Starlink星地资产收集检测框架Seestar和Starlink星地情报数据收集汇总

太空安全 2024年7月20日 20:23

目录

摘要：Starlink 是一种新型通信网络架构，利用数千颗低轨道卫星提供高速、低延迟的互联网服务。然而，关于 Starlink 的信息仍有很多尚未向公众披露。Starlink 网络架构的细节以及对深入了解和评估 Starlink 的性能、安全性和影响等至关重要的关键节点仍不为人所知。

本文提出了一种基于主动检测、被动检测和非侵入式搜索引擎检测方法的高效 Starlink 资产检测框架，用于有效发现和识别 Starlink 资产。基于该框架，本文实现了 **Starlink 资产映射系统 SeeStar**，并对 Starlink 地面站和关键节点进行了详细分析，探讨了它们在网络中的作用和特点。最后，本文从设备和服务维度对 Starlink 资产进行了汇总分析，并尝试评估其安全性。本文的工作为揭开 Starlink 网络之谜提供了强有力的方法和系统。

关键词：Starlink·卫星互联网·网络资产·LEO·探测·测绘

1引言

Starlink[1]是SpaceX（太空探索技术公司）近年来打造的LEO（低地球轨道）卫星互联网通信系统，旨在通过部署覆盖全球的低轨道宽带卫星，提供高速、低延迟、高稳定的互联网服务。截至2023年3月，Starlink在轨卫星数量超过3800颗[2]，为50个国家和地区

提供互联网服务，目前拥有超过100万用户[3,4]，计划部署12000颗卫星，最终扩展到42000颗[5]。

作为利用太空技术提供互联网服务的项目，Starlink自2015年启动以来就引起了全球的关注。Starlink使用一种创新的网络系统，为卫星和硬件设备分配专用的IP地址和协议。此外，Starlink在卫星上安装了激光交联技术，改变了传统的卫星通信模式，该技术使卫星之间可以相互传输和转发数据，减少了对地面站的依赖。Starlink还采用了新的P2P网络协议和端到端硬件加密技术，在安全性方面优于传统互联网技术，可以防止数据被窃取或破解。

虽然Starlink已经发射了大量卫星，并为一些国家和地区提供服务，但其资产状况并不为人所知。Starlink资产被人们熟知为卫星运营，已知的TLE文件[6]和网站公布了空间段资产的状况。然而，作为互联网服务提供商，人们对其地面段网络资产知之甚少。为了深入分析和了解Starlink网络的特点和优势，需要对其地面段网络资产进行有效的检测和识别。目前，一些网络空间搜索引擎[7–11]已开始收录星链网络资产，但由于其搜索范围过于宽泛且缺乏针对性，且没有统一的星链网络资产识别标准和动态更新机制，其提供的数据往往存在时效性差、噪声大、准确率低等问题。针对这些问题，本文提出了一种融合主动检测、被动检测和基于非侵入式搜索引擎的检测方法的星链资产检测方法，旨在提高星链资产检测的效率和准确性。

具体而言，本文的主要贡献如下：

1.基于星链网络架构和开放数据源，提出第一个高效、有针对性的星链资产检测框架，并集成一种用于星链资产检测的启发式算法。

2.部署星链资产测绘系统SeeStar，实现对星链IPv4和部分IPv6资产的持续动态检测、星链地面站发现和关键节点分类与测绘。

3.获取星链资产数据并进行聚合分析，提炼星链资产特征，并能根据星链资产属性推断星链关键资产，并根据资产特征分析其安全性。

本文其余部分组织如下：第2节回顾相关工作。第3节介绍星链网络架构和星链资产定义。第4节详细描述了星链资产检测框架。第5节给出了评估。最后，我们在第6节和第7节中做最后总结。

2 相关工作

卫星互联网主要依靠空间卫星星座实现全球互联网无缝连接，为用户提供随时随地的宽带互联网接入，是新一代互联网基础设施，是未来网络基础设施发展的必然趋势。学术

界和工业界对以星链网络为代表的卫星互联网的研究也越来越感兴趣。

在 Starlink 的研究中，Michel 等人 [12] 总结了研究人员使用主动测量方法对 Starlink 性能的分析，以及他们使用 QUIC 对负载和数据包丢失下的性能评估。M. M. Kassem 等人 [13] 使用 Web 浏览器扩展来测量 Starlink 连接性能，旨在回答诸如 Starlink 连接与同一地理区域内的其他 ISP 相比如何、连接质量是否随时间变化以及天气是否影响性能等问题。Stock 等人 [14] 以 Starlink 案例研究为例，讨论了分布式按需路由在 LEO 巨型星座中的使用。Ma 等人 [15] 使用实验和观察来研究最大的 LSN 星座 Starlink 的网络特性和性能，重点关注端到端用户体验。

与我们的工作相关的另一个研究方面是资产检测，Feng 等人[16] 提出了一个可扩展的框架来分析互联网上的物理设备，使用网络侦察和横幅抓取来提取设备信息。Meidan 等人 [17] 描述了一种多阶段元分类器的开发，该分类器利用机器学习算法根据从一组异构设备收集和标记的网络流量数据准确识别和分类物联网设备。Leonard 等人 [18] 总结了作者使用 IRLscanner 工具执行 21 个互联网范围的服务发现实验，并分析了生成的反馈，同时提出了减少反冲的新方法。

目前，主流搜索引擎（如 ZoomEye [7]）已经扫描并收集了一些 Starlink 资产数据，但它们的探索范围太广，无法全面或动态。由于 Starlink 的不断发展和 IP 分配和资产的变化，其资产识别并不一致，导致数据准确性和及时性不理想。**我们提出采用基于主动探测、被动探测和搜索引擎的探测方法，结合使用公开数据源进行持续探测，以全面、及时、高精度地识别星链资产。**

