对国家主导的断网的多维网络取证调查

作者：Antonio Mangino 、Elias Bou-Harb
（美国德克萨斯大学圣安东尼奥分校网络安全和分析中心）

翻译：知道创宇404实验室

摘要：2019年11月，伊朗政府强制实施为期一周的全面断网，阻止了大部分互联网接入国内。本文阐述了伊朗断网的特点，通过互联网规模，近实时网络流量对事件展开测量。从调查扫描互联网的受影响设备开始，分析了近50TB的网络流量数据。本文发现了856625个受影响的IP地址，其中17182个属于伊朗。到互联网关闭的第二天，这些数字分别下降了18.46%和92.81%。对物联网（IoT）模式的实证分析显示，90%以上受影响的伊朗主机为物联网设备，在整个关闭过程中出现了显著下降（到断网第二天下降了96.17%）。进一步的检查将BGP可达性度量和相关数据与地理定位数据库相关联，以统计评估可连接的伊朗网关的数量（从大约1100个下降到200个以下的可连接的网络）。深入调查揭示了受影响最大的网关，为此类关键网络的纵向断开提供了网络取证。最后，强调了此次断网对比特币挖矿市场的影响，发现了比特币市场未成功（即未决）交易的激增。综合起来，这些网络流量测量提供了伊朗断网的多维视角。

索引词：断网，互联网背景辐射，物联网，网络取证

1.介绍

当今全球地缘政治中，内乱和抗议活动骤然增多。从南美洲到亚洲，各个国家的公民都开始表达他们对政府权威或相关法律政策的不满。持续的内乱可能会在全国范围内造成经济、外交和军事方面的影响。伊朗最近的抗议活动导致美伊外交关系紧张，一架乌克兰客机在伊朗领空上空被击落，多个国家的176人丧生，此后两国关系更加紧张。为了防止运动规模增大，伊朗政府实施了互联网关闭。从2019年11月16日开始，持续整整一周，伊朗公民无法使用互联网进行通信，无法进行金融交流，也无法连接到日常活动所需的大量应用程序。虽然之前也发生过国家主导的互联网审查（例如，土耳其对维基百科的三年禁令以及伊拉克对社交媒体的禁令），而伊朗此次的断网是最彻底的一次，媒体人士通常称之为全面关闭。为此，本文多维地、实证地分析伊朗国家主导的断网，并对此提出了自己的见解。

1.1 研究目的

伊朗国家主导的互联网关闭是一个历史性的重要事件，表明政府正在采取不断升级的措施，以平息内乱。社会越来越依赖有弹性的互联网连接，但各国政府现在却有了一个几乎切断本国互联网连接的先例。为了提供实证测量和量化伊朗断网的规模，本文提供了从各种互联网规模的角度观察和分析的有见地的网络流量测量，而本次伊朗断网可能成为未来国家主导的审查事件的先例。

1.2 贡献

由于猛烈的全球地缘政治动荡以及分析和记录这一重大事件以进行历史分析的必要性，本文为具体衡量伊朗国家主导的断网提供了以下贡献：

• **从宏观角度解读事件** 之前的一些工作通过使用大规模网络流量和互联网背景辐射来实证研究断网[1 – 3]。本文通过分析近50TB的近期互联网规模，以及两周时间间隔内的宏观网络流量，汇总了最近伊朗互联网关闭期间生成的数据指标，提供了独特的见解。这些数据显示，每天有80万个主机地址主动接入互联网，在伊朗断网高峰期下降到698532个。此外，伊朗的国家指标显示，伊朗地址受影响的人数大幅减少，从事件前的17677人减少到事件低点的1896人（减少89.3%）。此外，还有分析显示，伊朗网络空间的90%以上由物联网设备组成[4]（16296个物联网设备与886个非物联网设备）。

• **网关级BGP路由可用性分析** 先前对边界网关协议（BGP）在全国范围内断网期间的可达性进行的调查使我们获得了对网关级别的见解[5]。本文使用BGP流量实用程序，以捕捉跨度两周的BGP路由可用性。地理定位和国别分析显示，伊朗断网使网关可达性下降了近85%（11月14日为1120个网关，11月20日为173个网关）。从多个全球有利点对BGP可达性的进一步比较揭示了许多不一致之处，表明了伊朗可能对其他国家的IP地址进行了全国范围的过滤。北美和澳大利亚的BGP节点无法与阿富汗等国通信，而南美和非洲的BGP节点却没有收到相同的连接错误。

