软件定义网络安全研究进展

翟亚红,崔峻玮

湖北汽车工业学院电气与信息工程学院,十堰 442002

摘要 软件定义网络(software defined networks,SDN)是一种新型的网络体系架构,通过集中式面向软件的管理方法,简化了新应用和服务的开发,目前已成为下一代互联网的研究热点。为了解决SDN中存在的安全问题,从SDN的3层架构方面综述了现有解决方案,分析了SDN安全问题上所面临的技术挑战。介绍了SDN的概念和3层架构,梳理了SDN的相关安全问题,依次总结了应用层、控制层和数据层中存在的安全问题和解决方案,展望了SDN安全问题未来研究可能面临的挑战。

关键词 软件定义网络;OpenFlow技术;网络安全;安全威胁;安全对策

软件定义网络(software defined networks,SDN)是一种未来网络的新范式,对互联网产生了很重要的影响,广泛应用于5G、物联网(internet of things,IoT)[1]等领域。尽管SDN自提出以来已经有10多年的历史,但它仍在不断发展,技术界的需求越来越多,并要求SDN更加动态、灵活和安全。

2020—2025年,预计SDN的使用将增加19%。有诸多因素影响着这一增长速率,其中,大部分因素与云服务提供商(Cloud Service Provider,CSP)有关,CSP在创新服务过程中发现,与传统网络相比,SDN架构提供了构建高度可扩展、可靠和自动化的数据中心基础设施的解决方案[2]。SDN架构通过OpenFlow技术将网络设备的数据平面与控制平面进行解耦,控制器是整个架构中最敏感的部分,通过南向接口与数据平面交互,北向接口与应用程序交互,东/西向接口负责互连分布式控制器。与传统网络架构不同,SDN特殊的3层结构存在一些漏洞[3]。

自2020年初以来,全球网络安全漏洞数量增加了15%,预计未来几年还会增加,这可能会严重影响SDN的性能。SDN的安全问题是当前SDN研究领域中的一个重要课题。随着SDN新的应用不断涌现,以及研究人员对SDN架构研究的日益深入,近年来有关SDN安全问题的研究取得了大量的成果,其安全架构设计及攻击防御等成为了判断一个SDN系统是否可以交付使用的重要依据。因此,针对该问题的深入研究对提高和保障SDN软件产品的质量具有重要意义。为了应对SDN的安全威胁,已经布局组织了相关工作,以研究相应的

收稿日期:2022-09-21;修回日期:2022-10-13

基金项目:湖北省教育厅科研计划重点项目(D20211802)

作者简介:翟亚红,副教授,研究方向为智能网联、大数据,电子信箱:120514045@qq.com

引用格式:翟亚红, 崔峻玮. 软件定义网络安全研究进展[J]. 科技导报, 2023, 41(13): 76-88; doi: 10.3981/j.issn.1000-7857.2023.13.008

安全挑战和解决方案。同时,提出了一些针对SDN安全威胁的解决方案,包括控制器复制方案、身份验证和授权机制,防止控制器遭受拒绝服务(denial of service,DoS)和分布式拒绝服务(distributed denial of service,DDoS)攻击的方案、流量监控和分析、流表溢出攻击防护等[4-5]。

综上所述,相关研究人员不断致力于SDN安全领域的研究。因此,有必要以具体且统一的方式对已有SDN安全问题及解决方案进行综述研究。其中包括用于解决SDN架构相关安全问题的最新技术进展,相关安全保障机制和工具等[6]。基于此,本研究着重梳理和总结SDN架构中存在的主要安全问题,提出相应的解决方案。

1　SDN的概念及系统架构

软件定义网络是一种新兴的、快速发展的技术,它将控制平面与数据平面解耦,以便根据特定策略和安全措施为网络控制提供更多的灵活性。在传统网络中,网络设备部署在静态硬件设备中,用来共同实现控制和数据转发。而控制逻辑将被从网络设备中分离出来,部署在SDN控制器或网络操作系统的外部实体中。

数据层中的网络设备负责根据控制层的决策转发数据流,而控制层包括控制器软件,负责配置和管理数据流转发的策略。应用层包括所有网络应用,如服务质量(quality of service,QoS)、路由和安全应用等。API(application programming interface)可连接这3层,使用2种不同的API。第1种是开放的南向接口,负责管理控制层和数据层之间的通信,以便允许控制器配置、管理数据流的转发策略并将其发送到网络设备。第2种是开放的北向接口,由控制层提供的网络可编程接口,为开发者提供了诸多便利条件。此外,在多控制器体系结构中,每个单独的控制器仅负责控制一部分交换机,为了保持网络状态的一致性并协同工作,单个SDN控制器可以通过东西向API与网络中的其他控制器进行通信。SDN架构由3层框架和2个应用接口API组成,如图1所示。

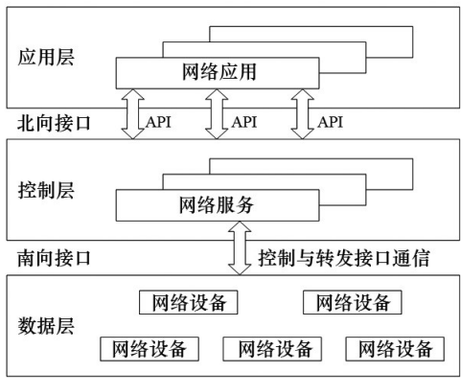

图1　软件定义网络的3层框架

1)SDN数据层。该层包括1个或多个网络设备,如交换机或路由器,主要负责网络数据包的转发功能。数据层设备是通过SDN控制器下发的转发规则转发流量,数据层与控制层通过南向API进行通信,有许多协议(如OpenFlow协议)管理数据层网络设备和SDN控制器之间的交互。当有新报文发送到SDN交换机后,首先匹配流表中的流表项,若匹配失败,则需要上报给上层控制层,等待控制层下达转发规则给数据层,规则一旦下发,报文将匹配流表项完成报文转发功能。

2)SDN控制层。该层的控制器是网络的关键核心元素,它负责管理和控制网络,并拥有整个网络拓扑的全局视图。能通过北向接口和南向接口分别与上层的应用层和下层的数据层进行互通,也可以对转发数据包进行任何必要的更改,如更新、安装和删除转发规则。

3)SDN应用层。该层由1个或多个可应用于SDN网络的应用程序组成。包含提供管理及云端虚拟化等服务,主要为用户提供服务级别协议SLA(service level agreement)、体验质量QoE(quality of experience)、监控、负载均衡、拓扑发现、安全与防火墙等网络服务功能,这些服务最终都以应用程序的方式表现,通过北向接口与SDN控制层进行数据交互。