3 星链架构与资产定义

星链作为一个卫星星座系统，采用低地球轨道卫星星座，旨在为互联网连接不可靠或不存在的农村和偏远地区提供高速互联网服务，最终实现全球互联网覆盖。星链系统分为三个主要部分：用户段、空间段和地面段。星链系统架构如图 1 所示。

图1.星链系统架构

用户段属于用户内联网。此段主要包含用户设备和星链终端。无线路由器用于为用户设备提供Wi-Fi信号，以访问星链支持的本地局域网。带有相控阵天线的卫星接收器用于跟

踪近地轨道上的星链卫星信号。

空间段是星间网络的一部分，在此段中，各部件通过星链尚未正式披露的专有新型硬件加密技术进行通信和中继，而非传统的TCP/IP协议栈。由于此段公开数据极其有限，其具体技术细节不明确，协议层面的工作也不足，目前无法通过现有的测绘技术探测此段，电磁或信号分析可作为后续研究的切入点。

地面段包含地面关口站、接入点和数据中心网络。地面站用于与卫星通信，并将从卫星读取的数据发送到接入点。数据中心是互联网服务提供商聚合其网络并共享带宽的地方。在星链网络中，地面关口站并不直接接入互联网，而是通过光纤接入附近的接入点，到达数据中心，由数据中心提供互联网接入。

简单来说，在Starlink网络中，用户设备通过本地局域网向Starlink用户终端发送数据包，用户终端对数据包进行编码并通过上行链路将数据发送到LEO卫星。经过星间传输后，LEO卫星根据预先设计的路由算法，通过下行链路将数据发送到特定的地面关口站，地面关口站对数据进行进一步处理并通过光纤将数据传输到接入点，最后通过数据中心进入互联网。

本文根据Starlink网络架构，将Starlink资产按功能和位置分为三部分：**用户段资产、空间段资产和地面段资产**。

用户段资产主要包括Starlink终端和用户使用的其他设备。

空间段资产主要包括Starlink卫星网络、传感器等设备。

地面段资产主要包括Starlink地面站和PoP(接入点)等关键节点。

本文认为，由于星链网络采用了不同于传统TCP/IP协议栈的新型通信协议和数据传输方式，且公开数据源较少，用户段和空间段资产难以得到有效检测和测绘。因此，本文的研究重点是地面段资产的检测。通过收集和整理公开数据源，获取星链关键节点的公开信

息以及地面站的位置和参数。然后在此基础上进行主动检测、被动检测以及基于非侵入式搜索引擎的检测，以获取更多关于星链资产的信息。最后，本文构建了星链资产检测框架，部署了星链资产测绘系统，实现了星链地面段资产的检测和测绘。

4、星链资产检测框架

本文提出了一种高效的星链资产检测框架。该框架分为检测、收敛和分析三个模块。Starlink 资产检测框架架构如图 2 所示。

图2.星链资产检测系统架构

4.1 检测

检测标准。目前，互联网上存在着大量的网络资产，从大规模网络资产中准确获取与 Starlink 相关的 IP 并识别其资产是一个非常重大的挑战。为了提高 Starlink 资产识别的准确性和效率，我们制定了以下 Starlink 资产识别标准，利用 Starlink 官方数据 [1]、Whois 数据库 [19]、BGP 数据库 [20] 等多元化情报实现准确识别。对于收集到的网络资产，我们验证 whois 数据库中的相关属性是否满足表 1 所示的规则，其中任何一个都将被视为候选的 Starlink 相关资产。

表 1. Starlink 资产检测与识别标准

检测方法。本节重点介绍 Starlink 资产检测方法。检测部分主要采用主动检测、被动检测以及基于非侵入式搜索引擎的检测方法，旨在利用多源数据和多维方法增强星链资产数据获取能力，提高星链资产数据的有效性和准确性。

主动探测。主动探测通过对目标主机进行活体扫描和端口扫描，实现对星链资产信息的获取。主动探测的输入是网络IP地址列表，输出是与星链关联的IP地址。该模块的主要功能是从互联网IP地址空间中提取与星链关联的IP地址，以便后续获取星链关联资产数据。具体来说，采用ICMP、TCP等多种探测包结合Zmap[21]和Nmap[22]的方式对网络IP地址进行主动探测。IP地址对应的Whois信息中包含网段名称、所属组织等信息，因此需要对网络IP地址进行扫描收集数据。通过对全网IP地址进行扫描，收集存活的IP地址，结合Whois数据库中的信息，即可根据上述资产识别标准准确高效地挖掘出与星链关联的IP地址。然后对星链关联的IP地址进行标记，构建星链资产关联IP数据集。最后在每条数据上添加主动探测标识符。此外，作为补充，结合DNS数据、自治系统信息和公开信息，还可以挖掘出其中具有某些特征的Starlink关联IP地址。对全球IP地址空间进行rDNS探测，可以得到rDNS[23]。如果探测结果中的域名文本包含starlinkisp等Starlink关联关键字，则对应IP即为候选Starlink关联IP地址。由于目前全球IP地址空间异常庞大，低效扫描无法完成快速扫描的目的，因此采用基于全球扫描节点、采用分布式架构的分布式扫描方式，对全球IP地址进行高效扫描。

被动探测。被动探测利用网络嗅探工具获取流量，分析其中的IP等数据，结合IP对应的域名信息和Whois信息，获取Starlink资产。被动探测的输入是利用网络嗅探工具获取的互联网流量（可能涉及Starlink关联IP地址），输出是Starlink关联IP地址。对于采集到的流量中的IP，我们首先查询其Whois信息，判断其域名、组织名称等是否符合Starlink资产的特征，比如域名为customer.*.starlinkisp.net、组织名称为SpaceX等。将Starlink关联IP地址也进行标记，纳入Starlink资产关联IP数据集，并在每条数据中添加被动探测标识。

