计算机科学
COMPUTER SCIENCE

基于主被动结合的新型UDP反射放大协议识别方法

陈宏伟, 尹小康, 盖贤哲, 贾凡, 刘胜利, 蔡瑞杰

引用本文

陈宏伟, 尹小康, 盖贤哲, 贾凡, 刘胜利, 蔡瑞杰. 基于主被动结合的新型UDP反射放大协议识别方法[J]. 计算机科学, 2024, 51(8): 412-419.

CHEN Hongwei, YIN Xiaokang, GAI Xianzhe, JIA Fan, LIU Shengli, CAI Ruijie. New Type of UDP Reflection Amplification Protocol Recognition Method Based on Active-Passive Combination [J]. Computer Science, 2024, 51(8): 412-419.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500227

基于主被动结合的新型 UDP 反射放大协议识别方法

陈宏伟　尹小康　盖贤哲　贾　凡　刘胜利　蔡瑞杰
信息工程大学　郑州 450001
(1134673436@qq.com)

摘　要　反射放大攻击因具有优质的流量倍增能力和反追踪溯源能力正逐步成为主流的 DDoS 攻击手段。近年来不断涌现以 OpenVPN 等物联网协议为代表的新型 UDP 反射放大攻击方法,并且呈现出多协议组合反射放大的趋势。然而,当前 UDP 反射放大检测方法存在检测结果不准确、检测效率不足等问题。针对上述问题,为提升 UDP 反射放大检测能力,提出了一种基于主被动结合的新型 UDP 反射放大协议识别方法。首先,通过主动探测的方法获取已知的物联网反射放大协议流量,并将其作为实验数据集;其次,在流量自动化分析过程中使用双重阈值判定和多元特征匹配方法捕获未知的反射放大协议和触发方式;最后,通过重放的方式进行验证。实验结果表明,该方法可有效检测 UDP 反射放大流量,精度达到 99.88%,并且发现了 QUIC 协议潜在的反射放大能力,有效提升了反射放大攻击的防护能力。

关键词:DDoS 攻击;UDP 反射放大;主被动结合;主动探测;流量分析
中图分类号　TP393

New Type of UDP Reflection Amplification Protocol Recognition Method Based on Active-Passive Combination

CHEN Hongwei,YIN Xiaokang,GAI Xianzhe,JIA Fan,LIU Shengli and CAI Ruijie
Information Engineering University,Zhengzhou 450001,China

Abstract　Reflection amplification attack has gradually become a mainstream DDoS attack method because of its high-quality traffic doubling ability and anti-traceability capability. In recent years,new UDP reflection amplification attack methods represented by Internet of Things protocols such as OpenVPN have emerged constantly,showing a trend of multi-protocol combination reflection amplification. However,current UDP reflection amplification detection methods have some problems,such as inaccurate detection results and insufficient detection efficiency. In order to improve the UDP reflection amplification detection capability,a new type of UDP reflection amplification protocol recognition method based on active-passive combination is proposed. Firstly,the known Internet of Things reflection amplification protocol traffic is obtained through active detection method and is used as the experimental dataset. Secondly,in the process of automatic traffic analysis,dual threshold determination and multivariate feature matching are used to capture the unknown reflection amplification protocol and trigger mode. Finally,verify the authenticity through replay. Experimental results show that this method can effectively detect the reflection amplification traffic targeting UDP protocol,with an precision of 99.88%. The potential reflection amplification ability of the QUIC protocol has been discovered,effectively improving the protection ability against reflection amplification attacks.

Keywords　DDoS attack,UDP reflection amplification,Active-Passive combination,Active detection,Traffic analysis

1　引言

相比传统的基于僵尸网络的 DDoS 攻击,UDP 反射放大攻击无需组建僵尸网络,控制过程相对简单,成本较低,且具有放大效果显著、追溯困难的特点,近年来已成为 DDoS 攻击的主流[1]。2013 年 3 月,欧洲的反垃圾邮件公司 Spamhaus 网站遭受了峰值达到 300 GB/s 的反射型 DDoS 攻击,导致全球互联网大堵塞[2]。2022 年 3 月,国际拉美地区某客户遭受了 UDPFlood 攻击,黑客利用 Mitel 公司生产的 MiCollab 和 MiVoice Business Express 协作系统上运行的 TP-240drv 驱动程序存在的漏洞(CVE-2022-26143)发送大量带有被害者 IP 地址的 UDP 数据包给放大主机,然后放大主机对伪造的 IP 地址源做出大量回应,从而形成反射型 DDoS 攻击,放大倍数达到 40 亿倍,创下历史新高[3]。因此,开展基于 UDP 的反射放大协议发现相关研究对防御 DDoS 攻击具有重要价值。

UDP 是面向无连接的协议,通常不对来源请求进行安全性校验就可以直接传输数据。利用这一特性,攻击者可以轻易地将 UDP 请求报文中的源地址伪造成被攻击主机的地址,然后向互联网某些服务开放的服务器发送请求报文,数倍于请求报文的回复报文被发送到被攻击主机,使其带宽耗尽,

到稿日期:2023-05-30　返修日期:2023-10-16
通信作者:蔡瑞杰(wsxcrj@163.com)

