doi:10.3772/j.issn.2095-915x.2022.05.010

开放科学（资源服务）标识码（OSID）

可编程网络中一种轻量级 DDoS 攻击缓解机制研究

王卓昊[1] 方琦[2] 尹建辉[2] 刘颖[2] 董平[2]

1. 中国科学技术信息研究所 北京 100038；
2. 北京交通大学移动专用网络国家工程研究中心 北京 100044

摘要：[目的 / 意义] 分布式拒绝服务（DDoS）攻击是互联网中威胁性最大且较难防御的攻击之一。针对传统的 DDoS 攻击缓解机制检测较为复杂且缓解策略生成较慢的问题，文中提出了一种基于带内遥测的轻量级 DDoS 攻击缓解机制。[方法 / 过程] 首先，本文将 DDoS 攻击事件视为一种威胁情报，通过情报学方法研究提取普遍的 DDoS 攻击特征；然后，在数据平面利用带内遥测技术检测 DDoS 攻击，从而有效降低网络开销，实现轻量化；最后，控制平面生成限速策略并下发到数据平面交换机，通过源端限速的方法减小攻击流量对网络的影响。[结果 / 结论] 该机制能够及时检测到 DDoS 攻击并有效缓解 DDoS 攻击造成的网络拥塞，并且通过缩短限速阈值中数据包的统计周期可以提高缓解机制的灵敏性，对 DDoS 攻击做出更快的反应。

关键词：可编程网络；DDoS 攻击缓解；带内遥测；拥塞避免；威胁情报

中图分类号：G35

Research on a Lightweight DDoS Attack Mitigation Mechanism in Programmable Networks

WANG Zhuohao[1] FANG Qi[2] YIN Jianhui[2] LIU Ying[2] DONG Ping[2]

1. Institute of Scientific and Technical Information of China, Beijing 100038, China;
2. National Engineering Research Center of Advanced Network Technologies, Beijing Jiaotong University, Beijing 100044, China

Abstract: [Objective/Significance] Distributed denial-of-service (DDoS) attack is one of the most threatening and difficult to defend attacks on the Internet. In response to the problems that traditional DDoS attack mitigation mechanisms are more complex to detect and slower to generate mitigation policies, a lightweight DDoS attack mitigation mechanism based on in-band telemetry is proposed in this paper. [Methods/Processes] First, in this paper, DDoS attack events are considered as a kind of threat intelligence, and the universal DDoS attack characteristics are extracted through intelligence research methods. Then, in-

作者简介 王卓昊（1977-），博士，副研究员，研究方向为计算机应用、信息系统建设，E-mail：wangzh@istic.ac.cn；方琦（2000-），硕士生，研究方向为带内遥测、网络安全；尹建辉（1999-），博士生，研究方向为网络安全、新型网络协议；刘颖（1978-），博士，教授，研究方向为新型网络体系与协议、网络与信息安全；董平（1979-），博士，教授，研究方向为新一代互联网、智慧车联网、移动互联网。

引用格式 王卓昊 , 方琦 , 尹建辉 , 等 . 可编程网络中一种轻量级 DDoS 攻击缓解机制研究 [J]. 情报工程 , 2022, 8(5): 115-126.

doi:10.3772/j.issn.2095-915x.2022.05.010

band telemetry is used in the data plane to detect DDoS attacks, thus effectively reducing the network overhead and achieving lightweighting. Finally, the control plane generates a speed-limiting policy and sends it down to the data plane switches to reduce the impact of attack traffic on the network through the source-side speed-limiting method. [Results/Conclusions] That this mechanism can detect DDoS attacks in time and effectively mitigate the network congestion caused by DDoS attacks, and the sensitivity of the mitigation mechanism can be improved by shortening the statistical period of packets in the speed limit threshold to make faster response to DDoS attacks.

Keywords: Programmable networking; DDoS attack mitigation; in-band telemetry; congestion avoidance; threat intelligence

引言

科技情报行业作为科研和生产服务的行业，大部分业务主要依托网络平台开展实施[1]。随着互联网的应用范围越来越广，信息化进程不断推进，科技情报服务得到了快速发展，随之而来的网络攻击也日渐频繁。频繁的网络攻击以及不断出现的网络安全问题，严重威胁着个人隐私、财产安全，也使科技情报工作面临着安全风险压力，因此，保障科技情报服务应用环境中的网络安全越来越重要。在所有网络攻击中，分布式拒绝服务攻击（DDoS）仍是发生频次最高的攻击方式之一。根据《2021 年全球 DDoS 威胁报告》[2] 统计分析，DDoS 攻击峰值及大流量攻击发生的次数持续增长，攻击手法和行业分布呈现多元化的趋势。报告显示，2021 年共发生 2039 次超 500 Gbps 攻击，其中包含 7 次超 800 Gbps 的攻击，DDoS 攻击对互联网连接系统安全性造成了严重的威胁。

从更加宏观的层面来看，网络空间的安全对抗日趋激烈，传统的安全技术不能全面满足安全防护的需要[3]。安全威胁情报可以让安全分析和事件响应工作处理变得更简单、更高效，是做到持续有效的检测与快速响应的基础。例如，可建立威胁情报的检索，从而实现对安全线索的精准发掘；可利用威胁情报预测现有的攻击线索可能造成的恶意行为，从而有效确定攻击范围；可依赖威胁情报区分不同类型的网络攻击，识别出潜在的高危级别攻击，从而实现对攻击的及时响应[4]。本文利用情报学方法分析了已发生 DDoS 攻击事件特征，发现大多数 DDoS 攻击事件会消耗大量的网络带宽，从而造成网络拥塞。