基于搜索引擎的非侵入式检测。目前主流网络空间搜索引擎已经收录了一部分Starlink资产数据，但由于检测周期等因素，这些数据可能存在时效性差等问题。为了更加全面地了解星链资产概况，本文采用基于网络空间搜索引擎的非侵入式检测方法来获取星链资产数据，以扩充主动和被动检测所获得的数据。基于搜索引擎的非侵入式检测模块的输入是基于资产识别标准设计的搜索语句，输出为星链相关资产列表。依托于目前相对成熟的网络空间搜索引擎Zoomeye [7]、Shodan [8]、Quake [9]、fofa [10] 和 Censys [11]，此类网络空间搜索引擎开发较早，技术较为成熟，通常提供 IP、端口号、地理位置信息、服务类型、设备类型和产品类型等信息。因此，采用上述开发的星链资产检测与识别标准来构造符合各搜索引擎语法的搜索语句。通过各搜索引擎提供的API获取星链资产数据，将每条数据纳入星链资产关联IP数据集，添加基于搜索引擎的非侵入式检测标记，标注其数据来源。

资产识别方法。针对获取的星链资产关联IP地址列表，根据搜索引擎结果，结合经验设计候选扫描端口列表。我们使用TCP协议连接目标IP的指定端口，打印出端口返回的信息，得到如图3所示的banner。

图 3. 根据横幅识别资产

然后通过指纹匹配和开源工具识别资产对应的设备、操作系统、产品和服务，将识别结果与基于非侵入式搜索引擎检测获得的资产数据合并，存储在原始Starlink资产数据集中。

本节通过更新原始三个数据表，进一步处理数据表。对于每条Starlink资产数据，包含检测类型及数据来源、资产标识（IP和端口号）、IP地址、端口号、主机名、自治系统号、服务、设备、操作系统、产品、纬度、经度、国家和横幅等原始信息。

启发式算法。基于Starlink资产检测框架的描述，我们总结了算法1所示的相关启发式算法。

该算法主要用于Starlink资产检测。本算法的输入为待探测IP地址列表I（由于IPv6地址空间过大，本算法描述中待探测IP地址列表为IPv4地址空间的子集）、被动流量数据T、星链资产鉴别规则R和待扫描端口号列表P，输出为星链资产数据表A。

为避免对同一网段进行密集扫描，可能引起目标网段防御机制失效，从而影响检测过程，待扫描IP列表首先进行随机重排，若IP存活，则根据预定义的星链资产识别标准（如域名信息、自治系统信息、组织信息等关键字）将该IP识别为星链关联IP，若通过识别策略，则将该IP地址以主动检测标识存入IPSL列表，若通过识别策略，则将该IP地址存入IPSL列表并附加主动检测标记。

对于采集到的被动流量数据T，从每条信息中提取IP地址并按上述方法判断是否为星链关联IP，若通过识别策略，则将该IP地址存入IPSL列表并附加被动探测标记。星链关联IP的服务/请求类型以及使用的端口号和协议可能存在于被动流量中，保存这部分数据有助于后续资产数据的获取。

对于IPSL中的每个IP，扫描待扫描端口列表P中的每个端口，提取端口返回的banner并进行指纹匹配，若有匹配信息，则将资产数据以（探测类型（主动/被动），IP地址，端口号，资产详情）的形式存入资产数据表A。

接下来利用星链资产鉴别规则生成一系列网络空间搜索引擎查询语句并检索，将返回结果中的每条信息以（探测类型（搜索引擎）、IP地址、端口号、资产详情）的形式存储在资产数据表A中。

4.2 融合

本节主要对通过主动检测、被动检测以及基于非侵入式搜索引擎的检测方法获得的星链资产数据进行合并和去重，根据星链资产特点对数据进行提取、验证和清洗，并进行数据库设计和数据存储。数据提取和验证使得来自不同来源的同一对象数据符合统一的形式，为多种异构数据的融合提供保障；数据清洗可以提高后续数据融合分析结果的可信度和有效性。

数据合并与去重。通过主动检测、被动检测以及基于非侵入式搜索引擎的检测方法获得的星链资产可能会有重复的数据，因此需要对这部分资产进行合并和去重，形成最终的星链资产数据集。

数据补充。对于来自搜索引擎的星链资产数据，可能会有资产数据缺失，也可能存在原有存活资产不再存在的情况，因此需要对这部分数据进行补充。首先我们利用活体扫描筛查出存活资产，然后我们结合Nmap和传统指纹匹配的方法识别资产的服务和操作系统等。数据清洗。对获取的资产数据进行初步分析发现，由于用户定义或供应商差异，Starlink资产信息中存在对同一操作系统、服务、产品和设备信息描述不同的情况。另外，还存在国家名称不一致（例如使用国家中文名、国家英文名、国家代码等）和默认值不一致的情况，因此制定了数据清洗规则，以方便统计和分析。

– 属性命名统一（例如 Ubuntu/ubuntu/UBUNTU）

– 空值替换（例如将 unknown/UNKNOWN 转换为 null 值）

– 属性大小写转换（例如将 UBUNTU/Ubuntu 转换为 ubuntu）

– 国家名称转换（例如将 US 转换为 United States）

– IP 资产扩展（例如展开 IP 地址列表）

– 数据更正（例如修改 ASN 等不正确的数据）

– 相同资产数据冲突解决（例如资产随时间变化，不同的冲突方法可能根据数据收集时间产生不同的结果）。

4.3 分析

本节重点对 Starlink 资产数据进行深入分析，主要涉及以下三个方面：Starlink 资产特征筛选、资产数据汇总和安全评估、资产数据可视化展示。

图 4. Starlink 系统实现

Starlink 资产特征筛选。该方面主要包括按照一定的标准如操作系统、产品、设备类型等从星链资产数据库中抽取星链资产数据，提取符合条件的星链资产数据。例如需要分析产品类型为相机的所有资产的数据，系统会返回一个包含所有产品类型为相机的资产数据的表格，以供后续分析。

