网络安全测量研究综述

张宇昊
1024041137
zhangand76@outlook.com

摘要—本报告通过调研 2020 年到 2025 年间发表在 IEEE S&P，USENIX Security，NDSS，CCS 与 IMC 上与网络安全测量有关的论文，使用系统性文献回顾的方法较为全面系统的梳理了近年来网络安全测量领域的研究进展。调研所选择的会议范围被公认为代表了该领域的最高研究水平和前沿方向。论文的筛选主要基于 DBLP 计算机科学文献库以及各会议官方网站公布的论文列表和程序册。本报告旨在通过对这些权威来源的系统性分析，提炼出该领域的核心问题、关键发现和未来趋势。

***Index Terms*—Network security measurement, cyber security measurement, security metrics, security assessment, network security evaluation**

I. 导论

网络安全并非一个纯粹的理论概念，而是一个在现实世界复杂系统中体现出的经验性属性。它要求我们不仅要设计理论上安全的协议和系统，更要理解这些设计在实际部署中的表现。在这一背景下，测量成为连接理论与现实的桥梁，是评估网络空间安全态势的核心科学方法。通过测量，研究人员能够量化威胁的普遍性、评估防御措施的有效性、揭示全球规模系统中各组件之间复杂的相互作用，并为安全策略的制定提供数据驱动的依据。

本报告中，“网络安全测量”一词涵盖了广泛的研究活动。它不仅局限于对网络协议（如 TCP/IP、DNS、BGP）本身安全性的量化分析，还延伸至对利用网络进行活动的恶意生态系统的测量，例如僵尸网络、钓鱼攻击和网络审查。此外，它还包括对影响网络安全的用户行为、新兴技术（如 5G、物联网、QUIC 协议）的安全部署现状，以及构成现代互联网的平台和基础设施（如云服务、内容分发网络）的安全性的实证研究。这些测量活动共同构成了一幅动态的、数据驱动的网络安全全景图。

为全面系统地梳理 2020 年至 2025 年间网络安全测量领域的研究进展，本报告采用系统性文献回顾的方法。通过使用 IEEE 数据库、DBLP 计算机科学文献库与 Engineer Ingvillage 文献搜索引擎调研了发表在 IEEE S&P，USENIX Security，NDSS，CCS 与 IMC 上与网络安全测量有关的论文。

本报告分为两大部分。第一部分（第 2 至 3 章）旨在提供一个网络安全测量研究的全景式概览。第 2 章将提出一个该领域研究主题的分类法，并通过一个详尽的表格来系统化地展示各个子领域的核心问题、代表性工作和主要研究方法。第 3 章将讨论贯穿于这些研究中的一些共性挑战和方法论趋势。

第二部分（第 4 至 8 章）将聚焦于分类法中的一个特定方向——“互联网基础设施安全测量”——进行深入的综述分析。该部分将详细剖析 DNS 和 BGP 安全测量的关键问题，并以具体的、具有里程碑意义的论文作为案例，深入探讨其研究方法、核心发现及其对整个领域的深远影响。最后，第 8 章将对全文进行总结，并展望该领域未来的研究方向。

II. 现代网络安全测量分类

通过对 2020 年至 2025 年间五大顶级会议发表论文的系统性梳理，我们将网络安全测量的研究主题划分为七个主要类别。这些类别涵盖了从核心基础设施到新兴应用，从技术漏洞到人类行为的广泛领域。下表（表 1）提供了一个简要的分类概览，旨在为研究人员提供一个清晰的研究地图，揭示各个子领域的关键问题、代表性工作。

