软件定义网络安全研究①

章喜字　徐燎源
（黎明职业大学　福建泉州　362000）

摘　要 SDN（软件定义网络）以 OpenFlow 技术为支持，将网络控制和数据面分离，实现对流量的个性化控制。伴随 SDN 的深入应用，如何更好地保障网络安全性是 SDN 领域待解决的首要问题。目前国内外学者积极研究 SDN 的安全领域，下文对 SDN 3 层架构面对的安全问题及如何解决进行分析，为 SDN 数据、控制及应用层的安全运行打下基础，以此为如何更好地解决 SDN 的安全问题提供一定的参考。

关键词 SDN；软件定义网络；数据；控制；安全

Research on Software Defined Network Security

Zhang Xizi　Xu Liaoyuan
(Liming Vocational University，Quanzhou，Fujian，362000，China)

Abstract SDN(Software Defined Network) is supported by OpenFlow technology, which separates network control from data plane to achieve personalized control of traffic. With the in-depth application of SDN, how to ensure network security better is the primary problem to be solved in the field of SDN. At present, scholars at home and abroad are actively studying the security field of SDN. The following passage analyzes the security problems faced by the SDN 3 layer architecture and how to solve them, laying a foundation for the safe operation of SDN data, control and application layer, so as to provide a certain reference for solving SDN security problems better.

Keywords SDN；Software Defined Network；Data；Control；Security

①本文系 2019 年福建省中青年教师科研基金项目（高校教育信息化专项）“基于 SDN 的高校网络体系构建研究”（项目编号：JAT191929）的研究成果之一。

1 引言

SDN（软件定义网络）属于网络体系结构的一种，其出现、发展的周期较短，相关技术有待进一步的研究[1]。在SDN安全方面，其网络架构和传统架构不同，故衍生出的攻击方式及安全问题也有所不同，需要有针对性地落实多种安全防范措施。

2 关于 SDN 及其构成

2.1 SDN

SDN是指具有OpenFlow技术链的网络，其网络控制模式特殊，底层网络分为控制层和数据层，控制层为集中管控设备，以安全通道和交换机通信，下发流表及控制规则，实现流量灵活调整，实现路由机制、封包分析、网络虚拟化等多项功能[2]。SDN具有可编程的特点，在P4编程的支持下，可将软件定义延伸到硬件方面，以P2编程控制转发及数据包分析，实现SDN迅速编程。

2.2 SDN 的构成

OpenFlow因其灵活性和规范性被用作SDN通信协议标准。和TCP/IP协议类似，OpenFlow支持控制器和SDN交换机通信，传统网络以交换机、路由器实现报文转发，该技术可以通过控制器和交换机完成[3]。流表生成、维护、规则下发由控制器负责，OpenFlow协议对各类信息分别进行处理，落实控制器和交换机的路由控制。OpenFlow协议支持对称及异步消息[4]。

2.2.1 应用层

含有管理及云端虚拟化服务，为客户提供SLA、QoE监控、拓扑发现、防火墙保护等功能，最终以应用程序的方式展现给客户，以北向接口和SDN控制层数据交互，如图 1 所示。

