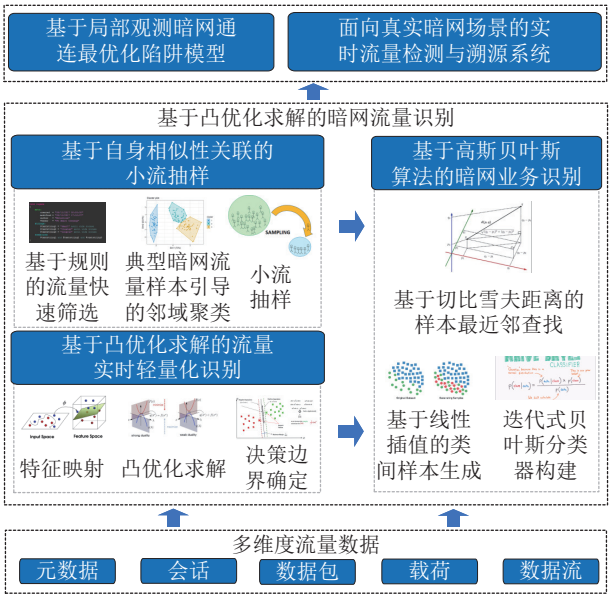

图 4 任务2轻量化暗网流量识别的技术路线

Fig. 4 Technical route of Task Two lightweight detecting method for darknet traffic

3.3 任务3连接预测与通连关系绘制的技术路线

针对异构网络下暗网连接表示多样，连接规模庞大，暗网连接在跨位点、跨时间、跨链路下呈现出连接差异性导致通连关系绘制困难的难题，提出一系列方法来实现对多网络全时域通信连接的预测与通连关系绘制，其技术路线如图5所示。

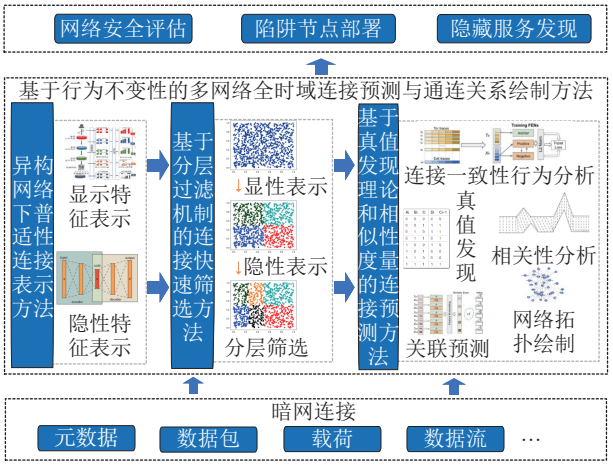

图 5 任务3连接预测与通连关系绘制的技术路线

Fig. 5 Technical route of Task Three link prediction and connectivity mapping

首先，分析与实现机制无关的暗网连接一致性的显性及隐性属性，提出异构网络下普适性连接表示方法。由于多网络下网络结构不一呈现出连接的复杂性和多样性，为了实现多网络下连接的通用表示，将传输层协议、数据包长度和方向、时延序列、流量突发包序列等公有信息作为连接显性特征表示；构建基于深度学习的多网络连接通用特征提取模型，通过连接切片、报文填充等方式，将连接表示为同一长度，并在自动编码器的帮助下，采用无监督学习提取连接的隐性特征表示，通过连接自身信息强化模型学习隐性特征表示的提取方法。将连接显性特征表示和隐性特征表示共同作为连接表示，为下一步的无关连接筛选和连接预测奠定基础。

其次，分析通用表示下动态网络连接的行为一致性和特异性特征，提出基于分层过滤机制的连接快速筛选方法。针对同一时间捕获的连接数量规模庞大带来的连接预测代价高、周期长等问题，采用分层过滤策略对无关连接进行筛选，在显性特征表示的帮助下通过传输协议、连接构建时间、连接持续时间、传输报文总大小等信息对连接进行初步聚类，构建显性特征连接池，实现无关连接过滤和相关连接聚类；计算同一显性特征连接池中不同连接隐性特征表示的信息熵，基于连接中包含的信息量相似性对连接池进行二次过滤，进一步降低连接池中连接数量，为后续连接快速预测奠定基础。