达到拒绝服务的目的，从而实现 UDP 反射放大攻击，场景如图 1 所示。Rossow 等[4]提出了 BAF(带宽放大因子)和 PAF(数据包放大因子)的概念，将其作为反射放大的评价标准，并且发现 NTP，CharGen 和 SSDP 等 14 种流行的基于 UDP 的网络协议适用于反射型 DDoS 攻击。Li[5]讨论了基于流记录进行扫描检测的可行性，在此基础上设计了一个以流记录为分析数据源的基于端口匹配的水平扫描检测算法，将该算法部署到 NBOS 平台上，并检测到了大量的 TCP SYN 和 UDP 水平扫描。Lu 等[6]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，从日常网络流量中筛选出符合反射放大特性的流量样本，然后通过流量重放验证样本是否具备可重复性。

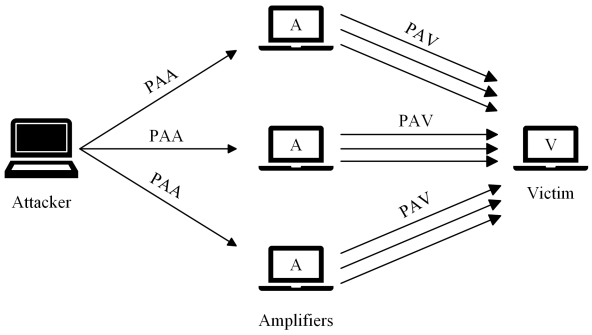


图 1 UDP 反射放大攻击场景

Fig. 1 UDP reflection amplification attack scenario

然而，当前的研究中存在如下问题：1)当前研究成果面向 NTP，CharGen 和 SSDP 等发现时间较早的 UDP 协议，缺乏对近年来新发现的 UDP 反射放大协议的研究；2)当前研究成果将 BAF 当成单一的反射放大评价标准，忽略了 PAF，并且传统 BAF 计算方法不够合理；3)当前研究成果集中在对已知协议的检测，对通过检测发现新型 UDP 反射放大协议的研究不足。

针对上述问题，本文提出了一种基于主被动结合的新型 UDP 反射放大协议发现方法。通过构造带有反射放大 Payload 的请求报文对网上收集的节点资源进行探测验证，在判定有效放大器的同时提取反射放大流量，然后通过双重阈值判定和多元特征匹配的方式对 UDP 流进行检测识别。同时应用该方法对实网流量进行筛选和重放验证，最终发现潜在的新型反射放大协议和触发方式。

本文的贡献如下：1)构建了包含 OpenVPN，WS-Discovery 等多种近年来新发现的反射放大协议的数据集，有利于归纳梳理最新的反射放大流量特征；2)提出了一种新的 BAF 计算方法用于解决 IP 分片问题，以应对未来新型反射放大检测；3)提出了一种基于主被动结合的新型 UDP 反射放大协议识别方法，能实现对已知和未知 UDP 反射放大流量的检测。

2 相关工作

2.1 UDP 反射放大计算方法的改进

文献[4]介绍了 BAF 和 PAF 是反射攻击放大因子的测量单位，其计算式如式(1)、式(2)所示：

$$BAF=\frac{len(UDP\,payload)\text{amplifier to victim}}{len(UDP\,payload)\text{attacker to amplifier}} \tag{1}$$

$$PAF=\frac{\text{number of packets amplifier to victim}}{\text{number of packets attacker to amplifier}} \tag{2}$$

反射放大可以分为流量倍增攻击和有效载荷放大攻击。流量倍增攻击会放大数据包的数量，早在 2000 年，Othman[7]就已经将 Smurf 攻击和 Fraggle 攻击归纳为流量倍增攻击。有效载荷放大会放大数据包的大小，从攻击者的角度来看，发送的是小规模的查询，接收的是较大的响应。文献[4]按照式(1)和式(2)的计算方法找到了 14 个基于 UDP 的反射放大协议，并且统计了对应的 BAF、PAF 和利用场景，如表 1 所列，其中 all 表示所有放大器的平均 BAF，50% 和 10% 表示使用最严重的 50% 或 10% 的放大器的平均 BAF。

表 1 各协议带宽放大因子

Table 1 Bandwidth amplifier factors of each protocol

Protocol	BAF(all)	BAF(50%)	BAF(10%)	PAF(all)	Scenario
SNMP v2	6.3	8.6	11.3	1.00	GetBulk request
NTP	556.9	1083.2	4670.0	3.84	Request client statistics
DNS(NS)	54.6	76.7	98.3	2.08	ANY lookup at author. NS
DNS(OR)	28.7	41.2	64.1	1.32	ANY lookup at open resolv.
NetBios	3.8	4.5	4.9	1.00	Name resolution
SSDP	30.8	40.4	75.9	9.92	SEARCH request
CharGen	358.8	n/a	n/a	1.00	Character generation request
QOTD	140.3	n/a	n/a	1.00	Quote request
BitTorrent	3.8	5.3	10.3	1.58	File search
Kad	16.3	21.5	22.7	1.00	Peer list exchange
Quake 3	63.9	74.9	82.8	1.01	Server info exchange
Steam	5.5	6.9	14.7	1.12	Server info exchange
ZAv2	36.0	36.6	41.1	1.02	Peer list and cmd exchange
Sality	37.3	37.9	38.4	1.00	URL listexchange
Gameover	45.4	45.9	46.2	5.39	Peer and proxy exchange