DDoS 攻击呈现出攻击强度增加、多样性增强、攻击方式更加隐蔽的趋势，对网络安全设备的性能产生了更高的要求。最早出现的基于规则的检测方法虽然速度较快，但很依赖过往发生过的攻击，需要庞大的知识库作为支持。熵是反映网络流量变化的一种特征，因此可以作为攻击检测的一种手段。但作为评判指标的特征选取较为困难，泛用性不高。近年来，基于机器学习的 DDoS 攻击检测逐渐成为主流方向，具有误报率低、准确性高的特点，但该方法往往需要大量的标准化数据集，训练成本高

昂 [5]。总结来看，以上所有的检测手段都需要具体的 DDoS 攻击特征，并且由于检测成本高、存储和计算开销大等问题难以在传统网络中实际部署，无法做到对 DDoS 攻击的轻量级检测。

针对 DDoS 攻击呈现的三个特征，可编程数据平面在处理网络攻击时具有三个关键优势，即数据包的可见性、可扩展性和高速处理能力。可编程网络中将攻击检测功能迁移到控制器中，数据平面仅仅负责执行限速缓解策略，从而大大降低数据平面开销，同时控制器的全局视角也可以快速定位攻击源，采取源端限速的方式减小攻击对网络的危害。带内遥测技术随包测量的方式能够在减小网络开销的同时不影响交换机内部状态，适用于 DDoS 攻击导致网络拥塞的场景。因此在可编程数据平面中进行基于带内遥测的 DDoS 攻击缓解的研究具有一定的价值。

1 相关工作

随着网络安全态势日趋复杂化，威胁情报的研究越显重要。石波等 [6] 通过构建知识图谱的方式解决了安全威胁情报来源不清、难以理解问题，提高了威胁情报的可用性和可读性。传统的入侵检测系统往往只能提取已知攻击的行为特征，无法应对复杂变化的热点网络攻击事件。刘亮等 [7] 利用开源的威胁情报数据设计了一种可以自动生成检测规则的方法，从而有效提升入侵检测系统应对热点攻击事件的能力。

流量攻击是 DDoS 的一种表现形式，因此，高效监控网络流量、快速定位网络故障、迅速启动流量限制是防范 DDoS 攻击的一种思路。在流量检测相关工作中，带内网络遥测（In-band Network Telemetry，INT）是延时性低、细粒度高的一种网络测量方法 [8]。带内网络遥测的思想在 2000 年便已被提出，之后学术界提出了诸多的改进方案，包括在可编程网络环境下的尝试。Wang 等 [9] 在 P4 交换机中设计并实现了一种可以实时或过去跟踪与流数据包匹配的规则。Tang 等 [10] 通过扩展 OpenvSwitch 平台设计了一种运行时可编程的选择性 INT 系统。目前带内网络遥测技术解决了许多网络测量方面的难题，但这些技术仍然存在一定的局限性，带内网络遥测技术仍然处于发展中 [22]。

从拥塞控制方法部署的位置来看，可以分为基于源端的拥塞控制和基于链路的拥塞控制。最早得到了广泛应用的基于源端的拥塞控制方法是 Jacobson[11] 提出的 TCP 拥塞控制，该机制最初由“慢启动”和“拥塞避免”组成，后来在其中增加了“快速重传”“快速恢复”算法 [12]，之后又对“快速恢复”算法进行了改进 [13]。Vo 等 [14] 开发了一种多路径拥塞控制协议 mFast，用于高 BDP 连接场景，实现了负载平衡和吞吐量提高的目标。最初提出的基于链路的拥塞控制方法是 RED 算法 [15]。1998 年，Braden 等 [16] 提出了主动队列管理（active queue management，简称 AQM）的方法。Hao 等 [17] 利用 SDN 技术提出了一种高效的重新路由算法，该算法在缓解网络拥塞和保证网络性能方面表现较好。

为了应对 DDoS 攻击的泛滥，近年来出现了大量的 DDoS 攻击缓解机制。Liu 等 [18] 提出了一个可扩展的抗 DoS 网络架构 NetFence。NetFence 可证明地保证合法的发送者公平地分

doi:10.3772/j.issn.2095-915x.2022.05.010

享网络资源，而无需保持拥塞链路的每主机状态。Piedrahita 等 [19] 提出了一种用于软件定义网络（SDN）的轻量级快速拒绝服务检测和缓解系统 FlowFence，该系统可以有效区分攻击流和合法流。从长远看，DDoS 攻击和防御仍然会处于对立阶段，在建立高效全面的防御缓解体系方面仍将面临许多的困难和挑战。

2 可编程网络中轻量级 DDoS 攻击缓解机制设计与实现

2.1 缓解机制总体方案设计与实现

结合现有的研究工作，本文针对可编程网络中 DDoS 攻击进行研究，提出了一种基于带内遥测的轻量级 DDoS 攻击缓解机制。该攻击缓解机制重点在可编程网络架构下通过设计数据平面和控制平面功能来达到快速准确检测网络拥塞的目的，数据平面和控制平面之间通过 API 进行通信，整体设计结构如图 1 所示。

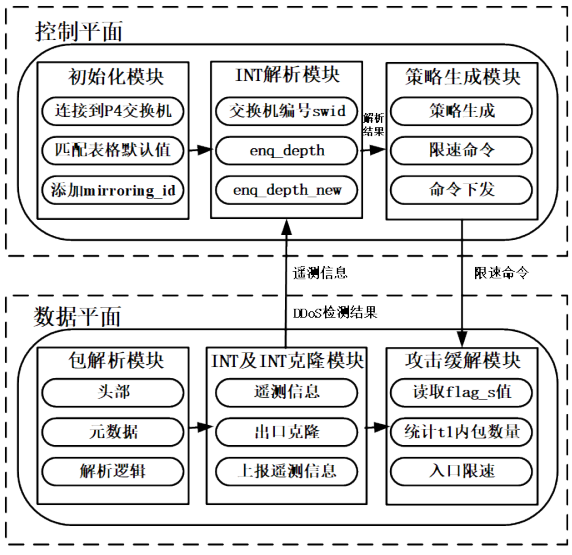

图 1 缓解机制整体架构

数据平面主要负责利用网络遥测检测 DDoS 攻击和执行攻击缓解策略；控制平面主要负责解析数据平面上报的遥测信息，生成并下发相应的限速缓解策略。该缓解机制的整体实现流程如图 2 所示。