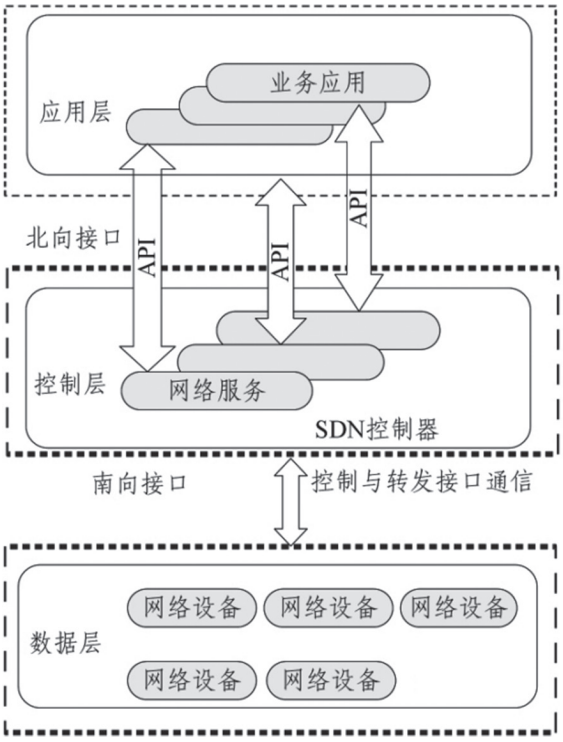

图 1 SDN

2.2.2 控制层

控制层可以实现网络远程控制，配合SDN软件，以北向接口、南向集中管理系统，实现对SDN交换机的集中控制。单个SDN可以配置多个控制器，各个控制器可以按照对等或主从的方式看设置[5]。利用SDN交换机下发流表原理，各个控制器可以实现多台设备管理，单个设备也可以由多个控制器联合控制。

2.2.3 数据层

交换机、路由器等共同构成SDN数据层，负责对数据包进行转发，交换机、路由器端口和流表实现了与控制层的数据联动，向控制层下达转发规则[6]。若有新报文传递给交换机，则先匹配流表内容，匹配不上才反馈给控制层，控制层提供转发规则，数据层报文匹配流表项完成报文转发。

3 SDN 可能发生的安全问题

3.1 应用层

SDN以编程方式管理设备资源，但用控制器管理的模式可能会遭受恶意软件的攻击。SDN软件未受到恶意攻击或北向接口正常时，OpenFlow可以起到对SDN的保护，但是DDoS的攻击无法用OpenFlow化解，若SDN应用软件受到破坏，会影响系统的正常运行。

对应用层问题，可以从以下两个角度进行论述。一方面，SDN应用及控制层需以应用服务支持交互，确保应用服务安全，才能保证数据交互安全[7]。可以在其中加入身份认证，以身份认证访问者是否有访问、使用权限，来避免恶意程序、资源破坏网络。另一方面，一些应用程序中的恶意代码会破坏整个SDN，如网络中敏感数据提供的传输路径、应用程序的访问控制、内容检查和入侵检测服务。恶意程序会逃过访问控制，威胁系统。SDN应用程序可以直接和控制器通信，但程序间接通信的数据报格式特殊，具有“未知”的特点，可能导致SDN应用成为未经授权的访问控制层网关[8]。

3.2 控制层

控制层是系统决策中心，可能面临应用攻击和Dos及DDos攻击。

3.2.1 应用攻击

控制层应用配置对控制层的威胁较大，应用配置的认证直接影响控制层的安全，通过认证的应用可以获取各方面的访问权限，故程序获取资源前，需进行充分限制并分类，各个应用的功能不同，需对各个应用进行安全需求分析。例如，负载均衡的应用需统计报文字节数，入侵检测应用要考察报文头部信息。

3.2.2 DoS 及 DDoS 攻击

SDN控制器中最常见的就是DoS及DDoS，且其对SDN的威胁较大[9]。OpenFlow中复杂的任务都由控制层决策。但在10Gbps网络中控制层无法处理大量新流量，控制层易受到DoS及DDoS攻击。控制层的控制器数量为单个，若网络流增加，控制器无法及时处理，将造成时延过长，时延受控制器处理速度影响较大。若控制器自身局限性明显，将导致单点失效。

3.3 数据层

数据层是否安全和控制层安全关系较大，若控制层受到攻击，数据层多半也会受到影响。交换机无法从控制器转发信息，或控制层异常导致连接异常，数据层离线，这将导致系统瘫痪。网络中某个节点容易受到攻击，黑客探索安全漏洞、脆弱节点，尝试攻击，实施拒绝服务式攻击。黑客还可能以特定协议服务完成欺骗拦截，组织流量传输，引入恶意操控的新流量，并在交换机内增加流表项。原OpenFlow定义传输层、数据层安全，保障控制层和路由器连接稳定，但其TLS构建的认证加密机制过于复杂，导致TLS易成为供给对象。TLS无法起到理论上对系统的保护作用，此外，还会导致系统受到多方面的攻击。

