计算机科学
COMPUTER SCIENCE

基于流量分析发现未知UDP反射放大协议

陆炫廷, 蔡瑞杰, 刘胜利

引用本文

陆炫廷, 蔡瑞杰, 刘胜利.基于流量分析发现未知UDP反射放大协议[J]. 计算机科学, 2022, 49(11A): 211000089-5.

LU Xuan-ting, CAI Rui-jie, LIU Sheng-li. Discovery of Unknown UDP Reflection Amplification Protocol Based on Traffic Analysis [J]. Computer Science, 2022, 49(11A): 211000089-5.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.211000089

基于流量分析发现未知 UDP 反射放大协议

陆炫廷　蔡瑞杰　刘胜利
数学工程与先进计算国家重点实验室　郑州　450001
战略支援部队信息工程大学　郑州 450001
(251758821@qq.com)

摘　要　近年来,DDOS 攻击的频率和规模日益扩大,对网络安全造成了极大挑战。其中,UDP 反射放大攻击因其攻击成本低、攻击流量巨大、难以追踪溯源等特征成为了黑客青睐的攻击手段。当前的过滤和防御策略大多来源于受攻击后的分析与复盘,面对层出不穷的新型 UDP 反射攻击存在一定的被动性和滞后性。文中提出了一种基于流量分析来发现存在 UDP 反射放大潜力的未公开协议的方法。该方法立足放大性和反射性这两个根本特征,从日常网络流量中筛选出符合反射放大特性的流量样本,然后通过重放攻击验证样本是否具备可重复性,记录符合条件的样本,用于对相关服务协议进行研究,最终成功发现新型未公开反射放大协议。用所提方法构建的检测程序,在实验环境和互联网中分别进行了准确率及处理速率测试,成功发现了多种反射放大协议,以积极主动的方式来防御可能出现的反射放大攻击。

关键词:分布式拒绝服务攻击;UDP 反射放大攻击;网络安全;流量检测;主动防御
中图法分类号　TP393

Discovery of Unknown UDP Reflection Amplification Protocol Based on Traffic Analysis

LU Xuan-ting,CAI Rui-jie and LIU Sheng-li
State Key Laboratory of Mathematical Engineering and Advanced Computing,Zhengzhou 450001,China
Information Engineering University,Zhengzhou 450001,China

Abstract　In recent years,the frequency and scale of DDOS attacks have increased,which has posed great challenges to network security. Among them,UDP reflection amplification attacks have become the attack method favored by hackers due to their low attack cost,huge attack traffic,and difficulty in tracing the source. Most of the current filtering and defense strategies are derived from the analysis and review after the attack,and there is a certain degree of passivity and lag in the face of the endless new UDP reflection attacks. This paper proposes a method based on traffic analysis to discover undisclosed protocols with the potential of UDP reflection amplification. Based on the two fundamental characteristics of magnification and reflectivity,this method selects traffic samples that meet the characteristics of reflective amplification from daily network traffic. Then,the replay attack is used to verify whether the samples are repeatable,and the qualified samples are recorded for research on related service protocols. Finally,a new type of undisclosed reflection amplification protocol is successfully discovered. The detection program constructed with this method has been tested for accuracy and processing rate in the experimental environment and the Internet respectively,and a variety of reflection amplification protocols are found to proactively defend against possible reflection amplification attacks.

Keywords　DDOS,UDP reflection amplification attack,Cyber security,Flow detection,Active defense

1　引言

全球主要安全研究机构的报告表明,近年来中国已经成为 DDOS 攻击最大受害国家。尤其是在过去一年,受疫情影响,大量社交、娱乐、购物和工作等场景从线下转移到线上。与之对应,DDoS 攻击在经历了 2019 年的低谷后迎来强势反弹,攻击次数创下历史新高。其中 UDP 反射攻击仍然占据主流,占总攻击数量的 88%,CoAP,WS-DD 和 ARMS 等新型 UDP 反射攻击手法开始涌现。

2016 年 7 月 19 日,Arbor Networks 发布了 2016 年上半年的 DDoS 攻击报告,报告介绍反射攻击时的标题为 A Time For Reflection,指出未来是反射攻击的时代。报告显示,反射型攻击呈上升趋势,此类攻击也是 2016 年上半年大型 DDoS 攻击数量上升的原因之一。