在数据平面中，交换机实时接收用户发送的数据流。进入交换机时，数据包被解析后先判断入口交换机有没有收到限速命令，若收到则开始限速，此时在接入交换机入口维护一个计数器统计一段时间 t1 内的数据包数量，若计数器的值未超过阈值则继续匹配数据包，否则丢弃数据包。若入口交换机并未收到限速命令，则直接向数据包中插入遥测包头，之后的每一跳交换机都进行遥测包头的匹配，同时插入和更新所要测量的遥测信息，出口交换机通过遥测包头中的队列深度 enq_depth_new 的值来检测是否发生了 DDoS 攻击。若队列深度大于某一阈值则表示此时检测到了 DDoS 攻击产生的拥塞，通过 P4 语言中原生的 clone 函数克隆数据包，从而将遥测信息上报至控制平面；若队列深度不超过阈值，则由出口交换机删除遥测包头后将数据包发给目的主机，交换机继续接收新的数据包。

在控制平面中，控制器收到带有遥测信息的克隆数据包则表示网络遭受了 DDoS 攻击并产生了拥塞，需要生成并下发限速缓解策略。控制器首先解析收到的遥测信息，读取其中交换机编号 swid 的值，然后根据 swid 的值向与恶意主机相连的接入交换机下达限速命令。控制器继续监听，等待下一次 sniff 克隆数据包和解析遥测信息。

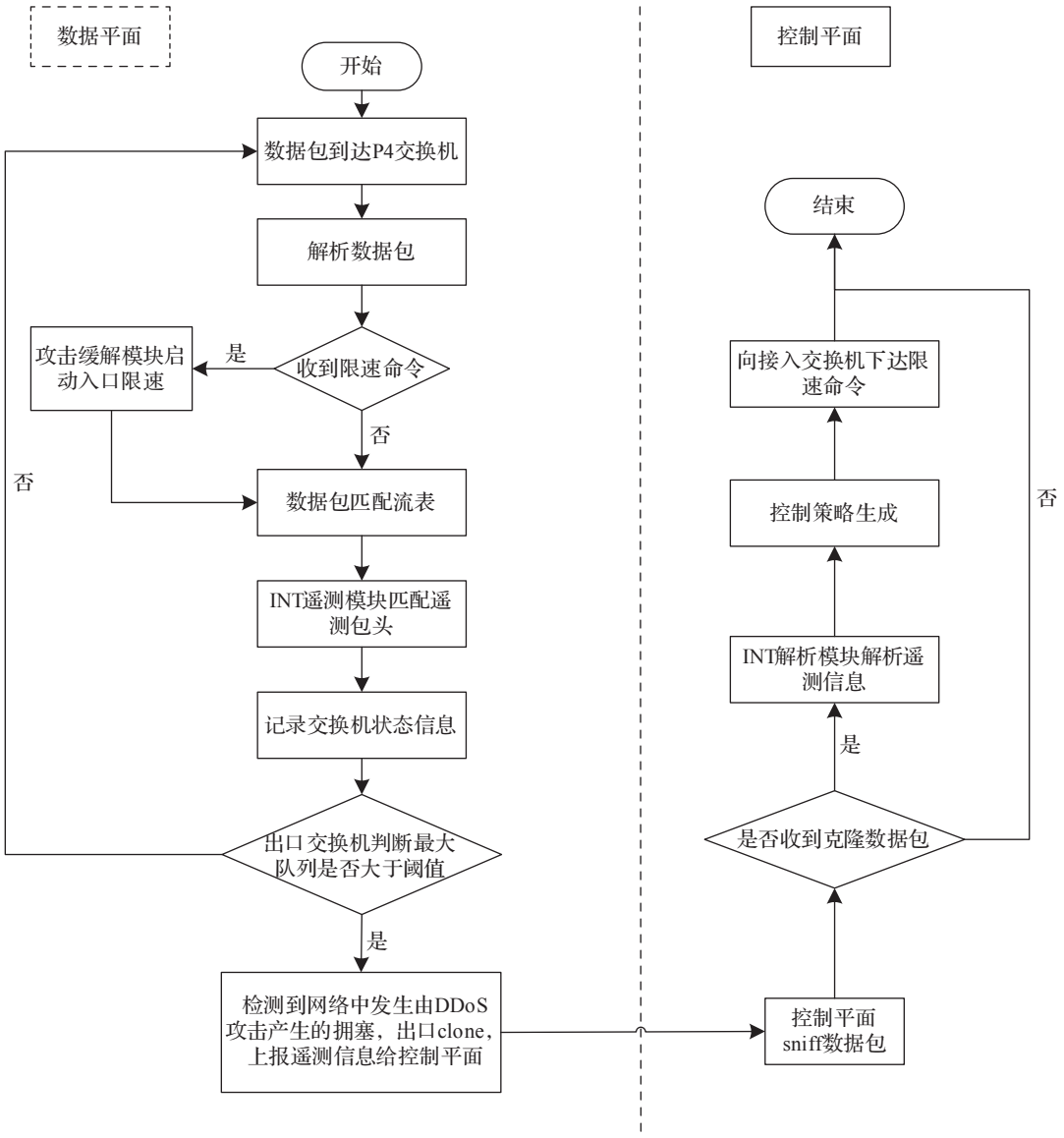

图 2 缓解机制实现流程

2.2 数据平面功能的设计与实现

数据平面的代码都是用 P4 语言 [20] 实现，通过编写 P4 程序代码可以定义交换机对数据包的处理逻辑。数据平面在每台 P4 交换机 [21] 上部署了 INT 功能，用于测量网络中数据包经过的每个网络节点的信息以此来检测 DDoS 攻击，在每台 P4 交换机入口部署了限速算法，通过拥塞控制的手段缓解 DDoS 攻击，在出口交换机部署了克隆算法，当检测到 DDoS 攻击后将遥测信息克隆至控制平面。