资产数据聚合与安全评估。该方面主要是将获取的资产数据按照具体的资产特征在开放端口、操作系统、设备类型等不同维度进行聚合分析，并生成相应的统计图表。同时利用CNVD(国家信息安全漏洞共享平台)[24]等漏洞知识库进行聚合分析，并根据资产数据的操作系统、产品类型查询其历史漏洞和当前未修补漏洞，实现对资产数据的安全评估。

资产数据的可视化展示。这方面主要利用一些可视化库比如Echarts、Leaflet等，将汇聚分析和安全评估的结果以更直观、视觉化的方式呈现，比如通过图表、地图等方式展现Starlink资产数据的整体情况和分布特征。

5 评估框架构建

5.1 实现

本文提出了一个星链资产检测框架，并基于该框架实现了一个可以自动检测、识别和分析星链资产的映射系统 SeeStar。该系统自下而上主要由检测、聚合和分析组成。

如前所述，整个系统运行分为三个部分，即检测、聚合和分析：在检测阶段，主要是主动和被动检测，获取资产信息并使用工具进行验证；在聚合阶段，主要是数据处理和整合；在分析阶段，主要是从各个维度对资产进行统计和呈现。每个环节使用的主要技术和整体架构流程如图4所示。本文采用主动检测的方法，基于公共数据源和开源工具，发送检测包并提取星链相关IP。然后，我们结合来自多个搜索引擎的数据来收集星链的资产信息。然后，我们将数据与CNVD数据库融合，并使用Django框架构建我们的星链资产映射系统 SeeStar。最后利用Echarts和Leaflet对数据进行可视化呈现。

5.2应用

地面站发现与关键节点分类。基于FCC[25]、Google Map[26]等公开数据，共收集并分析了**211个地面站，分布在27个国家**。我们将地面站的地理位置映射到地图上，最终得到它们的全球分布，如图5所示。

Fig. 5. Distribution of Starlink Ground Station

我们对Starlink网络的IP地址进行了深入分析，揭示了Starlink网络在自治系统、主机名和网络架构方面的结构和特征。在本文中，我们首先统计了与Starlink相关的IP地址所属的自治系统，发现这些IP地址主要分布在三个自治系统中，即AS14593、AS27277和AS397763[27]。然后本文对这些IP地址进行反向域名解析得到其主机名，并根据主机名的命名规则对Starlink网络的节点进行分类识别。本文发现Starlink网络中主要有以下几类节点：

– **PoP节点：**这是Starlink网络中的重要节点，位于地面站附近，与卫星进行通信，并连接到互联网核心，为Starlink用户提供互联网接入服务，PoP节点还可以与其他PoP节点或MC节点互联，实现网络的互联互通和冗余。

– **MC节点：**这是Starlink网络中的另一个重要节点，负责协调卫星、地球站和用户终端之间的数据传输，以及分配IP地址和子网掩码等。MC节点是Starlink用户接入网络的核心组件。

– **CGNAT节点：**这是Starlink网络中用于解决IPv4地址耗尽问题，保护用户终端安全的节点。CGNAT节点可以实现私有IP地址与公有IP地址的转换，从而支持双向通信。

图6 AS14593、AS27277、AS397763中主机名的分布

本文分析了三个自治系统中的主机名类型，如图6所示，得出以下结论：

- **AS14593是Starlink网络中最重要的自治系统，其中包含大量的PoP节点和MC节点，这些节点是Starlink提供卫星互联网接入服务和管理网络设备的关键组成部分。**在这些节点中，PoP节点的数量明显多于MC节点的数量。在检测结果中，资产占比最高的也是AS14593。

- **AS27277主要由CGNAT节点组成**，用于解决IPv4地址耗尽问题并保护用户终端安全。此外，该自治系统包含少量邮件服务和特殊节点，可能与Starlink的其他功能有关。

– AS397763 有大量与 Starlink 无明显关联的主机名，例如包含 skymall、mail、unisys 等关键字的主机名。这些主机名可能是此自治系统的历史遗留，或计划未来使用的域名。此外，自治系统中还有一定数量的 MC 节点和少量的 PoP 节点，因此推测自治系统尚未被 Starlink 充分利用，可能处于建设或测试阶段。

图 7. Starlink 资产设备类型分布

最后，本文还发现，除了公开数据源提供的 AS14593、AS27277 和 AS397763 外，还存在 Starlink 关联 IP 附属于其他自治系统（例如 AT&T 的 AS7018、Google 的 AS39462 等）或属于独立网络前缀的情况。这些情况可能反映了 Starlink 网络与其他网络之间的合作或竞争。

Starlink 资产数据聚合分析。基于我们部署的 SeeStar，我们积累了 10,188 个与 Starlink 关联的 IP 和 23,132 条资产数据。我们对 Starlink 资产数据进行了专门分析，发现所有资产数据涉及 2073 个开放端口、219 个开放服务、22 个操作系统。然后我们对 Starlink 资产中的设备类型进行了深入分析，发现 Starlink 资产包含 40 种不同的设备类型，其中以防火墙和网络摄像头为主。这些设备类型反映了当前的网络安全和物联网趋势，也揭示了 Starlink 资产的主要用途和功能。图 7 显示了设备类型的具体分布。

本文对 Starlink 资产中的设备产品进行了识别和统计，发现 Starlink 资产主要使用一些知名公司的产品，例如 Amerest、Hikvision、foscam、Dahua 等网络摄像头产品，以及 Sonic WALL、Fortinet、pfSense 和 FortiGate 等防火墙产品。这些产品的特性和性能可以帮助我们进一步了解Starlink资产的管理和配置策略，以及其潜在的攻击面和漏洞。为了了解Starlink资产的漏洞情况，本文基于Starlink资产的设备和产品数据，整合CNVD，得到Starlink资产中已经存在的漏洞和尚未修复的漏洞。