• **对全球比特币交易所的影响分析** 对比特币加密货币市场的分析显示，因2019年11月伊朗互

联网的关闭，成功交易大幅减少。近几年来，随着全球矿商和交易所的迅速扩张，全时外汇市场出现了爆炸性增长，出现了提供纯粹的“在线”网络测量的体系。全球大约25%的比特币交易被切断（11月14号的350023笔交易，11月17日的264370笔交易）。如此大规模的断网导致加密交易的大量延迟，用于存储暂停事务的内存池聚合内存突然膨胀（最大等待大小达到89770655字节）。

本文的其余部分如下。下一节列举了我们的数据汇总和方法，第3节报告了我们的结果，提供了伊朗互联网关闭的详细测量。第4节简要回顾了相关的工作，第5节总结了本文的贡献，同时指出了一些未来感兴趣的话题。

2.方法和数据汇总

在这里，我们讨论为本文汇编的各种数据源，以及进行大规模网络流量测量所采用的方法。

2.1 IBR集合

为了提供一个宏观的、互联网规模的IBR视角，我们使用了由应用互联网数据分析中心（CAIDA）运营的a/8网络运动传感器。CAIDA网络运动传感器由超过1600万个分配的IP地址组成，可以路由，但不提供任何服务。在此之前，收集到的网络流量是未经请求的，并且通常是由入侵设备接入互联网空间以试图传播而产生的。这样一个广泛的网络运动传感器提供了非常好的可视化主动互联网流量。CAIDA传感器每天收集大约3.6 TB的网络流量。监测近两周的全球IBR（2019年11月14日- 11月25日），该传感器在全球范围内捕获了近50TB全球生成的IBR-提供了与伊朗互联网关闭相关的综合数据集。

2.2 推断主机节点

接下来，开发了Treshold Random Walk（TRW）探测算法[6]，用于提取压缩源地址生成的包流。类似于Rossow[7]所提议的方法。TRW算法识别聚合IBR中的恶意端口扫描。为了确认这些主机有意扫描网络运动传感器，并且收集的流量不是配置错误的产物，这些设备被描述为在

300秒的时间间隔内发送64个数据包。我们还使用各种公开的列表筛选出典型的良性扫描仪。如果在该时间间隔内未收到任何数据包，并且未满足数据包阈值，则流将被丢弃，并且不会被视为受到攻击/未经请求的主机。从收集到的IBR中，使用TRW算法发现了大约850000个不同的，全球范围内每天扫描的主机。

2.3 应用指纹技术的物联网设备

在发现受影响的主机后，进一步分析将物联网设备与发现正在扫描的非物联网设备进行分类。为了实现这一点，本文使用了Pour等人开发的技术。在被动收集的横幅上操作一组学习算法，并结合主动探测。该技术使用了广泛的功能集，包括IP/TCP数据包头字段和TCP选项[10]。这样的分组信息容易从IBR数据中获得，并且通过主动收集服务横幅能够进一步增强。该技术进一步对每个识别的IP地址进行即时反向扫描，以探测近50个端口和服务，这些扫描旨在检索服务横幅和应用程序级协议详细信息（例如HTTP(s)、TELNET、 SMTP(s)、SSH、FTP等）。不安全的物联网设备通常会对此类扫描作出响应，以包含重要操作系统信息（例如embedded、RouterOS、FritzOS）的基于文本的横幅进行响应，以便在物联网设备指纹识别期间使用。读者如果对所使用技术及其详细操作方法感兴趣，请参阅[8,9]。

本文提出了一种Random Forest（RF）分类器作为所使用的技术的一部分，该技术每天识别超过250000个全球和16000个伊朗物联网设备。采用浅层机器学习分类器（如RF模型）可减少处理时间和复杂性，同时提供准确的特征和可解释的特征集。

2.4 调查AS可达性

在对全球被使用的设备进行指纹识别后，我们采用了二维方法纵向测量其可达性。首先，使用MaxMind Ge-oLite 2数据库对所使用的TRW算法确定的受影响的主机进行地理定位。确定了位于伊朗IP地址以及邻国（如阿富汗、土耳其等）的网络块。发现由将近150个伊朗的网关托管这种被破坏的设备。接下来，我们通过使用CAIDA的BGPStream框架来细化测量[5]。BGPStream框架由多国节点组成，不断地扫描Internet空间以寻找可使用的网关（例如/24网络）。这些扫描检索到的信息包括直接从响应路由器、其路由表和相邻对等方检索到的BGP路由。