由于近年来新发现的 UDP 反射放大请求报文负载较小，有的甚至为空，原先的 BAF 计算方法未将以太网帧、IP 报头，以及 UDP 首部字段算入报文负载之中，容易产生误差，最终结果不能客观反映各协议的反射放大效果；同时，有些协议单个回复报文长度较大，会产生 IP 分片的报文，这会被常用的端口匹配的方式所忽略；另外，实验发现有些协议涉及到多包触发问题，即在一次 UDP 反射放大过程中，存在发送多个请求报文的情况。上述问题均对原先的 BAF 计算方法形成了巨大的挑战。因此，为了真实客观地反映反射放大的效果，本文将滑动时间窗口算法套用在 BAF 的计算式上，并采用请求与响应全报文负载的方式，重新定义了 BAF 计算方法以解决上述问题。

原先的反射放大几乎全是有效载荷放大攻击，形式较为单一，因此以往的研究成果将 BAF 作为反射放大的唯一评价标准，但是近年来新发现的许多物联网反射放大协议有流量倍增攻击的特点，即黑客发送一个请求报文会返回多个响应报文。本文为了解决这一问题，将 PAF 引入反射放大计算指标中，扩充了对流量倍增攻击这一反射放大形式的检测。

2.2 反射放大协议的识别方法归纳

当前反射放大攻击主要是基于 UDP 协议，虽然 TCP 的 3 次握手会阻碍反射放大的实现，但是仍有部分 TCP 协议可用于反射放大攻击。反射放大协议的识别方法主要可以分为以下 3 种：基于人工协议分析的识别方法、基于实网流量捕获分析的识别方法和基于模糊测试的识别方法。

2.2.1 基于人工协议分析的识别方法

基于人工协议分析的识别方法曾是最主流的反射放大识别方法，其针对不同的协议和公共服务可以采用不同的分析策略。对于网络服务协议，可以研究对应的 RFC 文档和开源代码实现，许多经典的反射放大协议都是通过阅读 RFC 文档中定义的消息格式发现的，通过构造一些诸如查询请求之类的操作来触发反射放大。对于游戏服务器，可以在游戏供应商提供的公共 API 文档中发现可能的放大向量。

早在 2001 年，Paxson 等[8]就已经论述 ICMP，TCP，UDP，DNS，SNMP 和 HTTP 等协议在假冒源地址的 DDoS 攻击模型下具备反射放大的潜在能力，可以利用协议中字段的设计缺陷生成发射放大流量。

2014 年，Prolexic 组织发表了技术白皮书[1)]，分析了 CharGen，DNS，NTP，SNMP 等协议的反射攻击场景和造成流量放大的具体实施方案，并尝试给出了攻击者的攻击脚本，给了模拟探测实验一些参考。

2021 年，Bock 等[9]在 USENIX 大会上正式提出这种利用中间盒发起的新型攻击手法：攻击者可以利用部分网络中间盒在 TCP 会话识别上的漏洞，实现一种全新的 DDoS 反射放大攻击。与 2018 年出现的利用协议栈发起的 TCP 反射无法放大攻击流量的情况不同，这种新型攻击实现了基于 TCP 协议的流量放大效果。

然而，随着物联网的普及，近年来越来越多的攻击者采用物联网设备的协议漏洞，对目标进行反射放大攻击。研究人员分析协议设计缺陷的时间成本过大，单一地通过基于人工协议分析的识别方法来发现反射放大协议已不能满足当今的研究需要。

2.2.2 基于 DDoS 流量捕获分析的识别方法

随着近年来实网反射放大攻击事件的不断涌现，通过 DDoS 流量捕获分析的方法已成为反射放大协议识别的主流方法。当黑客伪造的反射请求对监控系统进行攻击时，监测节点会实时上报攻击事件到安全态势中心，并采集攻击流量，提取攻击请求指令，这能帮助安全人员复盘未知的反射放大攻击，并进行重放验证。

2018 年，百度安全智云盾团队便展开了针对网络协议漏洞进行 DDoS 攻击的“捕获行动”，并在次年先后完成了对 WS-DD，CoAP 及 IPMI 这 3 种全新 DDoS 攻击方式的 2 秒快速识别及流量实时隔离清洗，有效抵御了上述 DDoS 攻击事件，有力保障了用户的网络安全。

2020 年，腾讯安全宙斯盾团队对游戏行业某云客户遭受到的大流量 DDoS 攻击进行跟进溯源研究，在对抓取的攻击样本进行深入分析之后，发现其是一种新的 UDP 反射放大攻击手法。该次新型反射攻击利用 IoT 网络摄像头 DVR 服务完成，服务端口为 37810，若将请求响应的包头以及网络间隙考虑在内，则放大倍数约为 6。

使用基于 DDoS 流量捕获分析的识别方法，可以识别多个新型反射攻击类型，近年来发现了多种物联网反射放大协议。许多安全公司与团队都应用该技术进行分析研究与安全预警，提升了抗 DDoS 反射攻击的能力。

2.2.3 基于模糊测试的识别方法

反射放大攻击方式种类较多，不同反射攻击的载荷差异较大，仍然有许多新型反射放大类型难以识别。近年来开始出现运用模糊测试的方法对路由器节点、物联网设备及公开服务进行深入挖掘，通过 Fuzz 算法生成大量的反射请求数据包，对于捕获到大量响应包的反射攻击，精准生成触发 Payload。