4 SDN 安全策略

将SDN的控制层及数据层分离，采取集中管理的方式，可以采取全局视图辅助集中决策，使SDN发挥自身的结构优势，集中管理、快速响应，提高网络安全性。

4.1 应用层安全策略

应用层处于SDN最上层，其北向接口和控制器连接，内部有多种应用程序及服务，SDN控制器采取上述集中管理的方式，可以迅速对安全服务进行部署并应用。为进一步减少SDN开发的难度和复杂程序，开发人员将多种网络编程语言应用到其中，开发设计出FRESCO语言。采用该脚本语言，可以帮助开发人员迅速

在控制器及OpenFlow交换机上对新的应用进行开发。除此之外，还有多种其他安全策略。

4.1.1 访问控制

要求应用程序通过对应的访问权限才可以使用网络资源，PermOF为利用OpenFlow实现控制应用程序访问的权限系统，其采用一组权限、隔离机制控制权限。权限分为读写及系统权限，且各权限被划分为多个子类。读取仅限于管理敏感可用信息，写则是让应用程序对控制、交换机状态进行更改，系统权限则是让程序具有资源访问的权利。

4.1.2 程序安全防范

SDN应用程序需实时观测网络变化。设计一种基于断言方式的调试及验证语言，设计人员可以通过高级程序验证控制器属性。采用该调试方式可以在具体程序部署之前发现漏洞。VeriFlow在运行中可以提供流规则检查，故可以设计具有增量数据结构的VeriFlow算法，对动态变化条件属性进行验证。

4.2 控制层安全策略

4.2.1 程序攻击防范

应用程序通过控制层访问网络资源。为了保证控制层的安全，需按照具体程序的功能划分好其权限，实现对恶意程序的准确控制。可以设置一个安全的SDN控制器，添加一个可编程的安全北向API中间构件，实现对特权的分配，程序运行过程中给予交换机应用验证机制，对产生的流规则模块进行全面的验证、分析。也可以利用相互冲突的规则角色的权威性，指定授权角色给交换机应用程序，有效化解角色冲突的问题。还可以通过多种应用及安全的流规则对消息产生限制，或通过引进OpenFlow对应的审计子系统，使系统对发生的和安全有关的事件进行实时跟踪。

4.2.2 DoS、DDoS 攻击防范

对DoS、DDoS的防范，可以在控制层对流行为及交换机的流量统计信息进行分析，减少此类供给的产生，可以在OpenFlow更便捷地获取更多交换机的统计信息。和其他的控制器相比，采取OpenFlow支持的控制器投入成本更少，效果更显著。OpenFlow支持的SDN控制器和各个客户端连接，路由器的数据流较大，且控制器往往受到大负荷的影响。因此，可以研究以分布式的控制层方式，大大提高控制层的处理能力，扩大控制器内存，以此优化其负载。OpenFlow支持使用通配符，可以将客户端发出的请求保存为副本数据。利用通配符的机制，可以优化控制器的负载均衡，也可以完成对目标流量的分布，针对具体流量的分布，调整好负载均衡操作所导致的变化。

4.2.3 设置可靠的控制器

控制器以及拓扑的位置也会影响ADN的扩展性，故应设计最佳的控制器位置。可以采用专业选取算法得到最佳的控制器位置。例如，可以采用模拟退火算法，以这种概率算法的方式选取最佳的控制器位置。为进一步提高控制器的网络适应能力，也可以应用基于图划分的最小割边算法。