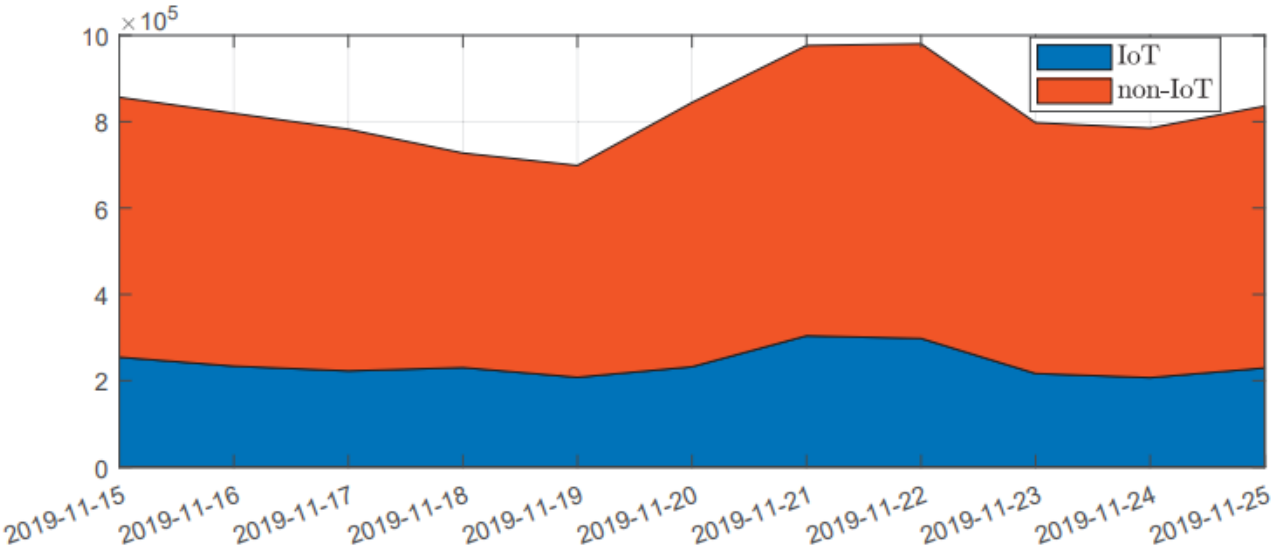


图1:扫描互联网的受影响的物联网设备和非物联网（桌面）机器的总数

通过BGP探测发现了1000多个位于伊朗的网关，在伊朗断网期间下降到略低于200的低点。

2.5 CAIDA IODA项目

我们通过分析和检验从CAIDA的IODA项目中获得的测量数据来验证我们的发现[11]。IODA项目通过分析IBR、进行ICMP扫描和执行BGP分析以进行操作监控，提供全面的网络测量。IODA发布的数据提供伊朗互联网关闭的详细测量，且通过补充网关水平和地理结果，对本文的结论作出了贡献。

3.实证结果

为了阐明伊朗断网的影响，我们论证说明伊朗互联网的状况。这一部分列举了对伊朗互联网空间进行的多维测量。

3.1 发现受影响设备

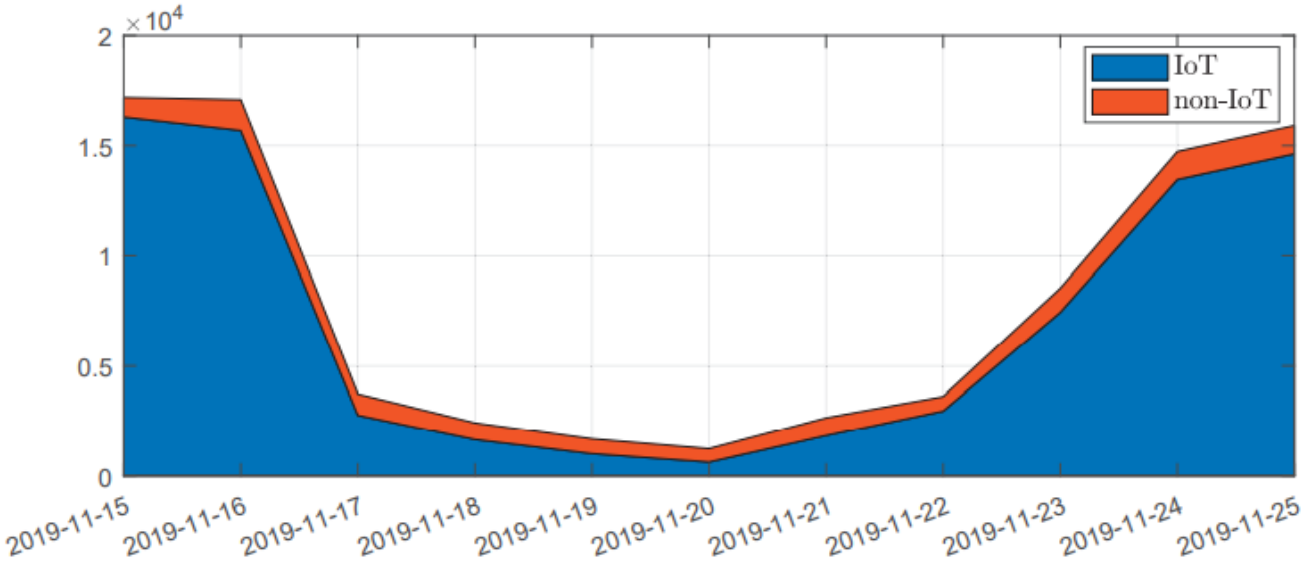
通过分析近50TB的IBR发现，有856625台设备在扫描互联网空间，如图1所示。在伊朗断网的第一天，全球受影响设备（819392个地址）减少了4.35%，而第四天发现的记录设备数量最低，减少了18.46%（698532个地址）。虽然如此显著的下降不仅仅是由于伊朗互联网的关闭，在