此外，本文还统计了Starlink资产IP地址开放端口数量，发现Starlink资产IP地址开放端口数量存在较大差异，这可能与它们在Starlink网络架构中的作用和重要性有关。我们认为，开放端口数量越高，IP地址的功能性和利用率越高，因此可以根据开放端口数量来评估Starlink IP地址的重要性。

图8 检测到端口开放前10的IP

以图8中开放端口数量最多的IP为例，IP 129.222.251.***位于美国，主机名为customer.*.pop.starlinkisp.net，因此我们通过收集地面站互联网卫星传来的数据导入地面互联网，判断该主机作为PoP节点存在。开放端口数量越多，说明其服务种类越多，反映该IP在Starlink网络架构中的地位越重要。

系统准确性及优势证明。本节旨在评估系统在数据准确性、广度和数据时效性两方面的优势。

在数据广度和准确性方面，本文采用了主动检测、被动检测以及基于搜索引擎的非侵入式检测三种方式，针对Starlink IP分配进行深入分析，通过多源数据融合显著提升了数据广度。同时，本文利用Whois数据库等Starlink资产特征对全网IP地址空间进行全面检测识别，也提升了数据的准确性。为了验证本文的检测效果，将检测结果和数据量与本文收录各大搜索引擎的Starlink资产数据进行对比，如表所示。从表中可以看出，本文的资产检测框架能够更有效、更准确地获取更多的Starlink资产数据。

在数据时效性方面，本文构建的SeeStar通过不断检测并利用Starlink IP分配公开数据源、Whois信息等Starlink资产特征，实现了全网Starlink资产的实时更新。相比之下，常规网络空间搜索引擎是对全网各类资产进行广泛探测，并未重点关注星链资产，因此在制定探测标准时较为宽松，会漏掉大量星链资产，而且由于网络空间搜索引擎的搜索范围较大，运行周期较长，其获取资产的时效性与本系统相比较低，系统收录的存活IP比例较高。

表2 SeeStar与搜索引擎的比较

我们对各搜索引擎提供的星链IP和资产进行了存活性探测，并将我们系统（SeeStar）的结果与各搜索引擎提供的结果进行比较，得到表2的结果。事实证明，我们的系统在数据准确性和广度方面提供了更多的IP和资产数据。我们的系统检测到的IP存活率（29.59%）和资产存活率（31.63%）在时效性方面均高于现有搜索引擎。

6 讨论

本文提出了一种高效的Starlink资产检测框架，该框架结合了主动检测、被动检测和基于非侵入式搜索引擎的检测技术，旨在高效、准确地获取Starlink资产数据。

本文利用该框架实现了一个Starlink资产测绘系统SeeStar，用于测绘Starlink地面站和关键节点，实现地面站发现和关键节点分类，并对Starlink资产数据进行汇总和分析。本文的检测方案结合了Starlink IP分配的公开可用数据源，采用了多种检测方法，并结合使用了指纹匹配和开源工具，因此具有较高的准确率。

本文的工作也存在一些局限性。一方面，本文对Starlink IP分配的理解相对有限。由于Starlink公开数据源的发布与IP的分配使用之间存在时间差，且Starlink IP分配较为复杂，除了三个公开可用的自治系统外，还有一些IP附加在其他自治系统或独立的网络前缀上。另一方面，由于IPv6地址空间过大，本文并未深入探讨IPv6资产，尽管公开数据源和现有研究都表明Starlink中存在IPv6资产。

7 结论

本文提出了一种结合主动检测、被动检测和基于非侵入式搜索引擎的检测方法的Starlink资产检测框架，并基于该框架实现了Starlink资产测绘系统SeeStar。

该系统实现了地面站发现和关键节点分类。在地面站方面，研究发现地面站的分布与Starlink正式发布服务的国家和地区相匹配。通过分析Starlink IP，我们发现Starlink IP分布不仅限于AS14593、AS27277和AS397763，还有一小部分附属于其他自治系统或附属于独立的网络前缀。在关键节点方面，研究发现Starlink关键节点主要分为PoP、MC和CGNAT三类，此外还有其他特殊节点和未知节点。此外，我们专门分析了Starlink资产数据，从服务、设备、操作系统和产品等不同维度对Starlink资产进行汇总和分析。

最后，我们比较了所提系统与现有搜索引擎之间的性能差异，并证明了该系统在准确性、广度和有效性方面均优于它们。

未来，我们将进一步融合多源数据，扩展Starlink IP分配智能以增加Starlink资产数据量，并结合IPv6地址空间预测算法更全面地探测Starlink IPv6资产。我们还将进一步优化检测策略，通过调整检测范围和检测周期来实现更有效、更高效的检测。

8 附件数据源

8.1、专业技术文档

1、SpaceX公司的FCC文件

https://fcc.report/company/spacex

https://forum.nasaspaceflight.com/index.php?topic=46726.0

2、SpaceX公司的专利文件

https://patents.google.com/?assignee=SPACE+EXPLORATION+TECHNOLOGIES+CORP.