（1）数据包解析模块

解析模块在 P4 中通过定义 header、metadata 和 parser 结构实现。P4 数据包的头部包括 Ethernet 头部、Telemetry 头部、IPv4 头部和 UDP 头部，其中 Ethernet 头部、IPv4 头部和 UDP 头部根据当前协议标准进行定义。

数据包解析模块的完整实现流程如图 3 所示。

doi:10.3772/j.issn.2095-915x.2022.05.010

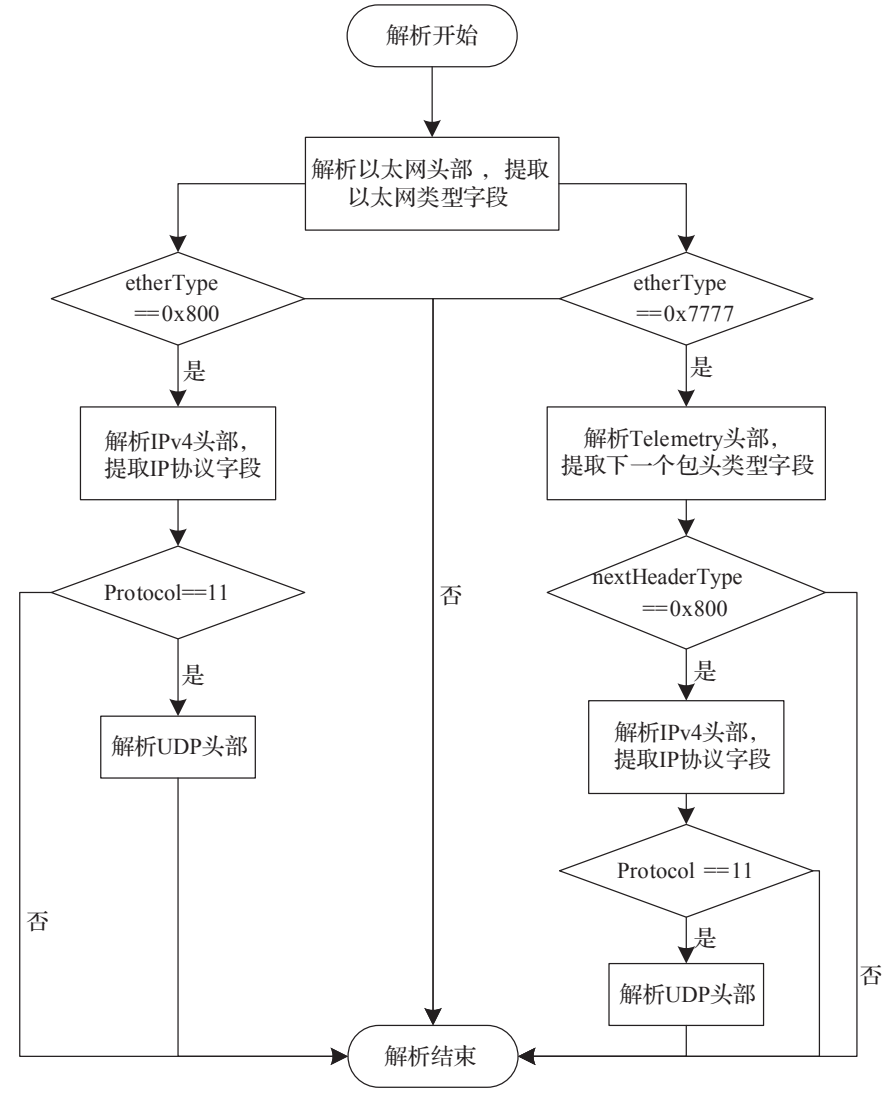

图 3 数据包解析流程

（2）INT 及 INT 信息克隆模块设计与实现

在本设计中主要利用 INT 功能测量交换机编号 swid 和交换机队列深度 standard_metadata.enq_qdepth，通过带内遥测 [16] 将遥测包头里所记录的队列深度更新为较大值。具体过程如图 4 所示。

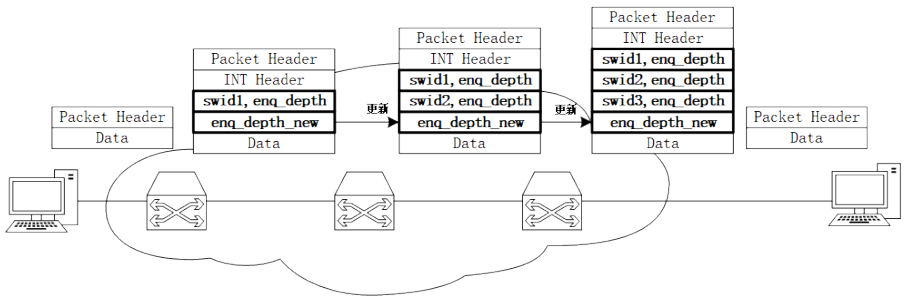

图 4 INT 设计原理

数据包经过交换机时，交换机就将自己的编号和队列深度插入数据包中，并更新 enq_depth_new 字段为队列深度较大值。当数据包到达出口交换机后执行克隆算法，该算法首先判断遥测包头中 enq_depth_new 的值是否大于阈值，若大于阈值则表明网络中某处发生了拥塞，需要将遥测信息克隆至控制平面，由控制器根据最大队列深度值确定发生拥塞的交换机位置；否则在删除遥测包头后将数据包发给目的主机，交换机继续接收新的数据包。具体实现流程如图 5 所示。