2021 年，Soo-Jin 等[10]设计应用了 AMPMAP 工具，采用智能采样策略对 6 种基于 UDP 的协议（DNS，NTP，SNMP，Memcached，CharGen，SSDP）和 3 种协议（QOTD，Quake，RPCbind）进行测量，对大规模的搜索空间进行检索，发现了反射放大查询新方式与新变种，证明了反射放大因子的可变性，发现过往低估了反射放大风险。

2022 年，Krupp 等[11]设计应用了 AMPFUZZ 工具，首次系统地在 UDP 服务中利用了协议无关的方式寻找放大型攻击向量。AMPFUZZ 基于目前最先进的灰盒测试技术，在新的 UDP 可感知基础上，显著提升了性能。在 28 个 Debian 服务上进行了测试，发现了 7 个未知和 6 个未报告的放大型漏洞。

基于模糊测试的识别方法证明，过往低估了反射放大 DDoS 的风险，使用该类方法可以帮助研究人员发现更多反射放大协议和新的反射放大查询模式。

当前的研究成果虽然可以准确地捕获反射放大攻击流量以及还原反射放大攻击场景，但是缺乏对新型 UDP 反射放大协议的研究，无法通过流量分析主动发现新型的 UDP 反射放大协议，同时反射放大的计算方法不够合理。为了解决上述问题，本文提出了基于主被动结合的新型 UDP 反射放大协议识别方法，将主动探测与流量分析相结合，通过构建指纹库对公网已知的 UDP 反射放大特征进行收集，通过构造反射放大请求报文获取大量样本，经过预处理之后对样本数据进行 BAF+PAF 双重阈值检测验证，并运用该检测方法对实网流量进行挖掘，通过 Port+Payload 多元特征匹配方法筛选出符合条件的新型反射放大协议和触发方式流量，通过重放验证之后，将新发现的指纹加入指纹库。

1) https://vdocuments.mx/an-analysis-of-drdos-snmp-ntp-chargen-reflection-attacks-white-paper-a4-042913.html?page=1

3 基于主被动结合的新型 UDP 反射放大协议识别方法

3.1 系统架构设计

为了解决当前研究中存在的问题，本文提出了一种基于主被动结合的新型 UDP 反射放大协议识别方法。该系统分为 6 个模块，即指纹库构建模块、样本获取模块、数据预处理模块、阈值检测模块、特征匹配模块和重放验证模块，如图 2 所示。指纹库构建模块对已知的 UDP 反射放大类型和特征进行动态指纹学习，不断更新数据库内容；样本获取模块面向近年来新发现的物联网反射放大协议，获取了 IP 分片的响应报文，收集的流量更能够体现反射放大流量特征；数据预处理模块筛选出符合条件的 UDP 反射放大流量，提高了海量数据的处理效率；阈值检测模块提出了全新的 BAF 计算方法，并采用 BAF 和 PAF 的双重阈值检测方法，提高了 UDP 反射放大检测的准确率；特征匹配模块将符合条件的 UDP 反射放大流量的 Port 和 Payload 特征与指纹库对应特征进行比较，从而判定该流量是否为新型反射放大协议和触发方式流量；重放验证模块对筛选出的符合条件的新型反射放大协议和触发方式流量进行重放验证，降低了误报率。

3.2 指纹库构建

攻击者在寻找新的 UDP 反射放大方式上不再拘泥于传统公共服务，而是对暴露在公网，并且具备一定规模的 UDP 服务都进行尝试利用，并将其作为反射源。通过查阅多方资料，发现现网公开的 UDP 反射放大类型多达 50 多种，包括各类型协议、服务、设备以及游戏等，并且其中有些类型有着多种触发方式。因此，本文构建了 UDP 反射放大多源指纹库，采用动态指纹学习的方式通过反射型 DDoS 事件曝光、安全团队披露等多种方式不断收集新的指纹特征，在测试环境中复现攻击利用场景，确认该手法具备反射放大能力后向指纹库添加新特征。

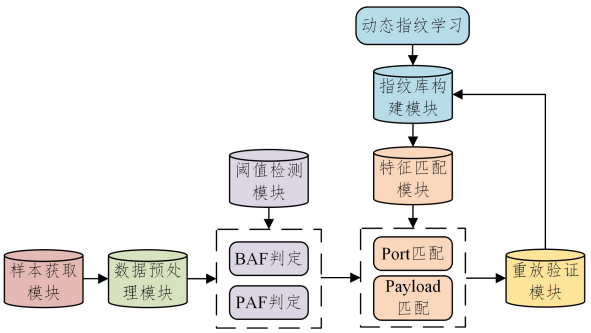


图 2 系统架构

Fig. 2 System architecture

3.3 样本获取

由于不同协议的 UDP 反射攻击原理不尽相同，相应的流量检测算法也要随之调整，因此在样本获取阶段就要收集具有代表性的具备不同特征的流量。本文选取了近年来发现的 OpenVPN，WS-Discovery，CoAP 和 Ubiquiti 这 4 种物联网反射放大协议，其中部分协议的响应报文包含 IP 分片报文，可以代表最新的 UDP 反射放大流量特征。样本获取模块流量的来源分为两部分：1）主动探测得到的流量。本文通过 OSINT（开源网络情报）搜索获取了大量的不同协议及服务的 IP 地址资源，并通过脚本将带有 Payload 的请求报文自动化地发送到对应的 IP，并将交互的流量保存为 pcap 文件。2）实网捕获的流量。本文通过在电信骨干网络节点和校园网骨干网络节点部署流量行为观测系统，获取互联网中海量的流量数据。