3、Starlink Company Information.

https://www.starlink.com/

4、StarLink Manual

https://starlink-enterprise-guide.readme.io/docs/peering-with-starlink

8.2、发射信息

1、CelesTrak: NORAD Two-Line Element Set Format.

https://celestrak.org/NORAD/documentation/tle-fmt.php

2、Launches.

https://www.spacex.com/launches/

https://en.wikipedia.org/wiki/List_of_Starlink_and_Starshield_launches

3、来自非官方 Starlink 全球网关和 PoP 的众包信息：

https://www.peeringdb.com/net/18747

4、关于一些轨道面的数据，已经有很多架构的系统。

https://satellitemap.space/

https://starlink.sx/

https://findstarlink.com/

8.3、运营信息

1、Satellite Earth Station: License.

https://fcc.report/IBFS/Filing-List/SES-LIC

2、Starlink Global Gateways & PoPs.

https://www.google.com/maps/d/viewer?mid=1805q6rlePY4WZd8QMOaNe2BqAgFkYBY&hl=en US&ll=47.6144489%2C-122.33867770000002&z=8

3、Starlink AS.

https://whois.ipip.net/search/SPACEX

4、 Zoomeye.

https://www.zoomeye.org/

5、FOFA.

https://fofa.info/

6、Censys.

https://search.censys.io/

7、 ASN/IP Whois Query–IPIP.NET.

https://whois.ipip.net/

8、BGP.Tools.

https://bgp.tools/

9、rDNS.

https://en.wikipedia.org/wiki/Reverse DNS lookup

10. What is Shodan? - Shodan Help Center. Shodan. https://help.shodan.io/thebasics/what-is-shodan. Accessed 11 Nov 2021

11、National Information Security Vulnerability Sharing Platform.

12、Starlink 星链内幕

https://starlinkinsider.com/starlink-gateway-locations/

13、https://tech-pt.netlify.app/articles/pt526386/index.html

14 、 https://tecnoblog.net/noticias/2021/05/25/anatel-libera-equipamentos-da-starlink-internet-via-satelite-de-elon-musk/

15 、 https://sistemas.anatel.gov.br/mosaico/sch/publicView/listarProdutosHomologados.xhtml **06622-21-13890**

8.4、其他参考文章

1. Quake. https://quake.360.net/quake/#/index

2. McDowell, J.: Starlink Launch Statistics. Planet4589 (2022). https://planet4589.org/space/con/star/stats.html. Accessed 18 Dec 2022

3. SpaceX [@SpaceX]. Starlink now has more than 1,000,000 active subscribers(Tweet) (2022). https://twitter.com/SpaceX/status/1604872936976154624.Accessed 13 Mar 2023

4. Starlink Internet Review 2023: Plans, Pricing, and Speeds. https://www.satelliteinternet.com/providers/starlink/

5. Michel, F., Trevisan, M., Giordano, D., Bonaventure, O.: A first look at starlink performance. In: 22nd ACM Internet Measurement Conference (IMC 2022), pp.130–136. Association for Computing Machinery, New York (2022)

6. Kassem, M.M., Raman, A., Perino, D.: A browser-side view of starlink connectivity. In: 22nd ACM Internet Measurement Conference (IMC 2022), pp. 151–158.Association for Computing Machinery, New York (2022)

7. Stock, G., Fraire, J.A., Hermanns, H.: Distributed on-demand routing for LEO mega-constellations: a starlink case study. In: 2022 11th Advanced Satellite Multimedia Systems Conference and the 17th Signal Processing for Space Communications Workshop (ASMS/SPSC), Graz, Austria, pp. 1–8. IEEE (2022). https://doi.org/10.1109/ASMS/SPSC55670.2022.9914716

8. Ma, S., Chou, Y.C., Zhao, H., Chen, L., Ma, X., Liu, J.: Network characteristics of LEO satellite constellations: a starlink-based measurement from end users. arXiv(2022). http://arxiv.org/abs/2212.13697. Accessed 22 Apr 2023

9. Feng, X., et al.: Active profiling of physical devices at internet scale. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN),Waikoloa, HI, USA, pp. 1–9. IEEE (2016). https://doi.org/10.1109/ICCCN.2016.7568486

10. Meidan, Y., et al.: ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. In: Proceedings of the Symposium on Applied Computing, Marrakech Morocco, pp. 506–509. ACM (2017) https://doi.org/10.1145/3019612.3019878

11. Leonard, D., Loguinov, D.: Demystifying internet-wide service discovery.IEEE/ACM Trans. Netw. 21(6), 1760–1773 (2013). https://doi.org/10.1109/TNET.2012.2231434

12. Durumeric, Z., Wustrow, E., Halderman, J.A.: ZMap: fast internet-wide scanning and its security applications (2013)

13. Lyon, G.F.: NMap Network Scanning: The Official NMap Project Guide to Network Discovery and Security Scanning (2009)

8.5 Starlink的IP资产信息

通过多日的跟踪发现Starlink IP地址，Starlink IP 空间似乎是由谷歌云通过 AS36492 发布的。

SpaceX 服务的 IP 分配：

- 143.131.0.0/20 (ARIN)
- 206.214.224.0/20 (ARIN)
- 205.174.156.0/23 (ARIN)
- 198.54.100.0/22 (ARIN)
- 149.19.108.0/23 (ARIN)
- 2605:59C0::/28 (ARIN)
- 135.129.240.0/20 (ARIN)
- AS397763 (this ASN has never been seen on the Internet) [ARIN]
- 2a0d:3340::/29 (RIPE)
- 162.43.192.0/22 (RIPE)
- 176.116.124.0/23 (RIPE)
- 188.95.144.0/23 (RIPE)

- 217.65.136.0/23 (RIPE)
- 2406:2d40::/32 (APNIC)
- 103.152.126.0/23 (APNIC)
- 103.235.92.0/22 (APNIC)
- 149.19.160.0/20 (LACNIC)
- 2803:9810::/32 (LACNIC)

ARIN 分配给 SpaceX:

- AS14593
- 2620:134:B000::/40
- 192.31.242.0/23
- 199.175.188.0/24
- AS27277 (SpaceX Corporate)

IPv4 announcements by Google Cloud:

NA:

- 143.131.0.0/24 - LAX1
- 143.131.1.0/24 - LAX2
- 206.214.224.0/24 - LAX (advertised from SEA)
- 206.214.225.0/24 - "reserved" (advertised from SEA)
- 206.214.226.0/24 - LAX3
- 206.214.227.0/24 - LAX4
- 135.129.240.0/24 - LAX5
- 143.131.2.0/24 - SEA1
- 143.131.3.0/24 - SEA2
- 206.214.232.0/24 - SEA5
- 206.214.233.0/24 - SEA6
- 206.214.234.0/24 - SEA3
- 206.214.235.0/24 - SEA4
- 143.131.4.0/24 - ORD1

