基于可编程数据平面的网络防御技术研究综述

胡宇翔[1),2),3)] 潘 璠[1)] 崔鹏帅[1),2),3)] 田 乐[1),2),3)] 常德显[4)]
崔子熙[1)] 夏计强[1)] 占 奇[1)] 邬江兴[1),2),3)]

[1)](信息工程大学信息技术研究所 郑州 450002)
[2)](先进通信网全国重点实验室 郑州 450002)
[3)](网络空间安全教育部重点实验室 郑州 450002)
[4)](信息工程大学密码工程学院 郑州 450002)

摘 要 可编程数据平面(Programmable Data Plane, PDP)允许用户自定义网络设备的数据包处理方式,支持定制化网络操作,利用PDP的特性实施网络防御,在实时性、灵活性、扩展性等方面取得了良好效果,近年来受到学术界和工业界的广泛关注。本文以基于PDP的网络防御技术为主要研究内容,首先介绍了PDP的基本概念,并结合典型案例阐述其应用于网络防御的优势;随后根据实施网络防御的阶段,将基于PDP的网络防御技术分为防护技术、检测技术、响应技术3大类,对各类方案的现有研究进行深入分析、概括总结,归纳不同方法的优缺点;最后,本文对基于PDP的网络防御技术未来的研究方向进行展望。

关键词 可编程数据平面;网络防御;防护技术;检测技术;响应技术
中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2025.01943

A Review of Network Defense Technologies Based on Programmable Data Plane

HU Yu-Xiang[1),2),3)] PAN Fan[1)] CUI Peng-Shuai[1),2),3)] TIAN Le[1),2),3)] CHANG De-Xian[4)]
CUI Zi-Xi[1)] XIA Ji-Qiang[1)] ZHAN Qi[1)] WU Jiang-Xing[1),2),3)]

[1)](Institute of Information Technology, Information Engineering University, Zhengzhou 450002)
[2)](National Key Laboratory of advanced communication networks, Zhengzhou 450002)
[3)](Key Laboratory of the Ministry of Education for Cyberspace Security, Zhengzhou 450002)
[4)](Institute of Cryptography Engineering, Information Engineering University, Zhengzhou 450002)

Abstract Programmable Data Plane (PDP), a groundbreaking advancement in network technology, has revolutionized the way data packets are processed and managed on network devices. Unlike traditional network architectures with fixed and rigid data processing methods, PDP empowers users with the flexibility to customize and tailor data packet processing according to specific needs and requirements. This programmability extends to network operations as well, enabling the creation of customized network functions and services that were previously difficult or impossible to implement, leveraging the distinctive characteristics of PDP for network defense has

收稿日期:2024-09-23;在线发布日期:2025-03-29。本课题得到国家重点研发计划(2023YFB2903902)、中原科技创新领军人才项目(244200510038)、河南省重大科技专项项目(221100210900-02)资助。 **胡宇翔**,博士,教授,中国计算机学会会员,主要研究领域为新型网络架构、网络空间安全。E-mail: chxachxa@126.com。 **潘 璠**(通信作者),博士研究生,主要研究领域为可编程数据平面、零信任。E-mail: panfan2024@126.com。 **崔鹏帅**,博士,副研究员,主要研究领域为可编程数据平面、网络内生安全。 **田 乐**,博士,副研究员,主要研究领域为新型网络体系架构、网络内生安全等方向。 **常德显**,博士,副教授,主要研究领域为网络主动防御、软件定义安全。 **崔子熙**,博士研究生,主要研究领域为可编程数据平面、软件定义网络。 **夏计强**,博士研究生,主要研究领域为新型网络架构、可编程数据平面。 **占 奇**,博士研究生,主要研究领域为网络空间安全、异常流量检测。 **邬江兴**,教授,中国工程院院士,主要研究领域为网络空间安全、信息技术。

yielded remarkable outcomes across various dimensions. In terms of real-time performance, PDP-based defense mechanisms can swiftly respond to and mitigate emerging network threats without introducing significant latency, ensuring the smooth and uninterrupted operation of network services. The flexibility inherent in PDP allows for rapid adaptation to evolving threat landscapes, enabling network administrators to update defense strategies on-the-fly without extensive infrastructure overhauls. Regarding scalability, PDP solutions can be seamlessly expanded to accommodate growing network sizes and increasing traffic volumes, making them suitable for diverse network environments ranging from small-scale enterprise networks to large-scale data centers and cloud computing platforms. This paper delves into the promising field of network defense technology based on PDP. The research commences with an in-depth exploration of the fundamental concept of PDP, unraveling its technical underpinnings and architectural principles. By examining typical cases where PDP has been successfully applied to network defense, the paper vividly illustrates the tangible benefits and advantages that PDP brings to enhancing network security postures. Following the foundational exposition, the paper categorizes PDP-based network defense technologies into three major classes according to the stages of implementing network defense. Protection technologies focus on proactively shielding networks from potential threats before they materialize. This includes mechanisms such as access control, firewall configurations, and encryption techniques that establish robust barriers at network entry points. Detection technologies, on the other hand, are concerned with identifying and alerting against malicious activities that have infiltrated the network. These technologies employ network monitoring and traffic analysis to scrutinize network behaviors and pinpoint suspicious patterns. Response technologies come into play after a threat has been detected, taking immediate actions to contain and eliminate the threat. This may involve automated response scripts, traffic diversion strategies, and threat intelligence sharing to minimize the impact of the attack and restore normal network operations. For each category of defense technology, this paper meticulously reviews the existing research landscape. It dissects various proposed solutions, analyzing their technical approaches, implementation details, and performance metrics. Through comprehensive summary and comparison, the paper distills the strengths and weaknesses of different methods. For instance, some protection technologies may offer high security levels but incur substantial computational overhead, while certain detection technologies might achieve rapid threat identification at the cost of accuracy. This critical evaluation provides valuable insights for researchers and practitioners to make informed decisions when selecting or developing PDP-based defense solutions. Looking ahead, this paper presents a forward-looking outlook on the future research directions of PDP-based network defense technology. As network environments continue to evolve with emerging technologies such as 5G, Internet of Things (IoT), and Large Language Model (LLM), new challenges and opportunities arise for network defense. This paper proposes potential innovative approaches, such as PDP-based intelligent defense and PDP endogenous security technology. By elucidating the fundamentals, analyzing current research achievements, and charting future research courses, the paper serves as a valuable reference for academics, researchers, and industry professionals dedicated to advancing the state of network security in the era of programmable networks.

Keywords programmable data plane; cyber defense; protection technology; detection technology; response technology

1 引　言

信息化进程持续深入推进以及大数据[1-2]、虚拟化[3-4]、云计算[5-6]等技术蓬勃发展，为各行业带来新的机遇的同时，也对网络架构的数据传输能力、灵活调整能力以及管理控制能力提出更高要求。然而，传统网络架构下设备控制逻辑与数据平面紧密耦合，使得控制平面的管理日益复杂。同时，各厂商按照各自的标准生产封闭化的网络设备，内置了过多复杂的通信协议，增加了网络定制化的难度[7]，严重阻碍了新技术的应用和推广。

软件定义网络（Software Defined Networking，SDN）是一种新型网络架构，其设计理念是将网络设备的数据转发功能与管理控制功能分离，由逻辑上集中的控制器统一控制，并提供开放、标准的编程接口，使硬件设备能够摆脱对网络架构的依赖。相较于传统网络，SDN具有“数控分离、集中控制”的特点，可大大提升网络管控的能力和效率[8]，也有助于促进新兴网络技术的部署、应用与创新发展。

在SDN发展初期，学术界与工业界的研究面向控制平面可编程，对于数据平面的关注较少。这导致交换机报文转发逻辑、数据处理逻辑以及业务逻辑的可编程性不足，只能依靠更新设备的方式实现对新协议与新功能的支持，但真正的网络可编程应当能够对数据平面重新配置[8]。由此，斯坦福大学的Nick McKeown教授提出可编程数据平面的概念和可编程协议无关报文处理（Programming Protocol-Independent Packet Process，P4）语言[9]。P4通过定义抽象转发模型，设计解析器与包处理动作，并支持自定义协议，可实现对数据报文的灵活处理[10]，当前已在广域网、数据中心、云网融合等多个领域中发挥重要作用。

网络防御是利用PDP赋能的关键领域之一。网络中可能遭遇多种安全威胁，网络层中可能面临地址欺骗、路由劫持、拒绝服务等攻击，传输层可能遭受会话劫持、端口扫描等攻击，而应用层也面临着SQL注入、跨站脚本攻击等威胁，需要实施网络防御。根据美国国际互联网安全系统公司（ISS）提出的PDR（Protection-Detection-Response）网络安全框架[11]，网络防御由防护、检测、响应三个环节组成。传统网络防御方案主要依赖专用硬件设备来实现三个环节的安全功能，尽管这些专用设备在安全性方面表现良好，但硬件内部固有的逻辑可能导致其在面对新型威胁时难以快速适应并及时更新安全策略；另一方面，多个孤立设备间的管理给运维人员带来较大负担。虽然SDN和网络功能虚拟化（Network Functions Virtualization，NFV）技术能够在一定程度上提高网络资源的利用率并简化管理流程，但在实际部署中，由于虚拟化带来的额外开销，可能会影响整体防御性能，无法达到与专用硬件相同的处理效率[12]。

相比之下，PDP为网络安全带来了新的解决思路，不仅克服了专用硬件灵活性不足的问题，同时也弥补了SDN/NFV在性能上的不足。PDP使用如P4语言定制数据包处理逻辑，直接在设备上执行，既保证了数据转发的高效性，又能够实现安全策略的即时优化与适配。此外，PDP通过提供精细化访问控制、深度包检测（Deep Packet Inspection，DPI）、快速响应等能力，能够显著增强网络防御的防护灵活性、检测准确性和响应实时性。因此，PDP以其高可扩展性、高精度与高性能的融合优势，已成为当前网络安全解决方案中重要组成部分。

为了对基于PDP的网络安全防御技术进行全面综述，我们从WOS、DBLP、CNKI等数据库中，以“Programmable Data Plane”、“P4”、“Cyber Security”等为关键词进行检索，选择2015～2024年间发表的论文，然后通过大语言模型（Large Language Model，LLM）通读论文进行首次筛选，排除与本文研究问题无关的部分，共得到相关论文247篇。接着人工精读论文，优选其中高质量、具有代表性的论文，最终归纳并整理了这些论文。

尽管有一些优秀的综述论文[12-17]已对PDP的相关研究进行总结，但其中对PDP赋能网络防御方向相关文献的总结存在一定不足。文献[13，15-17]作为PDP研究的整体性综述，侧重于对PDP语法、抽象模型、工作流程等内容的总结，虽然涉及PDP应用于网络安全的内容，但不够深入，缺乏系统性的梳理。Chen等[12]对PDP赋能网络安全领域文献进行详尽总结，但其将网络防御技术分为流量攻击防御技术、非流量攻击防御技术的分类方法不够全面。AlSabeh等[14]虽然引入了STRIDE安全威胁模型，但仅用于对PDP安全应用的分析。随着网络安全攻击手段的日益复杂多样以及以生成式人工智能为代表的新型技术的涌现，不断促进了网络防御手段的发展，同时也催生了一些新的挑战和应用场景，因此现有综述缺乏一定的时效性。本文围绕基于PDP的网络防御技术展开研究和讨论，按

照PDR网络防御体系将研究内容划分为三个部分：基于PDP的网络安全防护技术、基于PDP的网络安全检测技术以及基于PDP的网络安全响应技术。针对每一分类，本文进行详细的方法论剖析，深入阐述各类技术的核心特征、独特优势及局限性。

本文组织结构如图1所示。第二节简要描述基于PDP的网络防御方案，主要包括对PDP的介绍、典型网络防御方案以及PDP赋能网络防御的优势；第三节介绍基于PDP的网络安全防护技术，主要包括边界安全、数据安全和通信安全相关的防护技术；第四节介绍基于PDP的网络安全检测技术，主要包括网络监控和流量分析；第五节介绍基于PDP的网络安响应技术，主要包括流量过滤和欺骗防御；最后，在对相关研究进行归纳总结的基础之上，对未来趋势进行展望。值得注意的是，虽然存在多条实现数据平面可编程的技术路线，但P4作为当前学术界和工业界最受关注的可编程语言，已成为绝大多数相关研究的主要对象。因此本文将以P4语言为主介绍基于PDP的网络防御技术。

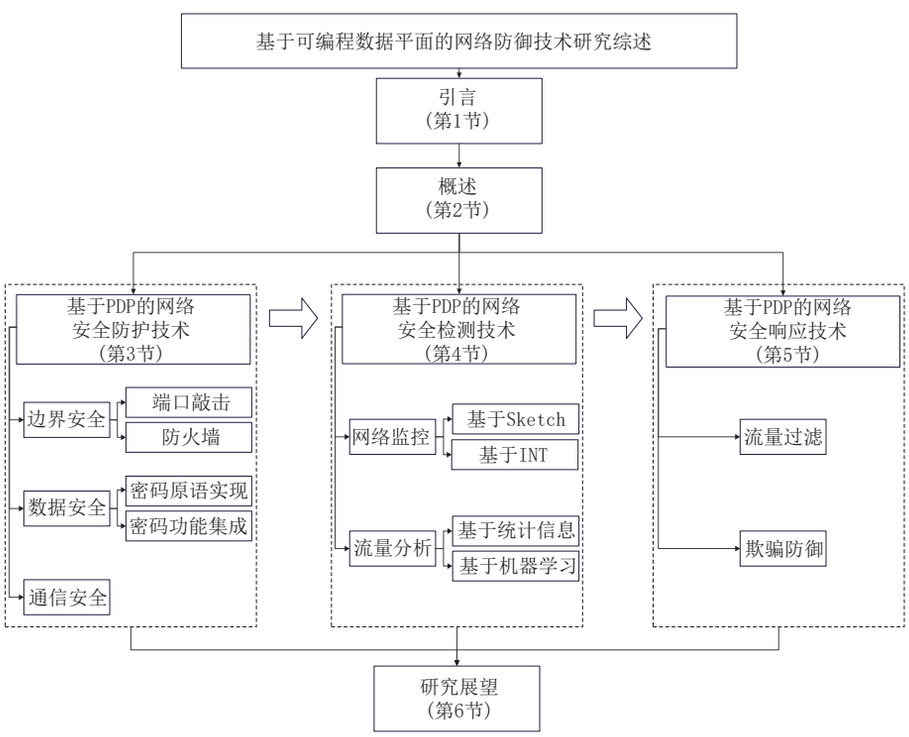

图1 论文组织架构

2 基于PDP的网络防御概述

2.1 PDP简介

传统SDN架构主要关注控制平面的可编程性，数据平面则往往依赖于硬件级别的专用集成电路(Application-Specific Integrated Circuit，ASIC)，虽然ASIC能提供高速的数据转发能力，但其功能相对固定，难以适应快速变化的网络应用需求。

以P4为代表的PDP技术通过引入可编程的硬件或软件元素，允许网络管理人员根据实际需求灵活定义和修改数据平面的处理逻辑。这不仅增强了数据平面的灵活性，还促进了网络功能的快速迭代与创新，使得网络能够更好地适应云计算、大数据、物联网等新兴应用场景下复杂多变的网络流量模式和服务质量要求。

PDP采用的典型模型是协议无关交换架构(Protocol Independent Switch Architecture，PISA)，其构成及与控制平面的交互如图2所示。从组成部分看，该架构中PDP主要包含以下几个部分：

(1)解析器(parser)：根据自定义的数据包头结构和解析流程，提取并解析报文头部。

(2)多级流水线(pipeline)：解析后的数据包经过多级匹配动作表(Match Action Table，MAT)，这些MAT在逻辑上组成一个有向无环图(Directed Acyclic Graph，DAG)，即pipeline。管理员可以根据数据平面语法规范定义每个MAT匹配何种数据包、执行何种动作。

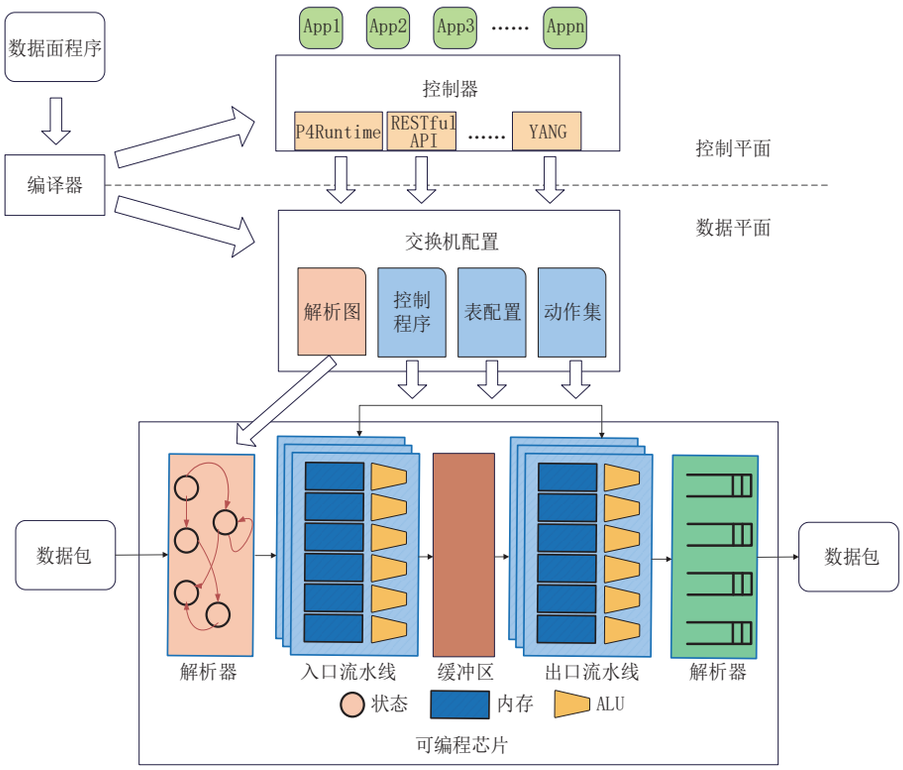

图2　PISA架构及其与控制平面交互

(3)缓冲区(buffer):缓存载荷并临时存储交换机队列中未被处理的数据包头。

(4)逆解析器(deparser):按照原有的包头结构重新封装数据包。以P4为例,基于PISA架构的PDP的工作流程如下:

首先,网络管理员根据P4语言规范编写程序,定义数据平面行为,描述需要的网络功能和处理逻辑等,如流量监控和防火墙等。

其次,将P4程序输入到P4编译器中,生成交换机配置文件和控制平面运行时调用的控制管理接口,配置文件中包含的内容有数据包解析图、控制程序、表配置和动作集合等。

最后,配置文件成功加载到交换机后,数据平面按照P4程序定义的逻辑处理数据包,而运行在控制平面的应用程序调用接口向数据平面下发匹配规则,常用的接口协议有P4Runtime、RESTful API、YANG等[18]。

在上述工作流程中,网络设备的数据包处理方式能够在设备部署后以编程的方式改变;网络管理员可以自定义交换机所支持的协议;所编写的P4程序能够跨平台移植。总的来说,PDP具有可重配置性、协议无关性、平台无关性。

2.2　基于PDP的典型网络防御方案

图3展示了一个典型的基于PDP的网络防御方案,该方案在可编程交换机上综合利用草图(Sketch)、带内网络遥测(Inband Network Telemetry,INT)、网内计算(In-Network Computing)等技术实现在网恶意流量检测与防御。