最后，分析同一连接在流入、流经、流出暗网通道全过程中不同位置表现出的行为一致性和内容不变性，提出基于真值发现理论和相似性度量的连接预测方法。针对动态网络空间下暗网实现机制多样、通连行为局部观测呈现时空差异性、全局通连关系绘制难等问题，在通用连接表示中提取连接的时间特性和内容特性，通过表征学习消减连接在捕获位置变化、流量形态变化、链路协议变化、流量捕获时间变化而产生的无关噪声，抽取不同连接中的一致性行为；通过真值发现理论推断不同连接中的内容不变性和行为一致性，采用相似性度量推断节点带宽波动对连接的影响，实现多跳暗网通连行为间的关系确认，从而实现高效、快速的多网络全时域连接预测和局部观测暗网通连的多点全局关联；对来自同一链路的不同连接之间的暗网节点的通连关系，绘制网络关系拓扑，构建全时域连通图。

3.4 任务4陷阱节点部署与溯源的技术路线

陷阱节点部署与溯源任务的研究目标是通过陷阱节点的部署和溯源技术，实现对暗网的深入分析和有效监控，其技术路线如图6所示。首先，对于暗网关键节点的预测，具体过程为：基于图推理技术对暗

网路由节点的通连关系进行分析；由于暗网中的路由节点在系统接入、流量加密和数据转发中发挥着重要作用，是整个匿名通信网络的核心，因此在暗网复杂的关键节点选择机制下，可以从通连图的拓扑属性、关联属性和行为属性等多个维度出发，对不同时期、不同通连关系的关键节点进行同源性分析，提取关键节点的共性属性，构建多维细粒度的属性模型；考虑到暗网的动态时变特性，可以在带有属性的网络通连图中运用图推理技术，进行暗网关键节点的预测。

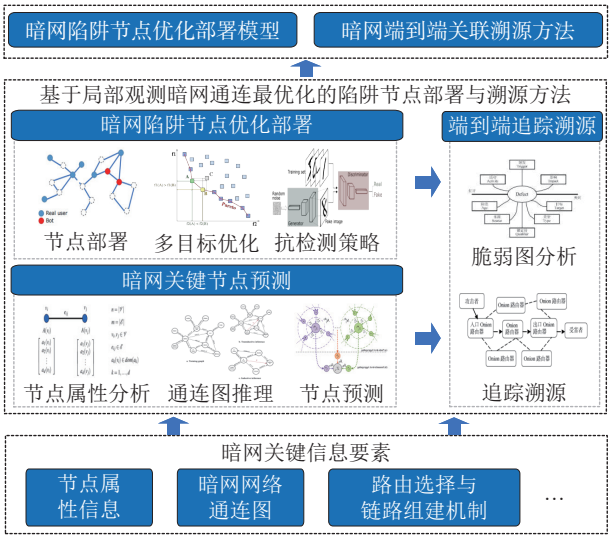

图 6　任务4陷阱阶段部署与溯源的技术路线

Fig. 6　Technical route of Task Four trap deployment and tracking

然后，在陷阱节点的部署上，提出基于多目标优化的方法，以应对暗网链路的高时变性和节点共识机制带来的部署难题，具体过程为：通过嗅探节点的生存时间、监控视野和带宽能力等信息，分析节点部署的成本，构建局部网络下的多目标优化评估模型；在已知通连图中选取局部最优位置来部署陷阱节点，以最大化局部暗网网络数据监控效能；考虑到陷阱节点在网络中的存活率较低，利用专家知识与多维度隐藏策略，结合随机化算法隐藏数据包结构特征，以提升其对多种检测攻击的抵抗效果，从而实现高存活率和高效监听的陷阱节点部署。

此外，为解决强认知对抗下的暗网通信关联追踪与溯源难题，提出基于部分受控节点条件下的端到端追踪溯源方法，具体过程为：从暗网协议设计与实现机理的脆弱性、节点部署环境的差异性、组件及服务漏洞等多个方面入手，构建生态脆弱图，分析节点间的脆弱性依赖关系，从而挖掘节点的脆弱性；结合实时监测下的多时段通连图，动态追踪节点间的交互关系，应用关系推理机制发现可疑通信行为；利用可控出入口节点与陷阱节点，实现对暗网通信的去匿名化，达成在部分受控节点条件下的暗网端到端关联追踪与溯源目标。

3.5　任务5示范应用系统的技术路线

基于上述研究，以暗网抑制为核心，构建暗网实时流量检测与溯源示范应用系统，其技术路线如图7所示。具体工作为：设计系统硬件架构，保证系统的性能、可靠性和稳定性；部署系统数据存储，支撑数据持久化，满足数据访问、检索、分析等需求；获取暗网多源异构信息，全方位多维度汇聚整合暗网信息，为暗网抑制提供数据支持；研发暗网网络的业务应用，包括暗网流量检测、暗网节点分析、站点发现。