- 143.131.5.0/24 - ORD2
- 135.129.242.0/24 - ORD5
- 143.131.6.0/24 - LGA1
- 143.131.7.0/24 - LGA2
- 206.214.230.0/24 - LGA3
- 206.214.231.0/24 - LGA4
- 135.129.244.0 - LGA5
- 143.131.8.0/24 - MIA1
- 143.131.9.0/24 - MIA2
- 143.131.10.0/24 - DFW1
- 143.131.11.0/24 - DFW2
- 143.131.12.0/24 - DEN1
- 143.131.13.0/24 - DEN2
- 143.131.14.0/24 - SJC1 (advertised from ORD)
- 143.131.15.0/24 - SJC2 (advertised from ORD)
- 206.214.236.0/24 - SJC3
- 206.214.237.0/24 - SJC4
- 205.174.156.0/24 - IAD1 (advertised from NYC)
- 205.174.157.0/24 - IAD2 (advertised from NYC)
- 206.214.238.0/24 - IAD3
- 206.214.239.0/24 - IAD4

SA:

- 149.19.160.0/24 - SCL1
- 149.19.161.0/24 - SCL2
- 149.19.162.0/24 - BOG1
- 149.19.163.0/24 - BOG2

APAC:

- 103.152.126.0/24 - SYD1 - New Zealand (?)

- 103.152.127.0/24 - SYD2
- 103.235.92.0/24 - TBD - maxmind JP
- 103.235.93.0/24 - TBD - maxmind JP
- 103.235.94.0/24 - TBD - maxmind SG
- 103.235.95.0/24 - TBD - maxmind SG

EU:

- 162.43.192.0/24 - MAD1
- 162.43.193.0/24 - MAD2
- 162.43.194.0/24 - LHR3
- 162.43.195.0/24 - LHR4
- 176.116.124.0/24 - LHR1
- 176.116.125.0/24 - LHR2
- 188.95.144.0/24 - FRA1
- 188.95.145.0/24 - FRA2
- 217.65.136.0/24 - SOF1
- 217.65.137.0/24 - SOF2

谷歌也为 SpaceX 公布了这些 IPv6 前缀，但它们更难定位并且没有 PTR 记录。编辑：2021 年 4 月 23 日-我将很快提供更好的 IPv6 前缀更新。

如果你对其中任何一个运行 traceroute/mtr，你会注意到它们在最近的 AS15169 互连处进入谷歌的网络，因为谷歌（通常）到处宣布这些路由，选择使用他们自己的主干而不是互联网来承载流量 . 接近最后一跳的延迟对于这些位置来说是正确的。

Announcements by AS14593:

- 2620:134:b003::/48
- 192.31.243.0/24

AS14593 公告似乎是针对位于雷德蒙德的 SpaceX 公司，因为它似乎都与基础设施相关，包括 CGNAT、防火墙、路由器和服务器。此 ASN 也在 Seattle IX 上对等，并从 Zayo 和 HE.net 传输。

- SpaceX对外服务的网站
- *.spacex.com

- *.starlink.com
- *.starlinkisp.net
- *.pop.starlinkisp.net
- customer.*.pop.starlinkisp.net
- customer.sttlwax1.pop.starlinkisp.net
- shop.spacex.com

SpaceX官方 Starlink iOS和Android应用程序

- 192.31.242.0/24
- 192.31.242.107
- 192.31.242.108
- 192.31.242.109
- 192.31.242.111
- 192.31.242.112
- 192.31.242.113
- 192.31.242.115
- 192.31.242.116
- 192.31.242.120
- 2620:134:b000::/40
- 192.31.243.0/26
- 192.31.243.64/28
- 192.31.243.96/27
- 192.31.243.80/28
- 199.175.188.0/24
- 192.31.242.107
- 192.31.242.108
- 192.31.242.109

- 192.31.242.111
- 192.31.242.112
- 192.31.242.113
- 192.31.242.115
- 192.31.242.116
- 192.31.242.120

数据来源:

- **stat.ripe.net**
- **bgp.he.net**
- **arin.net**
- **peeringdb.com**
- **https://bugcrowd.com/spacex**

网络控制中心 (NCC)

网络控制中心 (NCC) 提供整个卫星通信网络的控制、关口站和用户站操作的协调、网络中单一时间的设置、关口站操作（传输数据）卫星频率槽的分配以及订户、计费维护、传输和接收信息数据收集、系统状态数据收集。

鉴于NCC的重要性，网络通常包括一个主NCC和一个以热备状态运行的备份NCC。

本质上，NCC 是通过光纤通信线路连接到网关站的服务器集合。NCC与网关之间通过光通道的通信非常重要，因为它保证了NCC信息包以恒定的延迟传输到网关，这可以让你有效地控制向卫星传输信息的过程，更重要的是，卫星从一个网关切换到另一个网关的过程，以及卫星之间的终端。使用任何通信系统，例如蜂窝或无线，如果它们具有允许浮动延迟的协议，则在这里是不可接受的。

根 Elon Musk 的说法，该网络将使用一种专有协议，该协议将比 IPv6 更简单并且标头尺寸较小：“”将比 IPv6 更简单并且数据包开销很小。“它也将‘肯定’是点对点连接。”此外，该网络将使用端到端流量加密：

现在几乎不知道有关 Starlink NCC 网络的更多信息。

NCC 综合体还包括 StarLink 网络遥测指挥和控制综合体。

SpaceX 使用 4 个站（传送站），其自己的控制和遥测收集站安装在 Ku 和 Ka 波段。

它们是布鲁斯特（美国华盛顿州）、科尔多瓦（阿根廷）、特罗姆瑟（挪威）、阿瓦鲁阿（新西兰）。每颗卫星的遥测和控制信道每天在轨道上最多可激活 2.5 小时（每绕地球一圈 12 分钟），尽管遥测会话的估计时间为每天 60 分钟.