首先,在本地可编程交换机构建基于Sketch的流量特征提取模块,利用Sketch高效区分“象流”与“鼠流”[19],线速提取出海量网络流量数据的多样化特征,实现低内存占用条件下的大规模流量预处理与高效特征统计。

其次,在数据平面利用MAT实现决策树算法,检测并过滤恶意流量。通过将计算任务卸载到网络设备中执行,确保了对恶意流量的即时响应,同时有效减少控制平面计算与存储资源开销。

然后,利用INT技术向数据包中插入转发路径上的网络测量数据,在数据平面主动收集、传递全网实时状态信息,包括网络延迟、丢包率等关键指标信息。

最后,控制平面根据上传的测量数据,重新训练模型至收敛,然后利用P4Runtime向数据平面下发决策树表项,从而完成数据平面防御策略的更新。该方案充分利用PDP特性,实现了防护、检测、响应一体化的纵深防御。

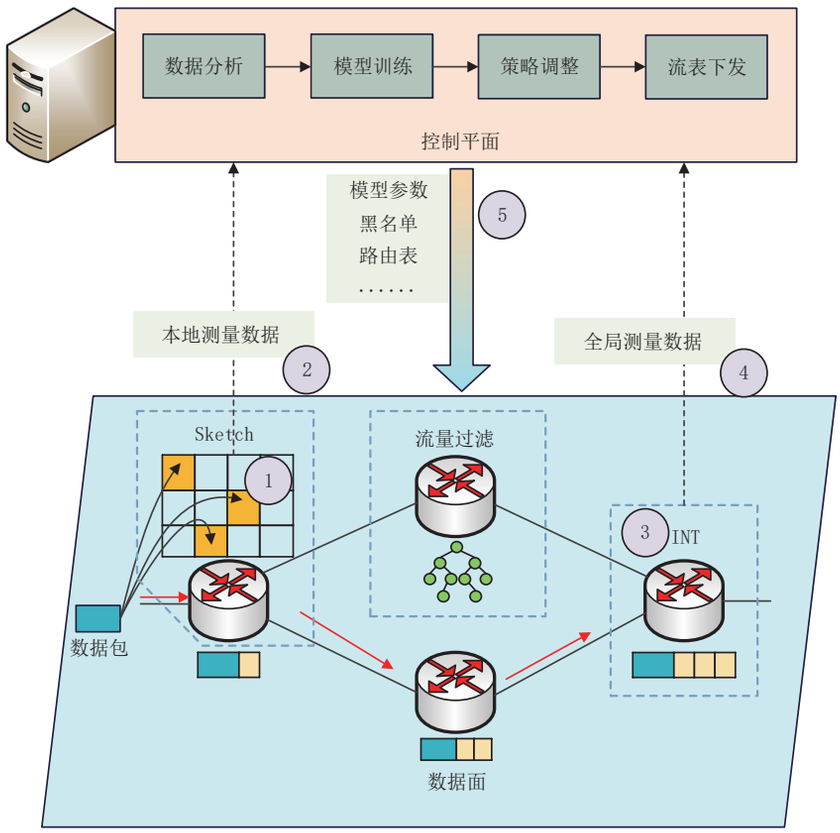

图3 基于PDP的网络防御典型案例

2.3 基于PDP的网络防御优势

表1展示了传统交换机、SDN交换机、可编程交换机的特征对比，结合PDP的工作流程、特点及典型案例，概括基于PDP实施网络防御具有以下优势：

表1 传统交换机、SDN交换机、可编程交换机对比

特征	传统交换机	SDN交换机	可编程交换机
控制平面 数据平面	控制平面和数据平面紧密结合在一起，每种设备都有自己的控制逻辑	数据平面与控制平面分离，通过开放接口与交换机通信并集中统一管理 转发逻辑可编程，但受限于硬件	数据平面与控制平面分离，能够对数据平面进行管理和编程 可以通过编程实现高度定制的功能
灵活性	灵活性较低，依赖硬件转发处理，难以适应快速变化的网络需求	较高灵活性，可以通过控制器灵活修改转发规则	极高的灵活性，允许开发者使用P4等语言编写数据包处理逻辑
扩展性	扩展性有限，每个设备都需要单独配置和管理	易于扩展和管理，可以通过修改控制器策略扩展功能	非常高，能够适应复杂的网络需求
适用场景	适合小型网络环境，如家庭或小型办公室网络	适用于需要频繁调整网络配置和策略的环境，如园区网	适合于需要高度定制化数据包处理逻辑的环境，如高性能计算中心

支持自顶向下开发网络程序：传统网络架构多采用自下而上的设计范式，其中硬件层限定了网络设备的操作范围与协议集，极大地制约了网络应用的灵活性和定制化能力。相反，PDP赋予了开发者采用自顶向下的策略构建网络程序的能力。在这一模式下，编译器充当了底层硬件与高层应用之间的桥梁，为开发者屏蔽了硬件实现细节。这不仅简化了开发流程，还允许在运行时动态调整数据平面的安全策略并迅速集成新型安全功能，极大地提高了网络安全功能部署的效率与灵活性。

能够提供细粒度实时防御：PDP通过提供对数据包级网络行为的可见性，为网络管理员构建了更细粒度的防御视图。另一方面，PDP将对网络流量的检测、修改及控制操作无缝集成于数据转发流程之中，摆脱了对控制平面或额外安全组件的依赖。这确保了在毫秒级时间尺度内识别并隔离恶意活动[15]，极大地缩短了响应时间，降低了系统受攻击的风险窗口。

提高程序性能和资源利用率：相较于传统固定功能交换机所承载的庞大且往往冗余的协议集，PDP允许开发人员根据实际需求精选必要的协议和功能，避免了资源浪费与不必要的处理复杂度；另一方面，可编程交换机支持线速数据包处理性能，例如Intel的Tofino系列交换机可以达到12.8 Tbps的处理速率[16]，这意味着使用PDP实现网络防御不仅可以避免性能损失，反而能在某些情况下提供比固定功能交换机更优秀的性能。

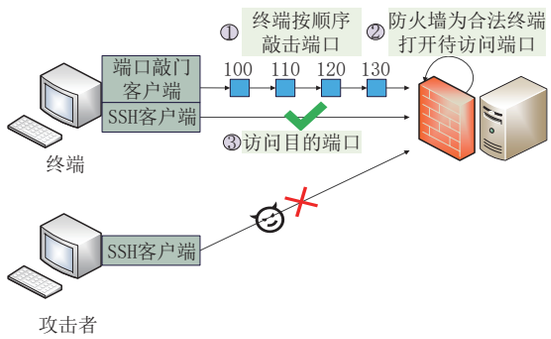

图4　端口敲门机制

3　基于PDP的网络安全防护技术

防护技术是指采用身份认证、访问控制、数据加密、防火墙等手段保障数据的机密性、完整性、不可否认性的技术，旨在将网络攻击行为扼杀在实施之前。当前，基于PDP的防御技术研究主要可以归结为三个方面：边界安全、数据安全、通信安全。

3.1　边界安全

边界安全是网络安全的第一道防线，旨在保护边界内网络不受恶意活动的影响。在SDN环境中，保护边界安全的常见方式有防火墙和端口敲门两种，当前在PDP中也有相关研究。

3.1.1　端口敲门

端口敲门是一种身份验证机制，通过特定的端口序列来开启或关闭网络服务，只有当正确的端口序列被“敲击”后，相应的服务才会开放，图4展示了端口敲门机制的原理。

在数据平面实现端口敲门的难点是如何将基于主机的身份验证功能卸载到网络，并使该机制对终端设备透明。P4Knocking[20]用寄存器跟踪端口敲门序列状态，每个源IP地址都有一个对应寄存器存储敲门序列进度；Almaini等[21]提出利用有限状态机（Finite State Machine，FSM）描述端口敲门过程中的状态转移过程，不同事件将触发对应的状态转移，当访问者敲击错误端口时，将触发回滚操作，直到按照正确顺序转换到最终状态。

采用静态、单一的序列号可能会由于序列号泄露而造成安全风险。为了保持解决方案的动态性，在P4Filter[22]中，每当新主机第一次尝试连接时，控制器随机生成新的序列号；PortSec[23]中根据序列号的动态性程度，分别设计了静态、部分动态、动态三种具有不同安全级别的端口敲门协议，并通过XOR和Hash函数保证序列号传输过程中的机密性；为进一步完善端口敲击技术中加密传输、身份认证等机制，P4-sKnock[24]提出一种两级访问控制机制：通过动态加密端口敲门的序列号确保安全传输，通过挑战-响应机制验证主机身份。实验表明，P4-sKnock可以在500 ms内对新主机进行身份认证，能够有效防御中间人攻击和重放攻击等。

表2对于PDP端口敲门研究总结，可以看出当前端口敲门相关研究存在的不足主要在两方面：一是局限在BMv2平台上以软件形式实现，认证效率可能不高；二是虽然通过特定端口序列号能够隐藏服务，但序列号本身在传输过程中的安全性未得到有效保障，易被攻击者嗅探、篡改。

表2　PDP中端口敲门研究总结

工作	平台	主要思想	存在限制
P4Knocking[20]	BMv2	比较端口敲门在数据平面和控制平面的效果	序列号未加密，易被嗅探
Almaini等[21]	BMv2	利用FSM描述端口敲门过程中的状态转移	序列号未加密，易被嗅探
P4Filter[22]	BMv2	控制器为每次连接生成新的序列号	动态端口敲击序列的传输安全性
PortSec[23]	BMv2	设计三种不同安全界别的端口敲门协议	仅分析中间人攻击
P4-sKnock[24]	BMv2	两级访问控制机制	仅分析中间人攻击

3.1.2　防火墙

防火墙是一种常用的网络边界防护设备，用于监控并控制进出网络的流量，传统防火墙存在规则配置复杂、难以扩展、无法进行DPI等问题。基于PDP技术实现的防火墙，能够定制化数据包处理逻辑，为实现更灵活、更动态的访问控制提供了可能，

大致分为有状态过滤防火墙和无状态过滤防火墙两种。

无状态过滤：此类防火墙独立地检查每一个数据包，根据预设的规则决定是否允许数据包通过。Ricart-Sanchez等[25]提出基于P4-NetFPGA结构实现5G防火墙，利用P4解析VxLAN和GTP等协议，利用FPGA进行硬件加速，满足5G移动性、多用户隔离需求、高性能等应用需求。

有状态过滤：此类防火墙不仅需要考虑数据包头的信息，还需要考虑是否属于已建立的连接以及数据包之间的关联性质。Péter Vörös等[26]利用Counters、Meters、Registers记录状态信息，实现对IPv4、IPv6、TCP、UDP等协议头部字段的有状态过滤；李健等[27]通过在pipeline中添加FSM实现对连接状态的检测、记录、更新；P4SF[28]同样通过FSM处理状态转移，并进一步设计匹配块存储必要的流量状态和标志，设计状态块验证并更新流状态，设计动作块根据ACL规则转发数据包。实验表明P4SF支持384 000个表项，达到100 Gb/s的线速数据包转发。

两类防火墙的协同能够提升防护效果。P4Filter[22]提出动态防火墙逻辑，利用有状态和无状态防火墙协同过滤数据包，阻止来自未授权源的包，可以防范IP欺骗攻击，具有更高的灵活性和安全性。Chou等[29]结合两类防火墙的特点，提出一种基于P4的双层防火墙系统。第一层防火墙不考虑连接状态，仅检查数据包的源IP地址；第二层防火墙进行更复杂的检查，包括IP地址匹配和数据包方向的判断，并根据数据包的状态更新Bloom过滤器。两层防火墙的协作机制显著增强了对DDoS攻击的防御能力。

表3对上述研究进行总结。现有基于PDP的防火墙技术尚在初级阶段，相较于传统防火墙虽然在灵活性、扩展性等方面具有优势，但在功能完备性等方面还存在差距。尤其对于有状态防火墙而言，由于数据来源和防御策略的多样性，存储记录复杂的状态空间对于PDP有限的资源来说存在一定困难。此外，下一代防火墙（Next Generation Firewall，NGFW）提供更深层次的安全防护，包括DPI、应用控制、智能分析等高级功能，但在PDP上结合NGFW的研究相对较少。

表3 PDP中防火墙技术研究总结

工作	平台	过滤字段	主要思想	存在限制
P4Filter[22]	BMv2	源IP，源MAC	利用有状态和无状态防火墙协同过滤数据包	需要依赖控制器
Ricart-Sanchez等[25]	NetFPGA	IP，TCP，UDP，GTP，VXLAN头部字段	基于P4-NetFPGA实现5G防火墙	无法检测到需要统计数据的攻击
Péter Vörös等[26]	-	IP，TCP，UDP头部字段	对各种等协议头部字段的过滤和检查	应用层支持的缺失；未说明实验平台
CoFilter[30]	Tofino	IP地址和端口号	ASIC与CPU联合包过滤	仅支持TCP连接
李健等[27]	BMv2	IP地址和端口号	在pipeline中添加FSM记录状态信息	大规模网络中处理状态有限
P4SF[28]	NIC	5-tuple，SYN/TCP标识	通过FSM处理状态转移	大规模网络中处理状态有限
Li等[31]	-	源/目IP，源/目TCP端口	通过FSM和FST实现	仅支持TCP连接；未说明实验平台
Chou等[29]	BMv2	源IP、标志位	双层防火墙机制	考虑状态单一

3.2 数据安全

数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。在网络安全领域，利用密码学技术保护数据的机密性、完整性、不可否认性是保护数据安全的基本方法。

3.2.1 密码原语实现

密码学是保障网络安全的基石，在保护信息安全方面发挥关键作用。密码学原语是实现密码学功能的基础单元，实现密码学原语是保护数据安全、实施网络防御的基础。在数据平面实现安全原语具有以下优势：从计算成本角度看，避免了与控制平面的不必要交互，有效减少开销；从流量处理角度看，可实现对经过设备流量的细粒度、灵活加密，根据需求精确控制加密级别和范围；从安全角度看，密码参数直接存储在交换机中，无需离开数据平面，减少密码参数在传输过程中的安全风险，减少暴露的攻击面。

以P4为例，当前PDP仅原生支持少数简单密码学原语如循环冗余校验（Cyclic Redundancy Check，CRC），如表4所示，其作用主要有索引、完

表4　CRC在PDP中的应用

应用	工作	主要思想	存在问题
索引	PRECISION[32]	CRC值作为索引	可能会产生哈希冲突
	P4RTT[33]	计算数据包指纹	
完整性校验	Jaqen[34]	防止数据包被篡改	可能被碰撞攻击
采样	Chen等[35]	实现均匀采样	不完全真随机

整性校验和采样三种。

索引：对数据包部分头部字段计算CRC值并构建哈希表，在查找时可用于表示较长的流ID。如PRECISION[32]中将流量标识符（源IP、目的IP等信息）作为输入传递给CRC函数，输出值作为索引可用于访问流量计数器或状态信息；类似的P4RTT[33]使用CRC计算数据包指纹，有效存储和管理数据包记录。

完整性校验：CRC用作伪随机哈希函数，计算数据包的校验和，提供消息认证的功能。如Jaqen[34]使用CRC检测数据包传送的正确性，避免传输过程中发生错误或被篡改。

采样：CRC函数具有一定的随机性，可以一定程度上确保所有包或流在采样过程中有相等的机会被选中，可用于数据包采样。如Chen等[35]将CRC用于在数据平面实现均匀采样机制。

然而CRC在严格意义上不属于一种安全的密码学函数，其输入输出之间存在线性关系[36]，攻击者可以手动构造CRC获得期望值，将CRC作为哈希函数存在较大的攻击风险，因此需要扩展PDP支持的密码学原语。但是大多数密码学原语中的计算是复杂且资源密集的，PDP中支持的运算操作仅限于基本算术（加法、乘法、移位等）。为了克服P4存在的限制，研究人员提出了以下三类解决方案：

P4 extern方法：P4 extern允许P4程序调用外部软硬件模块提供的功能，从而实现更复杂的网络行为。Péter等提出一个P4编译器T4P4S[37]，可以将P4程序与C语言实现的extern库链接。基于T4P4S，Horp'acsi等[38]在v1Model体系中添加了加解密操作，Scholz等[39]扩展T4P4S并添加了SipHash-2-4、Poly1305-AES、BLAKE2b和HMAC-SHA256/512四个Hash函数；类似的，Mafioletto等[40]在NPU平台上利用Micro-C编写P4 extern解决P4的限制。

查找表（Look Up Table，LUT）：在密码学中，为减少计算时间，可采用“空间换时间”的策略。对于某些复杂的运算操作，可以预先计算并存储结果，在实际使用时直接查找结果而不需要重新计算。在PDP中也可以采取这种策略，以较小的存储开销加速安全原语实现。dh-aes-p4[41]在PDP中存储AES的两个S盒，分别用于加密和解密时的字节代替变换，并预计算LUT加速列混合变换。在BMv2交换机的仿真实验表明，dh-aes-p4比基于控制器的加密方案效率提升了约10倍；Chen等[42]借助MAT的匹配特性，提出Scrambled Lookup Table技术，用表查找操作简化了AES算法中的字节替换和轮密钥异或操作，减少加密时的算术操作。在Barefoot Tofino芯片上的实验表明，该技术仅占用不到15%的内存实现了高达10.92 Gbit/s（AES-128）、8.76 Gbit/s（AES-192）和7.37 Gbit/s（AES-256）的数据加密速度。

Pipeline优化：为了实现对数据包的线速处理，可编程交换机中的pipeline存在严格约束，限制了密码学操作的执行。一些研究对pipeline进行针对性的改进优化，扩展其对安全原语的支持。

其中一种优化思路是在基础pipeline上添加用于实现密码学原语的模块，这是一种类似于extern的方法。Malina等[43]在Parser与MAT之间以及MAT与Deparser之间添加控制模块，可以将P4程序转化为FPGA数据流，从而借助FPGA在数据平面高效实现加密、签名、Hash三类密码原语，提供高达26.24 Gbps的加密速度、4.51 Gbps的哈希速度以及每秒462次签名和222次验证操作；Scholz等[39]优化P4->NetFPGA模型，在egress pipeline中集成Hash模块，可通过metedata决定插入Hash模块的位置并传递计算的Hash值，解决NetFPGA没有实现用于外部数据输入和输出的流接口的问题。

另一种思路是针对pipeline本身在资源分配等方面存在的问题进行优化。Yoo等提出了一种Hash函数实现方案SipID[36]。SipID通过变量重命名、依赖分组、数据包再循环和入/出口流水线组合使用等操作节省pipeline资源，并利用切片语义进行紧凑的循环位移，克服有限操作数限制，能够支持Hash计算中不同变量存在的复杂调用、赋值、运算等关系，实现了在Tofino交换机上的高效运行，仅占用0.3%的SRAM、8.3%的指令和33.3%的哈希单元等极少数资源。实验结果表明，SipID能够每秒能处理高达30 400万次哈希操作。Yoshinaka等[44]提出一种在可编程交换机上部署ChaCha流密码的方法：将奇数轮和偶数轮的QR（Quarter Round）分别部署在不同的pipeline中避免变量依

赖，解决不同QR之间的依赖关系；利用Tofino的特殊指令在一个stage内完成旋转和加法操作减少额外的循环操作，解决QR内部的依赖性；通过旋转数据块避免keystream和数据块之间的依赖。实验表明，ChaCha实现了较小的内存占用和高达203 Gbps的吞吐量，显著优于传统的AES实现。