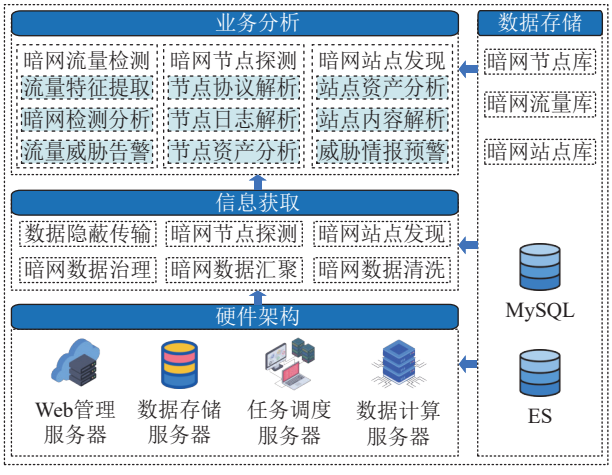

图 7　任务5暗网流量检测与溯源系统的技术路线

Fig. 7　Technical route of Task Five darknet traffic detection and tracing system

由图7可见：研发的流量检测与溯源验证系统主要由硬件架构层、数据存储层、信息获取层、业务分析层组成；该系统通过硬件架构层提供基础支撑，通过数据存储层确保数据的持久化和高效访问，通过信息获取层提供多维度的数据采集能力，通过业务分析层实现深度的数据分析和溯源功能。

4　结　论

本研究重点从基础理论、应用技术和示范系统3个层面，实现1个框架、3个方法、1个系统。上述5方面研究内容具体为：一是，提出面向暗网抑制的流量差异性与行为共性的协同量化理论框架，实现对时空差异化条件下异构暗网的一致性安全量化评估；该框架采用了多维度数据分析、机器学习和神经网络技术，能够有效识别和量化不同类型的暗网流量。二是，提出基于凸优化问题求解的流量实时轻量化识别方法，能突破高速网络空间中轻量化暗网流量实时识别技术瓶颈，显著提高检测量级和准确性，能应对传统方法在骨干网络环境下检测延迟的问题。三

是，提出基于行为不变性的多网络全时域连接预测与通连关系绘制方法，利用图论和动态系统理论，能突破多网络全时域连接预测的技术难题，为暗网行为分析提供新的视角和工具。四是，在暗网通连最优化的陷阱节点部署方面，提出基于局部观测暗网通连最优化的陷阱节点部署方法，有效提高关键节点的生存率，突破暗网端到端反侦测溯源机制，增强对暗网活动的监测能力。五是，研发面向真实暗网场景的实时流量检测与溯源示范应用系统，并落地应用。研究将为相关执法机关提供强有力的技术支持，助力打击暗网犯罪，提升网络治理能力和公共安全保障。

参考文献：

[1] Weimann G.Terrorist migration to the darknet[J].Perspectives on Terrorism,2016,10(3):40–44.

[2] Dingledine R,Mathewson N,Syverson P.Tor:The second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium.San Diego:USENIX Association,2004:303–320.

[3] Goldschlag D,Reed M,Syverson P.Onion routing[J].Communications of the ACM,1999,42(2):39–41.

[4] Ali A,Khan M,Saddique M,et al.TOR vs I2P:A comparative study[C]//Proceedings of the 2016 IEEE International Conference on Industrial Technology(ICIT).Taipei:IEEE,2016:1748–1751.

[5] Angel Y,Winter P.obfs4(the obfourscator).[EB/OL].(2019–01–15)[2024–12–15].https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/lyrebird/-/blob/HEAD/doc/obfs4-spec.txt.

[6] Liu Shaoteng,Zhang Yuechen,Li Wenbo,et al.Video-P2P:Video editing with cross-attention control[C]//Proceedings of the 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR).Seattle:IEEE,2024:8599–8608.

[7] Ma Zhanyou,Yan Miao,Wang Rong,et al.Performance analysis of P2P network content delivery based on queueing model[J].Cluster Computing,2024,27(3):2901–2915.

[8] Kiffer L,Rajaraman R.Stability of P2P networks under greedy peering(full version)[EB/OL].(2024–02–22)[2024–12–15].https://arxiv.org/abs/2402.14666v1.

[9] Chen Zhicong,Jardine E,Liu Xiaofan,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.