2　SDN的安全问题和解决方案

近年来,相关学者在安全机制和解决方案方面

展开了研究,以确保SDN架构的可用性、机密性和完整性。Ahmad等[7]讨论了涉及SDN体系结构多层问题和安全方面的解决方案。Kreutz等[8]对SDN进行了广泛而全面的分析,包括体系结构安全性,但没有详细说明用于解决安全问题的机制。Cox等[9]阐述了SDN网络及各种应用的进展,并认识到SDN中部分基本的安全问题,包括体系结构安全和检测防御攻击的措施,开始关注控制器的安全性。Khan等[10]讨论了SDN中的网络拓扑发现过程和潜在的安全问题。黄颖祺等[11]分析了SDN的安全隐患,并提出相应对策和建议。Han等[12]考虑了SDN控制器的一些安全威胁和缓解技术。徐玉华等[13]探讨了SDN架构下异常流量检测机制,并简要阐述了一些解决方案。易芝玲等[14]关注5G技术的安全和隐私方面,简要阐述了SDN架构存在的问题,但没有详细说明可行的解决方案。Ahmad等[15]对控制器体系结构进行了研究,并考虑了其安全性。然而,关于SDN架构中包含所有层和接口的相关安全问题研究较少,对这些问题的解决方案也需要进行详细的分类。

随着SDN技术的发展,SDN的安全性问题引起了制造商和运营商越来越多的关注。本节将详细描述已提出的主要安全威胁和对策。根据上述介绍的相关安全性分析并结合SDN分层结构,即数据层、控制层和应用层,将网络安全威胁和安全对策分为3类,并详细介绍每层所面临的安全问题和解决方案。根据SDN层级结构列出了各种威胁,列举了各个层面可能存在的安全问题及隐患,如图2所示。

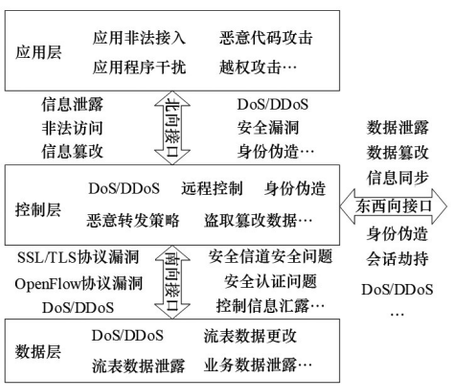

图2 SDN架构中存在的安全威胁类型

2.1 应用层/北向接口安全问题

SDN应用层平面提供了一组应用程序,这些程序对于满足系统自身的需求至关重要,从而可以通过控制器生成SDN安全环境的请求。目前,已有广泛的应用程序,包括防火墙、路由策略、协议等,可以由开发人员或第三方提供。

由于SDN应用程序非常多样,并且通常由第三方提供。这些应用程序可能会构成安全威胁,因为恶意应用程序可能会模拟成合法应用程序,进入控制器并对其配置采取恶意行动,甚至插入错误规则,完全修改网络行为[16]。针对各种现有的应用程序,研究人员已经进行了安全分析,确定了可能导致攻击的漏洞[17-21]。为了防止这种情况发生,制定了一些解决方案,例如Lee等[22]提出的INDAGO方案通过使用安全敏感行为图(SSBG)和机器学习主动检测恶意流量,并提供了针对信息操纵、模拟、权限分配和信息泄露等攻击流量的对策。Lee等[23]提出的SHIELD是一个框架,主要通过使用控制流图(CFG)分析应用程序的行为,使用此解决方案,可以识别可能导致修改内部网络参数的恶意行为。

2.1.1 应用程序间的干扰

来自第三方的多个应用程序之间可能会存在干扰,从而在网络策略中产生冲突[24],这种干扰可能来自攻击或导致攻击。Li等[25]提出了多种SDN应用的干扰检测器(MSAID),分析了多个应用程序的复杂交互行为,并开发了新的算法来识别多个应用程序的干扰。此外,这些算法有助于确定受干扰影响的流量,这可以帮助用户避免不必要的行为。Hu等[26]提出了一种SAIDE方案,首先将策略的操作和重构字段结合起来,以检测应用程序干扰;然后通过多标准决策,为冲突的策略分配优先级,以消除相应的应用程序干扰。

2.1.2 访问控制

当SDN应用程序缺乏有效的身份验证和访问控制机制时,北向接口将允许对控制器进行信任关系攻击,使网络暴露于处理非法请求,从而导致资源消耗增加且网络耗尽。为了解决应用程序中的授权问题,提出了细粒度和粗粒度访问控制机制。粗粒度访问控制机制通常用于独立系统或应用程

序的外部漏洞;另一方面,细粒度访问控制机制在应用程序权限中具有更大粒度和细节的控制,在更动态的环境中非常有用。通常,SDN体系结构用于多租户、多服务、多提供者、多域环境。因此,合并粗粒度或非常严格的访问控制可能会导致滥用权限或降低网络功能。Ujcich等[27]认为粗粒度访问控制机制不足以控制信息流上的完整性攻击,例如跨应用程序中毒(CAP)的攻击,其中非特权应用程序操纵访问控制器并欺骗其他应用程序代替其执行动作。