表5对当前PDP中密码原语研究进行总结。可以看出，当前PDP中密码学原语的相关研究主要集中在软件平台上，且在输入长度、程序规模、密钥使用等方面存在诸多限制。此外，当前在PDP上大多数支持的密码学算法多为对称密码和哈希函数，公钥体制算法由于基于数学困难问题，需要极大的计算资源，难以在PDP上运行。这些问题主要是受限于可PDP有限的计算存储资源，无法完整实现安全原语，还需要对PDP语言、PDP芯片做进一步的扩展和改进。

表5 PDP中密码学原语实现研究总结

工作	平台	算法	主要思想	存在的不足或限制
Horp'acsi等[38]	t4p4s	-	基于t4p4s实现，引入异步调用机制	使用了OpenSSL库实现加密
Mafioletto等[40]	NPU	SHA-256	Micro-C编写P4 extern	NPU支持大型应用程序时存在资源限制
Chen等[42]	BMv2	AES-128，AES-192，AES-256	提出Scrambled Lookup Table技术简化AES运算	侧信道攻击的安全性问题
dh-aes-p4[41]	BMv2	AES-256	预存储S盒，预计算LUT	潜在安全性分析不足，如中间人攻击
SipID[36]	Tofino	HalfSipHash	优化Hash计算中的pipeline“长依赖”特性	主要集中在短输入字符串
Malina等[43]	FPGA	AES-GCM-256，SHA-3，EdDSA	在pipeline中添加控制模块	不支持线速率操作
Scholz等[39]	t4p4s，NPU，FPGA	SipHash-2-4，Poly1305-AES，BLAKE2b，HMAC-SHA256/512	采用三种方式在三种平台上集成Hash函数	密钥未用于生成消息验证码
Yoshinaka等[44]	Tofino	ChaCha	优化密码算法需要的资源在PDP上的部署	循环带宽消耗偏大

3.2.2 密码功能集成

密码学功能是指通过使用一种或多种密码学原语来实现的具体安全目标或服务。在PDP中基于已经实现的安全原语，可以实现常见的密码学功能，包括数据机密性、完整性保护与身份验证。

SmartCookie[45]利用HalfSipHash-2-4函数在PDP上实现安全的SYN cookies计算，可以有效地阻止SYN泛洪攻击，同时保持低延迟和高吞吐量。dh-aes-p4[41]结合Diffie-Hellman密钥交换协议和AES加密，实现在PDP动态生成、协商密钥和自主执行加密，减轻了控制器的负担；Qin等[46]提出一种灵活加密机制，设计基于XOR和基于S-box的两种加密算法，分别适用于安全性能要求低和安全性需求高的数据，实现对不同类型数据的按需加密；MultiSec[47]针对异构网络提出一种多协议安全转发机制，集成了SM4-CBC、HMAC-SM3等多种加密算法，同时能自动更新密钥，确保在PDP实现多协议安全转发；P4NIS[48]对数据包进行双重加密应对窃听攻击：在应用层加密所有的数据载荷，防止攻击者直接获取数据明文；在传输层加密所有的数据分组包头，将同一流的数据包分散到各个流中，大大增加了窃听攻击的难度。

表6对当前利用PDP中密码功能集成相关研究进行总结。可以看出在PDP中，集成最多的密码功

表6 PDP中密码功能集成研究总结

工作	平台	安全性目标			主要思想	存在的限制
		机密性	完整性	不可否认性		
SmartCookie[45]	Tofino	√	√	×	安全计算SYN cookies	存在一定的假阳性率
dh-aes-p4[41]	BMv2	√	×	×	数据平面DH密钥交换	密钥管理问题
Qin等[46]	BMv2	√	×	×	基于XOR和S-box两种方法的灵活加密机制	加密算法安全性较低
MultiSec[47]	t4p4s	√	×	×	集成多种加密操作，实现多协议安全转发	多协议兼容性问题
P4NIS[48]	BMv2	√	×	×	数据包进行双重加密应对窃听攻击	加密过程实现在控制平面

能是对数据机密性的保护。然而受限于PDP所支持的密码学原语有限，加密认证过程中安全性、兼容性、密钥管理等方面存在问题，且当前还无法在数据平面实现数字签名和验签，缺乏对数据不可否认性的保障。

3.3　通信安全

在实现密码学功能的基础上，可以进一步研究安全通信机制。传统网络中，确保通信安全的方法有虚拟专用网络（Virtual Private Network，VPN）、SSL、TLS等。除了将这些技术迁移到数据平面，PDP的特性使得安全通信机制更加灵活。

MACsec是一种局域网安全通信方法，可以在二层对数据进行加密、认证、校验。针对传统交换机部署MACsec时间开销大、获取全网拓扑信息难的问题，Hauser等人提出P4-MACsec[49]方案。P4-MACSec由MAC地址学习、安全链路发现、自动化部署三个模块组成，利用两层控制平面结构进行管理和配置。Mininet仿真实验表明，P4-MACsec能够成功保护网络连接，抵御数据包操纵和重放攻击，能够在短时间内完成部署和更新。在此基础上，Hauser等人继续提出基于P4的IPsec VPN的方案[50]，给出了隧道模式下ESP协议原型系统的软件实现，保障网络层通信安全。P4-IPSec的数据平面包括L3转发模块、SPD匹配模块、ESP加密模块、ESP解密模块，当数据包经过网关时，P4-IPsec对数据包依次进行封装、加密、转发、安全性验证、解封装等操作。控制器通过P4Runtime接口维护隧道配置文件的方式对隧道进行管理。实验证明，P4-IPsec虽然引入了一定的延迟，但对整体功能影响较小。更进一步，P4Sec[51]结合P4-MACSec和P4-IPSec，提出数据平面的SDN网络安全通信方案，利用P4描述各类安全协议，实现802.1X、IPSec、MACSec等网络保护机制的自动部署。左志斌[52]针对SDN数据平面的特点及面临的安全威胁，应用密码标识技术，构建SDN数据平面安全通信框架，包括基于密码标识的报文细粒度安全控制转发、混合转发验证方法、安全隧道及其密钥协商协议、基于网关标识的隧道报文路由转发等。

上述方法属于端到端通信安全防护，主要保护通信过程中数据隐私，但是通信过程中的五元组、报文长度、标识等元数据依然会暴露，攻击者可以进行流量分析攻击，从而推断出用户身份隐私，因此需要引入匿名通信技术。ONTAS[53]提出在数据平面实现网络流量匿名化，首先通过定义配置文件表达匿名化策略，然后ONTAS编译器根据配置文件生成P4程序，当数据流经交换机时，在保证数据包转发行为不变的前提下进行在线匿名化处理；PANEL[54]采用随机化策略避免信息泄露和指纹攻击：通过随机重写源IP地址和TTL值来隐藏源信息，其次使用伪随机数生成器（PRNG）生成的“标签”来随机化会话标识符，保证会话不可链接；SPINE[55]对通信过程中的源目IP地址等字段进行加密，并采用定期密钥轮换策略防止密钥泄露，防止攻击者窃取关键信息。

表7对当前PDP中通信安全研究进行总结，可以看出对通信载荷的保护主要依靠数据平面安全原语的实现，在PDP中可以通过包头修改隐藏信息，其高灵活性、线速性能和低开销特性，使得在数据平面的在线流量匿名化技术显著优于传统的离线流量混淆。

3.4　其他防护技术

除了上述三方面，还有一些其他关于PDP的防护技术研究。

Black等[56]提出一种针对P4-uBPF程序的混淆方案，通过增加程序路径和变量之间的语法依赖性，使得攻击者在进行路径约束求解需要进行更加复杂的分析，提高攻击成本，间接提高了数据平面的安全性。

由于流表更新不一致、网络配置错误等因素，数据包实际转发路径可能与期望路径不一致，可能会被攻击者利用。吴平[57]提出利用探针测试的方法校验路径一致性，将其规约为最小集覆盖问题，并利用启发式算法求解；Borges等[58]提出PoT-PolKA方法，旨在保护数据包转发过程中的路径安全性，通过引入Proof-of-Transit（PoT）机制，对路径进行验证，确保数据包网络中按预定路径转发，防止流量偏移攻击。

Sankaran等[59]基于P4和NetFPGA提出一种安全执行模型，通过限制对持久状态的修改和内存访问，确保即使恶意指令被嵌入数据包中，也不会影响交换机的安全性。

左志斌等[60]提出一种基于PDP的动态网络防御方案。通过动态改变协议号和跳变数据包四元组信息，混淆端信息，有效抵御嗅探攻击。

综上，利用PDP实现防护技术具有以下优势：一是可以提供高度定制化的网络功能与策略。PDP允许根据特定安全需求定制网络功能，可以针对不同类型的流量或用户群体，设置差异化的安全策略，

表7 PDP中通信安全研究总结

工作	平台	安全性目标			主要思想	存在的限制
		机密性	完整性	不可否认性		
P4-MACsec[49]	NetFPGA	√	√	×	MACsec数据平面实现	P4 extern函数的使用在平台上受到了限制
P4-IPSec[50]	NetFPGA	√	√	×	IPsec VPN数据平面实现	仅支持ESP模式
P4Sec[51]	BMv2	√	√	×	数据平面802.1X、IPSec、MACSec等网络保护机制部署	无硬件部署
ONTAS[53]	Tofino	√	√	×	简化匿名策略上部署在数据平面	不支持TCP/UDP头部匿名化
PANEL[54]	Tofino	√	×	×	修改源IP和TTL隐藏源信息	会话初始化过程开销大;连接会话数有限
SPINE[55]	BMv2	√	√	×	加密通信双方IP地址和相关TCP字段	仅支持IPv4
左志斌[52]	BMv2	√	√	√	SDN数据平面安全框架	无硬件部署

提高安全防护的针对性和有效性,也确保了网络资源的合理分配;二是动态适应与实时响应能力。PDP支持动态的安全策略,在网络环境和威胁态势不断变化的情况下,PDP能够实时监测并快速更新安全策略,以应对最新的攻击模式,提高安全防护的有效性和实时性;三是利用PDP实现防护技术可以提高安全防护的透明性和可管理性,用户通过标准化的编程接口,不仅可以直观地监控数据平面的安全状态,还能通过控制平面统一管理和配置安全策略,便于故障排查和性能调优。

4 基于PDP的网络安全检测技术

网络安全检测技术是指用于检测网络流量中异常行为和潜在威胁的一系列技术。从检测过程来看,检测技术可以分为网络状态获取和网络状态分析两个核心环节。本节对基于PDP的网络安全检测技术将主要从网络监控和流量分析两个角度介绍。

4.1 网络监控

网络监控是指对网络设备的状态、性能、可用性进行持续监视的过程,确保网络的稳定运行。传统网络中的监控技术包括简单网络管理协议(Simple Network Management Protocol, SNMP)、NetFlow、安全信息和事件管理(Security Information and Event Management, SIEM)等。在PDP中,常用的网络监控技术主要有基于Sketch和基于INT两种。

4.1.1 基于Sketch的网络监控

Sketch意为数据概要,如图5所示,其基本结构由k行w列的计数器构成,k个不同的哈希函数对经过的数据报文进行哈希运算,映射到w个计数器中。每一行的计数器都各自记录数据流的信息,当查询信息时,需要综合k个不同的返回值确定最终测量结果。Sketch方法特别适用于处理大规模数据流的情况,能够以较低的空间复杂度对数据流的某种统计特征提供接近准确的结果。当前利用Sketch进行网络监控主要关注流大小估计(Flow Size Estimation, FSE)、重要流检测(Heavy Hitter Detection, HHD)、重要变化检测(Heavy Change Detection, HCD)、流大小分布估计(Flow Size Distribution Estimation, FSDE)、熵估计(Entropy Estimation, EE)、流基数估计(Cardinality Estimation, CE)等。

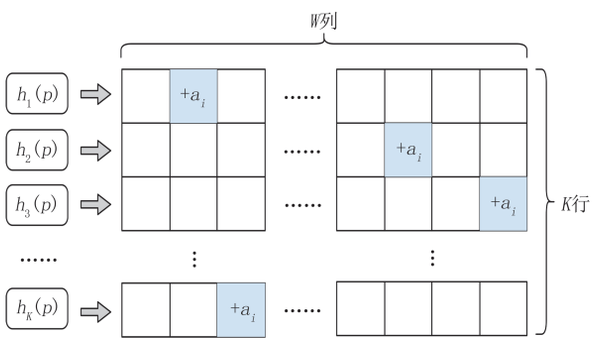

图5 Sketch基本原理

与传统网络环境不同,在PDP环境中可以直接在网络设备上部署和运行Sketch算法,而不需要将数据发到中心服务器处理,能够实现实时、持续的流量统计,无需额外的硬件或软件开销。当前在PDP上利用Sketch进行网络监控的研究主要分为两方面,即Sketch结构设计与优化和Sketch配置优化。

(1) Sketch结构设计与优化

在实际测量过程中,哈希碰撞的存在,使用Count-Min Sketch等结构往往会导致测量结果偏大[61]。且由于PDP有限的资源,部署复杂的Sketch算法存在各种限制,需要对Sketch结构进行设计和优化以支持丰富复杂的测量任务。

分级存储的思想经常运用在Sketch结构中,能够节约存储和查找开销。Elastic Sketch[62]提出一种

分离技术Ostracism，将象流和老鼠流信息分别存储在Hash表和Count Min结构中。当数据包速率变高时，仅处理Heavy Part部分信息并对Light Part进行压缩与合并。实验表明，Elastic Sketch以合理的精度下降为代价实现更高的处理速度和更低的带宽开销，能够弹性适应网络条件变化，执行多种监控任务；类似地，Filter-Sketch[63]为了减少计算熵值时的存储和计算开销，用两层Sketch结构分别存储大象流和老鼠流，并对熵值的计算过程进行优化，可以运用于精细流量分类、负载均衡、异常检测等任务。实验表明Filter-Sketch比现有数据平面算法具有更高的精度，相对误差平均降低了0.65%；FCM-Sketch[64]进一步在数据平面采用多级树状结构，考虑到网络流量中规模较小的流量占比更高，FCM-Sketch在叶子节点处使用大量小规模计数器，在核心节点处使用少量大规模计数器，传入的流量首先在叶子节点处计数，溢出后向高级计数器“进位”。控制平面采用EM算法从数据平面收集的信息中恢复各种统计信息，能够支持各种测量任务。实验表明，FCM-Sketch与CM Sketch、Elastic Sketch、UnivMon等测量方案相比，可以减少50%～80%的误差。

一般的Sketch结构仅能存储计数值而不能反推出流标签，而可逆Sketch能够从Sketch结构中恢复所有的流标签。MV-Sketch[65]引入多数投票机制，支持更新（插入新投票）和查询（估计流的值）两种基本操作，更新操作遵循主选票算法（majority vote algorithm，MJRTY），而查询操作通过计算行估计值并取最小值来估计流的值，能够有效地跟踪候重要流量，减少了更新和查询操作中的内存访问次数，同时维持了高检测精度。

QPipe[66]是一种能够计算分位数的Sketch结构，通过巧妙设计delete()、recirculate()、findMin()等操作实现argmin()函数，在数据平面实现了SweepKLL算法，得到流的顺序统计信息，其在HHD任务上的表现优于CM Sketch。

实时检测网络数据中持久性和不频繁（Persistent and Infrequent，PI）流量对于检测入侵等活动具有重要意义。PISketch[67]是首个旨在实时发现PI流量的Sketch结构，通过定义每个流量的权重并设计奖励和惩罚机制，描述并挖掘流量的持久性和不频繁性特征；进而提出权重融合策略，即使权重不断变化也能识别高权重流量。作者对PISketch的准确性和效率进行了严格的理论分析，并通过实验实现了APT流量和FRP流量的初步检测，验证了PISketch的有效性。

对每个键维护一个单独的Sketch结构会造成计算和存储资源的浪费，而大部分研究不能同时支持多个键值。CocoSketch[68]能够实现任意键查询，根据USS（Unbiased SpaceSaving）的思想，CocoSketch通过巧妙的设计将部分键查询转化为子集和估计问题，通过引入随机方差最小化策略能够减少更新操作需要的内存访问次数，减少包的更新时延，同时移除数据包更新逻辑中的循环依赖关系。实验表明，同时测量6个键时，CocoSketch将平均分组处理吞吐提高了27.2倍，精度提高10.4倍。

表8对PDP中Sketch结构设计与优化的相关内容进行总结。当前，大部分此类研究主要采用对数据结构、测量算法优化的思路，从而使得在数据平面支持复杂的测量任务。其中能够完成流大小估计和重要流检测任务的Sketch结构最多，而对其他任务的支持相对较少，这可能是因为这两项任务以计数为主，需要的资源最少，需要执行的操作最简单。

表8　PDP中Sketch结构设计与优化研究总结

工作	平台	测量任务						主要思想
		FSE	FSDE	HH	HC	EE	CE	
QPipe[66]	Tofino BMv2	√	×	√	×	×	×	数据平面实现SweepKLL算法计算分位数，得到流的顺序统计信息
Elastic Sketch[62]	Tofino	√	√	√	√	√	√	提出大小流分离测量与Sketch压缩，适应网络环境变化
Filter-Sketch[63]	BMv2	√	×	√	√	√	×	双层Sketch结构获取流量熵值
MV-Sketch[65]	Tofino	√	×	√	√	×	×	一种快速紧凑型可逆Sketch，可用于全网大流检测
FCM-Sketch[64]	BMv2	√	√	√	√	√	√	数据平面采用多级树结构，不同层级采用不同大小的计数器
PISketch[67]	Tofino FPGA	√	×	√	×	×	×	检测网络数据中持久性和不频繁流量
CocoSketch[68]	Tofino FPGA	√	×	√	×	×	×	将任意键查询问题归结为子集和估计问题，能够支持多键查询

(2) 配置优化

在进行网络监控过程中,通常会同时运用多种Sketch结构执行多种测量任务,然而由于资源有限,需要进行配置优化,主要方案有动态优化、资源优化、参数配置优化三种方法。

动态优化:ChameleMon[69]提出当网络状态发生变化时,为数据包统计和丢包检测两类测量任务动态分配内存,其核心在于设计一种灵活的数据结构FermatSketch,可利用费马小定理进行流量ID的模加聚合,能够以较低内存开销检测数据包丢失;控制平面收集Sketch信息并进行分析,依据网络状态实时调整监控重点。

HeteroSketch[70]包含性能分析工具和优化器两个组件:性能分析工具用于离线性能特征化,生成设备性能与资源消耗的代数描述作为设备特征;优化器将资源分配问题转化为混合整数双线性规划(MI-BLP)问题,求解满足设备约束、监控需求、流量需求下的Sketch放置策略。为了适应大规模网络系统和网络动态变化,HeteroSketch进行如下优化:(1)采用分层优化策略将网络拓扑划分为互不相交的集群,在每个集群内分别进行优化,减少计算复杂度;(2)通过递归应用集群划分和优化步骤,构建集群层次结构,以进一步提高可扩展性;(3)引入快速路径机制,针对网络动态变化,快速重新计算受影响设备上的监控部署,实现快速响应。实验评估表明,与现有技术相比,HeteroSketch能够减少20%至60%的资源开销。

资源优化:Namkung等[71]详细分析了Sketch部署在可编程交换机上时存在的硬件资源瓶颈,并针对性提出一系列优化技术,包括合并短位哈希、消除依赖性、重构多级Sketch等,显著降低了硬件资源的使用,同时保持了准确性。这些优化技术集成到SketchLib库中,提供易于使用的P4接口。实验表明SketchLib对7种Sketch的优化降低了96%的硬件资源使用而不影响准确性。