[10] Abdo J B,Hossain L.Modeling the invisible internet[M]//Complex Networks & Their Applications Ⅻ.Cham:Springer,2024:359–370.

[11] Chao Daichong,Xu Dawei,Gao Feng,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.

[12] Sakib N,Wuthier S,Zhang Kelei,et al.From slow propagation to partition:Analyzing Bitcoin over anonymous routing[C]//Proceedings of the 2024 IEEE International Conference on Blockchain and Cryptocurrency(ICBC).Dublin:IEEE,2024:377–385.

[13] Clarke I,Sandberg O,Wiley B,et al.Freenet:A distributed anonymous information storage and retrieval system[M]//Anonymity 2000,LNCS 2009.Berlin:Springer,2001:46–66.

[14] Wang Liangmin,Ni Xiaoling,Zhao Hui.Survey of network-layer anonymous communication protocols[J].Chinese Journal of Network and Information Security,2020,6(1):11–26.[王良民,倪晓铃,赵蕙.网络层匿名通信协议综述[J].网络与信息安全学报,2020,6(1):11–26.]

[15] Soykan M,Bölük P S.Tor network detection by using machine learning and artificial neural network[C]//Proceedings of the 2021 International Symposium on Networks,Computers and Communications(ISNCC).Dubai:IEEE,2021:1–4.

[16] Wails R,Sun Yixin,Johnson A,et al.Tempest:Temporal dynamics in anonymity systems[J].Proceedings on Privacy Enhancing Technologies,2018,2018(3):22–42.

[17] Jansen R,Johnson A.Safely measuring Tor[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.New York:ACM,2016:1553–1567.

[18] Chen Zihan,Cheng Guang,Xu Ziheng,et al.A survey on Internet encrypted traffic detection,classification and identification[J].Chinese Journal of Computers,2023,46(5):1060–1085.[陈子涵,程光,徐子恒,等.互联网加密流量检测、分类与识别研究综述[J].计算机学报,2023,46(5):1060–1085.]

[19] Sharma M,Kumar N,Singh V P,et al.Hybrid intelligent feature selector framework for darknet traffic classification[J].Multimedia Tools and Applications,2024,83(14):40337–40360.

[20] Ding Jianwei,Chen Zhouguo.Watermark based Tor cross-domain tracking system for Tor network traceback[M]//Security and Privacy in New Computing Environments .Cham:Springer,2021:54–73.

[21] Wang Meiqi,Li Yanzeng,Wang Xuebin,et al.2ch-TCN:A website fingerprinting attack over Tor using 2-channel temporal convolutional networks[C]//Proceedings of the 2020 IEEE Symposium on Computers and Communications(ISCC).Rennes:IEEE,2020:1–7.

[22] Guan Zhong,Xiong Gang,Li Zhen,et al.ResTor:A pre-processing model for removing the noise pattern in flow correl-

ation[C]//Proceedings of the 2020 IEEE Symposium on Computers and Communications(ISCC).Rennes:IEEE,2020:1–6.

[23] Sarkar D,Vinod P,Yerima S Y.Detection of Tor traffic using deep learning[C]//Proceedings of the 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications(AICCSA).Antalya:IEEE,2020:1–8.

[24] Du Jie,He Yongzhong,Du Ye.Improved method of Tor network flow watermarks based on IPD interval[J].Chinese Journal of Network and Information Security,2019,5(4):91–98.[杜捷,何永忠,杜晔.基于改进IPD质心的Tor网络流水印检测方法[J].网络与信息安全学报,2019,5(4):91–98.]

[25] Buitrago López A,Pastor–Galindo J,Gómez Mármol F.Updated exploration of the Tor network:Advertising,availability and protocols of onion services[J].Wireless Networks,2024,30(9):7527–7541.

[26] Li Ji,Gu Chunxiang,Zhang Xieli,et al.AttCorr:A novel deep learning model for flow correlation attacks on Tor[C]//Proceedings of the 2021 IEEE International Conference on Consumer Electronics and Computer Engineering(ICCECE).Guangzhou:IEEE,2021:427–430.

[27] Oh S E,Yang Taiji,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).San Francisco:IEEE,2022:1915–1932.

[28] dos Reis E F,Teytelboym A,ElBahrawy A,et al.Identifying key players in dark web marketplaces through Bitcoin transaction networks[J].Scientific Reports,2024,14:2385.