2.1.3　身份验证

SDN应用程序授权问题的解决方案更面向细粒度访问控制。关于身份验证,已有基于现有控制器或具有独立机制的解决方案。Chang等[28]提出了一种基于MD-UCON(multi-domain usage control)和基于角色的访问控制机制,并引入跨域角色映射方法,支持跨域访问授权,从而使该机制能够应用于SDN北向接口的访问控制应用。祝现威等[29]提出了一种基于属性密码的转发控制架构,当数据流离开时,转发设备对其进行验证,确保数据流的有效性。同时通过属性标识定义网络转发行为,该机制与属性签名验证共同实现细粒度的访问控制。范广宇等[30]利用传输层安全(TLS)协议完成应用和控制器间的双向认证和安全通信,并设计了权限管理和身份认证机制,以确保能够合理地访问控制器。Tseng等[31]提出了一个独立于控制器的动态访问控制系统,用于保护SDN控制器免受API滥用。通过对OpenFlow应用程序进行身份验证和授权,并且可以使用基于密码和基于令牌的身份验证来验证用户ID请求的合法性。Padekar等[32]提出了AEGIS安全框架,以防止控制器API被恶意网络应用程序滥用。当控制器API运行时进行验证,AEGIS对可能被恶意应用程序滥用的重要控制器API执行细粒度访问控制。Toshniwal等[33]提出的BEAM是一种为第三方应用程序分配权限的解决方案,此方案根据对网络行为的分析动态授予权限。BEAM定期升级/降级分配的访问权限,验证并建立对应用程序的信任。Tseng等[34]针对恶意应用程序入侵、DoS攻击和API滥用等问题,提出了SENAD架构。该架构可以安全地部署有效的网络应用程序,同时保护SDN控制器免受恶意应用程序的注入。Cui等[35]设计了一种应用程序身份验证系统,该系统安全地解决不受信任的网络应用程序和请求之间的冲突。Kim等[36]提出了安全即服务(SEaaS)解决方案,它可以在SDN环境中提供安全性,并在应用程序和控制器之间使用身份验证机制。Banse等[37]提出了一个安全的北向接口框架,SDN控制器可以通过类似REST的API向注册的SDN应用程序提供网络资源。Tseng等[38]基于已识别的威胁模型,开发了一个轻量级插件,称为控制器SEPA,通过使用RESTful API来保护SDN控制器免受恶意的OF(OpenFlow)应用程序。Natanzi等[39]提出了一种基于NTRU算法和NSS数字签名的网络资源使用第三方应用程序的新解决方案,该解决方案通过控制器可以通过安全的REST API仅为经过批准和可靠的程序提供网络信息。Hu等[40]提出了一种基于REST API访问控制的安全应用程序管理框架——SEAPP,SEAPP框架包含2个主要模块:权限检测引擎,用于识别应用程序权限的合法性;注册授权引擎,用于使用NTRU算法执行应用程序的注册和授权,以避免窃听或篡改攻击。

2.2　控制层/东西向接口安全问题

SDN的控制逻辑集中在控制平面,通过控制器管理来自数据平面的请求。目前,可用的控制器达30多种,它们拥有自己的编程语言和接口,大多数是开源的,也有少数是专用的。控制器可分为集中式架构或分布式架构[41]。集中式架构是整个网络使用单个控制器,以简化其管理。这种集中式的架构对于吞吐量需求较低。然而依赖于唯一的控制实体的网络可能会产生单点故障。例如,在高峰流量事件中,大量的传入请求会给唯一的控制器造成网络拥塞,影响响应时间[42]。此外,从安全角度来看,该架构可能容易受到DoS或DDoS攻击[43]。另一方面,分布式架构在多域或异构网络中使用多个控制器[44]。分布式控制器主要由电信运营商在大规模部署中使用,用于不同的功能,例如用于广域网(WAN)。Macedo等[45]提出了一个方案,作者通过Gossip协议使用反熵方法,实现了对具有恶意流

量过载的控制器的检测,以选取一个稳定的控制器来对抗SDN网络的DDoS攻击。Yu等[46]提出了WECAN多控制器解决方案,一种高效的东西向控制相关网络,用于实现不同SDN实体之间的通信。Benamrane等[47]提出并实现了分布式控制平面(CI-DC)的通信接口,该接口允许在多个分布式SDN控制器之间进行同步,交换通知及服务,实现了防火墙和负载均衡器等分布式服务,以提高分布式SDN架构中的安全性和整体服务质量。特别是南向和东西向通信中,Lam等[48]提出使用基于身份的多域密码学(IBC)协议保护分布式SDN通信。Hashemi Natanzi等[49]提出了基于PKI证书方法的椭圆曲线密码学(ECC)算法,以增强分布式控制器通信的安全性。

除上述攻击外,还应考虑由零日漏洞引起的攻击,这可能影响所有控制器,从而影响整个SDN的体系结构,这些攻击可以通过实现IDS来解决。入侵检测系统有2种类型:基于特征的入侵检测系统(SIDS)和基于异常的入侵检测系统(AIDS)[50]。其中,SIDS在检测零日漏洞方面效率较低,因为其功能是被动的,只能检测已知攻击,不能检测未知攻击。AIDS试图通过使用基于统计、基于知识和基于机器/深度学习的方法来主动提供解决方案。Song等[51]提出了一种基于机器学习的威胁感知系统,用于及时检测和响应SDN中的网络入侵。提出的系统包括用于特征选择的数据预处理,用于机器学习和异常检测的预测数据建模,以及用于SDN中入侵响应的决策。该系统可帮助SDN控制器正确应对基于特征码的网络入侵检测系统无法阻止的已知或未知攻击。Garg等[52]提出一种基于深度学习的混合异常检测框架,用于可疑流检测,它由异常检测模块和数据传输模块组成。第1个模块,利用改进的受限玻尔兹曼机(RBM)和基于梯度下降的支持向量机(SVM)检测异常活动;第2个负责端到端的数据传输的模块,以满足SDN的严格QoS要求,即高带宽和低延迟,以提高体验质量。Malik等[53]提出了一种基于控制平面的方案,由支持CU-DA(compute unified device architecture)的混合DL(deep learning)驱动架构组成,利用长短期记忆(LSTM)和卷积神经网络(CNN)的预测能力,高效及时地检测多向量威胁和攻击。该方案主要针对应用型攻击进行训练,如端口扫描、跨站脚本和僵尸网络。Tang等[54]提出了一种支持SDN的门控递归单元递归神经网络(GRU-RNN)入侵检测系统。该系统由流量收集器、异常检测器和异常缓解器3个模块组成,流量收集器模块获得了包入信息的所有敏感信息,异常检测器模块使用(GRU-RNN)生成异常检测过程,异常缓解器模块决定是否丢弃流量或深入分析。

2.3 数据层/南向接口安全问题

数据平面和控制平面使用例如OpenFlow、OVSDB、OpFlex、NETCONF和ForCes等协议经由南向接口进行通信。目前研究最广泛的协议是OpenFlow,它已经被认为是一个标准。然而,SDN本身的安全性一直是一个有争议的话题。这主要是因为SDN使用的通信标准(OpenFlow)是由开放网络基金会开发的,由于TLS的配置非常复杂,许多供应商不强制使用传输层安全协议,而仅将其定义为可选。这可能会使网络基础设施容易受到攻击,从而影响整体的安全性,其安全性则是SDN成功的决定因素之一。Agborubere等[55]重点介绍了如何通过TLS的安全缺陷并提高TLS安全性来保护SDN中的OpenFlow通信。Benton等[56]指出,缺乏TLS配置会增加交换机的风险,因为缺乏认证。而且在许多情况下,“监听模式”处于激活状态,攻击者可以访问转发信息和规则。Lam等[57]提出利用多域身份密码学(IBC)协议保护SDN南向接口和数据平面的通信安全。