在执行大规模网络性能监控任务时,维持网络中每个流的状态是不切实际的。Liu等[72]基于重定义的流模型表征性能监控问题,定义了“流量可加性”属性,即某些性能指标可以通过聚合单一流量的数据来估计整个网络的指标。对于满足这一属性的指标,可以采用lean算法检测最显著的流,识别导致最高时延、丢包、乱序和重传的流量等,可以有效地检测网络性能问题,该算法仅使用与流数量成次线性关系的内存。

Sketchovsky[73]是一个支持多Sketch组合与优化的框架,能够在有限硬件资源下运行多个测量任务的Sketch实例。作者提出在多个Sketch实例运行时其中的部分重要硬件资源可以重用,据此将资源重新划分构建了五个优化模块;然后以最小化硬件资源开销为优化目标构建一个组合优化问题。由于搜索空间大、依赖关系复杂,Sketchovsky将搜索空间分解,利用启发式算法求解最优策略,能够将五个优化模块应用于不同Sketch实例。实验表明,Sketchovsky在集成数十个Sketch实例时可以减少45%的硬件资源开销。

多数测量任务需要在编译阶段完成配置,由于资源限制,不能同时支持大量任务同时运行。FlyMon[74]提出将测量任务执行与编译过程解耦,其核心特点是能够支持实时任务的重新配置。FlyMon引入可组合测量单元(Composable Measurement Units, CMUs)的概念,作为一种通用的操作单元,CMUs可以根据不同的流键和流属性进行灵活配置,使得系统能够在运行时动态调整测量任务,而不需要在编译阶段就绑定。FlyMon在Tofino芯片上实现了高效的资源管理和任务切换,支持多种流量属性的测量任务,且能在毫秒级别配置内存。

参数配置优化:网络测量资源分配与参数配置紧密耦合,然而对所有流量预先设置固定的参数给网络运维人员带来了极大的负担,测量结果的精度也难以量化。

SketchGuide[75]用于在PDP上自动配置和优化Sketch网络测量,能够解决Sketch部署过程中在参数配置、精度需求、资源开销预算等方面存在的问题。SketchGuide首先根据硬件相关原语确定可配置参数并使用P4模板文件重构程序;通过定义Sketch Skyline表达式明确资源和性能之间的权衡,然后利用贝叶斯优化器搜索最优配置;最后基于神经网络预测不同工作负载下的准确性,为用户选择配置提供支撑。利用SketchGuide,用户可以自由配置Sketch满足各种服务目标。

SketchLearn[76]提出一种避免手工配置参数的方法:理论分析表明多级Sketch的计数值应当服从高斯分布。据此,SketchLearn迭代地提取大流量,每一次迭代后更新统计模型,利用统计模型学习流量统计特性,直到所有计数器分布服从高斯分布,确保对小流量的准确建模,避免了手工参数配置。

表9对上述研究进行总结,根据动态优化、资源优化、参数配置优化三种策略,可以使得多个Sketch

表 9　PDP 中 Sketch 资源优化配置研究总结

研究思路	工作	平台	主要思想
动态优化	ChameleMon[69]	Tifino	依据费马小定理设计FermatSketch，能够为测量任务动态分配内存
	HeteroSketch[70]	SmartNIC	解决Sketch的放置策略与资源分配问题
资源优化	SketchLib[71]	Tofino	针对Sketch部署的硬件资源瓶颈提出一系列优化技术
	Liu等[72]	Tofino	设计lean算法用次线性内存实现大规模流数据的性能监控问题
	Sketchovsky[73]	Tofino	多Sketch在有限硬件资源上的优化与组合
	FlyMon[74]	Tofino	测量任务执行与编译过程解耦，支持实时重构
参数配置优化	SketchGuide[75]	Tofino	解决Sketch配置部署过程中参数配置、资源开销、精度需求方面问题
	SketchLearn[76]	OVS	构建多级Sketch学习流量统计特性解决资源冲突

结构能够利用有限的计算存储资源执行多样化的测量任务，未来可以研究多策略结合的方式，进一步优化Sketch资源配置。

4.1.2　基于INT的网络监控

INT是一个基于PDP的网络测量框架[77]，其工作原理如图6所示。INT通过在数据包中嵌入额外的元数据，使这些数据包在穿越网络时能够携带有关路径状态和性能的信息。随着数据包的传输，沿途的每个INT节点都可更新这些信息，最终服务器解析并分析这些数据。相较于传统测量方式，INT具有支持数据包级别的细粒度监控、支持端到端状态追踪监控、对用户透明的优点[78]。

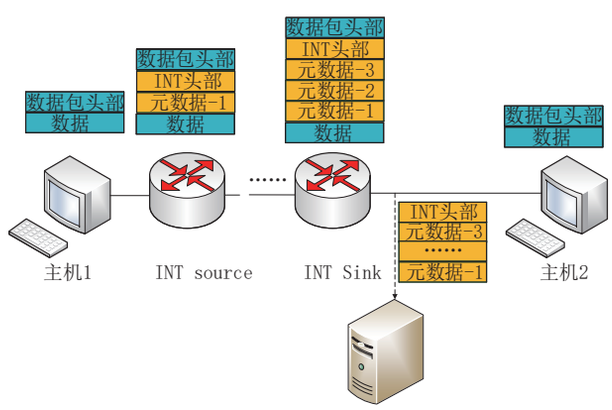

图 6　INT工作原理

近年来，利用INT技术，学术界和工业界都提出了很多网络监控方案，主要围绕如何在保障遥测精度的同时减小测量开销这一问题展开。

（1）遥测开销减少

减少INT开销有助于降低网络设备处理遥测数据时的负担，可以从采样机制和触发机制两个角度考虑。

采样机制：FS-INT[79]提出的INT监控方案，包含基于包速率和基于事件两种采样机制。基于包速率的机制，每间隔固定数量的数据包，插入一个INT头部和全部的INT元数据；基于事件的采样机制，对每一个数据包，由转发设备决定需要被插入的INT元数据。实验结果证明，基于包到达率的采样机制的开销随着采样频率的增加线性增加，但精度不高；基于事件的采样机制精度较高但开销降低不明显。P4InfoSen-INT[80]提出动态采样机制，利用信息熵衡量信息内容的重要性，从而决定是否插入INT头部。虽然算法复杂度高于传统算法，但通过设计表合并优化技术与状态更新机制，降低了资源消耗；DeltaINT[81]仅在网络状态变化较为显著的情况下将遥测数据嵌入数据包，减少了93%的网络带宽；ProML-INT[82]只选择属于同一IP流的部分数据包插入INT头部。上述方案通过设计不同的采样机制，兼顾遥测系统的精度和开销。

事件触发机制：由于大多数应用更为关心网络中突发的事件[83]，通过设定不同的事件触发机制，也能够降低系统开销。INTCollector[84]能够从INT原始数据中提取出重要的网络事件，通过正常路径将事件和遥测值存储到数据库中，而由快速路径处理INT报告数据，能够减少CPU负载和存储开销；Vestin等[85]提出INT事件检测机制，可以在控制平面自定义规则，决定每个流中需要上报的事件，可以减少遥测服务器的负载。实验表明，相较于传统方案，该方案单位事件内处理遥测头的容量增加了10-15倍。

除了上述通过设计采样机制和事件触发机制的方案以外，Papadopoulos等提出PFA-INT框架[86]，对流进行聚合，通过限制传输开销提升遥测系统性能；Alhamed等[87]在测量过程中实施两阶段遥测信息收集，并提出不同级别遥测数据的聚合方法，显著降低了遥测服务器的资源开销，提高系统扩展性。LossSight[88]通过交替标记遥测数据包进行丢包检测、定位、诊断，并可以通过生成对抗网络（Generative Adversarial Nets，GAN）[89]恢复缺失的

遥测信息；Jia C等[90]提出一种INT灰色故障快速检测和定位机制，当网络发生故障时，服务器可以主动执行源路由快速重定向，避免大量数据包丢失，保持网络不中断的服务。

(2)遥测任务编排

上述研究主要针对单一节点，对全网测量节点的合理调度、规划能够进一步提高测量效率。INT任务编排是指以较低成本和较高效率实现对网络遥测的范围的较大覆盖，充分满足上层应用的测量需求。现有的INT编排研究主要分为基于探针路径规划和基于遥测任务组合优化两类[78]。

探针路径规划：基于探针路径规划的方案，主要思想是以最小化开销为优化目标，通过设计探针路径，完成对遥测范围的全面、高效覆盖。Pan等提出INT-Path方案[91]，将源路由信息嵌入INT探针中，设计基于深度优先算法(Depth First Search，DFS)和基于Euler-trail的两种路径规划策略。前者简单高效，后者理论上能够生成覆盖网络的最小路径，具有最小的遥测开销；同样地，Castro等[92]利用路径规划模型，生成能够覆盖全部链路的探针最优路径。

INT任务组合优化：基于遥测任务组合优化的方案，主要是对多遥测任务的建模与优化[83]，合理编排各项测量任务。Marques等[93]首次提出遥测任务编排问题(In-band Network Telemetry Orchestration，INTO)。在INTO中，INTO-Concentrate模型可以归结为装箱模型，INTO-Balance模型可以抽象为多处理器问题，作者对于这两个NP-Complete问题给出了启发式算法求解；在此基础上Hohemberger等[94]提出INT编排计划问题(In-band Network Telemetry Orchestration，INTOPP)，通过形式化分析和理论证明，将INTOPP问题抽象为一个混合整数线性规划问题(Mixed Integer Linear Problem，MILP)，并利用机器学习方案求解；Bhamare等人提出IntOpt[95]方案，通过设计基于模拟退火和贪心算法，对监控任务进行编排优化，最大限度减少监控开销和时延。

除了上述研究遥测开销减少与遥测任务编排的工作，INT需要进行解封装、插入、封装等操作，可能会导致潜在的安全危险，如伪造测量数据包进行恶意非法攻击等，遥测数据以明文传输也可能会泄露用户隐私。Pan等[96-97]利用同态加密设计了一种INT数据加密方案，通过对加密的INT数据进行签名编码，INT服务器可以验证INT数据完整性，从而消除了数据篡改对遥测数据安全的威胁。

作为PDP当前最具有代表性的应用之一，INT已经在工业界进行推广部署，并取得了良好的效果。表10对当前INT相关研究进行总结，对于INT方案监控方案优化，基于采样机制和事件触发机制的方案各自存在优缺点，两者的结合能够兼顾开销和精度；而对于INT任务编排，主要局限在于对建模后的优化问题进行求解，未来研究可以考虑引入启发式算法、强化学习等方法求解。另外，在云网融合环境下，SRv6作为一种新型路由机制得到广泛应用，将源路由机制灵活的路径编排控制能力、网络编程能力应用于INT探针路径规划，具有很强实际意义。

表10 INT研究总结

研究方向	方案	主要思想	存在的限制
INT监控方案优化	FS-INT[79]、P4InfoSen-INT[80]、DeltaINT[81]、ProML-INT[82]	通过设计合理的采样机制减少测量开销	可能忽略网络中关键变化
	INTCollector[84]、Vestin等[85]	通过设计事件触发机制捕捉网络中流量关键变化	对网络的持续性监测存在不足
INT任务编排	INT-Path[91]、Castro等[92]	设计探针路径，完成对遥测范围的高效覆盖	对多INT任务的支持存在局限
	INTO[93]、INTOPP[94]、IntOpt[95]	对多遥测任务的建模与优化	优化问题求解困难

4.1.3 其他监控方式

SketchINT[98]是一种结合INT和Sketch的网络测量方案，利用INT准确获取细粒度的流量信息，利用Sketch压缩INT节约带宽。为了充分融合Sketch和INT的优势，SketchINT设计了TowerSketch结构，该结构仅由一些计数器阵列和Hash函数组成，利用不同大小的计数器对不同流量精准计数。实验表明，SketchINT在误差上优于Elastic Sketch 13.9倍，相较于INT载荷减少了3～4个数量级。类似的，LightGuardian[99]提出一种利用Sketch的带内测量方案。LightGuardian设计SuMax Sketch结构，该结构由sum cell和maximum cell构成，可以支持多种类型的测量任务。每一个设备本地的SuMax Sketch可以分解为更小的sketchlet结构嵌入数据包头部，在网络内传输，终端主机对收集到的sketchlet进行聚合、重建、分析。为

确保鲁棒性，LightGuardian设计一种能够容忍sketchlet丢失以及乱序的重建算法，可以通过部分sketchlet集合近似原本的Sketch。实验证明，在一个由16台主机，20台交换机构成的Fat-Tree的拓扑中，LightGuardian仅用0.07%的网络总带宽，可在1.0 s～1.5 s内持续以较小开销持续收集全网流量逐跳信息。

OmniMon[100]提出，通过全网实体间的协作可以避免对单一节点的资源限制。OmniMon将网络遥测重构为split和merge两个步骤。split将网络遥测分解为模块化操作，可在不同实体间调度；merge协调所有实体执行遥测任务；控制器对全网资源进行管理和联合分析。为支持分布式系统，OmniMon提出一种全网周期同步机制以保证一致性，推断每台交换机、每个流精确的流量损失保证可信，在数据中心取得了良好的实验效果。

4.2　流量分析

流量分析是一种重要的网络安全检测手段，用于识别恶意流量、异常行为等。利用PDP能够实时处理网络流量数据，提供及时、准确的流量分析结果。现有研究主要有基于统计信息和基于机器学习两种。

4.2.1　基于统计信息的流量分析

基于统计信息的方法主要思想是在数据平面用Hash表、Sketch等数据结构对网络流量的某项指标进行统计，当计数值偏离正常范围时，则视为异常流量，采取相应的措施。

BACKWARD[101]设计BACON sketch结构，利用多Hash表存储各源IP地址发送的数据包数量，从而确认top-k个可能的攻击者。P4-PSFP[102]监测不同时间片内数据包转发过程，并根据是否超过承诺信息速率和超额信息速率对数据包进行分类，对不满足合规性的数据包执行丢弃操作。4MIDable[103]是一个基于P4实现，将网络中间件和监控应用集成到SDN环境的框架。在4MIDable的数据平面pipeline中，parsing stage解析数据包头部，detection stage通过meters、registers和counters以计数的方式实现检测；在4MIDable框架基础上，Benjamin等开发P4ID[103]应用监控数据包数量，并在网络中部署Suricata IDS，一旦数据包数量超过阈值，将会触发IDS。

当遭受流量攻击时，源IP和目的IP的分布会受到干扰，由于攻击IP地址的广泛分布，源地址的熵往往会增加；相反，由于受害者IP地址的高重现性，目的地址的熵趋于减小，因此可以通过熵值进行检测。但目前P4不支持计算熵值需要的浮点数计算、对数计算操作，为此Lapolli等[104-105]提出在BMv2中计算IP地址熵值的方法：将熵值计算公式合理简化为对每个不同IP地址出现频率的函数，并利用count sketch进行频率近似，该结构可以用次线性空间表示数据流中事件发生的频率表。然后设计LPM lookup表，预计算熵值计算需要的对数函数值，从而可以得到熵值的近似测量值。最后计算实时熵值估计序列的集中趋势和离散度作为判断依据；类似地，BUNGEE[106]将数据包分为固定数量的数据包窗口，对每个窗口计算熵值并与正常网络操作期间观测的熵值范围比较，当观测值超过阈值时，说明存在攻击行为。为了使熵的阈值设定更加合理，Wang等[107]设计熵感知检测方案，使数据平面能够动态调整阈值，增强了对DDoS-F攻击的识别精度，减少了误报率；Li等[108]提出一种混合入侵统计阈值算法（Hybrid Intrusion Statistical Threshold Algorithm，HISTA）检测跨层恶意攻击，该算法利用熵值及其变化率评估恶意数据包分布情况，并利用粒子群优化算法确定最佳的阈值，提高检测准确性和响应精度。

除了上述对数据包计数以及计算熵值外，还有其他指标也可以用于检测攻击行为。HH-IPG[109]提出使用每流间隔（Inter-Packet Gap，IPG）分析替代传统的流计数方法，通过实时计算IPG并使用加权移动平均方法平滑流量波动，不仅在准确性上比现有方法提高了20%，还增强了检测的稳定性。Jin等[110]提出HCF方法，认为恶意流量数据包的跳数与正常数据包的跳数分布存在显著不同，可以用于检测攻击行为。NETHCF[111]将HCF解耦，数据平面缓存处理最频繁的IP，控制平面负责处理缓存未命中、网络变化以及路由改变的情况，两者协调运作维护IP2HC表，存储IP地址到跳数的映射关系，筛选出异常来源的数据包；Dimolianis等[112]结合流量的数量、子网重要性（子网流量占总流量比例）以及对称性（输入输出的流量比例）特征，提供快速的攻击检测。

表11对上述研究进行了总结，可以看出当前采用较多的数据结构是Sketch和Hash表，大多对数据包源IP、熵值等指标进行统计。然而，将统计结果与阈值比较判断流量是否异常，这种方法缺乏自适应性，当环境变化时需要手工调整，且能够检测的异常行为也相对单一。

表 11 PDP中基于统计信息的流量分析研究总结

工作	平台	统计指标	数据结构	主要思想	存在的限制
BACKWARD[101]	BMv2	源IP	BACON sketch	统计源IP数确认top-k个可能的攻击者	采用单一链路的流量数据集
P4-PSFP[102]	Tofino	流量速率	GCL	采用“两速率三标色”法对数据包分类	对流量的标识机制过于简单
4MIDable[103]	BMv2	-	Count-Min Sketch	统计指标超过阈值将触发IDS	需要依赖Suricata
Lapolli等[104-105]	BMv2	熵值	Count Sketch，LPM lookup table	将熵值计算简化为对每个不同IP地址出现频率的函数	部分参数更新时需要控制器重新部署新的P4程序
BUNGEE[106]	BMv2	熵值	Count-Min Sketch	数据包分为固定数量的数据包窗口计算熵值	采用静态阈值，对流量实时变化适应性差
Wang等[107]	BMv2	熵值	Count-Min Sketch	根据网络状态动态调整熵阈值	应对攻击类型有限
Li等[108]	BMv2	熵值	Count	利用PSO算法搜索最合适的熵值及变化率阈值	数据包头部中引入额外的长度
HH-IPG[109]	Tofino	IPG	Hash表	统计每流间隔信息进行检测	可能会忽略少量特殊模式的流量信息
NETHCF[111]	Tofino	跳数	IP2HC表	利用数据包跳数检测恶意数据包	不适用与网络中存在NAT的场景
Dimolianis等[112]	SmartNIC	子网重要性、对称性	Bloom Filter	提供快速的DDOS攻击检测	处理高流量时性能显著下降

4.2.2 基于机器学习的流量分析

传统网络中利用机器学习进行流量检测时，特征抽取、模型训练、模型更新等工作都在控制平面进行，导致控制平面容易成为性能瓶颈；且模型训练只能依赖提前收集的数据集而非实时流量，模型精度不高、迁移性较差。引入PDP后，可以将部分任务卸载到数据平面进行，减轻控制器的负担，同时可以利用实时流量进行模型训练。