2014 年 2 月,美国 CDN 服务提供商 Cloud Flare 遭受了峰值达到 400Gbit/s 的反射型 DDoS 攻击[1]。攻击者利用 NTP 协议中的 monlist 命令将流量放大了近 200 倍。2018 年 3 月,全球知名的软件代码托管网站 GitHub 遭受了峰值达到 1.35Tbit/s 的反射型 DDoS 攻击[2]。攻击者利用 memcached 中的漏洞将流量放大了近 51 000 倍。2020 年 2 月,AWS

基金项目:国家重点研发计划(2019QY1300);科技委基础加强项目(2019-JCJQ-ZD-113)
This work was supported by the National Basic Research Program of China(2019QY1300) and Science & Technology Commission Foundation Strengthening Project(2019-JCJQ-ZD-113).
通信作者:刘胜利(dr_liushengli@163.com)

遭受到了 DDoS 攻击，攻击手法主要为 CLDAP 反射，此次攻击达到 2.3Tbit/s，为有史以来最猛烈的攻击。

UDP 反射攻击是利用有漏洞的应用层服务协议发起的 DDoS 攻击，通过伪造地址来隐藏攻击源。由于无需组建僵尸网络、操作更加简单、攻击源不易被跟踪，UDP 反射攻击给安全事件的溯源和响应处置造成了很大困难。

从当前的网络防御策略来看，对已知攻击手段的防御能力要远高于对未知攻击方法防御的能力，因此美国计算机应急准备小组（United States Computer Emergency Readiness Team，US-CERT）官网上专门有一个模块介绍存在实施反射攻击潜能的以 UDP 为载体的服务协议[3]。该模块根据各大安全公司给出的 UDP 反射攻击报告以及相关科研机构的研究成果不间断地进行更新。该模块发布于 2014 年 1 月 17 日，最新更新时间 2019 年 12 月 18 日，增加了 WS-Discovery 服务协议。US-CERT 共给出了存在实施 UDP 反射攻击潜能的 19 种以 UDP 为载体的服务协议以及对应的 BAF 数据，具体总结如表 1 所列。其中 BAF 为一次请求和回复中，放大器回复报文的数据负载和接收到请求报文的数据负载的比值，是目前被普遍接受的评价反射攻击的主要测度。

表 1 UDP 放大协议列表

Table 1 UDP amplification protocol

协议	端口	带宽放大因子	协议描述
DNS	53	28 to 54	域名解析服务
NTP	123	556.9	时间同步服务
SNMPv2	161	6.3	简单网路管理服务
NetBIOS	137	3.8	网络基本输入/输出系统
SSDP	1900	30.8	简单服务发现协议
CharGEN	19	358.8	字符发生器协议
QOTD	17	140.3	今日名言服务
BitTorrent	任意	3.8	比特流分布式文件传输工具
Kad	任意	16.3	P2P 重叠网络传输协议
Quake Network Protocol	27960	63.9	Quake 3 游戏引擎服务
Steam Protocol	27015	5.5	Steam 游戏引擎服务
Multicast DNS (mDNS)	5353	2 to 10	组播 DNS
RIPv1	520	131.24	简单路由交换协议
Portmap(RPCbind)	111	7 to 28	RPC 端口映射服务
LDAP	389	46 to 55	轻量目录访问协议
CLDAP	389	56 to 70	无连接轻量级目录访问协议
TFTP	69	60	简单文件传输协议
Memcached	11211	10000 to 51000	高性能分布式内存对象缓存服务
WS-Discovery	3702	10 to 500	Web 服务动态发现

本文对比分析了目前更新 UDP 反射放大协议的两种主要手段，提出了基于日常流量监测的主动发现方法，并进一步验证了其可行性和工作效率。该方法通过对互联网日常流量执行检测，结合已知协议过滤的方法，筛选出具备反射放大行为的流量，用于发现新型 UDP 反射放大协议。