数据平面集中了所有网络基础设施(如交换机和路由器),网络基础设施用于实现响应请求的所有决策。涉及数据平面的最重要动作之一是拓扑发现、更新和转发决策,主要基于链路发现服务(LDS)和主机跟踪服务(HTS)[58]2种服务。尽管这2种服务都很重要,但拓扑更新的数据包交换过程存在安全问题,这些问题来自于控制器的主机跟踪服务缺乏安全机制及LLDP数据包的来源缺乏足够的认证机制。数据包到达控制器后会被转化为合法的包信息,因此,攻击者可以实现拓扑中毒攻

击[59-61],如主机位置劫持攻击或链接编造攻击[62],引入非法信息,建立新的路由,从而为恶意目的转移流量。此外,在更新网络拓扑结构的过程中,还可以触发其他攻击,如DoS攻击[63]、拓扑结构篡改攻击[64]和中间人攻击等。

然而,还有一些并非SDN网络独有的问题,如入侵主机的DoS和DDoS攻击。这些攻击对任何网络基础设施都构成了巨大的威胁,是否能进行准确识别和缓解,很大程度上取决于如何进行安全检测。DoS攻击是单个主机发起的,其处理可能更容易,而DDoS攻击则不同,它是通过多个主机发起的,通常是僵尸网络,对其识别过程更为复杂。DoS攻击可以与冒名顶替攻击一起发起,如MAC或IP地址欺骗等[65-66]。

为了解决数据平面中提到的这些安全漏洞问题,对无状态数据平面和有状态数据平面之间进行区分。在无状态数据平面中,交换机不存储网络状态并执行控制平面所做的决定。所有要由无状态数据平面执行的新行动必须通过控制器查询[67]。然而,控制平面可以在适当和必要的时候将功能委托给数据平面,以"动态化"网络行为。这种委托允许数据平面存储网络状态并采取行动,从而将无状态数据平面变成有状态数据平面。

2.3.1　无状态数据平面

Dhawan等[67]提出SPHINX框架,以检测来自SDN内部的攻击,包括对网络拓扑和数据平面转发的已知和潜在的未知攻击,可动态地学习新的网络行为,并在检测到现有网络控制平面行为的可疑变化时发出警报。Hong等[62]针对网络拓扑中毒攻击提出了TopoGuard的缓解方法,这是SDN控制器的一个新的安全扩展,可提供自动和实时的网络拓扑中毒攻击的实时自动检测。Shrivastava等[68]通过使用静默中继攻击在SDN交换机之间注入假链路,可以轻松执行拓扑中毒。为了防御数据包注入攻击,Deng等[69]提出了SDN控制器上的轻量级扩展模块Packechecker,用于有效检测和缓解伪造数据包的泛滥。INSPECTOR[70]是一个基于硬件的解决方案,通过验证访问网络资源的数据包传入消息的身份验证保护受感染的控制器免受数据包注入攻击。TopoGuard+[64]是Topoguand的改进版,其中增加了2个模块:控制信息监视器(CMM)用于检测LLDP数据包;链路延迟检测器(LLI)用于检测延迟异常,可以有效减轻端口探测的健忘性。

Azzouni等[61]提出了一种安全高效的OpenFlow发现协议,即sOFTDP新型协议。sOFTDP维护拓扑内存,其中包含1个链接数据库,用于选择转发的最短路径。sOFTDP具有快速故障检测,用于检查交换机端口状态,并在需要时生成对备份链路的更改,以消除拓扑发现过程中的主要漏洞。Imran等[71]提出了一种简单而轻量级的检测和缓解系统DAISY,在分析收集的统计信息后,通过阻止来自攻击者的恶意流量来保护SDN免受DoS攻击。尚立等[72]采用卷积神经网络和SVM支持向量机相结合的机器学习方法来检测攻击。Huang等[73]提出了一个基于熵的解决方案,使用一个安全网关和一个HoneyPot。安全网关通过防御和过滤算法,确定是否存在DDoS攻击。如果存在攻击,则将流量发送到HoneyPot。否则,就向控制器请求转发规则,将其部署在交换机中。Xu等[74]提出了一个用于SDN/OpenFlow网络的高效且独立于协议的防御框架SDNGuardian,以缓解资源消耗型攻击。Wang等[75]提出了一个用于SDN的轻量级和快速的拒绝服务检测和缓解系统SDNManager。根据统计数据预测流量带宽变化,并相应地更新网络,以确保全局网络状态的优化,提高防御效率。Sahoo等[76]提出了一个使用机器学习来检测和缓解DDoS攻击的框架:统计监测模块接收来自交换机的一定时间间隔的流量统计信息;特征提取器模块使用内核主成分分析(KPCA)获得流量特征;提取的特征被用于分类器模块,该模块与SVM分类器一起工作,通过使用遗传算法(GA)进行参数优化,从良性流量中识别恶意流量。Wu等[77]认为,当攻击目标有一个固定的IP地址时,用于DDoS攻击的熵措施是有效的;但当攻击是针对随机IP时,缓解措施是有限的。由于阈值没有考虑可能的变异,提出了一个用主成分分析(PCA)的解决方案,从收集的信息中提供新模型,从而预测攻击。

Shohani等[78]针对SDN的结构和流量进行分

析,引入统计梯形模型估算每个交换机的表未命中数;从交换机收集信息;使用EWMA(exponentially weighted moving-average)统计模型计算阈值的算法,利用该模型可以处理数据集的波动性;通过将从前一阶段获得的值与交换机的表未命中数进行比较执行攻击检测。Badotra等[79]通过使用SNORT IDS入侵检测系统创建了一个早期DDoS检测工具。Barki等[80]提出了一个具有机器学习算法的IDS以检测DDoS攻击,选择具有更高精度的机器学习算法实现签名IDS,处理检测结果,并将准确的检测结果提供给主机。Li等[81]提出了一种基于SDN的深度学习DDoS检测模型和防御系统,该模型可以从网络流量序列中学习模式,并以历史方式跟踪网络攻击活动;通过使用基于该模型的防御系统,可以在软件定义的网络中有效地清除DDoS攻击流量。Banitalebi等[82]提出一种SDN中检测DDoS攻击的方法,应用2种类型的阈值,即基于熵的静态阈值和机器学习的动态阈值。Mohammadi等[83]解决了路由欺骗和资源耗尽2种类型的攻击。对于路由欺骗攻击,引入了一种称为"选择性阻止"的新技术,该技术阻止对手节点使用真实用户的活动路由;对于资源耗尽攻击,提出了一种"定期监控"技术,该技术根据SDN数据平面交换机在一段时间内收集的流量分析统计信息检测攻击者节点。