对伊朗特定设备的分析中发现了相关的趋势。在使用MaxMind GeoLite数据库之后，对被使用的设备进行了地理定位，并发现了伊朗地址以供进一步处理。

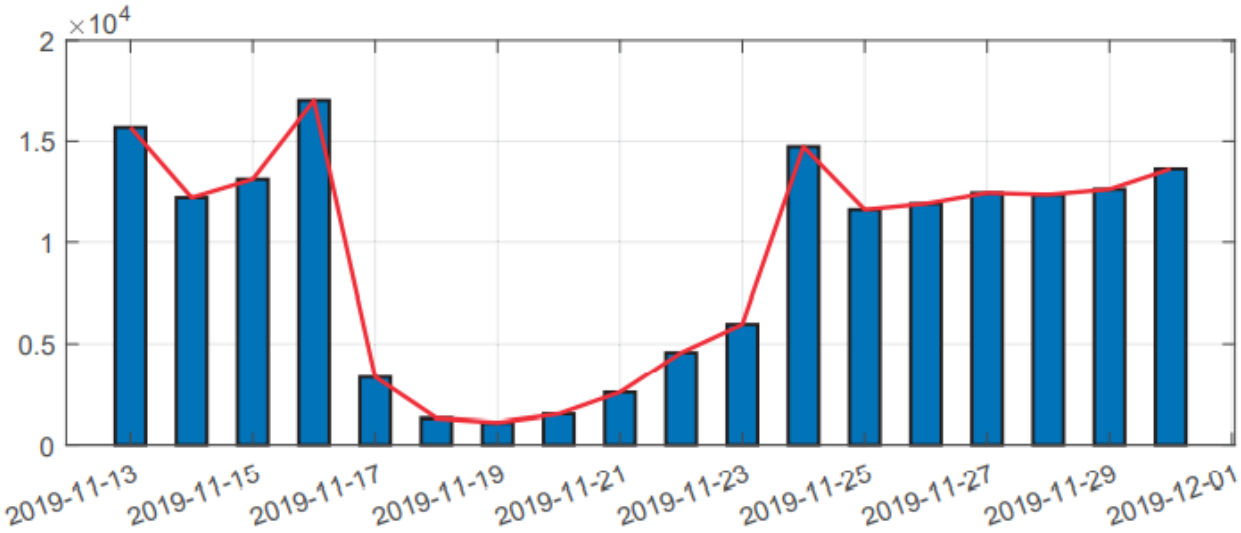
对伊朗IP地址的调查显示，11月15日，182个受影响的伊朗地址扫描网络空间，如图2a所示。在断网的第一天，活跃生产IBR的主机数量急剧下降，下降了78.24%（3739个唯一地址）。到11月20日，伊朗的连通性达到了最低点，只有1237正在扫描的设备（下降92.80%）。11月起，伊朗政府在其首都德黑兰重启网络，与之相应，使用设备增长了26.67%。我们的研究还表明了伊朗网络的逐步恢复，其于11月24日大致回归常态。（14727台受影响设备，85.71%回归正常）为了证实我们针对伊朗的测量结果，我们提供了网络空间搜索引擎ZoomEye发布的公开数据，如图2b所示。网络空间搜索引擎不断地扫描互联网空间，努力识别具有开放端口和服务的面向互联网的设备。ZoomEye发表的统计数据显示与我们的研究结果有直接的相关性。11月14日识别到15502台伊朗受影响设备，11月20日降至1084（下降93.01%），达到最低点。伊朗断网几乎立竿见影，导致出站网络流量急剧下降。