这些会议被公认为代表了该领域的最高研究水平和前沿方向。本报告旨在通过对这些权威来源的系统性分析，提炼出该领域的核心问题、关键发现和未来趋势。

表 I
2020-2025 年五大顶会网络安全测量研究主要方向分布

研究方向	S&P	USENIX	NDSS	CCS	IMC
网络基础设施与路由安全	BGP 事件分析 路由安全部署	RPKI 生态系统 RPKI 部署审计	IPv6 安全测量 DNS 滥用检测	DNS 缓存投毒 BGP 劫持溯源	DDoS 攻击溯源 RPKI 验证分析
Web 与平台安全	Web PKI 生态 浏览器扩展安全	广告网络审计 隐私策略合规性	Web 跟踪技术 TLS 配置缺陷	第三方信任链 Web 服务滥用	UID 走私跟踪 TLS 1.3 部署
恶意软件与欺诈生态系统	恶意软件供应链 恶意基础设施分析	骚扰电话内容分析 加密货币欺诈	加密恶意流量检测 DNS 域名生成算法	安卓恶意软件演化 钓鱼工具包分析	恶意软件域名生态 基础设施复用分析
网络审查与干扰	长期审查平台 (ICLab) 规避工具指纹识别	审查事件关联性分析 移动端审查测量	审查过滤设备部署 DoH/ESNI 审查	审查平台 流量操纵检测	HTTPS 拦截测量 协议混淆有效性
物联网与网络物理系统	传感器安全形式化 固件供应链安全	智能家居滥用 IoT 设备指纹	车载网络安全 无人机安全	IoT 僵尸网络演化 工业控制系统测量	IoT 背景流量分析 消费级 IoT 安全审计
隐私与匿名	差分隐私应用 匿名网络安全	Apple 隐私标签合规性 敏感信息泄露测量	GDPR 合规性测量 移动端 App 隐私泄露	Tor 网络去匿名化 隐私增强技术有效性	加密 DNS 隐私分析 流量分析攻击

III. 网络安全测量的共性挑战

A. 核心互联网基础设施安全测量

互联网的稳定运行依赖于其核心基础设施，主要是域名系统（DNS）和边界网关协议（BGP）。针对这些基础设施的安全测量是网络安全研究的基石。

- DNS 安全测量：研究的焦点主要集中在两个方面：攻击测量和隐私测量。在攻击测量方面，DNS 放大反射拒绝服务（DRDoS）攻击仍然是主要威胁。研究工作不再仅仅是统计攻击数量，而是深入分析整个攻击生态系统。例如，《The Far Side of DNS Amplification》（IMC '21）通过结合 IXP（互联网交换点）和蜜罐数据，揭示了攻击流量的不同视角，并对攻击者行为进行了画像。而《TsuKing》（CCS '23）则通过主动测量发现了利用 DNS 解析器之间不一致性来指数级放大攻击流量的新型攻击方法。在隐私测量方面，随着 DNS-over-HTTPS（DoH）和 DNS-over-TLS（DoT）等加密 DNS 协议的兴起，研究人员开始测量其在全球的部署情况、对审查的抵抗能力以及可能存在的新的隐私泄露风险。
- BGP 安全测量：BGP 的安全性直接关系到互联网路由的稳定。相关测量工作主要围绕路由劫持事件的检测和防御机制的部署有效性展开。特别是，资源公钥基础设施（RPKI）作为防御 BGP 劫持的主要手段，其部署率、配置正确性以及对路由生态系统的实际影响，是研究人员持续关注的重点。研究人员通过分析全球路由数据，量化 MANRS（Mutually Agreed Norms for Routing Security）等行业倡议的采纳情况及其效果。

B. 网络审查与干扰测量

理解和对抗网络审查是网络安全测量的一个重要社会议题。近年来的研究趋势是从一次性的、针对特定国家或事件的研究，转向建立全球性的、可持续的长期监测平台。

- 审查测量平台：这方面的标志性工作是《ICLab: A Global, Longitudinal Internet Censorship Measurement Platform》(S&P '20)。该研究利用全球分布的商业 VPN 作为测量探针，实现了对 DNS 操纵、TCP 数据包注入等多种审查技术的持续监测。这种方法在覆盖广度和测量深度之间取得了新的平衡，使得研究人员能够捕捉到与政治事件相关的审查策略动态变化。
- 审查与反审查的攻防测量：研究也深入到审查方与规避方之间的技术对抗。例如，IMC '20 上的论文测量了审查系统如何通过主动探测等方式识别并封锁 Shadowsocks 等流行的规避工具，以及在国家层面进行的大规模 HTTPS 流量劫持事件。这些工作揭示了审查技术正变得越来越复杂和具有针对性。