2.3.2 有状态数据平面

SDN的大多数编程语言都基于OpenFlow 1.0,默认情况下具有无状态数据平面配置,因此交换机仅遵守由控制器发布的转发规则,但该过程有时会产生控制器的开销和延迟,以满足网络抽象的需求。综上,很多研究人员发现可以将网络应用程序的可编程性扩展到数据平面,将本地状态信息保留在交换机中,以便它们可以在不查询控制器的情况下控制包转发,为网络提供"更大的动态性"。

林耘森箫等[84]介绍了基于P4的可编程数据平面的最新研究进展,并且在网络安全方面展现了学术界与工业界基于P4与可编程数据平面取得的应用成果。Hwang等[85]提出了一个基于P4的安全框架StateFit,可以灵活地过滤SDN可编程交换机上的攻击流量;StateFit的目标是减少SDN控制器集中式架构带来的延迟和信令开销,并进一步为本地化安全服务提供创新功能。Lewis等[86]提出了P4ID,结合规则解析器,使用P4处理无状态和有状态的数据包;使用这种技术,可以显著减少IDS正在处理的流量。Silverira Ilha等[87]基于P4语言设计了Euclid,这是一种完全网络内细粒度、低占用空间和低延迟的流量分析机制,用于DDoS攻击检测和缓解。Hauser等[88]提出了一种新颖的安全链路发现机制MACsec,用来保护基于P4的交换机之间的链路。Xing等[89]更关注P4交换机之间的状态交换,提出了使用数字签名的身份验证解决方案,该解决方案创建一个哈希链,附加到状态交换传输中的每个数据包,其验证操作在数据平面中执行。Xing等[90]提出了可编程数据平面上链路洪泛攻击的解决方案。其思想是通过可用路径拓扑混淆恶意流量,如果检测出正在实行恶意攻击则将其丢弃。Musumeci等[91]将机器学习和P4 enab1状态数据平面相结合,设计了一个实时DDoS攻击检测方法,通过交换机获取流量信息,并使用K近邻(KNN)、随机森林和SVM等算法对其进行分类,以确定是否存在攻击。

3 有待研究的科学问题

现有的研究已经为SDN架构的各种场景和安全问题提出了不同的解决方案。然而,安全仍然是一个具有挑战性的研究领域,还有许多尚未解决的问题。

3.1 SDN架构问题

很多研究学者都在关注将功能从控制平面委托给有状态的数据平面,尽管这可能会导致失去SDN原有的架构。由于决策是在交换机层面上处理的,而且没有控制器参与,网络拓扑结构中可能会出现不一致的情况[92]。数据平面可编程性不断发展,如P4语言在解决安全问题方面获得很大的动力。同时,可编程逻辑器件(FPGA)的功能不断扩大,带来了可编程性和处理的敏捷性,从而可以减少网络中的延迟和抖动[93]。尽管本文是以SDN各层或接口为重点的方式对安全解决方案进行分

类,但也有探索整个SDN架构的解决方案。例如:Lee等[94]验证了网络流量策略中的不一致之处;在Lee等[95]使用模糊测试算法来评估SDN环境;Lee等[96]、Fawcett等[97]提出了检测和补救攻击的框架,如DoS/DDoS、扫描或入侵在SDN架构的不同层面;Karmakar等[98]通过根据特定策略执行访问控制列表(ACL)进行SDN域控制。

3.2　SDN接口问题

大多数学者的注意力集中在解决SDN架构各个平面的攻击上,而忽略了接口的安全问题。北向和东西向接口代表了SDN大规模部署的重要部分,因为其允许互操作性和访问各种的应用。在缺乏标准化接口的情况下,出现攻击情况的可能性会增加。因此,对于SDN架构的安全,需要考虑接口的标准化。接口标准化在安全方面的优势体现在资源优化方面。一方面,它将减少由第三方应用广泛性所产生的攻击数量;另一方面,缓解攻击的措施方案将被统一,并防止网络设备受到攻击。

3.3　SDN安全机制问题

攻击检测会考虑一些使用基于熵的解决方案,因为实现简单且成本低而成为广泛采用的机制。然而,由于SDN网络的不断发展,这种基于熵的方案已无法面对形式各样的攻击流量。大多数研究人员从熵转变到其他数学模型和统计模型。机器学习、深度学习和区块链等技术被用于解决SDN架构的安全问题[99]。陈何雄等[100]提出了基于区块链的软件定义网络数据帧安全验证机制,对伪造、受篡改数据帧可以进行有效地识别与过滤。由于存在额外的安全保障机制,虽然保证服务得到安全保障,但也可能对资源等成本效益产生影响。以最小的成本阻止SDN架构受到攻击,这是未来的挑战之一。

3.4　SDN可扩展性问题

尽管SDN架构本身带来了巨大的安全挑战,但也被其他技术用来解决安全问题。因此,有一些安全解决方案利用SDN来改进防御机制,而另一些则选择网络功能虚拟化(NFV)和SDN的联合参与,以在设备异构的环境中防止恶意行为,如IoT环境或云安全等[101-103]。

4　结论

概述了软件定义网络的基本概念、网络架构。SDN通过解耦控制平面与转发平面,赋予网络灵活的可编程性,可以更好地用于网络资源的集中管理和统一调度。尽管SDN的分层结构和可编程的特点给网络管理带来很多便利,但其集中式的控制方式给SDN带来了安全方面的诸多挑战。通过对SDN的3层结构特点进行分析,分别总结出SDN每层所面临的安全问题和解决方案。最常见的安全问题是认证、授权和DDoS攻击,大多数研究更偏向于实现细粒度的访问控制,包括机器学习、深度学习及区块链技术。结合当前已有的研究成果,归纳出各层在面临安全威胁和恶意攻击时所采取的一些对策。(1) 针对应用层,维护与控制层之间的可靠信任是加强安全举措的一个重要方向,通过应用程序间的干扰、访问控制和身份验证来解决应用层的安全问题。(2) 针对控制层,通过东西向接口部署多控制器,并利用建立新机制解决来自应用的攻击、单控制器单点故障、DoS和DDoS攻击等问题。(3) 针对数据层,通过有状态和无状态控制平面提出了更加细致的安全方案,用于解决恶意软件安装会修改数据路径上的流规则,造成错误流规则的产生,导致数据层的安全性受到威胁等问题。机器学习、深度学习、P4以及区块链新技术都被用来解决SDN的有关安全问题,并在一定条件下取得了不错的验证结果,可以在一定范围内有效应对SDN的安全问题和攻击。

参考文献(References)

[1] 强奇, 武刚, 黄开枝, 等. 5G安全技术研究与标准进展[J]. 中国科学: 信息科学, 2021, 51(3): 347-366.