3.2 识别被使用的物联网设备

在识别出全球和伊朗特定的受影响的主机之后，我们通过上述浅层机器学习分类器识别出被使用的物联网设备。11月14日检测到的伊朗受影响设备数为17182台，其中16296被鉴定为物联网设备。将近94.8%的伊朗IP地址是物联网，因此需要对伊朗物联网设备与非物联网的传统机器进行纵向分析。这些研究结果并不完全出乎意料，机器学习分类器的研发人普尔等人称伊朗有全世界受影响的设备的10.17%。我们的研究发现11月14日伊朗有16296台物联网设备，占全世界总数2544408台的7.32%。



(a) IBR results



(b) ZoomEye results

图2:分别从IBR和ZoomEye发现的伊朗设备总数

ASN	Nov15	Nov16	Nov17	Nov18	Nov19	Nov20	Nov21	Nov22	Nov23	Nov24	Nov25
48159	3,518	3,375	298	1	1	1	35	242	1,976	3,139	3,446
12880	1,845	1,792	1,792	313	10	9	53	205	1,110	1,790	1,721
16322	1,688	1,276	409	264	172	168	212	187	362	1,622	1,606
58085	1,036	1,056	0	0	0	0	0	34	51	694	1,119
43754	916	1,040	211	187	155	138	209	191	613	913	1,044
58224	880	931	381	0	0	0	0	195	755	910	935
31549	610	613	2	2	5	5	93	235	459	576	591
25124	369	272	0	0	0	0	64	239	163	305	354
1756	138	114	17	9	0	0	8	0	10	64	58

表1：按发现的IP地址计数排名靠前的伊朗网关

伊朗物联网设备受伊朗断网影响最大，截至11月17日，78.23%的设备不再接入互联网（2776台物联网设备，减少82.97%）。伊朗物联网专用连接在11月20日达到最低点，仅发现624个扫描设备（减少96.17%）。物联网设备下降96.17%（624台）。

对伊朗物联网设备和非物联网设备之间差异的进一步调查显示，受断网影响的物联网设备数量高于传统计算机。11月15日，受断网影响的设备组成比例分别为18.39物联网和1.00非物联网（16296物联网和886非物联网设备）。然而，到11月20日，这一比率分别降至1.02物联网和1.00非物联网（624物联网和613非物联网设备）。探测到的伊朗物联网设备的数量下降了96.17%，而非物联网设备中只有56.12%受到影响，如图3所示：