根据机器学习模型部署的位置，可以将PDP上基于机器学习的流量分析方法分为两类，即控制平面机器学习和数据平面机器学习。

（1）控制平面机器学习

如图7所示，控制平面机器学习的方法仅利用PDP解析数据包并提取数据包特征，收集各类统计信息，然后上传到控制平面。在控制平面部署ML模型，对数据包进行分类，同时负责模型的训练、更新，然后将分类结果下发至数据平面，对数据包执行相应的操作。

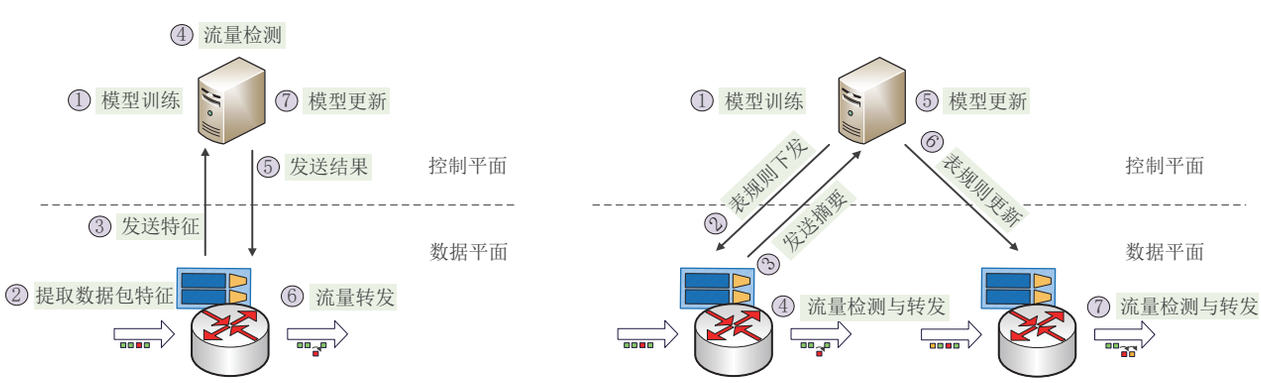

图7 PDP中基于机器学习进行流量分析的两种方法

ORACLE[113]中，数据平面负责收集和处理流量信息，存储在寄存器中。当信息更新时，上传至控制平面；控制平面计算流量特征，利用随机森立（Random Forest，RF）和K近邻（K-Nearest Neighbor）算法检测DDOS攻击，准确率高达96%；P4-HLDMC[114]基于P4设计多状态匹配函数MSMPF，通过9个state table监视、分析和提取网络流量特征，在控制平面根据6种机器学习分类器投票的结果识别DDOS攻击和ARP攻击，在AUC指标上达到了99.86%的最高值；Wang等[107]提出在控制平面部署DNN模型分析数据平面发送的摘要信息，识别非DDoS攻击。AlSabeh等[115]提出利用RF在数据平面和控制平面联合检测基于域名生成算法（Domain Generation Algorithms，DGA）的恶意

软件方法。在数据平面解析器逐步解析域名进行初步检测；当检测到DGA时，提取的特征会被发送到控制平面进行更深入的分析；唐馨[116]提出两种利用PDP检测LDoS攻击的方法：半卸载式的检测方法在数据平面进行基于固定预阈值的粗检测、控制平面进行基于LVQ-SVM算法的精细检测；全卸载式检测方法引入滑动窗口、自适应阈值等方法实现动态监测。两者检测时间均在毫秒级，且实现了控制平面的零消耗。

特征工程是机器学习的重要环节，对特征的选择、处理往往对模型的精度有很大的影响。MP-GUARD[117]在数据平面动态提取特征，并创建22个特征集实现对网络流量的全面分析，在多个性能指标上表现优异；P4DDLe[118]在利用数据平面提取数据包特征的基础上，采用Bloom过滤器高效选择和存储与机器学习模型相关的数据包特征，避免了冗余数据的存储；HybridDAD[119]定义多种用于检测的数据包特征，在P4 pipeline中克隆数据包并提出特征，随后通过多种机器学习算法对流量分类，可检测多种类型的DDOS攻击；Qin等[120]提出控制平面利用Dilated CNN模型，将原始包字节作为输入训练神经网络，然后在第二阶段中选择权重最大的子字符串加入数据包的头部中，并在MAT中添加相应的规则。这种方法无需手动预处理数据或针对每个协议重新设计特征提取算法，具有更广泛的适用性；此外，考虑到PDP内存资源有限，FlowLen[121]在数据平面对每个流固有特征压缩得到更为紧凑的特征，即flow marker。FlowLen设计FMA（Flow Marker Accumulator）这一数据结构收集flow market，并可以通过量化和截断操作选择最合适的特征。在隐蔽通道检测的实验中，FlowLen使得系统监控能力提升150倍而准确率仅下降3%；Krishnan等[122]基于FlowLen框架，在控制平面利用LightGBM模型进行窃听检测和Mirai僵尸网络检测，在不损失精度的条件下节约90%以上的内存。

表12对当前PDP中基于控制平面机器学习的流量分析研究进行总结。这种方法易于部署且适用于多种ML算法，存在的主要问题在于虽然PDP负责对数据包进行采样和特征提取操作，但模型训练和检测的过程仍依赖于控制平面，对控制器的负担太大，没有充分发挥PDP的各种优势，在检测效率和实时性上存在一定局限性。且由于模型需要预先在控制平面部署好，训练时依赖单一数据集对模型泛化能力、精度也有一定影响。

（2）数据平面机器学习

PDP不仅具备数据包解析和转发功能，还能通过编程实现复杂的计算任务和网络功能，在数据传输过程中进行实时计算和分析，这样不仅能降低通

表12　PDP中基于控制平面机器学习的流量分析研究总结

工作	采用模型	提取特征	主要思想	存在的限制
ORACLE[113]	RF、KNN	流的持续时间、包间到达时间标准差、包负载大小均值和标准差	数据平面收集和处理流量信息，控制平面负责计算和分类特征集	时间窗口的选择是否合理
P4-HLDMC[114]	SGB、KNN、DT等	数据包速率、平均窗口流数据包、目标IP熵、源端口入口速度等	设计多状态匹配函数MSMPF，通过9个state table监视、分析和提取网络流量特征	多状态表存储开销大
Wang等[107]	DNN	KDD-Cup99数据集特征	分析数据平面发送的报告，识别非DDoS攻击	对数据平面发送的报告要求较高
AlSabeh等[115]	RF	DNS数量、域名长度、n-gram、请求间隔等	数据平面进行初步检测，控制平面进行深入检测	数据平面和控制平面的交互延迟、隐私问题
唐馨[116]	LVQ-SVM	端口数据包出入差、数据包平均字节数、数据包个数	根据对数据平面两种利用程度提出两种LDoS攻击检测方法	泛化能力可能有限
MP-GUARD[117]	SELDP4-FS	流时长、报文计数、字节计数等	动态提取特征，构建新的特征集	多控制器部署问题
P4DDLe[118]	LUCID	时间戳、数据包长度、协议类型、数据包标志位、源IP地址熵值等	采用Bloom过滤器优选特征	控制平面和数据平面之间的并发访问可能导致竞争条件
HybridDAD[119]	RF、KNN、SVM、RNN	数据包平均长度、各类型数据包数量	定义多种特征用于多机器学习算法流量分类	多种机器学习算法是的控制平面开销大
Qin等[120]	Dilated CNN	原始数据包字节	自适应特征选取算法	无法进行实时检测与响应
FlowLen[121]	XGBoost、Bayes	flow market	对每个流的长度和分组间隔分布压缩得到更为紧凑的特征	依赖于特定机器学习和预定义特征，对新算法适应性受限
Krishnan等[122]	LightGBM	flow market	窃听检测和Mirai僵尸网络检测	实验对比标准不明确

信延迟，还能提高整体计算效率。但由于硬件资源限制，目前大多数ML算法无法直接在网络设备中部署，需要进行改进和适配。

决策树(Decision Tree，DT)是一种有监督的机器学习方法，用于分类和回归任务。由于DT涉及的运算操作简单，因而P4不支持浮点数的限制对决策树工作流程影响较小，这为将DT部署于数据平面提供了可能。DT是当前在数据平面部署最多的机器学习模型，可以将树状结构用pipeline流水线表示，如图8所示，每一层用一级pipeline表示，分类阈值在匹配规则中表示。

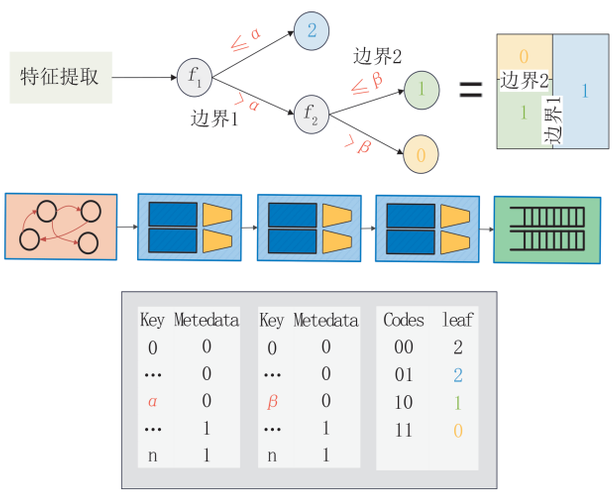

图8 PDP部署树模型

Haribabu等[123]利用决策树检测恶意数据包，重点研究数据包头部各字节对分类判定的重要程度；Ganesan等[124]提出在数据平面利用决策树和逻辑回归模型识别控制平面中决策边界，然后转换为MAT中的规则用于入侵检测。实验结果表明，所提出方法能够实现与离线运行检测算法相同程度的分类精度，且具有良好的性能和可扩展性。

在DT的基础上，可以进一步采用集成学习进行检测。pForest[125]利用随机森林(Random Forest，RF)模型对网络流量进行实时分类，通过贪婪算法生成多个局部最优的RF模型，每个模型针对网络流的前x个数据包进行优化，并能够实时动态切换这些模型，解决了动态适应特征和分类逻辑的问题。为了适应PDP的限制，pForest优化了模型的训练和特征选择过程，通过压缩特征存储、动态分配内存以及使用哈希索引策略管理，来优化内存使用并提高处理效率；P4Pir[126]在IOT网关中集成DT和RF模型，采用主动日志记录和无监督标记的方法，实现了流量特征的持续学习，增强了模型的自适应能力。为了解决检测过程中无缝更新模型的问题，P4Pir通过阴影表更新方案确保网关服务的连续性和稳定性；HorusEye[127]是一个专为物联网设计的恶意流量检测框架，分为两个阶段：第一阶段在数据平面部署Gulliver Tunnel检测模块，通过将训练好的孤立森林(iForest)模型转换为白名单匹配规则，能够利用无监督模型在数据平面上检测未知攻击，该模块设计了一种物联网流特征提取方案，利用双哈希方法，仅以O(1)的复杂度匹配双向流，从而快速区分异常行为。第二阶段在控制平面部署Magnifier检测模块，采用轻量级不对称自动编码器，结合分离卷积和膨胀卷积，实现了高吞吐量的同时不显著降低检测性能。数据平面Gulliver Tunne模块快速过滤出可疑流量，并将其报告给控制平面Magnifier模块进行进一步深入分析，两阶段协同工作，实现高效率和高精度的物联网异常检测，能够达到高达99%的异常检测率。

除了树模型外，二进制神经网络(Binary Neutral Network，BNN)也常用于部署在数据平面。P4-BNN[128]在PDP上实现BNN，通过设计特殊的数据结构、等价替换编程的方法代替乘法和矩阵运算，并提出一种不需要浮点运算的归一化方法，简化模型部署。实验结果表明，在异常检测任务的准确率达到了96.4%。

在数据平面对多模型的支持也有相关研究。Xiong等[129]详细讲述如何将决策树、SVM、朴素贝叶斯、K-means四种机器学习模型映射到MAT中，提出IIsy框架，应用于网内数据包分类。Planter[130]是一个通用的网内计算框架，旨在简化将ML模型部署到PDP的过程。Planter将机器学习模型按照在数据平面中的实现方式分为三类：基于编码的解决方案(Encode-Based Solutions，EB)、基于查找的解决方案(Lookup-Based Solutions，LB)和直接映射解决方案(Direct-Mapping Solutions，DM)，每种方案设计特定的实现方法和适用场景，通过数据加载、模型训练与转换、P4代码生成、模型编译与测试等步骤，能够将训练好的模型转换为适合在Tofiono、BMv2、P4Pi等可编程平台执行的格式。

大规模网络中控制平面与数据平面的交互可能会增加通信开销，同时在数据共享、模型参数更新过程中可能引起隐私问题。为此，Zang等提出一个基于联邦学习的分布式网络内流量分析框架FPIP4[131]，通过引入联邦学习和差分隐私协调模型训练和推理过程，在边缘网关上实现实时攻击检

测。在FPIP4中，Trainer部署在网关的控制平面负责预处理本地数据、训练本地模型；Mapper负责将本地模型映射到MAT中；Aggregator负责聚合各本地模型，更新本地模型参数。实验结果表明，FLIP4能够实现准确的攻击检测，同时保持数据隐私。

表13对上述研究进行总结，当前在数据平面进行ML已经取得了一定的进展。相较于传统ML流量检测以及控制平面部署ML流量检测的方法。在数据平面部署ML模型具有更快的检测速率，且可以直接利用现网流量训练，模型泛化能力更强。然而在数据平面部署ML模型在检测精度上未必能带来很大的提升，甚至由于当前PDP能够支持的ML模型相对有限，仅支持类似于DT、RF、SVM的简单模型，类似于CNN、RNN的深度学习模型由于模型结构复杂、参数过多，还无法部署在数据平面，这对检测的精度也会有一定影响。

表13　PDP中基于数据平面机器学习的流量分析研究总结

工作	平台	采用模型	提取特征	主要思想	存在的限制
Haribabu等[123]	BMv2	DT	数据包总长度、TCP标志位	研究数据包头部各字节对分类判定的重要程度	模型精度、泛化性存在缺陷
Ganesan等[124]	BMv2	DT、LR	数据包大小、数据包数量、端口号、协议类型	利用决策树和逻辑回归模型识别控制平面中决策边界	动态更新机制不明确
IIsy[129]	BMv2 NetFPGA	DT、SVM、Bayes、K-means	EtherType、端口号、协议类型	将四种机器学习算法映射到MAT中	特征集静态
pForest[125]	Tofino	RF	源/目IP、端口号、连接持续时间、包状态等	通过贪婪算法生成多个局部最优的RF模型	只能跟踪固定数量的并发流
P4Pir[126]	P4Pi	DT、RF	源/目IP、源/目端口、MQTT协议相关信息等	流量特征持续学习、模型无缝更新	单一网关下适用场景有限
HorusEye[127]	Tofino	iForest、Autocoder	数据包数量和大小、窗口内数据包间隔、时间特征等	数据平面和控制平面两阶段协同工作	量化可能会对模型性能产生影响
P4-BNN[128]	SmartNIC	BNN	端口号、数据包长度、TTL	将复杂运算简化	多分类任务精度显著下降
Planter[130]	Tofiono; BMv2;P4Pi	DT、RF、XGBoost等	源/目的IP、端口号、协议类型、KDD99数据集部分特征	一个通用的网内计算框架	某些情况下分类结果可能不准确
FPIP4[131]	BMv2	XGBoost	源/目的IP、端口号、协议类型、标志位	基于联邦学习的分布式网络内流量分析框	联邦学习中的隐私安全性没有考虑

4.3　其他检测技术

除了对网络状态监控和流量分析外，在PDP中还存在一些其他检测方法，如通过衡量正常行为与实际行为间的差异性可以检测异常。Sanghi等[132]通过跟踪和分析数据包在可编程交换机中的执行路径，并与预先定义的正常行为模型进行比较来检测异常行为。Kang等[133]通过概率性符号执行分析系统的预期行为，确定常见和边界行为。然后利用实时监控器来监测流量模式是否正常。实验证明，该方法能够有效发现并展示对简单数据平面系统的攻击可行性。

除了上述对正常行为建模的方法，对攻击行为的精准描述也有利于检测异常行为。Laraba等[134]提出在检测时用EFSM模型表示多步攻击中每一阶段的各类攻击行为；在决策时，将Petri Net模型映射到P4 pipeline中，可以通过MAT描述多步攻击过程中攻击事件的组合、同步、联合语义。

根据上述内容，对比发现：传统安全检测机制通常依赖于专用的安全设备，这些设备被部署在网络的关键节点以监控和分析流经的网络流量。但是为了使流量能够通过安全设备进行检查，必须将原本直接由交换机或路由器传输的数据包重定向至这些检测设备，这一过程不可避免地引入了额外的传输延迟，增加了整体检测时间的开销；另一方面，由于专用硬件的高度集成特性，在配置与管理方面往往面临复杂性和灵活性不足的问题，尤其是在面对不同环境需求时难以实现快速定制化扩展。引入PDP后，允许将流量检测逻辑直接嵌入到网络的数据平面之中，使得能够在可编程交换机上实时进行数据包检测，降低了检测过程中的传输时延，其线速数据包处理能力可以减少检测过程中的处理时延，从而提升检测效率；针对特定的网络流量模型和异常行为也可以进行定制化的设计，可以根据实时网络状况和安全威胁进行自适应动态防御。

5 基于PDP的网络安全响应技术

当信息系统受到安全威胁时，响应技术迅速发挥作用，其核心目标在于快速识别、分析处理安全事件，最大程度减少损失。响应技术涵盖流量过滤、攻击缓解、拥塞控制等。

5.1 流量过滤

流量过滤是网络安全响应技术中最基础的策略，通过筛选网络中的流量阻止潜在威胁，结合PDP中网络安全检测技术，可以在交换机进行实时流量过滤。

ConPoolUBF[135]在Bloom过滤器基础上，设计高精度可更新Bloom过滤器(Updatable Bloom Filter，UBF)进行SYN Flood响应。UBF用于跟踪网络流的状态，通过Bloom过滤器动态检查并删除过时的网络流条目，同时通过基于时间戳的更新机制保持了过滤器的高准确性；Scholz等[136]提出在P4目标平台上实现SYN cookie和SYN认证策略，并在不同的目标平台上针对cookie计算、白名单处理、数据包缓冲等关键技术进行特定修改，能够有效防范SYN flooding攻击。

DIDA[137]是一种针对放大反射DDoS攻击的分布式网络防御框架。一旦检测到攻击，DIDA会动态管理边界路由器上的ACL列表，实现对恶意源的快速封锁。实验表明，DIDA能够以99.8%的准确率缓解包含7000个不同源的放大反射攻击。类似地，InDDoS[138]通过配置访问ACL和速率限制来限制对受害者的访问。

Laraba等[139]将ECN协议的规范建模为EFSM并映射到P4程序，在数据平面上实时跟踪和处理不同的状态转换，当EFSM模型进入标记为滥用的状态时，可以触发不同的操作，如丢弃包、重新路由包、生成警报、应用纠正措施等。

当攻击者采用多种流量攻击方式时，单一的防御手段难以有效缓解。Friday等[140]基于P4的灵活性，对各类协议的流量进行独立处理：对于TCP流量，使用Bloom过滤器跟踪连接状态和SYN请求，以识别和缓解SYN flooding攻击；对于UDP和ICMP流量，监控带宽使用情况，并根据阈值进行限制；当检测到DDoS攻击时，通过修改数据包头信息立即终止恶意连接。