3.4 数据预处理

由于海量的流量中夹杂着大量的 TCP 报文等不相关的数据，因此需要对数据进行预处理。为了降低设备负载和提升数据处理效率，将样本获取模块产生的流量按照 100 MB 大小分割保存后发送到系统的数据预处理模块。对于单个文件，通过 Scapy 库加载文件，剔除非 UDP 流量及丢包严重的流量，按照 UDP 流的模式对数据进行分组筛选并对流数据进行处理，提取各数据包时间、IP、Port、Payload、字节长度等字段信息。

3.5 阈值检测

UDP 协议在进行数据传输之前不需要建立连接，并没有包含数据包排序的机制，这意味着 UDP 发送的数据包在网络传输过程中可能会遇到不同的延迟和丢包情况，这些因素都可能导致数据包以不同的顺序到达接收方。同时，UDP 协议缺少重传机制、拥塞控制和流量控制，因此在传输数据时，一旦网络出现拥塞，就会容易产生丢包或者数据包在传输过程中发生重叠的情况，进一步增加乱序的可能性。

因此，UDP 协议的数据包排序问题给计算反射放大带来了巨大的挑战。本文采用滑动时间窗口算法，以单个请求报文的时间为基准，在 Δt 的时间范围内，假设请求 m 个报文（$m\geqslant 1$），每个请求报文长度为 $len(Rq_i)$，i 表示第 i 个请求报文；响应 n 个报文（$n\geqslant 1$），每个响应报文长度为 $len(Rp_j)$，j 表示第 j 个响应报文，定义 BAF 的计算表达式如式（3）所示：

$$BAF=\frac{\sum_{j=0}^{n} len(Rp_j)}{\sum_{i=0}^{m} len(Rq_i)} \tag{3}$$

将 Δt 时间间隔内的源 IP 和目的 IP 对应交互的通信流量视为单次“交互”流量，其中的正向流量均视为请求流量，对应的反向流量均视为响应流量，并将数据预处理模块得到的数据添加到同一分组，根据数据预处理模块得到的信息计算请求报文总长度、响应报文总长度、请求报文数量和响应报文数量。通过本文新提出的计算公式计算 BAF 和 PAF，对 BAF 和 PAF 进行双重阈值判定，根据近年来新发现的物联网反射放大特征将 BAF 阈值设置为 3，PAF 阈值设置为 2。最终结果分为两种不同情况：1）BAF 和 PAF 均未达到阈值标准，代表流量不符合反射放大特征，丢弃即可；2）BAF 和 PAF 任意一项因子达到阈值，代表流量符合反射放大特征，则判定为反射放大流量。最后，将第 2 种情况的流量导入特征匹配模块进行后续检测。阈值检测流程如算法 1 所示。

算法 1 双重阈值判定算法

输入：UdpStream

输出：null

1. SendData←SendPacketSelect(UdpStream，Δt) /* 从 UDP 流中挑选请求流量，时间间隔设置为 Δts */
2. RecvData←RecvPacketSelect(UdpStream，Δt) /* 从 UDP 流中

```
    挑选响应流量,时间间隔设置为 Δts */
3. for i←1 to I do
4.    SendCount++
5.    SendLen←SendPacketLen(i)
6. for j←1 to J do
7.    RecvCount++
8.    RecvLen←RecvPacketLen(j)
9. if RecvCount>= 2 * SendCount or RecvLen >= 3 * SendLen
   then/* PAF>=2 或者 BAF>=3 时 */
10.   nextStep() /* 进行特征匹配 */
11. else
12.   exit()
13. endif
```

3.6 特征匹配

目前,UDP 反射放大攻击的触发方式都是通过伪造 IP,向反射放大器的某个端口发送精心构造的 Payload,继而达到反射放大效果。本文采用 Port+Payload 的方式,通过 UDP 反射放大多源指纹库提供的指纹对达到双重阈值检测标准的流量进行多元特征匹配,将最终结果分为 3 种不同情况:1)Port 和 Payload 均匹配成功,代表流量特征已在指纹库中,为已知的反射放大流量,丢弃即可;2)Port 匹配成功,Payload 匹配失败,代表流量为已知的反射放大协议,但其是新的触发方式;3)Port 匹配失败,不管 Payload 匹配与否,代表流量为新型反射放大协议。最后,将情况 2)和情况 3)的流量保存,由研究人员进一步分析研判,并导入重放验证模块进行验证。特征匹配流程如算法 2 所示。

算法 2 多元特征匹配算法

```
输入:SelectedStream
输出:New_Method or New_Protocol
1. Port←SelectPort(SelectedStream) /* 从挑选的流量中筛选出端口
   信息 */
2. Payload←SelectPayload(SelectedStream) /* 从挑选的流量中筛选
   出载荷信息 */
3. if Payload in Fingerprint_Database then
4.    if Port in Fingerprint_Database then/* 进行特征匹配 */
5.       exit()
6.    else
7.       print("New_Method")
8.       nextStep() /* 进行重放验证 */
9.    endif
10. else
11.   print("New_ Protocol")
12.   nextStep() /* 进行重放验证 */
13. endif
```