C. 在线滥用生态系统测量

现代网络安全测量的一个显著趋势是，研究视角从分析单个攻击事件转向对整个恶意生态系统的综合测量。研究人员不仅关心“发生了什么”，更关心“谁在做”、“如何做”、“为何做”以及“效果如何”。

- 电话诈骗与网络欺诈：《Diving into Robocall Content with SnorCall》（USENIX '23）是一个典型的例子。该工作不再局限于分析通话元数据（如主叫号码），而是利用半监督机器学习框架，对超过 23 万个诈骗电话的录音转录文本进行内容分析，从而能够大规模地识别诈骗主题、被冒充的机构、诈骗金额以及共享的后端基础设施。类似地，其他研究也对社交媒体上的评论诈骗、赠品骗局等进行了深入的生态系统级别的测量。
- 平台安全策略审计：这是一个新兴且重要的测量方向，即通过外部测量来审计大型在线平台自身安全与隐私政策的执行情况。《An Audit of Facebook's Political Ad Policy Enforcement》（USENIX '22）通过大规模分析 Facebook 的广告库，量化了其政治广告识别系统的准确率、漏报率和误报率，揭示了平台在政策执行层面存在的系统性问题和国家间的差异。

D. 隐私泄露与用户追踪测量

随着数据驱动的商业模式普及，用户隐私保护成为焦点。测量研究致力于揭示和量化无处不在的用户追踪和数据泄露行为。

- 网络追踪技术测量：研究人员持续关注网络追踪技术的发展。例如，《Measuring UID Smuggling in the Wild》（IMC '22）揭示了广告网络如何通过重定向“走私”用户唯一标识符（UID），从而实现跨站追踪。其他工作则专注于测量浏览器指纹的动态变化及其对抗措施，以及搜索引擎广告系统带来的隐私风险。
- 移动与物联网隐私：在移动端，研究人员通过大规模应用分析，揭示了 Android 生态系统中普遍存在的个人信息收集行为，以及移动即时通讯工具中滥用联系人发现功能导致的隐私问题。在物联网（IoT）领域，研究通过对智能家居设备的网络流量进行建模和分析，测量其行为模式，以发现潜在的隐私泄露和安全威胁。

E. 物理与侧信道威胁测量

这类研究关注的是跨越数字与物理边界的攻击。研究重点不仅在于发现新的攻击向量，更在于系统化地理解和量化这类威胁。

- 模拟传感器安全：《SoK: A Minimalist Approach to Formalizing Analog Sensor Security》（S&P '20）是一篇里程碑式的系统化知识（SoK）论文。它系统地梳理了过去利用声波、射频、激光等物理手段对模拟传感器进行干扰和控制的攻击，并提出了一个基于传递函数的简约安全模型。这项工作推动了该领域从“发现-修复”的被动模式，向量“安全设计”的主动模式转变。
- 实用化侧信道攻击测量：研究人员不断探索新的侧信道，并测量其在真实场景中的可行性。例如，有研究证明了通过分析视频会议的画面推断用户键盘输入是可行的，以及利用 Wi-Fi 信号进行键盘窃听。这些工作将理论上的侧信道攻击向量，转化为了可测量的、具有现实威胁的攻击。

F. 新兴领域安全测量

当新技术（如 5G、QUIC）和新应用场景（如智能电网、自动驾驶）出现时，安全测量研究扮演着“先遣队”的角色，旨在第一时间评估其在真实世界中的安全状况。

- QUIC 协议安全：《QUICsand: Quantifying QUIC Reconnaissance Scans and DoS Flooding Events》（IMC '21）是该领域的开创性工作。它利用网络望远镜数据，首次对新兴的 QUIC 协议的互联网背景流量进行了测量，发现尽管 QUIC 在设计上考虑了抗放大攻击，但其握手过程仍易受到资源耗尽型攻击，并且这种攻击已经在野外被利用。
- 5G 与蜂窝网络：随着 5G 的部署，研究人员开始构建用于 5G 网络安全实验的虚拟测试床，测量现有蜂窝网络基础设施面对野火等物理威胁时的脆弱性，以及分析 4G 网络中存在的身份假冒攻击。
- 物联网与网络物理系统（CPS）：测量范围已扩展到关键基础设施。例如，研究人员对物联网消息传递协议进行了系统的安全评估，对智能农业系统进行安全测量，并对智能电网和汽车网络等网络物理系统的安全风险进行了初步的实证研究。