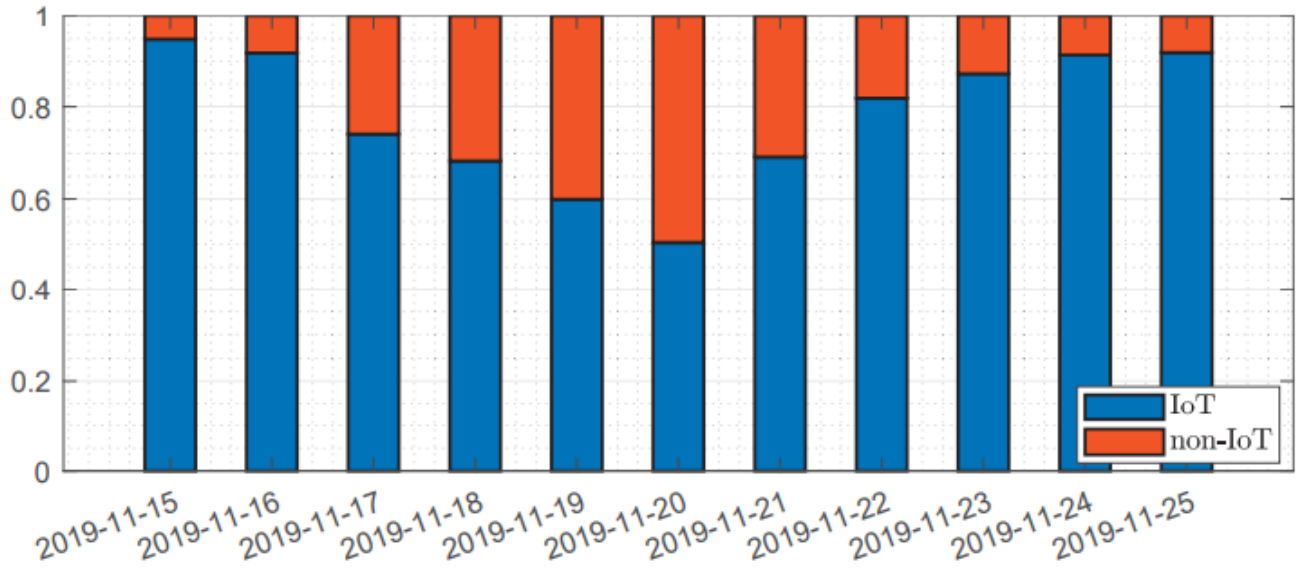


图3：受影响的伊朗物联网设备与非物联网设备的比率

造成如此差异的一个原因可能是物联网和非物联网设备的实际扫描技术。由于物联网设备以较低的吞吐量进行扫描，一旦这些速率因互联网关闭而降低，它们就不再被目前所有的技术识别。因此，由于非物联网设备通常以更高的频率扫描互联网空间，断网对其可识别性的影响较小。

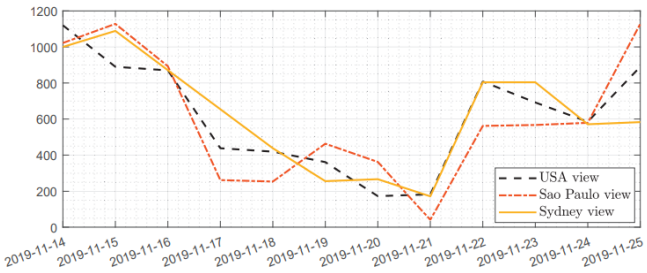
3.3 网关可达性研究

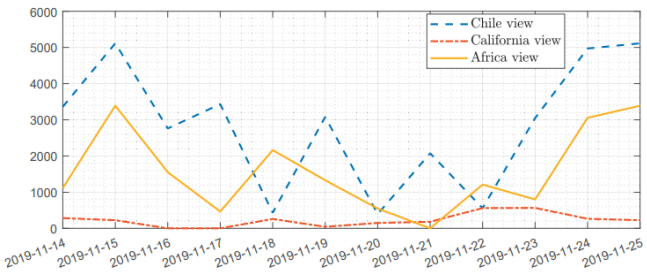
在确认来自伊朗互联网空间的受影响的扫描仪设备后，我们将已知设备归为他们的互联网服务提供商和相关的网关。11月15日，检测到145个伊朗的网关的网络流量。11月20日为93（下降35.86%），为所发现的伊朗网关最低数。伊朗的网关通信没有看到与主动通信设备下降相当的大幅下降；但是，通信受阻的网关覆盖了最多的受影响设备。我们的研究结果对此提供了证据，证明伊朗政府专门针对更大的网关，将其网络断开，埃及政府在2011年的审查中也使用了这一策略。

表1显示了伊朗受影响设备的数量最大的网关，以及被伊朗政府切断连接的日期。最大的网关连接了48159台设备，在11月15日托管了3518个被使用的地址。到11月17日，只有298个地址在使用，到11月18日，只有1个地址在使用。同样地，表中总结的大多数网关在这方面也出现了大幅下降。11月17日，大多数设备完全断网。

到11月18日（17565808525124台设备与主机断连），这些网关直到11月22日才开始恢复，到11月24日达到接近峰值的数量。有趣的是，许多特定的网关没有受到相同程度的影响。例如，网关16322遭受90.05%的下降（网关48159下降99.99%），但从未跌破160个活动地址。网关43754和42337也有类似的趋势，表明这些网关可能承载了关键的或重要的网络，因此免于完全断开连接。

与我们的IBR结果相比，本文使用了6个BGPStream节点来检索全局BGP可达性数据。这些节点位于北美、南美、非洲和澳大利亚。图4a显示了北美、南美和澳大利亚节点发现的可到达伊朗网关的总数。这些结果彼此相当一致，说明在整个伊朗互联网关闭期间，可访问的网关从大约1000个大幅下降到200个。然而，比较每个节点的结果发现BGP扫描数据普遍不一致，如图4b所示。位于智利的节点接收到的伊朗网关可到达响应数最高（11月15日的峰值为5114，紧随其后的是位于非洲的节点（11月15日峰值为3390）。





(a) 通过BGP扫描发现的可访问的伊朗网关总数　　（b）BGP扫描数据不一致

图4：网关可达性 来自BGPStream实用程序[5]