3.7 重放验证

重放攻击又称重播攻击、回放攻击,指攻击者发送一个目的主机已接收过的包,来达到欺骗系统的目的,主要用于在身份认证过程中破坏认证的正确性。由于实网流量存在诸多的不确定性,为了最大程度地减少误报率,发现更为真实的新型 UDP 反射放大协议,本文借鉴该方法的思想对构造好的带有新型反射放大协议和触发方式特征的数据包进行重放验证,相当于对流量进行二次检测,对比观察请求报文和响应报文,计算 BAF 和 PAF,用双重阈值检测方法衡量重放之后的反射放大。最后将重放之后发生反射放大的流量指纹作为新发现的特征加入指纹库。

4 实验验证

本文选择一台能访问互联网的高性能服务器作为请求代理,通过部署 Netcat 向 OSINT 获取的 IP 地址发送带有 Payload 的反射放大数据包,通过安装 Tcpdump 记录 UDP 通信过程的请求报文和响应报文。验证 Payload 的有效性之后,用脚本的方式实现自动化探测和抓包,并且读取经过筛选的报文,在实验环境下测算放大器 BAF 和 PAF 等数据信息。随后将脚本探测所得流量作为数据集加入基于主被动结合的 UDP 反射放大发现系统,以实验测试的方式验证其准确性和有效性。最后选取骨干网络节点获取的大规模实网流量进行验证,发现潜在的新型反射放大协议,进一步分析论证该方法的实际效果。

4.1 放大器测试

寻找有效的放大器是获取 UDP 反射放大样本的基础。本文面向 4 种物联网协议,利用其自身存在的漏洞进行放大器测试,漏洞产生的原因如下。

OpenVPN:当客户端发送出数据包后,若在超时时间内没有收到对应的确认包,则会进行多次数据重传,直到 Socket 超时(默认 30 s),该服务使用 1194 端口。

WS-Discovery:客户端向服务器发送广播消息,设备会以 Soap Xml 格式响应自己的 IP,UUID,EP Address 等信息,该服务使用 3702 端口。

CoAP:客户端发送默认./well-known/core 请求,服务端会返回./well-known/core 的 Uri-path 的 DISCOVERY 响应包,该服务使用 5683 端口。

Ubiquiti:客户端向 Ubiquiti 开放的 AP 发现服务发送数据包,服务器会回复数倍字节的数据包,该服务使用 10001 端口。

根据以上原理,本文利用实验室的高性能服务器,向潜在的放大器发送构造好的请求报文,验证 Payload 的有效性之后,进行大规模放大器获取并计算 BAF 和 PAF 等数值。

4.1.1 可行性测试

根据实验思路,对潜在的放大器进行可行性测试,单个放大器的测试结果如图 3 所示。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.[redacted].45.18	190.[redacted].89.30	DNS	46	Standard query 0x0100[Malformed Packet]
2	0.324423	190.[redacted].89.30	10.[redacted].45.18	DNS	234	Standard query 0x0100[Malformed Packet]

图 3 单个放大器的测试结果

Fig. 3 Test results of single amplifier

图 3 利用 Tcpdump 抓取了客户端和服务器的双向流量,可看出请求与响应数据包数量均为 1,请求报文

大小为 46 字节，响应报文大小为 234 字节，BAF＝234/46≈5.09，数值大于 3，符合本文反射放大评判标准，因此 190.*.89.30 对应的服务器为有效放大器，也验证了请求报文 Payload 的有效性。

4.1.2 实验结果

通过分析选取 Δt＝60 s 进行实验，实验中获取的 4 种协议放大器的 BAF 和 PAF 等信息如表 2 所列。

表 2 列出了各协议的端口号，并且每个协议选取 2000 个潜在放大器，并根据双重阈值判定方法计算各潜在放大器的 BAF 和 PAF，以此区分有效放大器和无效放大器。从实验结果来看，CoAP 协议的反射放大全是返回单个响应包，OpenVPN 协议的反射放大几乎全是返回数个甚至数十个响应包，WS-Discovery 和 Ubiquiti 协议有少部分返回多个响应包，而且其中部分含有 IP 分片的报文，如图 4 所示。

表 2 各协议带宽放大系数

Table 2 Bandwidth amplifier factors of each protocol

协议	端口	潜在放大器数量	有效放大器数量	BAF	PAF
OpenVPN	1194	2000	1071	3.7	5.86
WS-Discovery	3702	2000	306	27.5	1.22
CoAP	5683	2000	608	11.7	1.00
Ubiquiti	10001	2000	1399	4.0	1.01

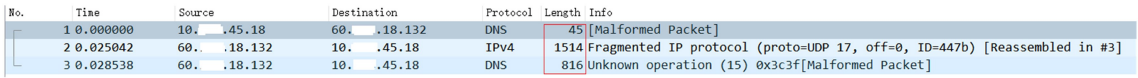


图 4 含有 IP 分片的反射放大响应报文

Fig. 4 Reflection amplification response messages containing IP fragments

4.1.3 分析讨论

WS-Discovery 和 Ubiquiti 协议会出现 IP 分片的响应报文的原因是，两个协议的反射放大响应信息一般承载于单个报文中，并且由于响应信息过长，超过链路层的最大传送单元(MTU)，因此数据分装在两个或更多个较小的 IP 数据包中。以太网的 MTU 为 1500 字节，因此图中 IP 分片长度为 1500＋14(以太网首部长度)＝1514 字节。4 种协议的 BAF 数值有些明显小于网上公开的数值，原因主要有以下两点：1)新的 BAF 计算方式将以太网首部、IP 报头，以及 UDP 报头部分算入负载长度的计算中，与原有的计算方法相比，BAF 明显变小，但改进了计算方法的合理性，更加真实地反映了反射放大的实际情况；2)相关协议的攻击手法在互联网已公开，并且其中一些协议产生的反射放大倍数过大，许多厂商已对其设备进行漏洞修复，降低了反射放大的威胁。