Ripple[141]是一个针对攻击者的动态、可编程、去中心化链路洪泛防御系统。Ripple通过开发一种策略语言来精确获取全局防御视图，包括攻击的位置、流量组成以及通过网络的路径。然后Ripple编译器分析策略，生成交换机本地防御程序，并通过分布式协议同步交换机本地视图，能够快速适应攻击策略的变化，实现对链路洪泛攻击的有效缓解；同样针对链路泛洪攻击，SatShield[142]在数据平面实现了高效的流量过滤和调度机制：调度器根据流量的速率和特征为每个数据包分配优先级，设计基于队列的流量调度方案，确保在攻击发生时优先转发正常流量而丢弃可疑流量；为了应对大规模动态的链路泛洪攻击，Mew[143]采用了一种资源高效且可自适应调整的防御机制。通过设计分布式存储机制和无损状态迁移机制，Mew解决了PDP的存储瓶颈问题，而动态防御机制能够实时分析网络状态，适应攻击策略变化而保持防御功能的连续性。

为了在ISP规模下有效应对流量攻击，Jaqen[34]设计了一套基于P4的API，包含11个模块，每个模块包含过滤、分析、更新三个组件，允许ISP在交换机上，按需定制化处理攻击流量。为了最小化对交换机硬件资源的占用，Jaqen提出了一种混合整数规划(MIP)模型，并介绍了一种贪心启发式算法，用于在网络拓扑中快速分配资源，以实现资源的最优或近似最优分配；通过广度优先搜索(BFS)和贪婪策略，优先处理攻击流量最大的路径，提高了对DDoS攻击的响应速度和效率。实验表明，Jaqen在处理混合和动态攻击时，能够在几秒内响应并有效缓解高达380 Gbps的攻击流量。

Poseidon[144]构建了一个针对DDOS攻击的防御系统，其中monitors类原语统计全网流量数据信息、actions类原语提供模块化的防御策略抽象语描述应对攻击时的防操作、branches类原语表示应对攻击的控制逻辑。当获取到细粒度的检测结果后，恶意流量被引流至流量清洗中心。根据防御策略，Poseidon会对流量清洗中心的各类资源进行优化编排，满足各类原语的需要。同时开发有效的运行时管理机制，可以重新配置策略而不打断正常流量。实验表明，Poseidon可以有效应对SYN泛洪攻击、HTTP泛洪攻击、DNS放大攻击等6类DDOS攻击。

表14对PDP中流量过滤研究现状进行总结，虽然当前流量过滤的响应策略已经广泛部署在PDP中，也取得了良好的防御效果，但仍然存在过滤粒度不高、资源开销大等问题，在应对大规模、多样化的网络攻击行为时，迁移性、鲁棒性存在局限性。

表 14　PDP中流量过滤研究总结

工作	应对攻击	目标平台	主要思想	存在的限制或不足
ConPoolUBF[135]	SYN flooding	BMv2	设计UBF进行SYN flooding响应	防御鲁棒性不足
Scholz等[136]	SYN flooding	BMv2 NetFPGA	数据平面实现SYN cookie和SYN认证策略	攻击者可能绕过认证机制
DIDA[137]	AR-DDoS	BMv2	动态管理ACL封锁恶意IP	未解决哈希碰撞问题
InDDoS[138]	DNS放大	Tofino	调整ACL和限速缓解攻击	占用pipeline资源过多
Laraba等[139]	ECN protocol abuse	BMv2	将ECN协议转换为EFSM模型	可能导致状态爆炸
Friday等[140]	SYN/UDP flooding、慢速DDoS攻击	BMv2	对TCP、UDP等各类协议的流量进行独立处理	对大规模网络环境的实验效果未知
Ripple[141]	Link flooding	BMv2 Tofino	可编程、去中心化链路泛洪攻击防御系统	不能进行全网响应
SatShield[142]	Link flooding	Tofino	实现了高效的流量过滤和调度机制	调度机制简单
Mew[143]	Link flooding	Tofino	分布式、动态链路泛洪攻击防御	分布式设计引入新的时延
Jaqen[34]	动态混合攻击	Tofino	基于P4定制化组合不同的缓解模块	响应时间较长
Poseidon[144]	各种流量攻击	Tofino	模块化部署防御原语	内存开销大

5.2　欺骗防御

在网络攻击中，攻击者会采用伪装、伪造信息等手段来误导或欺骗用户，从而达成攻击目的。针对欺骗攻击，已有部分研究基于PDP进行防御。

SECAP交换机[145]利用源地址验证机制来防止地址欺骗攻击，通过确保数据包中ARP、LLDP消息中MAC地址与以太网头部的源MAC地址一致，防御址欺骗和拓扑中毒攻击。

Narayanan等[146]讨论了DHCP饥饿和欺骗攻击、IP地址欺骗攻击以及ARP欺骗/毒化攻击，并介绍了相应的防御策略，如DHCP监听、IP源防护和动态ARP检查，这些策略通过P4实现，通过在数据平面验证MAC地址、IP地址和ARP包的有效性，有效地防止了攻击者通过伪造地址来实施的拒绝服务、数据访问和篡改攻击。

Gondaliya等[147]在NetFPGA SUME平台上实现IP地址反欺骗机制，包括网络入口过滤(NIF)、松散反向路径转发(RPF-Loose)、严格反向路径转发(RPF-Strict)、可行路径反向路径转发(RPF-Feasible)、欺骗预防方法(SPM)和源地址验证改进(SAVI)。这些机制部署在网络边缘路由器或自治域边界路由器上，检测并阻止带有伪造源IP地址的恶意数据包。

P4DAD[148]利用P4增强IPv6网络中的重复地址检测(DAD)过程的安全性。P4DAD通过创建并维护IPv6地址与主机链路属性之间的绑定关系，在网络内有效过滤伪造的邻居发现协议(NDP)消息，从而在不修改NDP及主机协议栈的情况下防止DoS攻击，具有轻量级、可部署性强和避免单点故障的特点。

DroPPPP[149]在数据平面检测欺骗数据包：首先检查与接收数据包端口相关联的攻击标志和上次攻击数据包的时间戳；然后对数据包进行哈希校验，丢弃MAC地址、IP地址被篡改的数据包。实验结果显示，DroPPP在DOS攻击下显著提高了网络性能，特别是在减少数据包丢失方面。

汪润虎[150]提出一种在PDP中实施地址欺骗攻击溯源与防御的机制，当溯源触发模块接收到异常统计结果时，控制平面根据网络传输流量的统计特征下发溯源标记策略，数据平面根据此策略对数据包进行标记。数据审计模块对数据平面上传的统计特征分析，获取攻击者信息。表15对上述研究进行总结。

5.3　其他响应技术

还有一些相关研究在数据平面实现了攻击响应，这些研究往往面向某一类具体的攻击行为，具有很强的针对性。

隐蔽通道是一种针对分布式系统的高级威胁，会造成隐私信息的泄露，现有的防御手段往往伴随着性能的损失，NetWarden[151]提出一种能够保证TCP连接性能防御方法。由于TCP性能与网络状态和接收方处理速率有关，因此NetWarden通过ACK Boosting和Receive Window Boosting方法制造一种网络时延低、接收方处理性能高的“假象”，其核心思想在利用TCP拥塞控制机制，人为提高TCP发送速率，从而减少性能损失。NetWarden将部分防御原语卸载到数据平面，利用PDP线速处理、支持复杂数据结构的功能，可以快速进行监控连接、特征提取以及存储式隐蔽通道攻击的防御。

表 15 PDP中欺骗防御研究研究总结

工作	欺骗类型						主要思想	存在的不足或限制
	平台	MAC	ARP	IPv4	IPv6	DHCP		
SECAP[145]	BMv2	√	√	√	√	√	利用源地址认证防御地址欺骗攻击	默认源地址可信
Narayanan等[146]	NetFPGA	√	√	√	√	√	验证MAC地址、IP地址的有效性	需要管理员维护
Gondaliya等[147]	NetFPGA	×	×	√	×	×	实现六种反欺骗机制	需要管理员维护
P4DAD[148]	BMv2	×	×	×	√	×	增强IPv6中的DAD过程的安全性	扩展性有限
DroPPPP[149]	BMv2	√	√	√	×	×	对数据包进行完整性校验	部署难度较大
汪润虎[150]	BMv2	√	×	√	√	×	地址欺骗攻击溯源与防御机制	防御策略不精细

针对ML模型在数据平面部署的脆弱性，Reddy等[152]提出一种基于P4的对抗性攻击缓解框架，提升了数据平面模型在响应对抗性攻击时的鲁棒性。

而面对流表溢出，Jain等[153]提出一种以可编程交换机为中心的流表溢出检测与响应机制。文章通过引入IP SourceGuard机制，实现了对特定端口威胁值的计数，并在威胁值超过预设警告阈值时，阻塞端口通过攻击流量，从而有效减轻了流表溢出攻击对网络性能的影响。

综上，在传统网络环境中，网络安全事件的响应流程往往高度依赖于人工干预。例如，在遭遇网络攻击时，安全团队通常需要手动执行一系列操作来减轻威胁的影响，包括网络隔离、修改过滤规则、攻击溯源等，然而，这种基于人工的操作模式存在显著的时间延迟问题，从检测到攻击的存在直至启动相应的响应措施之间存在一定的时间间隔，这段时间内攻击者可能会继续造成损害。而引入PDP后，可以在交换机上部署响应策略，应对攻击进行实时响应。一旦检测到异常活动或者确认了攻击行为，系统可以立即在硬件层面采取行动，而无需等待缓慢的人工介入过程。通过这种方式，不仅能够实现对攻击的即时反应，而且还能确保所有必要的防御措施被执行得更加一致且高效。此外，由于PDP支持灵活配置，可以根据不同的攻击场景定制特定的响应逻辑，并且随着网络条件的变化动态调整，从而提供了一种更为敏捷和有效的网络安全保障机制。

6 研究展望

综上，PDP在网络防御实施的各个阶段都具有广泛的应用，具有很强的功效。其中，利用PDP的高可扩展性、高性能等特点，能够动态调整网络安全防护策略，提高防护原语的执行效率；利用PDP定制数据包处理逻辑、DPI能力，可以提高网络安全检测的精度，减少检测开销；而PDP的实时性特点，大大提高了网络响应的效率。然而，就目前的研究现状而言，仍面临几个方面的问题与挑战，下面本文对此进行分析并探讨未来可能的研究方向。

6.1 PDP的安全原语扩展及其编程优化

虽然以P4为代表的PDP技术在数据包处理方面具有很多优势，但考虑到数据平面自身的局限性，P4在解决各类网络安全问题时仍存在一定的局限性，具体表现在语法局限性、功能局限性以及资源局限性三方面。

(1)语法局限性

P4作为一种领域专用编程语言在语法层面存在一些明显的局限性：第一，它仅支持加法、位运算、字段提取等基本操作，不支持诸如除法、对数计算等复杂运算；第二，P4并不支持循环操作，而是采用FSM来模拟循环行为，这在一定程度上限制了程序的灵活性和扩展性；第三，P4缺乏动态内存分配功能，所有存储单元的使用都必须在编译时确定，可能导致资源利用不充分；第四，P4不支持指针、引用，这限制了其对于复杂数据结构的支持。

(2)功能局限性

从功能的角度来看，P4同样存在一定的局限性。第一，P4本身不直接支持多播与广播功能；第二，P4缺少对队列管理、调度算法和多路复用机制的直接支持；第三，P4不支持报文分段和重组，不能完整地实现TCP协议等需要报文重组的协议；第四，P4只能处理已存在报文，不具备生成新报文的能力，这使其无法主动产生网络流量(如ICMP回复等)。

(3)资源局限性

从资源的角度考虑，P4同样面临一些挑战。在存储资源上，TCAM用于实现复杂匹配规则，SRAM用于存储查找表和其他数据结构，支持P4程序中的动作执行。但两者成本高昂且容量有限，过多的匹配规则可能会耗尽TCAM空间，影响硬件对程序逻辑的支持，SRAM的容量可能限制了计数

器、计量器等资源的使用；其次，PHV是P4程序中表示数据包头部信息的关键数据结构，尽管P4支持高度定制化的包头解析和处理，但PHV的大小和复杂度同样受限于硬件资源。此外，P4的pipeline的数量和每个pipeline中的处理单元（如ALUs、乘法器、队列等）是固定的，这意味着复杂的程序可能超过单个pipeline的处理能力或者整个芯片的并行处理能力。

鉴于上述三点局限，对PDP的安全原语扩展及其编程优化可以考虑以下三个方面：一是完善P4语言语法，支持更复杂的运算和控制结构，提高程序表达能力和功能性，增强数据包处理的灵活性。完善后的P4语言应当具备更强的抽象层次，以便更好描述和操作底层硬件特性；二是扩展新的安全功能模块，提高网络防御的多样性和有效性。同时要提高各安全组件间的联动与互操作性，形成有机的整体；三是优化资源管理和利用，确保在复杂网络环境下维持高性能数据包处理能力。考虑到不断增长的网络规模和流量密度，不仅需要考虑动态复杂均衡、资源调度等算法，还需要规划并实施弹性伸缩方案。

6.2　基于PDP的智能化防御

近年来，人工智能（Artificial Intelligence，AI）技术的快速发展为网络安全领域带来了突破性进展。利用AI技术，能够实现持续监控与优化、智能入侵检测、自动化威胁响应等，显著提升网络防御的智能化水平。将网络技术与AI技术结合，可以提升两者共同效能并为网络防御带来新的增益。两者的结合体现在两个方面，即AI for Network和Network for AI[154]。

AI for Network：利用AI技术，可以对网络流量进行智能预测和调度，优化资源分配，提升用户体验；可以实现网络管理的自动化，包括自动配置、故障检测和恢复、安全威胁的识别和响应等，减轻人工管理的负担；能够在复杂网络环境下快速准确识别网络攻击行为，提高网络防护能力。

Network for AI：构建一个能够支持AI应用需求的高效、安全、可靠的网络基础设施。利用网络节点的通信、计算和感知能力，支持分布式学习、群智式协同以及云边端一体化算法部署，从而为更加强大的AI应用提供支撑。

PDP作为一种新型网络技术，能够在网络设备上实现定制化的数据包处理逻辑，这为集成AI算法提供了坚实的基础[155-156]。将部分计算任务卸载到PDP执行实现“网络计算”是实现AI与网络技术结合的基本思路，4.2.2节介绍了一些在数据平面实现机器学习算法进行流量分析的研究，文献[157]对网内计算领域相关研究进行综述，展示了将PDP与AI技术结合实现智能化防御的可行性和良好发展前景。

当前PDP智能化防御相关面临的主要问题在于PDP有限的计算存储资源难以支撑复杂深度学习模型，仅能够部署一些简单的机器学习模型，如决策树、SVM、KNN[158]，这无法发挥AI技术在处理海量数据的优势，限制了PDP防御的智能化水平。未来可能的研究方向之一是将PDP技术与联邦学习技术结合，将每一台可编程交换机视为分布式计算架构中的一个计算节点，利用有限的计算能力执行一些简单的运算操作。通过这种方式，可以实现多个可编程交换机的联合学习过程，聚合网络中的计算资源处理复杂学习任务。

随着LLM的飞速发展，近期涌现出一些利用LLM解决网络任务的相关研究，涉及故障诊断[159-160]、网络配置[161]等，也出现了大量利用LLM赋能网络安全的相关研究[162-164]。其中，结合LLM强大的人类意图理解、推理、生成等能力和PDP灵活、可重配置的特点，可以为网络的智能、安全运维防御注入新的活力。利用LLM作为“控制大脑”可以在复杂网络环境下智能化编排各安全组件，根据用户意图生成应对攻击时的防御策略，而数据平面可以根据策略实时调整网络配置并即时响应。二者的结合将有助于实现一体化、自动化、智能化的网络安全防御。

6.3　PDP内生安全技术

尽管PDP将网络可编程性扩展到数据平面已经得到了广泛应用，然而由于其高度的灵活性，在网络中引入错误的机会也大大增加。主要体现在三个方面：一是PDP对数据包的修改可能导致网络中传递数据包的格式错误；二是攻击者可以利用PDP篡改数据包内容；三是利用PDP定制的协议和处理逻辑可能存在未知的漏洞。这是由PDP自身特性带来的内生安全问题。任何自然的功能或人造的功能，都存在伴生或衍生的显式副作用或隐式暗功能[165]。PDP的可编程性、灵活性带来极大便利的同时，也伴随着显著的内生安全问题。当前解决PDP内生安全问题主要有程序测试和程序验证两种方案。

程序测试旨在通过生成测试用例检验网络设备上的行为是否符合预期，当前代表性工作有

p4pktgen[166]、p4fuzz[167]、Meissa[168]、PTA[169]、Firebolt[170]等。然而，通过程序测试的方法无法确保生成的样例能够全面覆盖测试空间，即使通过测试也不能确保程序不出现错误。针对不同的应用程序生成不同的测试样例也大大增加了开发人员的负担。

程序验证是指通过形式化方法和技术确保程序在逻辑上正确，能够按照预期方式运行并满足设计规范。通常需要首先用符号执行语言描述P4程序，如SEFL语言、GCL语言，然后利用符号执行引擎进行验证，如Z3、Symnet、KLEE等。当前主要工作有p4v[171]、Vera[172]、Aquila[173-174]。程序验证方法面临的主要问题在于随着程序的复杂，状态呈指数增长，难以进行求解。

基于先验知识库的“测试”、“打补丁”或“附加防御”方法，确实可以通过持续的演进迭代有条件地降低已知漏洞后门等问题的危害。但由于无法保证测试空间、先验知识完备性等问题，不可能彻底消除由于PDP自身特性带来的内生安全问题[165]。如何通过不依赖漏洞后门发现和攻击特征分析等先验知识，解决PDP内生安全问题，对于推广促进PDP在网络防御中的应用具有十分重要的意义。

7 总 结

本文对基于PDP的网络防御技术相关研究进行详尽的调研，根据网络防御的实施阶段分为防护技术、检测技术、响应技术三类，根据具体防御方法划分为更加细致的子类。针对每一细分子类，调研总结了大量相关文献，详细说明每种方法的基本原理与特点。为了充分说明PDP应用于网络防御的优点和适用场景，本文深入分析每种方法的优势与存在不足并进行归纳总结，对基于PDP实施网络防御提供了一定指导。希望本文相关工作的综述可以为读者快速理清基于PDP的网络防御技术的发展脉络，对相关领域研究工作和研究人员提供有益的帮助，促进网络和安全行业的发展。

参 考 文 献

[1] Yin H, Qiao B. big data-driven network information plane. Chinese Journal of Computers, 2016, 39(1): 126-139 (in Chinese)
(尹浩，乔波. 大数据驱动的网络信息平面. 计算机学报，2016, 39(1): 126-139)

[2] Wang Y Z, Jin X L, Cheng X Q. Network big data: Current status and prospects. Chinese Journal of Computers, 2013, 36(6): 1125-1138 (in Chinese)
(王元卓，靳小龙，程学旗. 网络大数据:现状与展望. 计算机学报，2013, 36(6): 1125-1138)

[3] Zhou W L, Yang Y, Xu M W. A survey on network function virtualization technology. Journal of Computer Research and Development, 2018, 55(4): 675-688 (in Chinese)
(周伟林，杨芫，徐明伟. 网络功能虚拟化技术研究综述. 计算机研究与发展，2018, 55(4): 675-688)

[4] Chowdhury M, Boutaba R. A survey of network virtualization. Computer Networks, 2010, 54(5): 862-876