4.2.4 控制层和数据层的智能化权衡分析

加强控制器和交换机的智能权衡可以提高控制器的控制效果，中央控制器对所有流的可见性可能会增加控制器的可扩展性负担，故交换机可以使用OpenFlow规则，结合自身运作实际情况进行路由决策，不需要对控制器各个流进行审查。多数微流在数据层实施处理，但管理人员出于管理需要，可以管理、审查相关的各项流量。OpenFlow内单个控制器以链路层发现协议，可以获取交换机的端口连接信息，获取OpenFlow交换机的连接状

态。故障管理方面，控制器可以应用LLDP内监测网络链接，要求控制器参与到LLDP信息监测中，但这样一来避免不了控制器的扩展性受到影响。为了解决这一问题，可以在交换机上配置通用的消息产生和处理功能，充分提高控制器到交换机链路监视操作的管理能力，对OpenFlow协议进行扩展，使其支持监控。

4.3 数据层安全策略

对于数据层的安全策略，需要考虑到的是数据层的各项软件是否安全可靠。若安装了恶意软件，就会导致其修改数据路径上的流规则，从而影响数据层的整体安全性。落实安全机制工作要细化各项工作内容，重视对可能影响流规则的应用的身份验证及授权。可以在数据层加入NOX OpenFlow控制器支持的系统平台，对流规则进行科学检查，在改变流规则之前，就需要给OpenFlow的应用程序授权。该系统平台以数字签名的方式实现角色授权，以扩展的OpenFlow控制器来限制安全。系统平台采用一个规则冲突的检查引擎，调整各项OpenFlow规则冲突的插入请求，从而更好地开展规则插入算法分析。若安全应用程序插入流规则，在OpenFlow网中，该系统平台就会对其他可能产生冲突的流规则进行应用程序限制，禁止插入。

控制器及交换机的连通是否稳定也直接影响网络系统的安全性，要确保控制器和交换机在通信过程中落实冗余连接及快速链路的恢复机制，保障两者的连通性。OpenFlow协议也可以使用连接检测的技术方式，检查交换机和控制器是否连接好，若连接失败，则及时恢复交换机。OpenFlow协议定期给控制器发送消息，若控制器出现故障，OpenFlow协议可以配置备用控制器或临时代替控制器。

5 结语

SDN自身分层结构及便于编程的特点为新时期强化网络管理奠定了坚实基础，但是其集中控制方式及编程简单的特点也为SDN带来一些安全风险。本文对SDN的应用层、控制层及数据层的特点进行分析，总结各层存在的安全问题，并融入现代安全技术，论述了若各层遇到安全威胁、供给后该如何处理。目前SDN的一些安全问题已经基本得到解决，但一些深层次的研究内容及问题还需要技术人员的不懈努力，提出更加合理的解决方案。

参考文献

[1] 孙浩博，王海涛. 软件定义网络的安全解析及其在安防行业中的应用[J]. 中国安防，2021（Z1）：112—118.

[2] 谢珲，聂敏，杨光. 一种基于量子加密的软件定义网络南向安全防护策略[J]. 电讯技术，2020，60（9）：999—1004.

[3] 王世玲，张江，谢敬锐，等. 基于软件定义网络的大型企业安全内网设计[J]. 网络安全技术与应用，2020（7）：18—19.

[4] 李旭阳. 软件定义网络组播安全机制的设计与实现[D]. 北京：北京交通大学，2020.

[5] 左志斌. 基于密码标识的软件定义网络数据面安全关键技术研究[D]. 郑州：战略支援部队信息工程大学，2020.

[6] 聂敏，谢珲，杨光，等. 基于MDP模型决策安全策略的软件定义量子保密网络[J]. 光通信技术，2020，44（9）：1—6.

[7] 白昕硕. 面向SDN数据平面中安全事件检测的关键技术研究[D]. 哈尔滨：哈尔滨工业大学，2019.

[8] 杨涛. 工业软件定义网络环境下DDoS攻击检测方法研究[D]. 重庆：重庆邮电大学，2019.

[9] 刘敏，滕华，何先波. 基于核函数的软件定义网络DDoS实时安全系统[J]. 计算机应用研究，2020，37(3)：843—850.