G. 测量方法论创新

除了对具体安全问题的测量，研究领域本身的方法论也在不断创新。这些新方法、新工具的出现，使得过去难以测量或无法测量的问题变得可能。

- 利用侧信道进行测量：这是近年最引人注目的方法论创新之一。《Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels》（NDSS '23）是其中的杰出代表。该工作巧妙地将 IPv6 协议中用于网络稳定的 ICMP 速率限制机制，转化为一个信息侧信道，从而能够远程推断网络属性，相当于在全球范围内获得了上百万个无需控制的“虚拟探针”。
- 机器学习辅助测量：面对海量的非结构化数据（如音频、文本、图像），手动分析已不再可行。机器学习，特别是半监督学习框架（如 Snorkel），被越来越多地用于自动化和规模化数据分析。例如，SnorCall 利用该技术对海量电话录音进行内容分类，极大地提高了分析效率和规模。
- 测试床与数据集贡献：社区也越来越重视可复现研究。许多工作致力于构建并开放大规模的测试床和数据集，例如用于研究智能农业安全的测试平台或用于分析应用网络流量的数据集，这些都极大地推动了相关领域的研究。

IV. 基础设施安全测量概要

互联网的核心基础设施，特别是域名系统（DNS）和边界网关协议（BGP），是整个数字世界的基石。DNS 如同互联网的电话簿，负责将人类可读的域名翻译成机器可读的 IP 地址；而 BGP 则像全球的邮政系统，决定了数据包在成千上万个自治系统（AS）之间的传输路径。这两个系统的安全性、稳定性和可靠性，直接决定了其上运行的所有应用程序（从网页浏览到金融交易）的可用性和安全性。然而，这些协议在设计之初并未充分考虑安全问题，导致它们在现实世界中面临着持续的威胁。因此，对这些核心基础设施进行持续、精确的测量，以理解其安全规范与混乱的部署现实之间的差距，对于维护整个互联网的健康至关重要。以下将深入探讨 2020-2025 年间在 DNS 和 BGP 安全测量领域的关键研究进展。

V. 域名系统 (DNS) 安全测量

DNS 作为互联网的关键基础设施，其安全测量研究主要围绕两大主题展开：一是量化和分析利用 DNS 发起的各类攻击，特别是分布式拒绝服务（DDoS）攻击；二是在隐私日益受到重视的背景下，测量新型加密 DNS 协议的部署情况及其带来的安全与隐私影响。

A. 测量 *DNS-based DDoS* 攻击：放大攻击生态系统

DNS 协议由于其基于 UDP 的无连接特性和查询响应报文的尺寸差异，天然地成为反射放大 DDoS 攻击的理想工具。攻击者通过伪造源 IP 地址向开放的 DNS 解析器发送精心构造的查询请求，使得大量的响应流量被导向受害者。近年来的研究不再满足于简单地统计攻击事件，而是致力于描绘整个攻击生态系统的全貌，包括攻击者的策略、被利用的反射器网络的特征以及攻击流量的传播路径。

《The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core》(IMC '21) 是理解现代 DNS 放大攻击生态系统的一个里程碑式的工作。其核心贡献在于其创新的多源数据融合方法论，它没有孤立地依赖某一种数据源，而是将来自大规模蜜罐平台的数据与来自互联网核心交换点（IXP）的被动流量数据相结合，从而获得了对攻击事件的立体视角。该研究最令人震惊的发现是，通过 IXP 流量推断出的 DNS 放大攻击事件与一个大型蜜罐平台观察到的事件集合几乎完全不重叠——高达 96% 的 IXP 推断攻击在蜜罐中是不可见的。这一发现从根本上动摇了学术界长期以来依赖蜜罐数据来评估全球 DDoS 攻击态势的信心。它揭示了一个深刻的问题：任何单一的测量视角都可能存在巨大的盲区。蜜罐作为被动的“受害者”，只能捕获那些恰好以其为目标的攻击流量，而 IXP 作为流量的“十字路口”，则能观察到流经其上的、目标是其他网络的攻击流量。这两者视角的巨大差异表明，我们以往对 DDoS 攻击规模和特征的理解可能存在严重的系统性偏差。这一发现促使研究社区反思，必须推动多方数据（如来自 ISP、CDN、IXP、根服务器运营商等）的融合分析，才能构建出更接近真实的全球攻击视图。