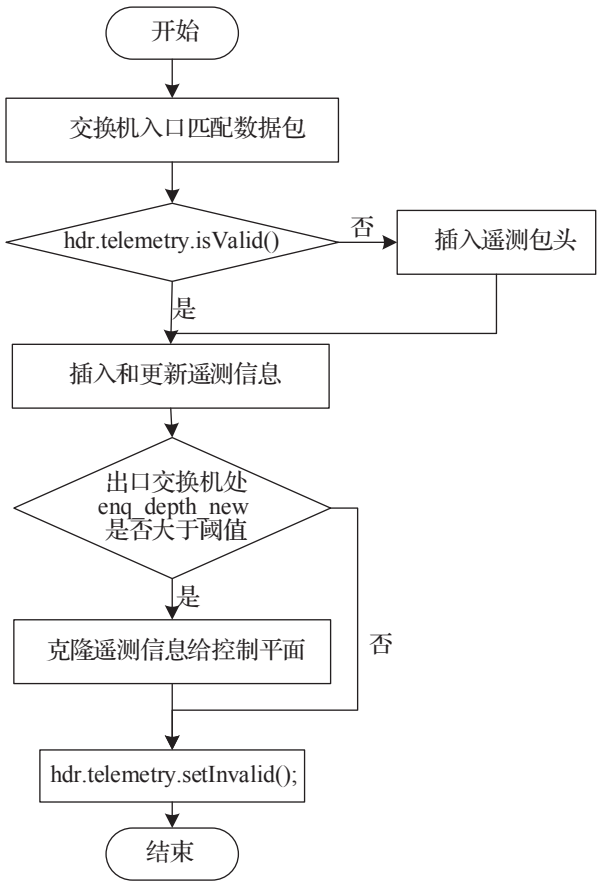

图 **5** **INT** 实现流程

（3）限速模块设计与实现

部署在 P4 交换机入口的限速算法设计思路是，当交换机收到控制器下发的限速命令时，入口启动限速功能，此时通过计数器计算一段时间 t1 内通过交换机入口的数据包的数量。当超过所设定的阈值时，开始丢包，并在超过一段时间 t1 后，计数器清零，重复上述操作，以此限速来达到缓解 DDoS 攻击的效果。若未收到限速命令，交换机执行正常的转发行为。具体过程如图 6 所示。

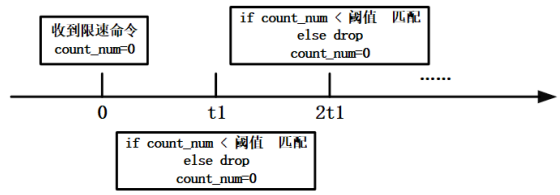

图 **6** 限速算法原理

限速算法的具体流程如图 7 所示。

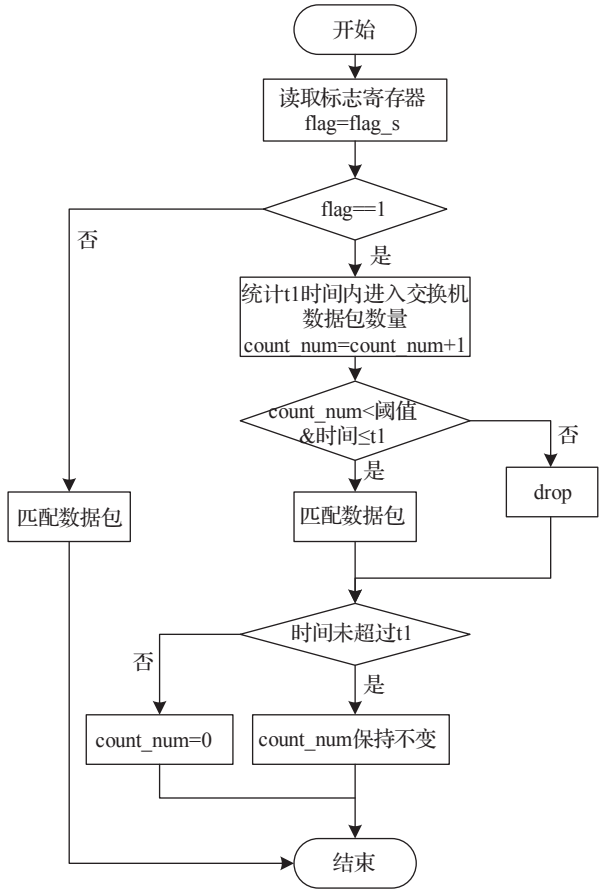

图 **7** 限速算法实现流程

doi:10.3772/j.issn.2095-915x.2022.05.010

2.3 控制平面功能的设计与实现

本机制中控制平面的控制器用来添加镜像，并且通过解析遥测信息来判断是否需要生成并下发限速策略。这里的设计思路是，若控制器收到了带有遥测信息的克隆数据包，则表示网络中受到了 DDoS 攻击，控制器生成限速策略，下发限速命令，同时根据解析到的遥测信息中 swid 的值，来决定给哪些接入交换机下达限速命令从而缓解 DDoS 攻击。

控制平面的代码是用 python 语言实现，python 中的 scapy 工具可用于监听数据平面发送的数据包。在网络拓扑运行时，控制器周期性地下发流表以支持数据包的匹配，同时也会解析收到的遥测信息。