2 相关工作

2.1 UDP 反射放大攻击原理

在 UDP 反射攻击中，攻击者利用互联网上开放的基于 UDP 协议提供服务的服务器（也称放大器或反射器）间接发动攻击。UDP 协议的无连接性使得请求报文的源 IP 很容易被伪造，攻击者将请求报文的源 IP 伪造为受害者的 IP，从而服务端返回的响应包就会返回到受害者的 IP，这就形成了反射攻击。同时，攻击者利用服务协议自身的漏洞，一次小的请求数据包会导致其数倍大小的响应数据包，这就形成了流量放大。在实际攻击过程中，攻击者往往会利用大量的放大器发动攻击，以达到拒绝服务的效果。

2.2 UDP 反射放大攻击的主要发现手段

2.2.1 直接分析协议

早先，研究人员对广泛应用的协议和公共服务进行系统性分析，判断是否存在 UDP 反射放大的可能。其过程类似于漏洞挖掘中的代码分析，对其执行过程进行逻辑分析然后验证判断。

早在 2001 年，VernPaxson 就提出了假冒源地址的 DDoS 攻击模型[4]，并且分析了 ICMP，TCP，UDP，DNS，SNMP 协议在上述攻击模型下，由于协议中的某些字段存在设计缺陷，存在被用于流量放大的风险。

2014 年 2 月，ChristianRossow 等系统地对 SNMP，DNS，NTP，SSDP，Char Gen 等 14 种 UDP 协议进行了系统性的研究[5]，认为这些协议存在实施反射攻击的可能。

此方法以主动分析为主，能够针对性地判断出某协议是否具备反射放大潜能。但由于网络协议不断更新发展，特别是 IOT 设备的广泛应用，伴随着更多非网络公共服务的出现，而这些服务在设计时安全性的标准较低，研究人员逐一分析它们需要耗费大量精力，因此通过该方法发现新反射放大协议变得越来越困难。

2.2.2 根据攻击痕迹分析

由于主动分析协议需要花费较大的研究成本，且效率低下。因此，近年来对 UDP 反射放大攻击协议的更新主要来源于记录到的网络攻击后的分析。通过入侵检测系统记录的攻击数据，来复盘攻击细节和过程，并对其展开相关拓展研究。

2017 年 11 月，360 网络安全研究院报告称，CLDAP 现在是第三大最常见的 DRDoS 攻击，仅次于 DNS 和 NTP 攻击[6]。2018 年 2 月，SENKI 分析了基于 Memcached 的反射 DDoS 攻击（通过 UDP/TCP 端口 11211），并且具有前所未有的放大系数[7]。2019 年 9 月，Akamai 报告了利用 WS-Discovery 协议的 DDoS 攻击行为[8]（通过 TCP/UDP 端口 3702）。

根据攻击行为痕迹来发现攻击手段的方法虽准确有效，且成本较低，但它存在被动性和滞后性，只有在受到网络攻击后才能有所发现。因此，我们希望通过更加积极主动的策略来最大程度地预防 UDP 反射放大攻击，先发制人，以减小 DDOS 攻击带来的损失。

3 基于流量分析的主动检测方法

从反射放大流量的生成场景来考虑，其主要有 3 个来源：1）用户正常使用服务时产生，流量层面体现出了反射放大的特点；2）攻击者在执行 DDOS 之前，必然会针对该服务进行资源扫描，以收集其可利用的反射资源，同时也必然会执行小规模的反射测试以保证其反射攻击的有效性；3）攻击者执行 DDOS 时，会产生大量 UDP 反射流量，这是最明显也是最容易被检测到的，也是安全机构大多采用的发现 UDP 反射放大攻击的方法。

本文则是主要针对前两种场景，采取主被动结合分析的

方式，借鉴漏洞挖掘中 fuzzing 的思路，以大规模互联网流量为测试源，通过流量分析的方法，提取具备 UDP 反射放大特性的流量样本，用于发现存在的未公开 UDP 反射放大协议。该方法分析筛选出存在反射放大特点的流量样本，再根据该样本进一步确认其所属服务，并分析服务过程和反射细节。

对比当前主要采用的两种分析方法，直接分析法基于原理推断并设计测试来判断协议是否存在反射放大攻击潜在危险，但需要消耗大量精力，且只能判断已研究过的协议，对于新产生的协议无法判断。而基于网络攻击痕迹的分析法，虽然低成本且高度准确地还原出了反射放大攻击细节，但发生在网络攻击之后，属于“亡羊补牢”，无法提前避免损失，缺乏主动性。