4.2 反射放大协议发现测试

通过实验验证 UDP 反射放大协议发现系统的可靠性是本文实验部分的重点。测试分为 3 个步骤：1)在探测有效放大器的同时记录了与之交互的通信流量，通过 Wireshark 工具自带的 Tshark 和 Mergecap 模块自主构建了反射放大流量数据集，按照 100 MB 大小的标准分割存储数据集，在 Python 环境中导入 Scapy 模块实现对数据集的自动解析和处理，最后自动计算出各协议反射放大的识别率和误报率；2)通过 Tcpdump 在骨干网络节点获取大规模实网流量，并按照 100 MB 大小的标准分割存储，依次输入 UDP 反射放大协议发现系统进行验证；3)采用内含大量真实 DDoS 攻击流量的 CIC-DDoS2019 数据集，将实验结果与同类方法进行比较。

4.2.1 数据集测试

根据测试方法，对本文所提的 UDP 反射放大协议识别方法进行数据集测试，具体测试结果如表 3 所列。实验结果表明，本文方法在 UDP 反射放大检测方面效果较好，原因在于本文结合对新发现的几种物联网反射放大协议的研究制定了阈值检测标准，具备较好的新型 UDP 反射放大协议检测能力。

表 3 数据集测试评价指标

Table 3 Evaluation indicators of dataset testing

协议	端口	*Accuracy*/%	*Precision*/%	*Recall*/%	*F1-score*/%
OpenVPN	1194	97.50	99.50	95.67	97.55
WS-Discovery	3702	99.70	98.08	100.00	99.03
CoAP	5683	100.00	100.00	100.00	100.00
Ubiquiti	10001	99.40	100.00	95.71	97.81

4.2.2 实网流量测试

将实网流量输入 UDP 反射放大协议发现系统，捕获到潜在的新型 UDP 反射放大协议流量，抓包结果如图 5 所示。

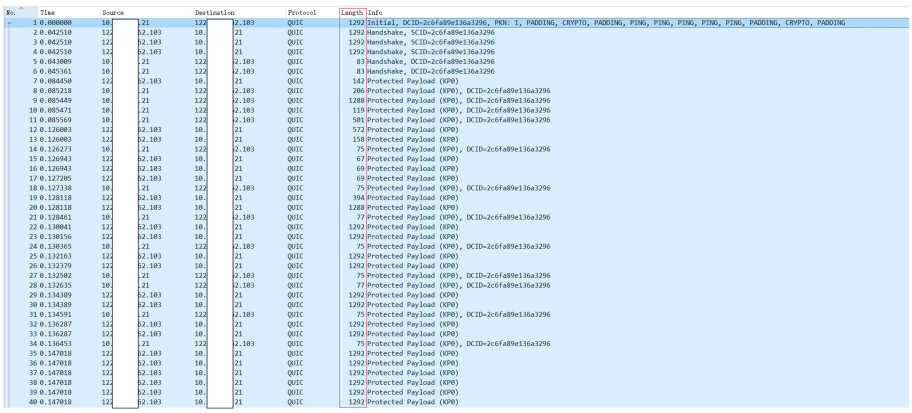


图 5 QUIC 协议反射放大流量

Fig. 5 Reflection amplification traffic of QUIC protocol

通过分析可知，潜在的新型反射放大协议为 QUIC 协议，该协议是谷歌公司制定的一种基于 UDP 的低时延的互联网传输层协议，其网页传输速度优于 TCP 协议。此次捕获流量反射放大效果如表 4 所列，其中 QUIC 协议的 BAF 数值约为 57.4，反射放大效果显著。

表 4 QUIC 协议反射放大效果

Table 4 Reflection amplification effect of QUIC protocol

协议	BAF	PAF
QUIC	57.4	1.83

通过重放验证已发现，该协议通用的反射放大 Payload 的反射放大倍数约为 4.1，但是未能完全有效发挥该协议的反射放大潜能。参考 ISAKMP，OpenVPN 等反射放大协议发现方法，若能分析源码绕过初始认证过程，预计可以完全发挥 QUIC 协议的反射放大潜能。

4.2.3 对比实验结果

本实验将本文方法与 DDoS 流量检测相结合，采用 CIC-DDoS2019 数据集中的 UDP 反射放大流量作为对比实验的数据集，与 4 种同类方法进行对比，实验结果如表 5 所列。其中，文献[12]使用 ID3 算法实现了 78%的最高精度；文献[13]评估了分类器的平均性能，并通过使用引导聚类算法获得了 96.9%的最高精度；文献[14]使用 LSTM-Fuzzy 算法实现的最高精度为 97.89%；文献[15]使用 4 种不同的分类算法进行评估，在使用 GRU 算法的情况下最高精度可以达到 99.83%。与上述 4 种方法相比，本文最高精度可以达到 99.88%，具备一定优势。

表 5 对比实验结果

Table 5 Results of comparative experiment

(%)

方法	*Precision*	*Recall*
文献[12]中的方法	78.00	65.00
文献[13]中的方法	96.90	96.40
文献[14]中的方法	97.89	93.13
文献[15]中的方法	99.83	99.79
本文方法	99.88	99.92