具体实现流程如图 8 所示。

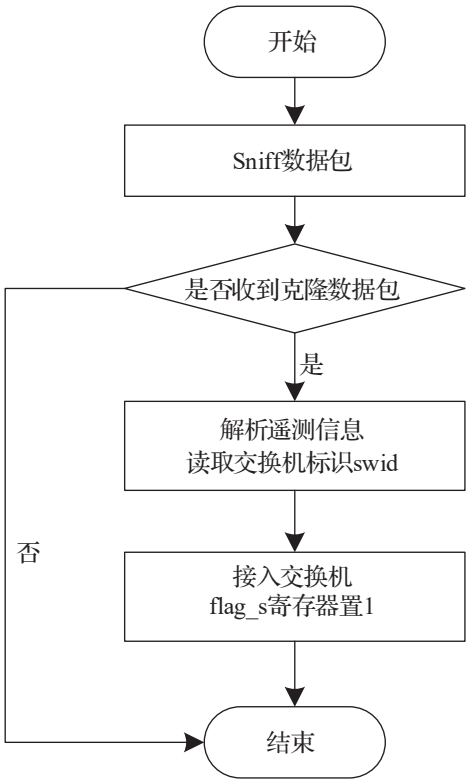

图 **8** 控制平面实现流程

3 可编程网络中轻量级 DDoS 攻击缓解机制测试

3.1 实验环境

本实验使用的实验软件是 Linux 系统中的 Ubuntu 系统，实验是在 Ubuntu 系统下搭建好的 P4 环境中进行测试的。本文利用 Mininet 软件平台搭建网络的实验环境，网络中的交换机采用 BMv2 交换机，控制器运行在单独的服务器上，以此完成整个实验的网络拓扑的搭建。运行整个系统环境的硬件参数如表 1 所示。

表 **1** 系统硬件参数配置

参数	版本信息
Linux操作系统	Ubuntu 16.04.6 LTS
内核	xenial
内存	4.00 G
Mininet	2.3.6
Python	2.7.12
Wireshark	2.6.8

搭建的实验网络拓扑如图 9 所示。拓扑中包含了一台控制器、三台交换机和四台终端主机，控制器和交换机之间通过 Thrift 端口实现相互通信。每个设备的详细配置信息如表 2 所示。

3.2 功能测试

3.2.1 运行系统

首先，对 Linux 系统的正常功能进行测试，打开 Terminal，通过指令 sudo p4run --config p4app-line.json 启动拓扑，运行 P4 代码和控制器代码。如图 10 所示，可以看到 P4 代码编译成功。

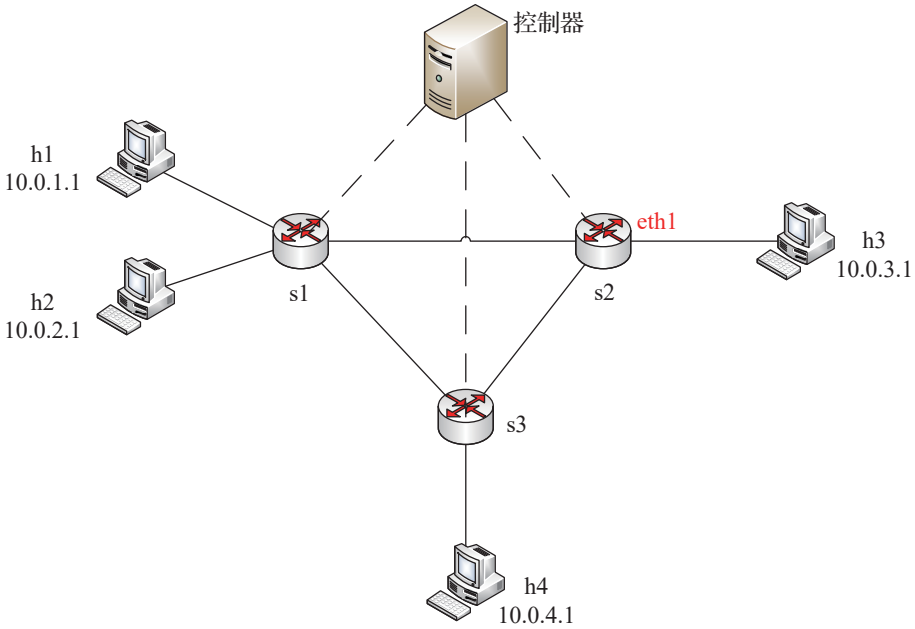

图 **9** 网络拓扑

表 **2** 设备地址和端口设置

设备	IP地址	网络接口
控制器	127.0.0.1	eth0
h1	10.0.1.1	eth0
h2	10.0.2.1	eth0
h3	10.0.3.1	eth0
h4	10.0.4.1	eth0

```
Starting mininet CLI

================================================================
Welcome to the P4 Utils Mininet CLI!
================================================================
Your P4 program is installed into the BMV2 software switch
and your initial configuration is loaded. You can interact
with the network using the mininet CLI below.

To inspect or change the switch configuration, connect to
its CLI from your host operating system using this command:
  simple_switch_CLI --thrift-port <switch thrift port>

To view a switch log, run this command from your host OS:
  tail -f /home/p4/p4-tools/p4-learning/exercises/10-Congestion_Aware_Load_Balan
cing/log/<switchname>.log

To view the switch output pcap, check the pcap files in
 /home/p4/p4-tools/p4-learning/exercises/10-Congestion_Aware_Load_Balancing/pcap
:
 for example run:  sudo tcpdump -xxx -r s1-eth1.pcap

*** Starting CLI:
mininet>
```

图 **10** 网络拓扑开启成功

3.2.2 实验参数设置

本实验用 iperf 模拟 DDoS 攻击，攻击主机通过 iperf -c 10.0.3.1 -u -b 3M -t 200 实现攻击，表示每秒向 IP 地址为 10.0.3.1 的主机发送 3 Mbit 的 UDP 数据包。根据前面部分所展示的链路信息，设置的链路带宽为 10 Mbit。阈值的

doi:10.3772/j.issn.2095-915x.2022.05.010

设置数值如表 3 所示。

表 3 阈值参数

参数	数值
拥塞阈值	50
限速阈值	80 packets/s

拥塞阈值指当交换机队列深度大于 50（约为 80% 的最大队列）时表明发生了拥塞，需要采取相应的限速缓解策略。限速阈值是从源端对单个攻击流的速率限制，可以有效应对多个攻击源的 DDoS 攻击场景。