[2] 付永红, 毕军, 张克尧, 等. 软件定义网络可扩展性研究综述[J]. 通信学报, 2017, 38(7): 141-154.

[3] 池亚平, 莫崇维, 杨垠坦, 等. 面向软件定义网络架构的入侵检测模型设计与实现[J]. 计算机应用, 2020, 40(1): 116-122.

[4] 岳猛, 王怀远, 吴志军, 等. 云计算中DDoS攻防技术研究综述[J]. 计算机学报, 2020, 43(12): 2315-2336.

[5] 陈兴蜀, 滑强, 王毅桐, 等. 云环境下SDN网络低速率DDoS攻击的研究[J]. 通信学报, 2019, 40(6): 210-222.
[6] 董仕. 软件定义网络安全问题研究综述[J]. 计算机科学, 2021, 48(3): 295-306.
[7] Ahmad I, Namal S, Ylianttila M, et al. Security in software defined networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2317-2346.
[8] Kreutz D, Ramos F M V, Esteves Verissimo P, et al. Software-defined networking: A comprehensive survey[J]. Proceedings of the IEEE, 2015, 103(1): 14-76.
[9] Cox J H, Chung J, Donovan S, et al. Advancing software-defined networks: A survey[J]. IEEE Access, 2017, 5: 25487-25526.
[10] Khan S, Gani A, Abdul Wahab A W, et al. Topology discovery in software defined networks: Threats, taxonomy, and state-of-the-art[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 303-324.
[11] 黄颖祺, 张宏斌, 卢赓, 等. 软件定义网络的安全问题及对策研究[J]. 信息安全研究, 2020, 6(3): 202-211.
[12] Han T, Jan S R U, Tan Z Y, et al. A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers[J]. Concurrency and Computation: Practice and Experience, 2020, 32(16): e5300.
[13] 徐玉华, 孙知信. 软件定义网络中的异常流量检测研究进展[J]. 软件学报, 2020, 31(1): 183-207.
[14] 易芝玲, 崔春风, 韩双锋, 等. 5G蜂窝物联网关键技术分析[J]. 北京邮电大学学报, 2018, 41(5): 20-25.
[15] Ahmad S, Mir A H. Scalability, consistency, reliability and security in SDN controllers: A survey of diverse SDN controllers[J].Journal of Network and Systems Management, 2020, 29(1): 1-59.
[16] Murillo A F, Rueda S J, Morales L V, et al. SDN and NFV security: Challenges for integrated solutions[M]// Computer Communications and Networks. Cham: Springer International Publishing, 2017: 75-101.
[17] 李可欣, 王兴伟, 易波, 等. 智能软件定义网络[J]. 软件学报, 2021, 32(1): 118-136.
[18] Artmann D, Khondoker R. Security analysis of SDN WiFi applications[M]//SDN and NFV Security. Cham: Springer International Publishing, 2018: 57-71.
[19] Bräuning M, Khondoker R. Analysis of SDN applications for smart grid infrastructures[M]//SDN and NFV Security. Cham: Springer International Publishing, 2018: 99-110.
[20] Chikhale A, Khondoker R. Security analysis of SDN cloud applications[M]//SDN and NFV Security. Cham: Springer International Publishing, 2018: 19-38.
[21] Jain R, Khondoker R. Security analysis of SDN WAN applications—B4 and IWAN[M]// SDN and NFV Security. Cham: Springer International Publishing, 2018: 111-127.
[22] Lee C, Yoon C, Shin S, et al. INDAGO: A new framework for detecting malicious SDN applications[C]//2018 IEEE 26th International Conference on Network Protocols. Piscataway: IEEE Press, 2013: 220-230.
[23] Lee C, Shin S. SHIELD: An automated framework for static analysis of SDN applications[C]//Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. New York: ACM, 2016: 29-34.
[24] Durairajan R, Sommers J, Barford P. Controller-agnostic SDN debugging[C]//Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. New York: ACM, 2014: 227-234.
[25] Li Y H, Wang Z L, Yao J Y, et al. MSAID: Automated detection of interference in multiple SDN applications [J]. Computer Networks, 2019, 153: 49-62.
[26] Hu T, Yi P, Hu Y X, et al. SAIDE: Efficient application interference detection and elimination in SDN[J]. Computer Networks, 2020, 183: 107619.
[27] Ujcich B E, Jero S, Edmundson A, et al. Cross-app poisoning in software-defined networking[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 648-663.
[28] Chang R, Lin Z W, Sun Y, et al. MD-UCON: A multi-domain access control model for SDN northbound interfaces[J]. Journal of Physics: Conference Series, 2019, 1187(3): 032091.
[29] 祝现威, 常朝稳, 朱智强, 等. 基于身份属性的SDN控制转发方法[J]. 通信学报, 2019, 40(11): 1-18.
[30] 范广宇, 王兴伟, 贾杰, 等. SDN应用平面与控制平面安全交互方法[J]. 信息网络安全, 2021, 21(6): 70-79.
[31] Tseng Y, Pattaranantakul M, He R, et al. Controller DAC: Securing SDN controller with dynamic access control[C]//2017 IEEE International Conference on Communications. Piscataway: IEEE Press, 2017: 1-6.
[32] Padekar H, Park Y, Hu H X, et al. Enabling dynamic access control for controller applications in software-defined networks[C]// Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies.

New York: ACM, 2016: 51-61.

[33] Toshniwal B, Joshi K D, Shrivastava P, et al. BEAM: Behavior-based access control mechanism for SDN applications[C]//2019 28th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2019: 1-2.

[34] Tseng Y, Nait-Abdesselam F, Khokhar A. SENAD: Securing network application deployment in software defined networks[C]//2018 IEEE International Conference on Communications. Piscataway: IEEE Press, 2018: 1-6.

[35] Cui H Y, Chen Z M, Yu L F, et al. Authentication mechanism for network applications in SDN environments[C]//2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC). Piscataway: IEEE Press, 2017: 1-5.

[36] Kim G, An J, Kim K. A study on authentication mechanism in SEaaS for SDN[C]//Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. New York: ACM, 2017: 1-6.