[5] Shi W S, Zhang X Z, Wang Y F, et al. Edge computing: current status and prospects. Journal of Computer Research and Development, 2019, 56(1): 69-89 (in Chinese)
(施巍松，张星洲，王一帆，等. 边缘计算:现状与展望. 计算机研究与发展，2019, 56(1): 69-89)

[6] Luo J Z, He Y, Zhang L, et al. Cloud-edge integrated architecture and key technologies for industrial internet. Scientia Sinica Informationis, 2020, 50(2): 195-220 (in Chinese)
(罗军舟，何源，张兰，等. 云端融合的工业互联网体系结构及关键技术. 中国科学:信息科学，2020, 50(2): 195-220)

[7] Niu W. Design and Implementation of In-band Networking and Fault Adjustment Mechanism for SDN System Based on ONOS and P4.Beijing: Beijing Jiaotong University, 2022 (in Chinese)
(钮伟. 基于ONOS与P4的SDN系统带内组网与故障调整机制设计与实现. 北京:北京交通大学，2022)

[8] Liatifis A, Sarigiannidis P, Argyriou V, et al. Advancing SDN from OpenFlow to P4: A survey. ACM Computing Surveys, 2023, 55(9): 1-35

[9] Bosshart P W, Daly D, Izzard M, et al. Programming protocol-independent packet processors. arXiv, 2013: 1312.1719

[10] Xia J Q. Research on Flow Table Consistency Technology in Software-Defined Network Data Plane. Zhengzhou: Information Engineering University, 2022 (in Chinese)
(夏计强. 软件定义网络中数据平面流表一致性技术研究. 郑州:战略支援部队信息工程大学，2022)

[11] Singer P W .Cybersecurity and cyberwar : what everyone needs to know. Oxford, UK: Oxford University Press, 2014

[12] Chen X, Wu C, Liu X, et al. Empowering network security with programmable switches: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1653-1704

[13] Lin Y S X, Bi J, Zhou Y, et al. Research and application of programmable data plane based on P4. Chinese Journal of Computers, 2019, 42(11): 2539-2560 (in Chinese)
(林耘森箫，毕军，周禹，等. 基于P4的可编程数据平面研究及其应用. 计算机学报，2019, 42(11): 2539-2560)

[14] AlSabeh A, Khoury J, Kfoury E F, et al. A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment. Computer Networks, 2022,(8):32-45

[15] Kaur S, Kumar K, Aggarwal N. A review on P4-programmable data planes: Architecture, effortsresearch, and directionsfuture. Computer Communications, 2021,(7): 109-129

[16] Kfoury E F, Crichigno J, Bou-Harb E. An exhaustive survey on P4 programmable data plane switches: Taxonomy, applications, challenges, and trendsfuture. IEEE Access, 2021, (9): 87094-87155

[17] Garzon C, Rios-Guiral S, Leal E, et al. P4 cybersecurity solutions: Taxonomy and open challenges. IEEE Access, 2024, (12): 6376-6399

[18] Josbert N N, Wei M, Wang P, et al. A look into smart factory for industrial IoT driven by SDN technology: A comprehensive survey of taxonomy, architectures, issues and future research orientations. Journal of King Saud University - Computer and Information Sciences, 2024,(3): 102-114

[19] Xiong B, Liu Y Q, Xia Z Q, et al. RobustSketch: A Flow Elastic Recognition Method that Supports Network Traffic Jitter. Journal of Software, 2025, 36(2): 660-679 (in Chinese)
(熊兵,刘永青,夏卓群,等. RobustSketch:支持网络流量抖动的大流弹性识别方法. 软件学报, 2025,36(2): 660-679)

[20] Ollora Zaballa E, Franco D, Zhou Z, et al. P4Knocking: Offloading host-based firewall functionalities to the network//Proceedings of the 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops. Long Beach, USA, 2020: 7-12

[21] Almaini A, Al-Dubai A Y, Romdhani I, et al. Delegation of authentication to the data plane in software-defined networks//2019 IEEE International Conferences on Ubiquitous Computing & Communications. Shenyang, China, 2019: 58-65

[22] Saxena A, Naya I, Ritvik R, et al. P4Filter: A two level defensive mechanism against attacks in SDN using P4//2021 IEEE International Conference on Advanced Networks and Telecommunications Systems. Hyderabad, India, 2021: 113-118

[23] Pali I, Amin R. PortSec: Securing port knocking system using sequence mechanism in SDN environment//Proceedings of the 2022 International Wireless Communications and Mobile Computing. Dubrovnik, Croatia, 2022: 1009-1014

[24] Bhattacharya A, Rana R, Datta S, et al. P4-sKnock: A two level host authentication and access control mechanism in P4 based SDN//Proceedings of the 27th Asia Pacific Conference on Communications. Seoul, Republic of Korea, 2022: 278-283

[25] Ricart-Sanchez R, Malagon P, Alcaraz-Calero J M, et al. NetFPGA-based firewall solution for 5G multi-tenant architectures//Proceedings of the 2019 IEEE International Conference on Edge Computing. Milan, Italy, 2019: 132-136

[26] Vörös P, Kiss A. Security middleware programming using P4//Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust. Toronto, Canada, 2016: 277-287

[27] Li J, Jiang H, Luo W, et al. Stateful Firewall Technology Based on Programmable Data Plane. Engineering Journal of Wuhan University, 2022, 55(1): 85-91 (in Chinese)
(李健, 江昊, 罗威, 等. 基于可编程数据平面的状态防火墙技术. 武汉大学学报(工学版), 2022, 55(1): 85-91)

[28] Teng L, Hung C-H, Wen C H-P. P4SF: A high-performance stateful firewall on commodity P4-programmable switch//Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022. Budapest, Hungary, 2022: 1-8

[29] Chou P-L, Wei H-W, Lee W-T. Resist denial-of-service attack and enhance network security with protocol-independent packet processor-based two-layer firewall//Proceedings of the 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data. Taipei, China, 2024: 150-154

[30] Cao J, Bi J, Zhou Y, et al. CoFilter: A high-performance switch-assisted stateful packet filter//SIGCOMM 2018: Proceedings of the ACM SIGCOMM 2018 Conference: Posters and Demos. Budapest, Hungary, 2018: 9-11

[31] Li J, Jiang H, Jiang W, et al. SDN-based stateful firewall for cloud//Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud. New York, USA, 2020: 157-161

[32] Basat R B, Chen X, Einziger G, et al. Designing Heavy-Hitter Detection Algorithms for Programmable Switches. IEEE/ACM Transactions on Networking, 2020, 28(3): 1172-1185

[33] Chen X, Kim H, Aman J M, et al. Measuring TCP round-trip time in the data plane//Proceedings of the Workshop on Secure Programmable Network Infrastructure. New York, USA, 2020: 1-6

[34] Liu Z, Namkung H, Nikolaidis G, et al. Jaqen: A high-performance switch-native approach for detecting and mitigating volumetric DDoS attacks with programmable switches//USENIX Security Symposium. Virtual Event,USA, 2021: 1-18

[35] Chen X, Feibish S L, Koral Y, et al. Fine-grained queue measurement in the data plane//Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies. Orlando, USA, 2019: 1-12

[36] Yoo S, Chen X. Secure keyed hashing on programmable switches//Proceedings of the ACM SIGCOMM 2021 Workshop on Secure Programmable Network Infrastructure. Virtual, USA, 2021: 1-7

[37] Vörös P, Horpácsi D, Kitlei R, et al. T4P4S: A target-independent compiler for protocol-independent packet processors//Proceedings of the 2018 IEEE 19th International Conference on High Performance Switching and Routing. Bucharest, Romania, 2018: 1-8

[38] Horpácsi D, Laki S, Vörös P, et al. Asynchronous extern functions in programmable software data planes//Proceedings of the 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems. Cambridge, UK, 2019: 1-2

[39] Scholz D, Oeldemann A, Geyer F, et al. Cryptographic hashing in P4 data planes//Proceedings of the 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems. Cambridge, UK, 2019: 1-3

[40] Mafioletti D R, Martinello M, Ribeiro M R N, et al. To embed or not to embed SHA in programmable network interface cards//Proceedings of the 2022 18th International Conference on Network and Service Management. Thessaloniki, Greece, 2022: 324-330

[41] Oliveira I, Neto E, Immich R, et al. Dh-aes-p4: On-premise

encryption and in-band key-exchange in P4 fully programmable data planes//Proceedings of the 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks. Heraklion, Greece, 2021: 148-153

[42] Chen X. Implementing AES encryption on programmable switches via scrambled lookup tables//Proceedings of the Workshop on Secure Programmable Network Infrastructure. Virtual, USA, 2020: 1-5

[43] Malina L, Smekal D, Ricci S, et al. Hardware-accelerated cryptography for software-defined networks with P4// Proceedings of the International Conference on Security for Information Technology and Communications. Bucharest, Romania, 2020: 1-10

[44] Yoshinaka Y, Takemasa J, Koizumi Y, et al. On implementing ChaCha on a programmable switch//Proceedings of the 5th International Workshop on P4 in Europe. Rome, Italy, 2022: 1-6

[45] Yoo S, Chen X, Rexford J. SmartCookie: Blocking large-scale SYN floods with a split-proxy defense on programmable data planes//Proceedings of the USENIX Security Symposium. Boston, USA, 2024: 1-18

[46] Qin Y, Quan W, Song F, et al. Flexible encryption for reliable transmission based on the P4 programmable platform// Proceedings of the 2020 Information Communication Technologies Conference. Nanjing, China, 2020: 147-152

[47] Liu Z, Cui P, Dong Y, et al. MultiSec: A multi-protocol security forwarding mechanism based on programmable data plane. Electronics, 2022, 11(15): 23-34

[48] Liu G, Quan W, Cheng N, et al. Softwarized IoT network immunity against eavesdropping with programmable data planes. IEEE Internet of Things Journal, 2021(8): 78-90

[49] Hauser F, Schmidt M T, Häberle M, et al. P4-MACsec: Dynamic topology monitoring and data layer protection with MACsec in P4-based SDN. IEEE Access, 2019(8): 45-58

[50] Hauser F, Häberle M, Schmidt M T, et al. P4-IPsec: Site-to-site and host-to-site VPN with IPsec in P4-based SDN. IEEE Access, 2019(8): 67-86

[51] Hauser F, Häberle M, Menth M. P4sec: Automated deployment of 802.1X, IPsec, and MACsec network protection in P4-based SDN. IEEE Access, 2023(11): 300-309

[52] Zuo Z B. Research on Key Technologies of Data Plane Security in Software-Defined Network Based on Cryptographic Identification. Information Engineering University, 2020 (in Chinese)
(左志斌. 基于密码标识的软件定义网络数据平面安全关键技术研究. 战略支援部队信息工程大学, 2020)

[53] Kim H, Gupta A. ONTAS: Flexible and scalable online network traffic anonymization system// Proceedings of the 2019 Workshop on Network Meets AI & ML. Beijing, China, 2019: 1-6

[54] Moghaddam H M, Mosenia A. Anonymizing masses: Practical light-weight anonymity at the network level. arXiv, 2019: 1911.09642

[55] Datta T, Feamster N, Rexford J, et al. SPINE: Surveillance protection in the network elements//FOCI@USENIX Security Symposium. Santa Clara, USA, 2019: 1-12

[56] Black C, Scott-Hayward S. Defeating data plane attacks with program obfuscation. IEEE Transactions on Dependable and Secure Computing, 2024, 21(3): 1317-1330

[57] Wu P. Research on Several Security Issues of Packet Forwarding in Software-Defined Network Data Plane . Information Engineering University, 2023 (in Chinese)
(吴平. 软件定义网络数据平面分组转发若干安全问题研究. 战略支援部队信息工程大学, 2023)

[58] Borges E S, Martinello M, Bonella V B, et al. PoT-PolKA: Let the edge control the proof-of-transit in path-aware networks. IEEE Transactions on Network and Service Management, 2024, 21(4): 3681-3691

[59] Sankaran G C C, Sivalingam K M M, Gondaliya H. P4 and NetFPGA-based secure in-network computing architecture for AI-enabled industrial internet of things. IEEE Internet of Things Journal, 2023, 10(4): 2979-2994

[60] Zuo Z B, Yang K, Deng M L, et al. Dynamic network defense scheme based on programmable software-defined network. Journal of Computer Applications, 2024(2): 1-11 (in Chinese)
(左志斌, 杨凯, 邓淼磊, 等. 基于可编程软件定义网络的动态网络防御方案. 计算机应用, 2024(2): 1-11)

[61] Qian H, Zheng J Q, Chen G H. A survey on network heavy flow detection methods. Journal of Software, 2024, 35(2): 852-871 (in Chinese)
(钱昊, 郑嘉琦, 陈贵海. 网络重要流检测方法综述. 软件学报, 2024, 35(2): 852-871)

[62] Yang T, Jiang J, Liu P, et al. Elastic sketch: Adaptive and fast network-wide measurements//Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication. Budapest, Hungary, 2018: 1-15

[63] Lu J, Zhang Z, Chen H, et al. Filter-sketch: A two-layer sketch for entropy estimation in the data plane. IET Communications, 2022, 16(20): 2422-2430

[64] Song C, Kannan P G, Low K H, et al. FCM-sketch: Generic network measurements with data plane support//Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies. Barcelona, Spain, 2020: 1-13

[65] Tang L, Huang Q, Lee P P C. A fast and compact invertible sketch for network-wide heavy flow detection. IEEE/ACM Transactions on Networking, 2019, 28(5): 2350-2363

[66] Ivkin N, Yu Z, Braverman V, et al. QPipe: Quantiles sketch fully in the data plane//Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies. Orlando, USA, 2019: 285-291

[67] Fan Z, Hu Z, Wu Y, et al. PISketch: Finding persistent and infrequent flows. IEEE/ACM Transactions on Networking, 2023, 31(6): 3191-3206

[68] Zhang Y, Liu Z, Wang R, et al. CocoSketch: High-performance sketch-based measurement over arbitrary partial key query. IEEE/ACM Transactions on Networking, 2021, 31(6): 2653-2668

[69] Yang K, Wu Y, Miao R, et al. ChameleMon: Shifting

measurement attention as network state changes//Proceedings of the ACM SIGCOMM 2023 Conference. New York, USA, 2023: 1-14

[70] Agarwal A, Liu Z, Seshan S. HeteroSketch: Coordinating network-wide monitoring in heterogeneous and dynamic networks//Proceedings of the 19th USENIX Symposium on Networked Systems Design and Implementation. Renton, USA, 2022: 719-741

[71] Namkung H, Liu Z, Kim D, et al. SketchLib: Enabling efficient sketch-based monitoring on programmable switches//Proceedings of the 19th USENIX Symposium on Networked Systems Design and Implementation. Renton, USA, 2022: 743-759

[72] Liu Z, Zhou S, Rottenstreich O, et al. Memory-efficient performance monitoring on programmable switches with lean algorithms. arXiv, 2019: 1911.06951

[73] Namkung H, Liu Z, Kim D, et al. Sketchovsky: Enabling ensembles of sketches on programmable switches//Proceedings of the Symposium on Networked Systems Design and Implementation. Boston, USA, 2023: 1-16

[74] Zheng H, Tian C, Yang T, et al. FlyMon: Enabling on-the-fly task reconfiguration for network measurement//Proceedings of the ACM SIGCOMM 2022 Conference. Amsterdam, The Netherlands, 2022: 1-14

[75] Zhou Z, Lv J, Cheng L, et al. SketchGuide: Reconfiguring sketch-based measurement on programmable switches//Proceedings of the 2022 IEEE 30th International Conference on Network Protocols. Lexington, USA, 2022: 1-11

[76] Huang Q, Lee P P C, Bao Y. Sketchlearn: Relieving user burdens in approximate measurement with automated statistical inference//Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication. Budapest, Hungary, 2018: 1-14

[77] Liu Z Z, Bi J, Zhou Y, et al. Active network telemetry mechanism based on P4. Journal of Communications, 2018, 39(S1): 162-169 (in Chinese)
(刘争争，毕军，周禹，等. 基于P4的主动网络遥测机制. 通信学报，2018(2): 162-169)

[78] Tang S F. Research on Adaptive Network Monitoring Technology Based on In-band Telemetry. Hefei: University of Science and Technology of China, 2022 (in Chinese)
(唐绍飞. 基于带内遥测的自适应网络监控技术研究. 合肥:中国科学技术大学,2022)

[79] Suh D, Jang S, Han S, et al. Flexible sampling-based in-band network telemetry in programmable data plane. ICT Express, 2020(6): 62-65

[80] Xu Z, Lu Z, Zhu Z. Information-sensitive in-band network telemetry in P4-based programmable data plane. IEEE/ACM Transactions on Networking, 2024(3): 1875-1888

[81] Sheng S, Huang Q, Lee P P C. DeltaINT: Toward general in-band network telemetry with extremely low bandwidth overhead//Proceedings of the 2021 IEEE 29th International Conference on Network Protocols. Dallas, USA, 2021: 1-11

[82] Tang S, Kong J, Niu B, et al. Programmable multilayer INT: An enabler for AI-assisted network automation. IEEE Communications Magazine, 2020, 58(1): 26-32

[83] Lyu H R, Li Q, Shen G B, et al. A Survey of In-band network telemetry methods. Journal of Software, 2024(3): 1-21 (in Chinese)
(吕鸿润，李清，沈耿彪，等. 带内网络遥测方法综述. 软件学报，2024(3): 1-21)

[84] Tu N V, Hyun J, Kim G Y, et al. INTCollector: A high-performance collector for in-band network telemetry//Proceedings of the 2018 14th International Conference on Network and Service Management. Rome, Italy, 2018: 10-18

[85] Vestin J, Kassler A, Bhamare D, et al. Programmable event detection for in-band network telemetry//Proceedings of the 2019 IEEE 8th International Conference on Cloud Networking. Coimbra, Portugal, 2019: 1-6

[86] Papadopoulos K, Papadimitriou P, Papagianni C A. PFA-INT: Lightweight in-band network telemetry with per-flow aggregation//Proceedings of the 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks. Heraklion, Greece, 2021: 60-66

[87] Alhamed F, Scano D, Castoldi P, et al. P4 telemetry collector. Computer Networks, 2023(3): 227-239

[88] Tan L, Su W, Zhang W, et al. A packet loss monitoring system for in-band network telemetry: Detection, localization, diagnosis and recovery. IEEE Transactions on Network and Service Management, 2021(4): 4151-4168

[89] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets//Proceedings of the 27th International Conference on Neural Information Processing Systems. Montreal, Canada, 2014: 2672-2680

[90] Jia C, Pan T, Bian Z, et al. Rapid Detection and Localization of gray failures in data centers via in-band network telemetry//NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary, 2020: 1-9

[91] Pan T, Song E, Bian Z, et al. INT-path: Towards optimal path planning for in-band network-wide telemetry//IEEE INFOCOM 2019-IEEE Conference on Computer Communications. Paris, France, 2019: 487-495

[92] A G deCastro, Lorenzon A F, Rossi F D, et al. Near-optimal probing planning for in-band network telemetry. IEEE Communications Letters, 2021, 25(5): 1630-1634

[93] Marques J A, Luizelli M C, Filho R I T da C, et al. An optimization-based approach for efficient network monitoring using in-band network telemetry. Journal of Internet Services and Applications, 2019, 10(1): 1-20

[94] Hohemberger R, A G deCastro, Vogt F G, et al. Orchestrating in-band data plane telemetry with machine learning. IEEE Communications Letters, 2019, 23(12): 2247-2251