因此，本文结合当前两种方法的优点，通过对日常流量的检测提取存在反射放大可能的协议，并自动进行测试，这属于基于行为特征的判断。相比直接分析具有更强的适应性，能够检测出流量中包含的所有具有反射放大特征的协议，而不必逐一判断，极大地提升了效率，相比根据攻击痕迹分析，本方法将检测分析的场景从受到网络攻击后提前到日常流量中，做到提前发现，以最大程度地减小网络攻击带来的损失。检测过程如图 1 所示。

(1)分布式网络节点将根据抓取规则获取 UDP 流量后牵引到数据处理服务器；

(2)服务器将从数据包中筛选出具备流量放大潜能的触发包；

(3)对触发包指向的潜在反射服务端执行重放测试，以验证该服务的可反射性；

(4)将验证后能够实现反射放大行为的触发包存入输出文件，并由研究人员进一步核验分析，从而确定该反射放大服务的有效性。

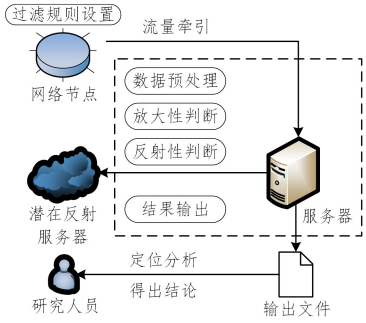

图 1　检测流程

Fig. 1　Detection process

3.1　前期工作

3.1.1　数据获取

本文方法从日常流量中筛选出符合反射放大特性的样本。而从目前新发现的 UDP 反射放大攻击来看，新服务和物联网设备引起的反射放大攻击日益增加。因此，除了大规模流量获取，在条件允许时，流量来源尽量丰富多样。优先选择在电信骨干网络节点、子网网关出入口以及包含大量物联网设备的局域网环境中获取流量。

3.1.2　数据预处理

将捕获到的数据报文按照地址对应关系分组，将每两个地址间的全部通信流量按照时间顺序添加到同一分组，并提取报文长度。其中，地址 A 到地址 B 的报文标记为正向流量，则 B 到 A 的报文标记为反向流量。

3.1.3　设置阈值

许多安全机构在公布反射放大倍数 BAF 时，计算方法为：在一次反射攻击中回复报文的 UDP 负载和请求报文 UDP 负载的比值。然而，在大部分反射攻击中，payload 实际很小，这就导致公布 BAF 与实际流量放大效果相差巨大[9]。在此，为了更加直观地反映出实际的流量放大效果，我们计算 IP 报文长度之和作为流量大小，定义放大系数 f：即一次反射攻击中回复流量与请求流量的比值。当流量放大系数 f 大于设定的阈值时，才会被判断选择。文中提到的所有实验测试中阈值均设为 5。

3.2　放大特性判断

对于所有满足反射放大特性的服务，从流量上看，其回复流量必然远大于请求流量。而请求流量和与之对应的回复流量的界定问题则是难点所在。由于涉及的协议类型多且复杂，且考虑了大量未知协议的存在，使用传统的内容识别判断或是当下比较流行的深度学习算法，均无法准确判断出上下文关系。因此在对分组内的报文进行具体分析时，我们采用最大化预判的原则。即将同一方向的连续报文与其后相反方向的连续报文视作一次“交互”。即认为“交互”中正方向的某些报文是请求流量，而与之相反的反向流量均视作潜在回复流量。

在实际网络信息交互时，网络传输时延一般远大于报文发送时间，因此回复流量几乎不可能在请求流量还未全部发出前到达，且如果将跨交互的情况考虑进去，则所有相反方向流量均可视作答复流量，则无法对流量进行筛选，因此暂时不考虑跨“交互”的极端情况。

具体处理时，由于目前所有已知的反射放大攻击都是通过单包触发的，为了尽可能减少漏报，同一方向的多个连续数据包都被视为同一次回复流量。回复流量的前一个数据包作为反射触发包的可能性最大，因此我们暂且认为该数据包是触发包，其长度即为请求流量大小。图 2 对比了实际流量交互场景和理想交互场景，在初步筛选时，根据最理想情况判断流量存在放大的可能，其他可能场景将在后续步骤中讨论。例如，分组内 IP 报文长度为[60，67，90，−300，−300，−300]时，我们计算出请求流量为 90，回复流量为 900，放大系数 f 为 10，若大于阈值，则满足放大性筛选条件。