B. 测量 *DNS* 隐私：*DoH/DoT* 的部署与效能

为了应对传统的 DNS 查询（基于 UDP/TCP 的 53 端口）在传输过程中明文暴露用户隐私的问题，

IETF 标准化了 DNS-over-TLS (DoT) 和 DNS-over-HTTPS (DoH) 协议。这些协议将 DNS 查询封装在加密的 TLS 隧道中，旨在保护用户隐私免受窃听和篡改。然而，新协议的引入也带来了新的测量问题。

2020-2025 年间，尤其是在 NDSS 等会议上，涌现了大量针对加密 DNS 的测量研究。NDSS 2021 的 DNS Privacy Workshop 就集中讨论了多个相关议题。研究人员利用 OONI Probe 等全球性测量平台，对 DoT/DoH 在不同国家和地区的可用性及被封锁情况进行了初步研究。另一些工作则从流量分析的角度评估了 DoH 的隐私性，探讨即使流量被加密，攻击者是否仍能通过流量大小、时间等元数据推断用户的访问行为。此外，研究还关注用户侧的认知和配置问题，例如，用户是否理解浏览器中加密 DNS 设置的含义，以及这些设置的默认状态对隐私保护的实际影响。这些测量工作共同揭示了 DNS 隐私保护是一个复杂的系统性工程，单纯的协议加密只是第一步，其实际效果还受到网络环境、审查策略、平台实现和用户认知等多种因素的影响。

VI. 域间路由 (BGP) 安全测量

BGP 是互联网的路由中枢，其安全性直接关系到整个网络的可达性和完整性。BGP 协议本身缺乏内在的安全机制，使得路由劫持（即一个 AS 谎称拥有不属于它的 IP 地址前缀）和路由泄露成为长期存在的严重威胁。为了应对这些问题，社区提出了以 RPKI 为核心的一系列安全增强措施。因此，BGP 安全测量的核心任务便是持续跟踪这些防御机制的部署进展，并评估其在真实环境中的有效性。

RPKI 通过为 IP 地址前缀的合法持有者颁发数字证书，允许路由器验证 BGP 路由通告的源 AS 是否合法，从而防止路由劫持。MANRS 则是一项行业倡议，旨在推动网络运营商采纳包括 RPKI 在内的一系列路由安全最佳实践。

相关的测量研究利用全球路由数据（如来自 RIPE RIS 和 RouteViews 等项目）进行大规模、长周期的分析。例如，NDSS 2021 的论文《Flexsealing BGP Against Route Leaks》通过主动测量和分析，探讨了如何更有效地防止路由泄露。IMC 2022 的论文《Mind your MANRS》则对 MANRS 生态系统进行了测量，评估了加入该倡议的网络的实际路由行为是否符合其规范。这些研究不仅量化了 RPKI 和 MANRS 的部署率，还深入分析了部署中遇到的问题，如证书配置错误、验证策略不一致等，为推动更安全的全球路由生态系统提供了宝贵的数据支持和洞见。

VII. 新型测量技术与目标

网络安全测量领域的发展不仅体现在对新问题的探索，更体现在方法论的不断突破。研究人员正在开发越来越巧妙的技术，以应对日益复杂的测量挑战。

A. 基于侧信道的测量

如前文所述，“测量点困境” 是互联网测量的一大难题，尤其是在 IPv6 网络中。NDSS 2023 的杰出论文奖作品《Your Router is My Prober: Measuring IPv6 Networks via ICMP Rate Limiting Side Channels》为此提供了革命性的解决方案。

该工作的核心洞见在于，一个被广泛部署用于防止网络滥用的协议机制，可以被逆向利用，成为一个强大的测量工具。根据 RFC 4443，所有 IPv6 节点都必须实现 ICMPv6 错误消息的速率限制，以防止 ICMP 洪水攻击。这意味着每个路由器内部都有一个类似 “令牌桶” 的机制来控制 ICMP 错误消息的发送频率。iVantage 技术正是利用了这一点。