实验结果表明，本文方法对反射型 DDoS 攻击流量的检测效果较好，原因在于本文方法采用双重阈值判定机制，并对 BAF 的计算方法进行优化，能实时检测流量倍增攻击和有效载荷放大攻击。

4.2.4 分析讨论

本文方法对几种物联网 UDP 协议反射放大的识别率较高，但只有 CoAP 反射放大的识别率为 100%，分析原因得知 CoAP 反射放大只会返回单个响应包，且不包含 IP 分片报文，本文方法在对 IP 分片报文的识别上还存在缺陷，有待进一步改进。另外，QUIC 协议的反射放大潜能未能完全发挥的原因是该协议虽然属于 UDP 协议，但是初始连接时的认证与传统的 TLS 基本一致，需要研究 QUIC 认证绕过才能实现对 QUIC 协议的反射放大攻击。

4.3 实验结果总结

通过实验测试，与已有的反射型 DDoS 检测的研究成果进行对比分析发现，本文方法对近年来新发现的 UDP 反射放大协议具备相对较好的检测能力。

1)全新数据集

本文选取了 OpenVPN，WS-Discovery 等 4 种物联网反射放大协议作为探测目标构建数据集，包含 IP 分片的响应报文，可以代表最新的反射放大流量特征。

2)实时检测能力

本文采用了双重阈值判定方法对流量进行实时检测，并且提出了全新的 BAF 计算方法，可以应对未来新出现的 UDP 反射放大类型。

3)新型 UDP 反射放大协议检测能力

本文采用了多元特征匹配的方法，通过与指纹库的特征比对来发现新型 UDP 反射放大协议和触发方式，发现之后采用重放验证的方法进行进一步验证，提升了新型 UDP 反射放大协议的检测能力。

结束语 本文提出的基于主被动结合的新型 UDP 反射放大协议识别方法通过主动探测的方式获取最新的 UDP 反射放大数据集，结合对反射型 DDoS 检测方法的研究，提出了双重阈值判定和多元特征匹配的方法对数据集和实网流量进行检测。通过实验评估，本文方法的实时性和通用性较好，并且发现了 QUIC 协议的反射放大方法，检测效果明显。

本文方法的不足之处在于，对 UDP 新型反射放大协议流量的检测效果较好，对其他类型协议的研究不够深入。下一步将探索基于 TCP 的新型反射放大识别方法，弥补本文方法的不足。

参 考 文 献

[1] SRINIVAS P. Are You Ready to Counter UDP-Based Amplification Attacks? [EB/OL]. (2018-03-27) [2023-03-22]. https://blogs. infoblox. com/company/are-you-ready-to-counter-udp-based-amplification-attacks/.

[2] MATTHEW P. The DDoS That Knocked Spamhaus Offline (And How We Mitigated It) [EB/OL]. (2013-03-21) [2023-03-22]. https://laptrinhx. com/the-ddos-that-knocked-spamhaus-offline-and-how-we-mitigated-it-542830916/.

[3] ALEX F. CVE-2022-26143: TP240PhoneHome reflection/amplification DDoS attack vector [EB/OL]. (2022-03-08) [2023-03-22]. https://blog. cloudflare. com/cve-2022-26143/.

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

[5] LI G. Research of scanning and drdos attack detection based on netflow[D]. Nanjing: Southeast University, 2016.

[6] LUX T, CAI R J, LIU S L. Discovery of unknown UDP reflection amplification protocol based on traffic analysis [J]. Computer Science, 2022, 49(S2): 211000089-5.

[7] OTHMAN R. Understanding the various types of denial of service attack [J]. Business Week Online, 2000.

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

[9] KEVIN B, ABDULRAHMAN A, YAIR F, et al. Weaponizing Middleboxes for TCP Reflected Amplification [C]// 30th USENIX Security Symposium (USENIX Security 2021). 2021: 3345-3361.

[10] SOO-JIN M, YINY C, RAHUL A S, et al. Accurately Measuring Global Risk of Amplification Attacks using Amp Map [C]// 30th USENIX Security Symposium (USENIX Security 2021). 2021: 3881-3898.

[11] JOHANNES K, ILYA G, CHRISTIAN R. AMPFUZZ: Fuzzing for Amplification DDoS Vulnerabilities [C]// 31th USENIX Security Symposium (USENIX Security 2022). 2022: 1043-1060.

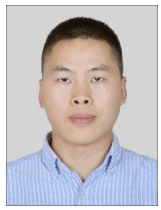
[12] IMAN S, ARASH H L, SAQIB H, et al. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy [C]// 2019 International Carnahan Conference on Security Technology (ICCST). IEEE, 2019.

[13] HUSSAIN Y S. Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks using Machine Learning Classification Techniques [D]. Toronto: University of Toronto, 2011.

[14] MATHEUS P N, LUIZ F C, JAIME L, et al. Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment [C]// IEEE Access. IEEE, 2020: 83765-83781.

[15] SAIF R, MUBASHIR K, SYED I I, et al. DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU) [J]. Future Generation Computer Systems, 2021, 118: 453-466.

CHEN Hongwei, born in 1995, postgraduate. His main research interests include network device security and network attack detection.



CAI Ruijie, born in 1990, Ph.D candidate, lecturer. His main research interests include network security, binary code analysis and vulnerability discovery.

（责任编辑：喻藜）