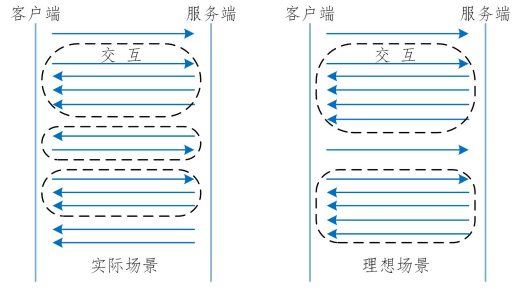

图 2　放大性判断

Fig. 2　Magnification judgment

3.3　可反射性判断

虽然 UDP 协议本身是无连接且无需认证的，但许多基于 UDP 协议的服务却需要认证，这样的服务无法作为反射器。因此，从流量中提取的具备放大特性的数据包样本，还需要进行可反射性验证。

在具体判断方法上，使用流量分析的方法直接判断“交互”中存在的身份验证行为时，存在准确率不足的问题，具体表现在：1）识别能力受算法和训练样本的影响较大，对未知行为识别存在较大偏差；2）部分服务具有非授权访问漏洞，即虽然在交互开始时进行了身份验证，但某些功能在未通过验证的情况下仍然会产生正常应答；3）未授权请求可能会产生异常应答，这同样具备反射器的特性。

由于流量分析方法存在如此多的不确定性，为了最大程度地减小漏报率，增加发现反射放大行为的可能，我们最终采用直接重放发包验证的方法：提取触发包的 UDP 载荷作为 payload，用设备本机作为源重新发送该 UDP 请求包到目的 IP，并接收对方的回复数据。图 3 列举了可能出现的 3 种响应结果：1）无响应，服务本身具备身份验证功能，新的请求未通过验证，因此对请求不予理会；2）正常响应，服务不具备身份验证功能，对任何地址发来的请求都会回复相同的内容，这也是最符合预期的情况；3）异常响应，服务具备身份验证功能，对来自未知 IP 的请求不提供服务，但会反馈一个错误信息。如果反馈的错误信息内容很大，远大于请求，则也可能具备反射放大的潜力。因此，针对正常响应和异常响应，统计收到的回复数据大小，计算回复数据与请求数据的比值 f'，f' 与 f 可能不一致，但只要 f' 大于设定的阈值，则认为该流量样本满足反射放大条件。

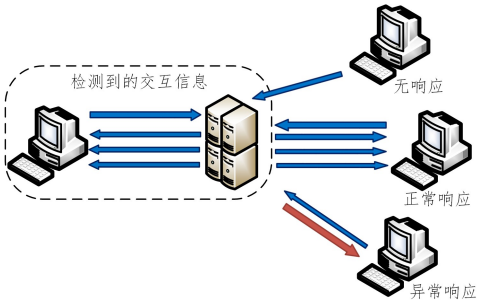

图 3 反射性验证

Fig. 3 Reflective verification

3.4 多包触发验证

尽管目前发现的反射放大攻击都是通过单触发包产生的，我们仍需要考虑存在通过多个请求包才能触发的反射攻击场景。在单包反射验证失败的情况下，我们加入了多包触发反射的验证方法。为了提高验证效率，降低计算力的损耗，我们采取了先判断后定位的两步检测法。

首先，将回复流量前的所有数据包（若太多，则取回复流量前 5 个数据包），分别按时间顺序提取载荷，以本机作为源按序重新发送。统计收到的回复数据大小，若实际回复流量与估算的回复流量大小相近，或是回复流量与请求流量之比仍大于阈值，则判断出数据包中包含可以触发反射放大攻击的请求流量。

在满足可反射性的基础上，定位出精准的请求报文。将所有报文按时间排列的组合方式依次进行反射性测试，筛选出反射系数 f' 最大的数据样本，若其大于阈值，则将其添加到输出结果中。