而位于加州的节点收到的结果却少得多，从未收到超过550条响应。节点之间的其他比较显示了伊拉克、巴基斯坦、阿富汗、沙特阿拉伯和土耳其的大致相同的接收数据。事实上，如果发送到阿富汗IP地址空间的所有BGP数据包不是来自位于非洲的节点，那么这些数据包都会被丢弃，而南美节点会在特定的日子收到响应。这些发现暗示了伊朗政府在全国范围内根据特定地址来源国对其进行过滤。

3.4 比特币加密货币交易所的检查

评估Blockchain.com提供的比特币加密货币交换数据，我们研究了伊朗断网与全球比特币挖矿趋势之间的相关性。虽然这些相关性可能不仅仅是由伊朗断网造成的，但研究“纯在线”的流量测量比特币加密货币等市场为全球互联网连接提供了另一种视角。而且成功的比特币交易揭示了与伊朗断网的线性关系。11月15日，325145笔比特币交易成功进行；然而，11月16日仅完成283468笔交易（下降12.82%）。截至11月17日，只有264370笔比特币交易最终成交（下降18.69%）。虽然加密货币市场相对不稳定，但这并不一定意味着开采或出售的比特币数量减少。更有可能是市场上出现了瓶颈，或报价未完成，或等待内存处理和出售。为了给这种符号性减少提供相关性检验，我们研究了聚合内存池中等待处理的总数量（当前节点帮助等待处理的事务的位数）。

先前成功交易量的典型下跌，例如从10月5日开始（32683笔交易）至10月6日（277613笔交易），但并没有未决交易的大幅增加（分别为4403至4057）。然而，从11月14日开始的交易量下降达到了峰值，达到了15088笔待处理交易。此外，总的内存池规模急剧膨胀。大小达到89770655位，比特币内存池总量周增长85.91%，与前一周的高点1264599位形成对比。因此我们可以确定，2019年11月全球比特币加密货币交易量的下降是一个特殊事件，而比特币市场最近出现了瓶颈。在2020年2月的头几周，针对伊朗互联网基础设施的大规模分布式拒绝服务攻击使伊朗的连接能力下降了近25%。比特币加密货币市场也受到了类似的影响，内存池的最大值为27351731位，高于前一周的峰值13559610位（增长101.71%）。这突出了伊朗断网与全球比特币市场之间的关系。这种相关性可能是由许多因素造成的，主要是伊朗大量开采加密货币的设备[12]。

4. 相关工作

在本节中，我们将研究有助于大规模网络流量测量的相关工作。具体来说，我们讨论了断网特征和基于预测的方法，并列举了大规模断网的分析度量。

4.1 大规模断网的预测和分类

尽管社会依赖于可靠的互联网连接，但断网仍然频繁发生。Aceto[13]等人对互联网普遍断网进行了全面调查，提出了断网分类的准则，同时系统分析了调查大规模断网事件的相关方法。此外，Quan[14]等人构建了一个基于ICMP的模型来识别全球断网，通过定期探测互联网空间，本文研究了整个互联网的稳定性。此外，改进了他们的断网检测系统。Quan等人后来开发了三目[15]，使用ICMP探测来扫描网络空间并检测断网事件，用一个高效、低交互的模型来确定兴趣点。这些研究说明了断网的多样性。尽管一些事件可能只持续几分钟或影响到少数人，但全国范围内的断网可能会削弱关键基础设施。对于国家主导的断网而言，一些重要的国家网络将会得以保持。我们的研究发现，在此次伊朗断网期间，一部分应用于政府和基础设施的网络得以保持。

4.2 国家主导的断网的实证测量

以前研究大规模断网的研究通常可分为两类：通过主动探测（如BGP或ICMP扫描）进行断网识别，以及通过分析互联网背景辐射（IBR）进行断网识别。Shavitt[16]等人对2011年阿拉伯之春进行了有效的调查。使用了363万个路由跟踪测量，说明了阿拉伯之春期间埃及、利比亚和叙利亚互联网的状况。Dainotti[17]等人使用有源BGP域间探测和分析IBR对2011年埃及和利比亚的断网进行了类似的调查。最近，Guillot等人开发了断网检测分类器Chocolatine[18]。使用网络运动传感器对互联网规模的IBR进行了调查，发现其趋势是一致的；来自每个地理网关的扫描IP地址数保持不变。使用这些观测，sea-sonal ARIMA被用于时间序列预测，预测和评估从单个网关生成IBR的唯一IP地址的数量，将偏差或下降归因于断网。