3.3 性能分析

本机制的性能分析从两个方面进行分析，分别是缓解效果和反应时间。

缓解效果是指吞吐量是否能从大流量的拥塞状态恢复到正常状态；反应时间是指从检测到 DDoS 攻击开始到缓解成功即吞吐量下降所用的时间，本实验中当发送相同的攻击流量时，检测到拥塞所用时间相同，在图中表示的时间段如图 11 所示。

（1）缓解效果

首先看本缓解机制对 DDoS 攻击的缓解效果，参数设置如表 4 所示。利用 wireshark 抓包查看 s2-eth1 链路上的吞吐量，实验效果如图 12 所示。可以看到，无论是哪种大小的攻击流量，最后都能被本缓解机制检测并限制至正常值 160 packets/s，可见缓解效果较好。

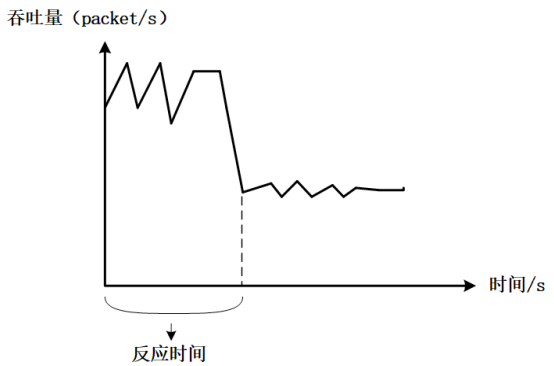

图 11 反应时间

表 4 实验参数设置

参数	版本信息
拥塞阈值	50
限速阈值	80 packets/s
h1发送流量	3、3.5、4 Mbit/s
h4发送流量	3、3.5、4 Mbit/s
发送时间	200 s

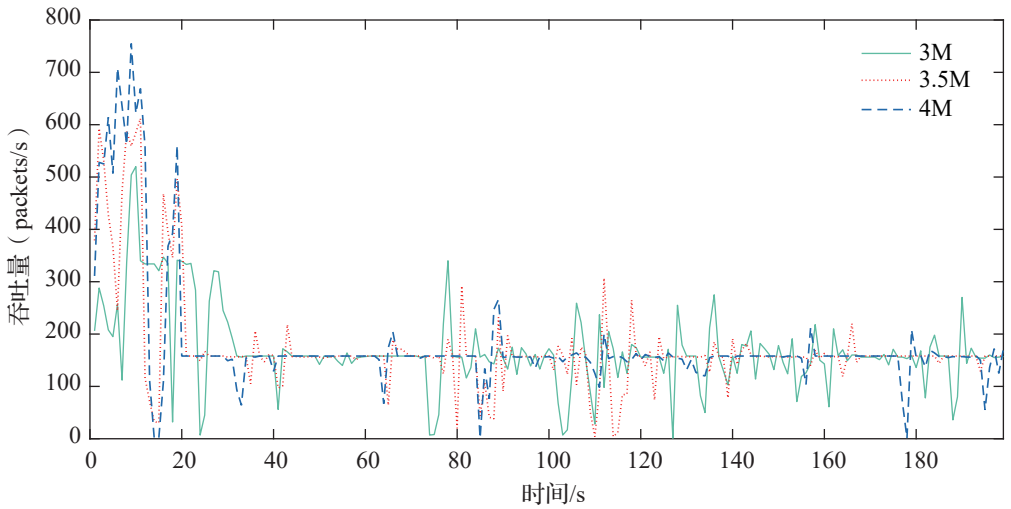

图 12 不同攻击流量下的吞吐量

在让h1和h4向h3发送3 M/s的攻击流量、拥塞阈值为50的情况下，将限速阈值分别设置为50 packets/s、80 packets/s、100 packets/s，再次观察缓解效果如图13所示，缓解后的吞吐量也达到了所设置的阈值，可见缓解效果较好。

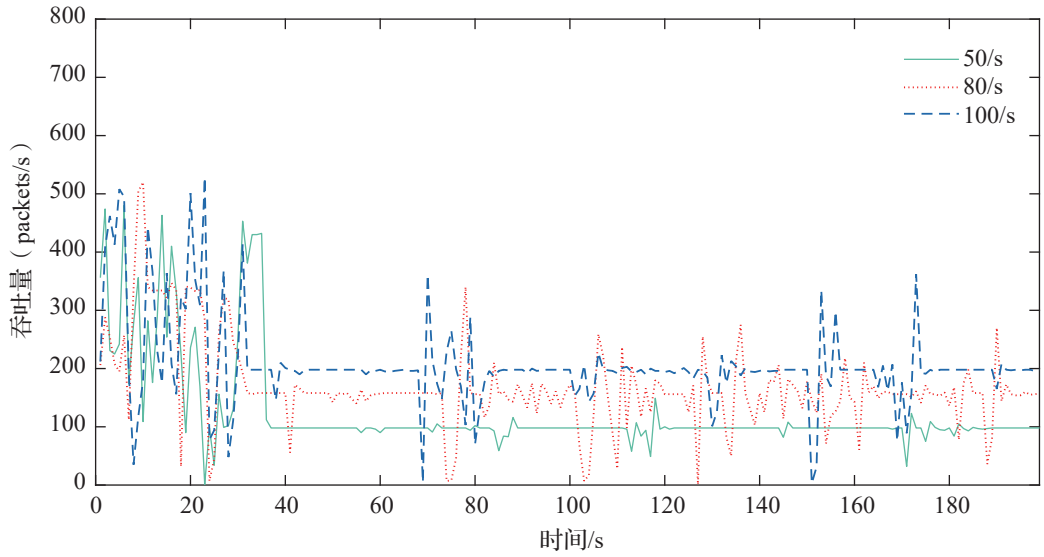

图 **13** 不同速率限制的吞吐量

（2）反应时间

测试反应时间参数如表5所示，分别测试100次的反应时间散点图如图14所示。三种限速情况下对应的反应时间的平均值大约分别为19s，22s，31s。由测试结果可以看到当限速阈值中数据包统计周期置的越小时，反应越迅速，反应时间越短，缓解机制更加灵敏，对DDoS攻击能作出较快的反应。