3.5 设置过滤规则

本文方法能够检测到所有反射放大行为，但针对已知的反射服务，用端口和特征标识匹配的检测方法更加快速准确。因此，为了检测到未知的反射放大行为，在流量获取时，设置合适的捕获规则。过滤掉已知的 UDP 反射放大服务，避免已知服务对检测结果造成的干扰。另外，对于已确定无法反射放大的 UDP 服务，也可以将其过滤掉，以减少在判定过程中的数据处理消耗。

4 实验验证

本文首先在局域网内搭建实验环境进行测试，以验证此方法的准确性和有效性。随后在互联网环境下，选取部分节点对网络流量进行抓取，以进一步分析论证该方法的实际效果。

4.1 实验环境测试

实验环境下，为了检验本文方法对反射服务的发现能力，故暂不对已知反射放大服务进行过滤。在局域网内对 Memcached，Chargen，NTP，DNS，snmp，tftp，ssdp，ws-discover 等 8 类反射放大协议进行测试。后期又加入了 US-CERT 未披露的 Ubiquiti 发现协议（端口 10001）和 DVR DUP 服务（端口 37810）作为测试数据执行反射测试。协议测试结果如表 2 所列。

表 2 协议测试结果

Table 2 Protocol test results

协议	执行反射次数	记录次数	准确率/%
Memcached	100	100	100
Chargen	100	100	100
NTP	100	100	100
DNS	100	100	100
snmp	100	100	100
tftp	100	100	100
ssdp	100	100	100
ws-discover	100	100	100
Ubiquiti	100	100	100
DVRDUP	100	100	100

该方法不依赖反射放大协议的特征指纹，因此，用于测试的反射数据都属于未知样本，尤其是后来添加了近一年新发现的两种反射放大协议，并在实验环境下成功检测并提取出所有反射放大行为，做到出现即发现，充分证明了该方法识别检测的有效性。

4.2 互联网环境测试

互联网环境下，在多个节点抓取 UDP 流量，每个节点每次抓取 100 M UDP 流量存为一个 pcap 文件。在抓取的流量中选取 100 份作为测试样本，用该方法执行测试。

在约 10000 MB 的流量中，检测出反射放大行为如表 3 所列。

表 3 互联网环境下的检测结果

Table 3 Internet environment test results

协议	记录次数	实际次数	准确率/%
Memcached	31	31	100
Chargen	65	65	100
NTP	54	54	100
DNS	876	876	100
snmp	128	128	100
ssdp	143	143	100

为了进一步确定检测的准确性，对于检测出的反射放大行为，在对应的流量样本中定位并进行人工核实，确认无误。

在互联网环境下，由于获取流量的节点数量有限，流量

样本缺乏多样性，因此尚未检测出新型反射放大协议，但能够全部检测到已知的反射放大行为，一定程度上验证了该方法的可行性。

4.3 处理能力测试

从前期实验的结果来看，该方法能够准确有效地提取所有存在 UDP 反射行为的流量样本，以发现对应协议存在 UDP 反射放大威胁。而本文方法的最终目的是通过流量检测发现新型 UDP 反射放大攻击，在实际运用中，大量的流量检测才是发现新型 UDP 反射放大攻击的关键。因此，对于流量的处理速度则也是该方法实用性的重要衡量标准之一。

由于本文方法通过主动发包的方式来验证服务的可反射性，等待服务响应以及判定超时都需要一定的等待时间。因此，检测程序多线程执行效率应高于单线程效率。

在执行检测程序时，将超时判定设置为 2 s，分别记录了 100 个流量样本（每个文件 100 MB）在单线程和多线程（10 线程）条件下的执行时间。实验结果如表 4 所列。

表 4 执行时间

Table 4 Execution time

（单位：s）

运行模式	最短时间	最长时间	平均时间
单线程	1565	5453	3456
多线程	231	703	412

可以看到，多线程执行时间远短于单线程执行时间。另外，在上述的测试中，采用的均是单反射包验证法，而为了增加发现新型反射放大协议的可能，实际使用中，应采用多包反射的验证方式。因此，在多线程的执行模式下，用同样的 100 份流量样本，再次测试了多包反射的判定条件下的执行时间，以及添加了过滤规则后的执行时间，过滤规则为排除已知的 19 种存在 UDP 反射放大功能的协议。测试结果如表 5 所列。