[29] Sun Yuchen,Luo Xiangyang,Wang Han,et al.A method for identifying Tor users visiting websites based on frequency domain fingerprinting of network traffic[J].Security and Communication Networks,2022,2022:3306098.

[30] Xia Pengcheng,Yu Zhou,Wang Kailong,et al.The devil behind the mirror:Tracking the campaigns of cryptocurrency abuses on the dark web[EB/OL].(2024–04–07)[2024–12–15].https://arxiv.org/abs/2401.04662v2.

黄诚，博士，四川大学副教授、博士生导师，院长助理，IEEE/CCF高级会员，国家重点研发计划青年科学家项目负责人，四川省学术和技术带头人后备人选，美国加州大学圣塔芭芭拉分校联合培养博士。长期致力于网络空间安全方面的科学研究和人才培养，目前主要从事网络攻防、攻击检测与溯源、情报分析、网络公害治理、供应链安全等方向的研究工作。先后主持国家自然科学基金青年/面上、国家科技部重点研发青年科学家、四川省科技厅重点研发等国家及省部级科研项目10余项；在USENIX Security、ASE、RAID 等CCF A/B会议及期刊上累计发表学术论文50余篇，授权发明专利15项；获省部级科技进步二等奖1项，学会科技进步一等奖1项；带领学生在全国大学生信息安全作品赛/技能赛、计算机设计大赛等赛事中荣获一等奖9项。

Towards a Universal Security Framework for Darknet Suppression: Conceptual Foundations and Future Prospects

HUANG Cheng[1], *DING Jianwei*[2], *ZHAO Jiapeng*[3], *CHEN Zhouguo*[2], *SHI Jinqiao*[3]

(1.School of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China;
2.The 30th Research Institute of China Electronics Technology Group Corporation, Chengdu 610093, China;
3.School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract:

Significance In recent years, anonymous networks and their underlying darknet have become vital tools for transmitting sensitive information, conducting cyberattacks, and engaging in cybercrime due to their strong concealment, high anonymity, and resistance to traceability. These characteristics pose serious threats to national security and social stability. This project researches a universal security theory for darknet suppression to address the challenges of darknet governance, such as difficulties in identifying concealed communication behaviors, mapping dynamic network topologies, and disguising trap node deployments.

Progress The main content includes: 1) Establishing a collaborative quantitative theoretical framework focused on darknet traffic differences and behavioral commonalities. This involves proposing heterogeneous darknet universal characteristics, differentiated element representations, unified security quantification, and ecological vulnerability graph construction theories. These approaches address the challenge of quantifying darknet suppressibility, which remains complicated by diverse network structures and dynamic communication behaviors. 2) Proposing a real-time lightweight traffic detection method based on solving convex optimization problems. This involves constructing a small flow sampling model based on self-similarity associations and a darknet traffic identification and service classification model using Gaussian kernel functions and multimodal optimization. This method enables precise, real-time identification and classification of darknet traffic. 3) Introducing a multi-network full-time domain connection prediction and relationship mapping method based on behavioral invariance. This approach represents cross-

point connections and filters out irrelevant connections in dynamic networks to predict multi-network full-time domain connections and map relationships, achieving multi-point global associations of darknet connections under local observation conditions. 4) Proposing a trap node deployment and tracing optimization method for darknet connections based on local observations, enabling tracking and tracing of the darknet under conditions of partially controllable nodes. 5) Developing a real-time traffic detection and tracing demonstration system for real-world darknet scenarios, which law enforcement agencies implement to achieve precise governance of darknet-related crimes.

Conclusions and Prospects This project significantly contributes to darknet governance by developing a quantitative framework for analyzing and managing darknet traffic. The proposed real-time lightweight traffic detection method enhances law enforcement's ability to identify and classify darknet activities. In addition, these methods for predicting multi-network connections and optimizing trap node deployment improve tracking capabilities in complex environments. Future work focuses on refining these methodologies and exploring additional dimensions of darknet behavior to strengthen efforts in combating illicit online activities, generating meaningful social and economic benefits.

Key words: darknet governance; traffic detection; behavior recognition; security quantification; trap node deployment

（编辑　赵　婧）

引用格式: Huang Cheng,Ding Jianwei,Zhao Jiapeng,et al.Towards a universal security framework for darknet suppression: Conceptual foundations and future prospects[J].Advanced Engineering Sciences,2025,57(1):1–10.[黄诚,丁建伟,赵佳鹏,等.面向暗网抑制的普适性安全理论研究构想和成果展望[J].工程科学与技术,2025,57(1):1–10.]