B. 测量新兴协议

对于 QUIC 这样旨在替代 TCP/TLS 的新一代核心传输协议，在其部署早期进行安全测量至关重要。这有助于在漏洞被大规模利用之前发现并修复它们，避免重蹈 TCP/IP 协议族在设计之初缺乏安全考虑的覆辙。

《QUICsand: Quantifying QUIC Reconnaissance Scans and DoS Flooding Events” 》(IMC ’21) 利用大型网络望远镜（一种被动收集发往未使用 IP 地址空间流量的系统）的数据，对全球互联网中的 QUIC 背景辐射进行了首次测量。这项工作深刻地揭示了协议的设计安全与部署安全的差距。一个协议在纸面上、在标准文档中可能是安全的，但在复杂、异构且充满对抗的真实互联网环境中部署时，其行为可能与预期大相径庭。协议设计者可能成功地防御了一类已知攻击（如反射放大），但却可能忽略了另一类攻击（如资源耗尽）。因此，经验性的、数据驱动的测量研究扮演了不可或缺的 “现实检验者” 角色。它为协议设计者和网络运营商提供了关键的反馈，帮助他们理解协议

在真实世界中的安全表现，从而及时地调整设计、更新实现和部署防御策略。

VIII. 综合与未来研究方向

A. 关键发现总结

通过对 2020 至 2025 年顶级安全会议中网络安全测量研究的系统性回顾，我们可以总结出以下几个核心发现：

测量视角的局限性与数据融合的必要性：以 DNS DDoS 攻击测量为例，研究表明单一数据源（如蜜罐）所能提供的视图是片面的、不完整的。未来的测量研究必须走向多源数据融合，结合来自 IXP、ISP、CDN、暗网等不同视角的数据，才能构建出对全球网络安全态势更全面、更准确的认知。

测量方法论的范式转移：面对“测量点困境”，最具创新性的突破是从“部署探针”转向“利用侧信道创造探针”。以 ICMP 速率限制为代表的协议副作用，正被创造性地开发为强大的测量工具，这极大地扩展了我们探测和理解远程网络的能力。

测量在协议生命周期中的关键作用：无论是对 DNS、BGP 等部署了几十年的传统协议，还是对 QUIC 等新兴协议，测量研究都扮演着“健康检查”和“安全审计”的关键角色。它验证了安全机制在现实世界中的有效性，并揭示了理论设计与部署现实之间的差距，为协议的演进和安全运维提供了数据驱动的指导。

B. 未解决的挑战与未来展望

尽管网络安全测量领域取得了长足的进步，但仍然面临着诸多挑战。

当前的数据融合研究多是临时性的、项目驱动的。如何构建一个可持续的、开放的、能够融合来自不同利益相关方（学术界、工业界、政府）数据的全球网络安全测量平台，是一个巨大的工程和协调挑战。

网络协议中可能还隐藏着许多未被发现的、可用于测量的侧信道。系统性地识别这些潜在的“预言机”，并将其转化为可靠的测量方法，是一个充满机遇的研究方向。

随着攻击者反测量能力的提升，未来的测量技术需要变得更加“智能”和“隐蔽”。如何设计能够自适应地对抗规避策略的测量系统，将是该领域的一个核心科学问题。

随着 TLS 1.3、QUIC、DoH 等加密协议的普及，传统的基于深度包检测（DPI）的测量方法正逐渐失效。如何在保护用户隐私的前提下，通过对加密流量的元数据、时序特征等进行分析，来有效地检测恶意活动和网络异常，是该领域面临的最紧迫的挑战之一。

网络安全测量是连接理论与实践、规范与现实的关键纽带。在 2020 至 2025 年间，该领域的研究展现出向生态系统级分析、方法论创新和对新兴技术快速反应的明显趋势。研究人员不仅在回答“是什么”的问题，更在深入探索“为什么”和“怎么办”。面对一个日益复杂、对抗性日益增强且流量日益加密的网络环境，持续的、创新的、方法论严谨的测量研究，不仅是一项学术追求，更是保障全球互联网健康、安全和可信赖运行的必要条件。