表 **5** 实现参数设置

参数	版本信息
拥塞阈值	50
限速阈值	16 packets/ 0.2 s 40 packets/ 0.5 s 80 packets/s
h1发送流量	3 Mbit/s
h4发送流量	3 Mbit/s
发送时间	200 s

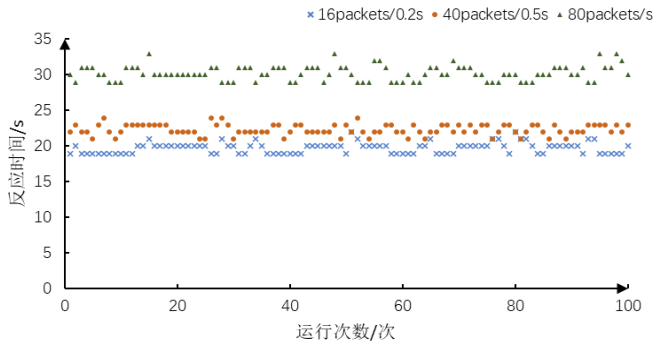

图 **14** 反应时间对比

doi:10.3772/j.issn.2095-915x.2022.05.010

4 结论

本文考虑到网络中由于 DDoS 攻击泛滥造成网络拥塞的场景，在了解 DDoS 攻击形式和 DDoS 攻击缓解机制的研究现状后，在可编程网络中，通过在源端限速的方式，对基于带内遥测的 DDoS 攻击缓解机制进行了研究。通过数据平面和控制平面的结合达到了 DDoS 攻击缓解的效果，同时未给网络带来过多负担，实现了可编程网络中轻量级的 DDoS 攻击缓解机制，并通过实验验证了本机制的有效性和可行性。

参 考 文 献

[1] 杨生举 , 曾硕勋 . 科技情报行业网络安全问题探讨 [J]. 甘肃科技 , 2010, 26(22):86-88.

[2] 2021 年上半年全球 DDoS 威胁报告 [Z]. https://mp.weixin.qq.com/s/5P1TAx-U5bnfA5ePdNPmkw.

[3] 何明祥 , 杨旭 , 李冠 . 大合规背景下我国网络空间安全政策文本研究 [J]. 情报工程 , 2022, 8(3):52-67.

[4] 郭渊博 , 李勇飞 , 陈庆礼 , 等 . 融合 Focal Loss 的网络威胁情报实体抽取 [J]. 通信学报 , 2022, 43(7):85-92.

[5] 王振东 , 张林 , 李大海 . 基于机器学习的物联网入侵检测系统综述 [J]. 计算机工程与应用 , 2021, 57(4):18-27.

[6] 石波 , 于然 , 朱健 . 基于知识图谱的网络空间安全威胁感知技术研究 [J]. 信息安全研究 , 2022, 8(8):845-853.

[7] 刘亮 , 赵倩崇 , 郑荣锋 , 等 . 基于威胁情报的自动生成入侵检测规则方法 [J]. 计算机工程与设计 , 2022, 43(1):1-8.

[8] 潘恬 , 林兴晨 , 张娇 , 等 . 基于高性能包处理架构 VPP 的带内网络遥测系统 [J]. 通信学报 , 2021, 42(3):75-90.

[9] Wang S Y, Chen Y R, Li J Y, et al. A bandwidth-efficient INT system for tracking the rules matched by the packets of a flow[C]. 2019 IEEE Global Communications Conference (GLOBECOM). IEEE, 2019:1-6.

[10] Tang S F, Li D Y, Niu B, et al. Sel-INT: A runtime-programmable selective in-band network telemetry system[C]. IEEE Transactions on Network and Service Management. IEEE, 2020, 17(2):708-721.

[11] Jacobson V. Congestion avoidance and control[J]. ACM SIGCOMM Computer Communication Review, 1988, 18(4):314-329.

[12] Allman M, Paxson V, Stevens W. RFC2581: TCP congestion control[J]. 1999.

[13] Henderson T, Floyd S, Gurtov A, et al. The NewReno modification to TCP's fast recovery algorithm[R]. 2012 (No. rfc6582).

[14] Vo P L, Le T A, Tran N H. mFAST: A multipath congestion control protocol for high bandwidth-delay connection[J]. Mobile Networks and Applications, 2019, 24(1):115-123.

[15] Floyd S, Jacobson V. Random early detection gateways for congestion avoidance[J]. IEEE/ACM Transactions on networking, 1993, 1(4):397-413.

[16] Braden B, Clark D, Crowcroft J, et al. Recommendations on queue management and congestion avoidance in the Internet[R]. 1998 (No. rfc2309).

[17] Hao J H, Shi Y, Sun H G, et al. Rerouting based congestion control in data center networks[C]. 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2019:1-6.

[18] Liu X, Yang X W, Xia Y. Netfence: preventing internet denial of service from inside out[J]. ACM SIGCOMM Computer Communication Review, 2010, 40(4):255-266.

[19] Piedrahita A F M, Rueda S, Mattos D M F, et al. FlowFence: a denial of service defense system for software defined networking[C]. 2015 Global Information Infrastructure and Networking Symposium (GIIS). IEEE, 2015:1-6.

[20] Bosshart P, Daly D, Gibb G, et al. P4: Programming protocol-independent packet processors[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3):87-95.

[21] Kaur S, Kumar K, Aggarwal N. A review on P4-Programmable data planes: Architecture, research efforts, and future directions[J]. Computer Communications, 2021, 170(7):109-129.

[22] Tan L Z, Su W, Zhang W, et al. In-band network telemetry: A survey[J]. Computer Networks, 2021, 186:107763.