[37] Banse C, Rangarajan S. A secure northbound interface for SDN applications[C]//2015 IEEE Trustcom/BigDataSE/ISPA. Piscataway: IEEE Press, 2015: 834-839.

[38] Tseng Y, Zhang Z H, Naït-Abdesselam F. ControllerSEPA: A security-enhancing SDN controller plug-in for OpenFlow applications[C]//2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). Piscataway: IEEE Press, 2016: 268-273.

[39] Natanzi S B H, Majma M R. Secure northbound interface for SDN applications with NTRU public key infrastructure[C]//2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation. Piscataway: IEEE Press, 2017: 452-458.

[40] Hu T, Zhang Z, Yi P, et al. SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment[J]. Journal of Parallel and Distributed Computing, 2021, 147: 108-123.

[41] 徐明迪, 高杨, 崔峰. 基于SDN的分布式欺骗防御系统[J]. 通信学报, 2018, 39(增刊2): 54-60.

[42] 周启钊, 于俊清, 李冬. SDN控制层泛洪防御机制研究:检测与缓解[J]. 通信学报, 2021, 42(11): 41-53.

[43] 柳林, 周建涛. 软件定义网络控制平面的研究综述[J]. 计算机科学, 2017, 44(2): 75-81.

[44] 李军飞, 兰巨龙, 胡宇翔, 等. SDN多控制器一致性的量化研究[J]. 通信学报, 2016, 37(6): 86-93.

[45] Macedo R, De Castro R, Santos A, et al. Self-organized SDN controller cluster conformations against DDoS attacks effects[C]//2016 IEEE Global Communications Conference. Piscataway: IEEE Press, 2016: 1-6.

[46] Yu H S, Qi H, Li K Q. WECAN: An efficient west-east control associated network for large-scale SDN systems [J].Mobile Networks and Applications, 2020, 25(1): 114-124.

[47] Benamrane F, Ben Mamoun M, Benaini R. An East-West interface for distributed SDN control plane: Implementation and evaluation[J]. Computers & Electrical Engineering, 2017, 57: 162-175.

[48] Lam J H, Lee S G, Lee H J, et al. Securing distributed SDN with IBC[C]//2015 Seventh International Conference on Ubiquitous and Future Networks. Piscataway: IEEE Press, 2015: 921-925.

[49] Hashemi Natanzi S B, Majma M R. Secure distributed controllers in SDN based on ECC public key infrastructure[C]//2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). Piscataway: IEEE Press, 2017: 1-5.

[50] Khraisat A, Gondal I, Vamplew P, et al. Survey of intrusion detection systems: Techniques, datasets and challenges[J]. Cybersecurity, 2019, 2(1): 1-22.

[51] Song C, Park Y, Golani K, et al. Machine-learning based threat-aware system in software defined networks [C]//2017 26th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2017: 1-9.

[52] Garg S, Kaur K, Kumar N, et al. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective[J]. IEEE Transactions on Multimedia, 2019, 21(3): 566-578.

[53] Malik J, Akhunzada A, Bibi I, et al. Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in SDN[J]. IEEE Access, 2020, 8: 134695-134706.

[54] Tang T A, Mclernon D, Mhamdi L, et al. Intrusion detection in SDN-based networks: Deep recurrent neural network approach[M]//Deep Learning Applications for Cyber Security. Cham: Springer International Publishing, 2019: 175-195.

[55] Agborubere B, Sanchez-Velazquez E. OpenFlow commu-

nications and TLS security in software-defined networks [C]//2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Piscataway: IEEE Press, 2017: 560-566.

[56] Benton K, Camp L J, Small C. OpenFlow vulnerability assessment[C]//Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. New York: ACM, 2013: 151-152.

[57] Lam J, Lee S G, Lee H J, et al. Securing SDN southbound and data plane communication with IBC[J]. Mobile Information Systems, 2016, 2016: 1-12.

[58] Marin E, Bucciol N, Conti M. An in-depth look into SDN topology discovery mechanisms: Novel attacks and practical countermeasures[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2019: 1101-1114.

[59] Nguyen T H, Yoo M. Attacks on host tracker in SDN controller: Investigation and prevention[C]//2016 International Conference on Information and Communication Technology Convergence (ICTC). Piscataway: IEEE Press, 2016: 610-612.

[60] Nguyen T H, Yoo M. Analysis of link discovery service attacks in SDN controller[C]//2017 International Conference on Information Networking (ICOIN). Piscataway: IEEE Press, 2017: 259-261.

[61] Azzouni A, Boutaba R, Trang N T M, et al. sOFTDP: Secure and efficient topology discovery protocol for SDN [J]. arXiv preprint: 1705.04527, 2017.

[62] Hong S, Xu L, Wang H P, et al. Poisoning network visibility in software-defined networks: New attacks and countermeasures[C]//Proceedings 2015 Network and Distributed System Security Symposium. Reston: Internet Society, 2015: 8-11.

[63] 朱良根, 张玉清, 雷振甲. DoS攻击及其防范[J]. 计算机应用研究, 2004(7): 82-84.

[64] Skowyra R, Xu L, Gu G F, et al. Effective topology tampering attacks and defenses in software-defined networks [C]//2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2018: 374-385.

[65] Lin T Y, Wu J P, Hung P H, et al. Mitigating SYN flooding attack and ARP spoofing in SDN data plane[C]// 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS). Piscataway: IEEE Press, 2020: 114-119.

[66] Akyildiz I F, Lee A, Wang P, et al. A roadmap for traffic engineering in SDN-OpenFlow networks[J]. Computer Networks, 2014, 71: 1-30.

[67] Dhawan M, Poddar R, Mahajan K, et al. Sphinx: Detecting security attacks in software-defined networks[C]// Network & Distributed System Security Symposium. San Diego, California, USA: 2015, 15: 8-11.

[68] Shrivastava P, Agarwal A, Kataoka K. Detection of topology poisoning by silent relay attacker in SDN[C]//Proceedings of the 24th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2018: 792-794.

[69] Deng S H, Gao X, Lu Z B, et al. Packet injection attack and its defense in software-defined networks[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(3): 695-705.

[70] Alshra'A A S, Seitz J. Using INSPECTOR device to stop packet injection attack in SDN[J]. IEEE Communications Letters, 2019, 23(7): 1174-1177.

[71] Imran M, Durad M H, Khan F A, et al. DAISY: A detection and mitigation system against denial-of-service attacks in software-defined networks[J]. IEEE Systems Journal, 2020, 14(2): 1933-1944.