原先提及的文献介绍了通过主动探测和IBR分析来识别和测量断网的方法。同样，本研究也使用BGP域间路由表和互联网规模的网络运动传感器，对伊朗互联网关闭事件进行了独特的调查和分析。此外，收集的IBR分类揭示了有关伊朗物联网的特定见解，并发现了关键运营网关的系统性关闭。

5.结束语

本研究实证性衡量了一个国家级的审查事件。通过处理近50TB的未经请求的互联网背景辐射，发现超过17000台受影响设备从伊朗IP空间扫描全球互联网，其中16296台属于物联网。此外，我们的研究结果表明伊朗网关可达性急剧下降（145个活跃网关下降到93个）。此外，我们还发现由于对特定IP地址空间进行全国范围的过滤而导致的全局BGP不一致性。最后，我们分析了比特币加密货币市场，揭示了成功交易相对于存储未决交易的内存池内存量的减少。未来的工作可以提供对网络分组的深入分析，特别是物联网设备分组。此外，未来使用加密节点

或相关基础设施[19]来描述断网的研究将会提出与互联网路由和连接相关的更有效的结论。

6.参考文献

[1] Karyn Benson el al. Gaining insight into as-level outages through analysis of internet background radiation. In 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 447–452. IEEE, 2013.

[2] Ryan Bogutz, Yuri Pradkin, and John Heidemann. Identifying important internet outages (extended). Technical report, TR ISI-TR-735, USC/ISI, 2019.

[3] Farooq Shaikh, Elias Bou-Harb, Nataliia Neshenko, Andrea P Wright, and Nasir Ghani. Internet of malicious things: Correlating active and passive measurements for inferring and characterizing internet-scale unsolicited iot devices. IEEE Communications Magazine, 56(9):170–177, 2018.

[4] Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. IEEE Communications Surveys & Tutorials, 21(3):2702–2733, 2019.

[5] Chiara Orsini et al. Bgpstream: a software framework for live and historical bgp data analysis. In Proceedings of the 2016 Internet Measurement Conference, pages 429–444, 2016.

[6] Elias Bou-Harb, Mourad Debbabi, and Chadi Assi. A novel cyber security capability: Inferring internet-scale infections by correlating malware and probing activities. Computer Networks, 94:327–343, 2016.

[7] Christian Rossow. Amplification hell: Revisiting network protocols for ddos abuse. In NDSS, 2014.

[8] Morteza Safaei Pour et al. Data-driven curation, learning and analysis for inferring evolving iot botnets in the wild. In Proceedings of the 14th International Conference on Availability, Reliability and Security, page 6. ACM, 2019.

[9] Morteza Safaei Pour et al. On data-driven curation, learning, and analysis for inferring evolving internet-of-things (iot) botnets in the wild. Computers & Security, page 101707, 2019.

[10] Elias Bou-Harb, Nour-Eddine Lakhdari, Hamad Binsalleeh, and Mourad Debbabi. Multidimensional investigation of source port 0 probing. Digital Investigation, 11:S114–S123, 2014.

[11] Internet outage detection and analysis (ioda). https://www.

caida.org/projects/ioda/.
[12] Iran seizes 1,000 bitcoin mining machines after power spike. https://www.bbc.com/news/technology-48799155, 2019.
[13] Giuseppe Aceto, Alessio Botta, Pietro Marchetta, Valerio Persico, and Antonio Pescape. A comprehensive survey on in- ´ ternet outages. Journal of Network and Computer Applications, 113:36 - 63, 2018.
[14] Lin Quan et al. Detecting internet outages with precise active probing (extended). USC/Information Sciences Institute, Tech. Rep, 2012.
[15] Lin Quan, John Heidemann, and Yuri Pradkin. Trinocular: Understanding internet reliability through adaptive probing. ACM SIGCOMM Computer Communication Review, 43(4):255 - 266, 2013.
[16] Yuval Shavitt and Noa Zilberman. Arabian nights: Measuring the arab internet during the 2011 events. IEEE Network, 26(6):75 - 80, 2012.
[17] Alberto Dainotti et al. Analysis of country-wide internet outages caused by censorship. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 1 - 18, 2011.
[18] Andreas Guillot et al. Chocolatine: Outage detection for internet background radiation. In 2019 Network Traffic Measurement and Analysis Conference (TMA), pages 1 - 8. IEEE, 2019.
[19] Elias Bou-Harb. A brief survey of security approaches for cyber-physical systems. In 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pages 1 - 5. IEEE, 2016.