表 5 多包反射执行时间

Table 5 Multi-packet reflection execution time

运行模式	平均时间/s	过滤后平均时间/s	过滤后平均处理速度/(MB/s)
单包反射	412	102	0.98
多包反射	1143	231	0.43

在使用了过滤规则的条件下，UDP 流量处理速率大约如下：单包反射检测为 0.98 MB/s，多包反射检测为 0.43 MB/s。而互联网中 UDP 流量远少于 TCP 流量，且该方法对时效性要求不高，因此适用于大部分应用场景。对于少部分流量较大、程序无法及时处理的场景，可采用动态添加过滤规则的方法。即在检测的同时，记录耗时最长的协议类型，每一轮检测后，对耗时最长的协议执行人工分析，基本确认该协议是否具备反射放大的潜能，然后将该协议添加到过滤列表中，以此来不断提升检测速率。

结束语 该方法能够对流量中存在的流量反射放大行为进行有效检测，并以此来发现新的 UDP 反射放大协议，因此大规模高质量的流量获取既是关键也是限制所在。网络节点、网络关口和包含物联网设备的局域网是流量获取的较好场所。只有多方参与协作、共同发力，才能有效地发现新型反射放大协议。在不具备大规模检测的条件下，小范围部署和检测同样具备发现的可能，但要注重流量采集的多样性。另外，由于采用了主动发包探测的方式，在处理大规模流量时，提高执行效率也是需要考虑的问题。文中提到了对消耗运算资源最多的协议进行人工核验后过滤以提升效率，该方法虽然具备一定的可行性，但需要人工参与，在这方面还可以尝试探索其他更好的方法。

网络安全是一个动态的对抗过程，DDoS 防御也是如此。遭到攻击后的补救固然很有必要，但采取主动防御的策略，提前发现隐患，在攻防对抗中取得先机，让攻击方法无所遁形才是更好的应对之策。为此，只有建构全面细致的安全防护体系，强化监测和应对能力，才有可能将威胁扼杀于萌芽。

参 考 文 献

[1] PRINCE M. Technical Details Behind a 400Gbs NTP Amplification DDos Attack [EB/OL]. (2014-02-13) [2021-10-12]. https://blog. cloudflare. com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/.

[2] NEWMAN L H. GitHub Survived the Biggest DDoS Attack Ever Recorded [EB/OL]. (2018-03-01) [2021-10-12]. https://www. wired. com/story/github-ddos-memcached/?utm_source=quora.

[3] US-CERT. UDP-Based Amplification Attacks [EB/OL]. (2019-12-18) [2021-10-12]. https://www. wired. com/story/github-ddos-memcached/? utm_source=quora.

[4] PAXSON V. An analysis of using reflectors for distributed denial-of-service attacks [J]. ACM SIGCOMM Computer Communication Review, 2001, 31(3): 38-47.

[5] ROSSOW C. Amplification Hell, Revisiting Network Protocols for DDoS Abuse [C] // Proceedings of the 2014 Network and Distributed Systems Security Symposium (NDSS 2014). 2014: 23-26.

[6] XU Y, KENSHIN. CLDAP is Now the No. 3 Reflection Amplified DDoS Attack Vector, Surpassing SSDP and CharGen [EB/OL]. (2017-11-01) [2021-10-12]. https://blog. netlab. 360. com/cldap-is-now-the-3rd-reflection-amplified-ddos-attack-vector-surpassing-ssdp-and-chargen-en/.

[7] BARRY G. Memcached on port 11211 UDP & TCP being exploited [EB/OL]. (2018-02-27) [2021-10-12]. https://www. senki. org/memcached-on-port-11211-udp-tcp-being-exploited/.

[8] RESPETO J. New ddos vector observed in the wild: wsd attacks hitting 35/GBPS [EB/OL]. (2019-09-27) [2021-10-12]. https://blogs. akamai. com/sitr/2019/09/new-ddos-vector-obser-ved-in-the-wild-wsd-attacks-hitting-35gbps. html.

[9] ZHOU W F. Research on detection and response technology of udp reflection attack [D]. Nanjing: Southeast University, 2018.

LU Xuan-ting, born in 1992, postgraduate. His main research interests include network device security and network attack detection.

LIU Sheng-li, born in 1973, Ph.D professor. His main research interests include network device security and network attack detection.