[72] 尚立, 陈明, 张磊, 等. SDN中基于机器学习的DDoS攻击协同防御[J]. 电力系统保护与控制, 2021, 49(16): 170-176.

[73] Huang X L, Du X J, Song B. An effective DDoS defense scheme for SDN[C]//2017 IEEE International Conference on Communications. Piscataway: IEEE Press, 2017: 1-6.

[74] Xu J F, Wang L M, Xu Z. An enhanced saturation attack and its mitigation mechanism in software-defined networking[J]. Computer Networks, 2020, 169: 107092.

[75] Wang T, Chen H C, Cheng G Z, et al. SDNManager: A safeguard architecture for SDN DoS attacks based on bandwidth prediction[J]. Security and Communication Networks, 2018, 2018: 1-16.

[76] Sahoo K S, Tripathy B K, Naik K, et al. An evolutionary SVM model for DDoS attack detection in software defined networks[J]. IEEE Access, 8: 132502-132513.

[77] Wu D, Li J, Das S K, et al. A novel distributed denial-of-service attack detection scheme for software defined networking environments[C]//2018 IEEE International Conference on Communications. Piscataway: IEEE Press, 2018: 1-6.

[78] Shohani R B, Mostafavi S A. Introducing a new linear regression based method for early DDoS attack detection in SDN[C]//2020 6th International Conference on Web Research (ICWR). Piscataway: IEEE Press, 2020: 126-132.

[79] Badotra S, Panda S N. SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking[J]. Cluster Computing, 2021, 24(1): 501-513.

[80] Barki L, Shidling A, Meti N, et al. Detection of distributed denial of service attacks in software defined networks [C]//2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Piscataway: IEEE Press, 2016: 2576-2581.

[81] Li C H, Wu Y, Yuan X Y, et al. Detection and defense of DDoS attack-based on deep learning in OpenFlow-based SDN[J]. International Journal of Communication Systems, 2018, 31(5): e3497.

[82] Banitalebi Dehkordi A, Soltanaghaei M, Boroujeni F Z. The DDoS attacks detection through machine learning and statistical methods in SDN[J].The Journal of Supercomputing, 2021, 77(3): 2383-2415.

[83] Mohammadi R, Javidan R, Keshtgary M, et al. Practical extensions to countermeasure DoS attacks in software defined networking[C]//2017 IEEE Conference on Network Function Virtualization and Software Defined Networks. Piscataway: IEEE Press, 2017: 1-6.

[84] 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[J]. 计算机学报, 2019, 42(11): 2539-2560.

[85] Hwang R H, Nguyen V L, Lin P C. StateFit: A security framework for SDN programmable data plane model[C]// 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN). Piscataway: IEEE Press, 2018: 168-173.

[86] Lewis B, Broadbent M, Race N. P4ID: P4 enhanced intrusion detection[C]//2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). Piscataway: IEEE Press, 2019: 1-4.

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

[88] Hauser F, Schmidt M, Häberle M, et al. P4-MACsec: Dynamic topology monitoring and data layer protection with MACsec in P4-based SDN[J]. IEEE Access, 2020, 8: 58845-58858.

[89] Xing J R, Chen A, Ng T S E. Secure state migration in the data plane[C]// Proceedings of the Workshop on Secure Programmable Network Infrastructure. New York: ACM, 2020: 28-34.

[90] Xing J R, Wu W Q, Chen A. Architecting programmable data plane defenses into the network with FastFlex[C]// Proceedings of the 18th ACM Workshop on Hot Topics in Networks. New York: ACM, 2019: 161-169.

[91] Musumeci F, Ionata V, Paolucci F, et al. Machine-learning-assisted DDoS attack detection with P4 language[C]// ICC 2020-2020 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2020: 1-6.

[92] Dargahi T, Caponi A, Ambrosin M, et al. A survey on the security of stateful SDN data planes[J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1701-1725.

[93] Scholz D, Gallenmüller S, Stubbe H, et al. SYN flood defense in programmable data planes[C]//Proceedings of the 3rd P4 Workshop in Europe. New York: ACM, 2020: 13-20.

[94] Lee S, Woo S, Kim J, et al. AudiSDN: Automated detection of network policy inconsistencies in software-defined networks[C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2020: 1788-1797.

[95] Lee S, Yoon C, Lee C, et al. Delta: A security assessment framework for software-defined networks[C]//The Network and Distributed System Security Symposium 2017. San Diego: NDSS , 2017: 1-5.

[96] Lee S, Kim J, Shin S, et al. Athena: A framework for scalable anomaly detection in software-defined networks [C]//2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2017: 249-260.

[97] Fawcett L, Scott-Hayward S, Broadbent M, et al. Tennison: A distributed SDN framework for scalable network security[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(12): 2805-2818.

[98] Karmakar K K, Varadharajan V, Tupakula U. On the design and implementation of a security architecture for software defined networks[C]//2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data

Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE Press, 2016: 671-678.

[99] 唐菀, 张艳, 杨喜敏, 等.引入区块链的SDN-IoT网络安全:架构、方案与挑战[J]. 小型微型计算机系统, 2022, 43(10): 2179-2199.

[100] 陈何雄, 罗宇薇, 韦云凯, 等. 基于区块链的软件定义网络数据帧安全验证机制[J].计算机应用, 2021, doi: 51.1307.TP.20211202.2148.004.

[101] 黄韬, 刘江, 汪硕, 等. 未来网络技术与发展趋势综述[J]. 通信学报, 2021, 42(1): 130-150.

[102] Tupakula U. On the design and implementation of a security architecture for software defined networks[C]// 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE Press, 2016: 671-678.

[103] Sahoo K S, Puthal D. SDN-assisted DDoS defense framework for the internet of multimedia things[J]. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2020, 16(3): 1-18.

Advances in software defined network security research and key technologies

ZHAI Yahong, CUI Junwei

College of Electrical and Information Engineering, Hubei University of Automobile Technology, Shiyan 442002, China

Abstract Software-defined networking(SDN) is a new network architecture that simplifies the development of new applications and services through a centralized software-oriented management approach and has become a research hotspot for the next-generation Internet. To address the security issues in SDN, this paper reviews the existing solutions in terms of the 3-layer architecture of SDN and analyzes the technical challenges faced by SDN security. In particular, it firstly introduces the definition of SDN and the 3-layer architecture then reviews the research advances on security related to SDN. Next, it summarises the security issues and solutions to the application layer, control layer and data layer, respectively. Finally, it provides an outlook on the challenges that SDN security future research may encounter.

Keywords software defined networking; OpenFlow; network security; security threats; security countermeasures

（责任编辑　刘志远）