此外，Space X 与挪威运营商 KSAT 达成协议，使用其在 X 和 S 波段运营的全球网络，包括斯瓦尔巴群岛（挪威）、南极洲、新加坡、南非、迪拜和毛里求斯。同一个全球网络广泛用于猎鹰 9 号运载火箭和 SpaceX 龙飞船的飞行。SpaceX还在华盛顿州设立了自己的跟踪监测站（索引号（“RED1”），用于承载主要有效载荷，必要时使用KSAT网络。

S 波段或 X 波段通信会话每天最多可以持续 2.5 小时（或每个循环 10 分钟），尽管计算值是每天 60 分钟。

SpaceX 还组建了一个测试站网络来测试 StarLink 网络上的服务。

地面测试站包括6个固定地球站和3个移动地球站。您的地址：

SpaceX 总部：加利福尼亚州霍桑市。

特斯拉汽车公司总部：加利福尼亚州弗里蒙特。

SpaceX 测试中心：德克萨斯州麦格雷戈。

SpaceX 布朗斯维尔：德克萨斯州布朗斯维尔

SpaceX 雷德蒙德：雷德蒙德，华盛顿

SpaceX 布鲁斯特：布鲁斯特，华盛顿州。

SpaceX 宽带测试车 1：便携式

SpaceX 宽带测试车 2：便携式

SpaceX 宽带测试车 3：便携式

计划在测试期间，卫星将仅通过这些地面站（仰角 40° 至 90°）进行传输，相当于每天约 10 分钟的会话。

每个地面站配备一到四组具有以下特性的相控阵和/或抛物面天线，遥测和 Ku 波段天线也可用于此目的。

9、参考文献

1. Starlink . https://www.starlink.com/

2. McDowell, J.: Starlink Launch Statistics. Planet4589 (2022). https://planet4589.org/space/con/star/stats.html. Accessed 18 Dec 2022

3. SpaceX [@SpaceX]. Starlink now has more than 1,000,000 active subscribers(Tweet) (2022). https://twitter.com/SpaceX/status/1604872936976154624.Accessed 13 Mar 2023

4. Starlink Internet Review 2023 : Plans, Pricing, and Speeds. https://www.satelliteinternet.com/providers/starlink/

5. Launches. https://www.spacex.com/launches/

6. CelesTrak: NORAD Two-Line Element Set Format. https://celestrak.org/NORAD/documentation/tle-fmt.php

7. Zoomeye. https://www.zoomeye.org/

8. What is Shodan? - Shodan Help Center. Shodan. https://help.shodan.io/thebasics/what-is-shodan. Accessed 11 Nov 2021

9. Quake. https://quake.360.net/quake/#/index

10. FOFA. https://fofa.info/

11. Censys. https://search.censys.io/

12. Michel, F., Trevisan, M., Giordano, D., Bonaventure, O.: A first look at starlink performance. In: 22nd ACM Internet Measurement Conference (IMC 2022), pp.130–136. Association for Computing Machinery, New York (2022) 156 L. Zhang et al.

13. Kassem, M.M., Raman, A., Perino, D.: A browser-side view of starlink connectivity. In: 22nd ACM Internet Measurement Conference (IMC 2022), pp. 151–158.Association for Computing Machinery, New York (2022)

14. Stock, G., Fraire, J.A., Hermanns, H.: Distributed on-demand routing for LEOmega-constellations: a starlink case study. In: 2022 11th Advanced Satellite Multimedia Systems Conference and the 17th Signal Processing for Space Communications Workshop (ASMS/SPSC), Graz, Austria, pp. 1–8. IEEE (2022). https://doi.org/10.1109/ASMS/SPSC55670.2022.9914716

15. Ma, S., Chou, Y.C., Zhao, H., Chen, L., Ma, X., Liu, J.: Network characteristics ofLEO satellite constellations: a starlink-based measurement from end users. arXiv(2022). http://arxiv.org/abs/2212.13697. Accessed 22 Apr 2023

16. Feng, X., et al.: Active profiling of physical devices at internet scale. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN),Waikoloa, HI, USA, pp. 1–9. IEEE (2016). https://doi.org/10.1109/ICCCN.2016.7568486

17. Meidan, Y., et al.: ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. In: Proceedings of the Symposium on Applied Computing, Marrakech Morocco, pp. 506–509. ACM (2017) https://doi.org/10.1145/3019612.3019878

18. Leonard, D., Loguinov, D.: Demystifying internet-wide service discovery. EEE/ACM Trans. Netw. 21(6), 1760–1773 (2013). https://doi.org/10.1109/TNET.2012.2231434

19. ASN/IP Whois Query–IPIP.NET. https://whois.ipip.net/

20. BGP.Tools. https://bgp.tools/

21. Durumeric, Z., Wustrow, E., Halderman, J.A.: ZMap: fast internet-wide scanning and its security applications (2013)

22. Lyon, G.F.: NMap Network Scanning: The Official NMap Project Guide to Network Discovery and Security Scanning (2009)

23. rDNS. https://en.wikipedia.org/wiki/Reverse DNS lookup

24. National Information Security Vulnerability Sharing Platform. https://www.cnvd.org.cn/

25. Satellite Earth Station: License. https://fcc.report/IBFS/Filing-List/SES-LIC

26. Starlink Global Gateways & PoPs. https://www.google.com/maps/d/viewer?mid=1805q6rlePY4WZd8QMOaNe2BqAgFkYBY&hl=en US&ll=47.6144489%2C-122.33867770000002&z=8

27. Starlink AS. https://whois.ipip.net/search/SPACEX