[95] Bhamare D, Kassler A, Vestin J, et al. IntOpt: In-band network telemetry optimization for NFV service chain monitoring//ICC 2019 - 2019 IEEE International Conference on Communications. Shanghai, China, 2019: 1-7

[96] Pan X, Tang S, Zhu Z. Multilayer network monitoring and data analytics over encrypted telemetry data//Proceedings of the

2020 IEEE 20th International Conference on Communication Technology. Nanning, China, 2020: 1577-1581

[97] Pan X, Tang S, Zhu Z. Privacy-preserving multilayer in-band network telemetry and data analytics//Proceedings of the 2020 IEEE/CIC International Conference on Communications in China. Chongqing, China, 2020: 142-147

[98] Yang K, Li Y, Liu Z, et al. SketchINT: Empowering INT with TowerSketch for per-flow per-switch measurement//Proceedings of the IEEE 29th International Conference on Network Protocols. Dallas, USA, 2021: 1-12

[99] Zhao Y, Yang K, Liu Z, et al. LightGuardian: A full-visibility, lightweight, in-band telemetry system using sketchlets//Proceedings of the 18th USENIX Symposium on Networked Systems Design and Implementation. Virtual Event, 2021: 1-15

[100] Huang Q, Sun H, Lee P P C, et al. OmniMon: Re-architecting network telemetry with resource efficiency and full accuracy//Proceedings of the ACM SIGCOMM 2020 Conference. Virtual, USA, 2020: 1-14

[101] Oh S, Han S, Lee H, et al. BACKWARD: A victim-centric DDoS detection and mitigation scheme in programmable data plane//Proceedings of the 2023 IEEE 20th Consumer Communications & Networking Conference. Las Vegas, USA, 2023: 1-6

[102] Ihle F, Lindner S, Menth M. P4-PSFP: P4-based per-stream filtering and policing for time-sensitive networking. IEEE Transactions on Network and Service Management, 2024, 21(5): 5273-5290

[103] Lewis B, Broadbent M, Rotsos C, et al. 4MIDable: Flexible network offloading for security VNFs. Journal of Network and Systems Management, 2023, 31(3): 1-28

[104] Ilha A da S, Lapolli A C, Marques J A, et al. Euclid: A fully in-network, P4-based approach for real-time DDoS attack detection and mitigation. IEEE Transactions on Network and Service Management, 2021, 18(3): 3121-3139

[105] Lapolli A C, Marques J A, Gaspary L P. Offloading real-time DDoS attack detection to programmable data planes//Proceedings of the 2019 IFIP/IEEE Symposium on Integrated Network and Service Management. Washington, USA, 2019: 19-27

[106] González L A Q, Castanheira L, Marques J A, et al. BUNGEE: An adaptive pushback mechanism for DDoS detection and mitigation in P4 data planes//Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management. Bordeaux, France, 2021: 393-401

[107] Wang Y-C, Su P-Y. Collaborative defense against hybrid network attacks by SDN controllers and P4 switches. IEEE Transactions on Network Science and Engineering, 2024(2): 1480-1495

[108] Li D C, Tu H-H, Chou L-D. Cross-layer detection and defence mechanism against DDoS and DRDoS attacks in software-defined networks using P4 switches. Computers & Electrical Engineering, 2024(4): 109-121

[109] Singh S K, Rothenberg C E, Luizelli M C, et al. HH-IPG: Leveraging inter-packet gap metrics in P4 hardware for heavy hitter detection. IEEE Transactions on Network and Service Management, 2023(3): 3536-3548

[110] Jin C, Wang H, Shin K G. Hop-count filtering: An effective defense against spoofed DDoS traffic//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA, 2003: 30-41

[111] Zhang M, Li G, Kong X, et al. NetHCF: Filtering spoofed IP traffic with programmable switches. IEEE Transactions on Dependable and Secure Computing, 2022, 19(6): 3819-3834

[112] Dimolianis M, Pavlidis A, Maglaris B S. A multi-feature DDoS detection schema on P4 network hardware//Proceedings of the 2020 23rd Conference on Innovation in Clouds, Internet and Networks. Paris, France, 2020: 1-6

[113] Macías S G, Gaspary L P, Botero J F. ORACLE: An architecture for collaboration of data and control planes to detect DDoS attacks//Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management. Bordeaux, France, 2021: 962-967

[114] Khedr W I, Gouda A E, Mohamed E R. P4-HLDMC: A novel framework for DDoS and ARP attack detection and mitigation in SD-IoT networks using machine learning, stateful P4, and distributed multi-controller architecture. Mathematics, 2023(12): 26-32

[115] AlSabeh A, Friday K, Kfoury E, et al. On DGA detection and classification using P4 programmable switches. Computers & Security, 2024(5): 62-75

[116] Tang X. Research on LDoS Attack Detection Methods Based on Programmable Data Plane in SDN. Zhejiang University, 2024 (in Chinese)
(唐馨. SDN中基于可编程数据平面的LDoS攻击检测方法研究. 浙江大学, 2024)

[117] El-Sayed A, Said W, Tolba A, et al. MP-GUARD: A novel multi-pronged intrusion detection and mitigation framework for scalable SD-IoT networks using cooperative monitoring, ensemble learning, and new P4-extracted feature set. Computers & Electrical Engineering, 2024(3): 23-34

[118] Doriguzzi-Corin R, Knob L A D, Mendozzi L, et al. Introducing packet-level analysis in programmable data planes to advance network intrusion detection. Computer Networks, 2024(6):75-89

[119] Roshani M, Nobakht M. HybridDAD: Detecting DDoS flooding attack using machine learning with programmable switches//Proceedings of the 17th International Conference on Availability, Reliability and Security. Vienna, Austria, 2022: 1-10

[120] Qin Q, Poularakis K, Tassiulas L. A learning approach with programmable data plane towards IoT security//Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems. Singapore, 2020: 410-420

[121] Barradas D, Santos N, Rodrigues L, et al. FlowLens: Enabling efficient flow classification for ML-based network security applications//Proceedings of the 27th Network and Distributed System Security Symposium. San Diego, USA, 2021: 1-15

[122] Krishnan A S, Sivalingam K M, Shami G, et al. Flow

classification for network security using P4-based programmable data plane switches//Proceedings of the 2023 IEEE 9th International Conference on Network Softwarization. Madrid, Spain, 2023: 374-379

[123] Gaikar M H, Haribabu K. A data-plane approach for detecting malware in IoT networks//Proceedings of the 2023 International Conference on Information Networking. Bangkok, Thailand, 2023: 578-583

[124] Ganesan A, Sarac K. Attack detection and mitigation using intelligent data planes in SDNs//Proceedings of the 2022 IEEE Global Communications Conference. Rio de Janeiro, Brazil, 2022: 4161-4166

[125] Busse-Grawitz C, Meier R, Dietmüller A, et al. PForest: In-network inference with random forests. arXiv, 2019: 1909.05680

[126] Zang M, Zheng C, Dittmann L, et al. Toward continuous threat defense: In-network traffic analysis for IoT gateways. IEEE Internet of Things Journal, 2024(6): 44-57

[127] Dong Y, Li Q, Wu K, et al. HorusEye: A realtime IoT malicious traffic detection framework using programmable switches//Proceedings of the USENIX Security Symposium. Anaheim, USA, 2023: 1-18

[128] Luo J, Liu W, Tan M, et al. Binary neural network with P4 on programmable data plane//Proceedings of the 2022 18th International Conference on Mobility, Sensing and Networking. Guangzhou, China, 2022: 960-965

[129] Xiong Z, Zilberman N. Do switches dream of machine learning?: Toward in-network classification//Proceedings of the 18th ACM Workshop on Hot Topics in Networks. Virtual , 2019: 1-7

[130] Zheng C, Zang M, Hong X, et al. Automating in-network machine learning. arXiv, 2022: 2205.08824

[131] Zang M, Zheng C, Koziak T, et al. Federated learning-based in-network traffic analysis on IoT edge//Proceedings of the 2023 IFIP Networking Conference. Barcelona, Spain, 2023: 1-10

[132] Sanghi A, Kadiyala K P, Tammana P, et al. Anomaly detection in data plane systems using packet execution paths//Proceedings of the 2021 ACM SIGCOMM Workshop on Secure Programmable Network Infrastructure. Virtual , USA,2021: 9-15

[133] Kang Q, Xing J, Chen A. Automated attack discovery in data plane systems//CSET@USENIX Security Symposium. Santa Clara, USA, 2019: 1-12

[134] Laraba A, Francois J, Chrisment I, et al. Detecting multi-step attacks: A modular approach for programmable data plane//Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022. Budapest, Hungary, 2022: 1-9

[135] Sahin M E, Demirci M. ConPoolUBF: Connection pooling and updatable bloom filter based SYN flood defense in programmable data planes. Computer Networks, 2023(4):23-33

[136] Scholz D, Gallenmüller S, Stubbe H, et al. Me love (SYN-) cookies: SYN flood mitigation in programmable data planes. arXiv, 2020: 2003.03221

[137] Khooi X Z, Csikor L, Divakaran D M, et al. DIDA: Distributed in-network defense architecture against amplified reflection DDoS attacks// Proceedings of the 2020 6th IEEE Conference on Network Softwarization. Ghent, Belgium, 2020: 277-281

[138] Ding D, Savi M, Pederzolli F, et al. In-network volumetric DDoS victim identification using programmable commodity switches. IEEE Transactions on Network and Service Management, 2021, 18(2): 1191-1202

[139] Laraba A, François J, Chrisment I, et al. Defeating protocol abuse with P4: Application to explicit congestion notification//2020 IFIP Networking Conference. Paris, France, 2020: 431-439

[140] Friday K, Kfoury E F, Bou-Harb E, et al. Towards a unified in-network DDoS detection and mitigation strategy//Proceedings of the 2020 6th IEEE Conference on Network Softwarization. Ghent, Belgium, 2020: 218-226

[141] Xing J, Wu W, Chen A. Ripple: A programmable, decentralized link-flooding defense against adaptive adversaries//Proceedings of the 30th USENIX Security Symposium. Virtual , USA, 2021: 3865-3881

[142] Jiang W, Jiang H, Xie Y, et al. SatShield: In-network mitigation of link flooding attacks for LEO constellation networks. IEEE Internet of Things Journal, 2024(16): 340-355

[143] Zhou H, Hong S, Liu Y, et al. Mew: Enabling large-scale and dynamic link-flooding defenses on programmable switches//Proceedings of the 2023 IEEE Symposium on Security and Privacy. San Francisco, USA, 2023: 3178-3192

[144] Zhang M, Li G, Wang S, et al. Poseidon: Mitigating volumetric DDoS attacks with programmable switches//Proceedings of the 2020 Network and Distributed System Security Symposium. San Diego, USA, 2020: 1-15

[145] Smyth D, Scott-Hayward S, Cionca V, et al. SECAP switch-defeating topology poisoning attacks using P4 data planes. Journal of Network and Systems Management, 2023, 31(1): 1-28

[146] Narayanan N, Sankaran G C, Sivalingam K M. Mitigation of security attacks in the SDN data plane using P4-enabled switches//2019 13th IEEE International Conference on Advanced Networks and Telecommunication Systems. Goa, India, 2019: 1-6

[147] Gondaliya H, Sankaran G C, Sivalingam K M. Comparative evaluation of IP address anti-spoofing mechanisms using a P4/NetFPGA-based switch//Proceedings of the 3rd P4 Workshop in Europe. Ghent, Belgium, 2020: 1-6

[148] Kuang P, Liu Y, He L. P4DAD: Securing duplicate address detection using P4//2020 IEEE International Conference on Communications. Dublin, Ireland, 2020: 1-7

[149] Simsek G, Bostan H, Sarica A K, et al. DroPPPP: A P4 approach to mitigating DoS attacks in SDN//Proceedings of the 20th International Conference on Information Security Applications. Jeju Island, Republic of Korea, 2019: 55-66

[150] Wang R H. Research on Address Spoofing Attack Tracing and Defense Mechanism in Programmable Network. Beijing Jiaotong University, 2023 (in Chinese)
(汪润虎. 可编程网络中地址欺骗攻击溯源与防御机制研究. 北京交通大学, 2023)

[151] Xing J, Morrison A, Chen A. NetWarden: Mitigating network covert channels without performance loss//USENIX Workshop on Hot Topics in Cloud Computing. Renton, USA, 2019: 1-6

[152] Reddy S S, Nishoak K, Shreya J L, et al. A P4-based adversarial attack mitigation on machine learning models in data plane devices. Journal of Network and Systems Management, 2024, 32(1): 1-24

[153] Jain LU. V. P4 based switch centric flow table overflow detection and mitigation in data plane devices//Proceedings of the 2023 5th International Conference on Recent Advances in Information Technology. Dhanbad, India, 2023: 1-6

[154] Pan J, Cai L, Yan S, et al. Network for AI and AI for network: Challenges and opportunities for learning-oriented networks. IEEE Network, 2021, 35(6): 270-277

[155] Sapio A, Abdelaziz I, Aldilaijan A, et al. In-network computation is a dumb idea whose time has come//Proceedings of the 16th ACM Workshop on Hot Topics in Networks. Palo Alto, USA, 2017: 1-7

[156] Sanvito D, Siracusano G, Bifulco R. Can the network be the AI accelerator? ACM SIGCOMM Computer Communication Review, 2018, 48(5): 12-18

[157] Kianpisheh S, Taleb T. A survey on in-network computing: Programmable data plane and technology specific applications. IEEE Communications Surveys & Tutorials, 2023, 25(1): 701-761

[158] Xiong Z, Zilberman N. Do switches dream of machine learning?: Toward in-network classification//Proceedings of the 18th ACM Workshop on Hot Topics in Networks. Princeton, USA, 2019: 1-7

[159] Wang Z, Liu Z, Zhang Y, et al. RCAgent: Cloud root cause analysis by autonomous agents with tool-augmented large language models//Proceedings of the 33rd ACM International Conference on Information and Knowledge Management. Birmingham, UK, 2024: 4966-4974

[160] Wang H, Abhashkumar A, Lin C, et al. NetAssistant: Dialogue based network diagnosis in data center networks//Proceedings of the Symposium on Networked Systems Design and Implementation. Renton, USA, 2024: 1-15

[161] Mondal R, Tang A, Beckett R, et al. What do LLMs need to synthesize correct router configurations?//Proceedings of the 22nd ACM Workshop on Hot Topics in Networks. Cambridge, USA, 2023: 189-195

[162] Xu H, Wang S, Li N, et al. Large language models for cyber security: A systematic literature review. arXiv, 2024: 2405.04760

[163] Motlagh F N, Hajizadeh M, Majd M, et al. Large language models in cybersecurity: State-of-the-art. arXiv, 2024: 2402.00891

[164] Zhang J, Bu H, Wen H, et al. When LLMs meet cybersecurity: A systematic literature review. arXiv, 2024: 2405.03644

[165] Wu J X. Endogenous security development paradigm in cyberspace. Scientia Sinica Informationis, 2022, 52(2): 189-204 (in Chinese)
(邬江兴. 网络空间内生安全发展范式. 中国科学:信息科学, 2022, 52(2): 189-204)

[166] Nötzli A, Khan J, Fingerhut A, et al. P4pktgen: Automated test case generation for P4 programs//Proceedings of the Symposium on SDN Research. Los Angeles, USA, 2018: 1-7

[167] Agape A-A, Danceanu M C, Hansen R R, et al. P4Fuzz: Compiler fuzzer for dependable programmable dataplanes//Proceedings of the 22nd International Conference on Distributed Computing and Networking. Virtual , 2020: 1-10

[168] Zheng N, Liu M, Zhai E, et al. Meissa: Scalable network testing for programmable data planes//Proceedings of the ACM SIGCOMM 2022 Conference. Amsterdam, The Netherlands, 2022: 1-14

[169] Bressana P, Zilberman N, Soulé R. PTA: Finding hard-to-find data plane bugs. IEEE/ACM Transactions on Networking, 2023, 31(3): 1324-1337

[170] Cao J, Zhou Y, Sun C, et al. Firebolt: Finding bugs in programmable data plane generators//Proceedings of the 2022 USENIX Annual Technical Conference. Carlsbad, USA, 2022: 819-834

[171] Liu J, Hallahan W T, Schlesinger C, et al. P4v: Practical verification for programmable data planes//Proceedings of the ACM SIGCOMM 2018 Conference. Budapest, Hungary, 2018: 1-14

[172] Stoenescu R, Dumitrescu D, Popovici M, et al. Debugging P4 programs with vera//Proceedings of the ACM SIGCOMM 2018 Conference. Budapest, Hungary, 2018: 1-15

[173] Tian B C. Research on Reliability Verification System for Cloud Network Data Plane. Nanjing: Nanjing University, 2022 (in Chinese)
(田冰川. 云网络数据平面的可靠性验证系统研究. 南京:南京大学, 2022)

[174] Tian B, Gao J, Liu M, et al. Aquila: A practically usable verification system for production-scale programmable data planes//Proceedings of the 2021 ACM SIGCOMM 2021 Conference, Virtural, 2021

HU Yu-Xiang, Ph. D., professor. His research interests include new network architecture and cyber security.

PAN Fan, Ph. D. candidate. His research interest include PDP and zero trust.

CUI Peng-Shuai, Ph. D., associate researcher. His research interests include PDP and endogenous security.

TIAN Le, Ph. D., associate researcher. His research interests include new network architecture and endogenous security.

CHANG De-Xian, Ph. D., associate professor. His research interests include activate defense and software defined security.

CUI Zi-Xi, Ph. D. candidate. His research interests include PDP and SDN.

XIA Ji-Qiang, Ph. D. candidate. His research interests include new network architecture and PDP.

ZHAN Qi, Ph. D. candidate. His research interests include cyber security and abnormal traffic detection.

WU Jiang-Xing, Ph. D., professor. His research interests include cyber security and information technology.

Background

With the vigorous rise of cutting-edge technologies such as cloud computing and the Internet of Things, the complexity and variability of network traffic have increased significantly, posing severe challenges to the ability of traditional static network devices (such as routers and switches) to handle large-scale and highly dynamic data flows, especially in defending against new security threats such as APT and DDoS. PDP-based network defense technology belongs to the intersection of network security and data communication technology, and mainly studies how to use the programmable characteristics of the data plane in modern network architecture to enhance the security defense capability of the network. At present, breakthroughs have been made in the research of network defense based on representative PDP technologies such as P4, which enable a variety of security applications, including VPN, firewall, and intrusion detection system, to be flexibly and efficiently deployed on the data plane, which greatly improves the flexibility and response speed of network defense.

This paper is dedicated to an in-depth discussion of PDP-based network defense technology, firstly systematically introduces the basic concept and theoretical basis of PDP, and then analyzes the unique advantages and potential value of PDP technology applied to the field of network defense by selecting typical cases. Furthermore, according to the implementation process of network defense, this paper divides the network defense technology based on PDP into three categories: protection technology, detection technology and response technology, and makes a detailed analysis and comprehensive review of the existing research results under each category. In this process, this paper not only summarizes the core ideas and implementation strategies of various schemes, but also objectively evaluates the advantages and limitations of different methods, aiming to provide valuable reference and enlightenment for future research and practice.

This paper is supported by the National Key R&D Program (2023YFB2903902), the Science and Technology Innovation Leading Talents Subsidy Project of Central Plains (244200510038), and the Songshan Laboratory Key R&D Project (221100210900-02). These projects study the application of programmable technologies in complex network environments to address cyberspace security threats, and have published more than ten papers and more than ten patents to date.