工程与应用

doi: 10.3969/j.issn.1673-5692.2015.04.016

SDN 安全技术研究

孙 鹏,刘秋研

(中国电子科学研究院,北京 100041)

摘 要: 随着大数据、云计算等互联网新技术的发展,对传统网络的带宽、速率、安全等方面提出了更高的要求,面对日益复杂的网络环境,传统网络在可扩展性、可编程性、灵活性等方面面临瓶颈。软件定义网络 SDN(Software Defined Network)将数据的控制面和转发面分离,向上为应用层提供可编程接口,向下统一管理网络设备,一经提出便成为下一代互联网研究的热门方向。SDN 技术的集中性和开放性也带来新的安全挑战,控制器本身的安全、应用层安全、数据通道安全等目前都缺乏有效的解决方案。本文阐述了 SDN 的优势与特点,面临的安全风险、一些增强安全的方式;然后提出一种基于 SDN 技术抗分布式拒绝服务攻击(DDoS, Distributed Denial of Service)的设计,最后对 SDN 安全问题进行思考和总结。

关键词: 软件定义网络; OpenFlow; 网络安全; 分布式拒绝服务

中图分类号: TP393.02 **文献标识码:** A **文章编号:** 1673-5692(2015)04-416-05

Security Research on Software Defined Network

SUN Peng, LIU Qiu-yan

(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: The development of big data, cloud computing and other new technologies of internet brings higher requirement for bandwidth, speed, and security of traditional network. However, the complexity of network environment blocks the developments of traditional network in different aspects such as programming and flexibility. Software Defined Network (SDN) separates the data control plane, providing programmable interface for the application layer and unified management of network equipment downward. Hence, SDN becomes one of the research directions proposed for the next generation internet. However, the concentration and open of SDN also bring new security challenges. There are few effective solutions for the controller security, application layer security and data security. The advantages and characteristics of SDN are first summarized. Then, the security risk introduced by SDN is analyzed. And a network security design based on SDN is proposed to resist DDoS (Distributed Denial of Service) attack. Finally, an outlook for SDN is concluded.

Key words: Software Defined Network; OpenFlow; network security; DDoS

0 引 言

随着大数据[1]、云计算等互联网新技术的发展,对传统网络的带宽、安全、速率等提出了更高的要求,传统网络在安全性、灵活性、可扩展性等方面面临瓶颈,世界各国都积极投入到下一代互联网体系结构的研制中,SDN 便是其中重要的方向之一。软件定义网络 SDN 通过分离网络设备的控制面与数据面,向上将应用程序接口提供给应用层,从而构

收稿日期: 2015-03-17 修订日期: 2015-07-10

建了开放可编程的网络环境,向下将路由策略下发到路由器,实现网络设备集中管理。它的出现解决了传统网络缺乏统一管理、可编程可扩展能力不足、灵活性不够高、升级缓慢等缺点,使得它一经提出便成为学术界产业界的热点话题。斯坦福、普林斯顿等著名大学投入到软件定义网络有关项目的研究,涉及到网络安全、路由决策、安全策略、虚拟化等领域,谷歌、思科、微软等互联网公司积极推动 SDN 的市场化标准化的发展。SDN 已成为一项可能对当今网络带来翻天覆地变化的热点技术。

作为一个新兴事物,SDN 不可能是尽善尽美的,SDN 控制集中性和开放性也带来了新的安全挑战,作为一种新技术,也为网络安全研究带来新的思路,挑战与机遇并存。一方面,SDN 采用集中式的控制方式,使得控制器成为网络攻击的重点,控制器面临极大的安全风险,控制器和应用层之间的安全(如授权认证、安全隔离)和控制器和转发设备之间的安全(数据通道安全)目前均缺乏有效的解决方案;另一方面,SDN 在流转发、深度包检查、流量重定向等方面具有先天优势,基于 SDN 的网络安全新技术不断涌现。本文首先介绍 SDN 的技术特点,然后介绍 SDN 的安全风险和解决思路,再介绍 SDN 安全技术应用,并提出一种基于 SDN 的抗分布式拒绝服务攻击技术。希望能平滑的引入 SDN 技术,为 SDN 发展做一些有益的贡献。

1　SDN 技术特点和安全挑战

SDN 诞生于美国斯坦福大学 Clean Slate 项目[2],以 Nike MicKeown 教授为首的团队提出 OpenFlow 概念[3-4],其之所以被提出是由于新型网络技术需要在真实网络环境中经受考验,而网络研发者却无法根据实际需要改造网络设备,所以提出将控制功能和转发进行分离的新型架构,将控制功能从网络设备中抽离,使得研发人员能在不修改网络设备的情况下而验证新型的网络架构,控制逻辑从网络设备中分离出来,网络管理员通过编程的方式可以进行网络资源分配,动态网络管理,相比传统网络大大加快了变更网络拓扑、控制网络流量的速度。McKeown 教授在 OpenFlow 的基础上进一步提出 SDN 概念,管理集中性、开放性、可编程性成为 SDN 的三个最主要的特点[5],然而,它就像一把双刃剑,带来了巨大好处便利的同时,也带来了不可低估的安全威胁。

1.1　SDN 的技术特点

SDN 将网路设备的控制面和转发面相互分离[6],如图 1 所示,SDN 逻辑架构图,SDN 向上为应用层提供可编程应用程序接口 API,从而构建了开放可编程的网络环境,向下通过虚拟化技术,实现对网络设备的统一管理和控制。从逻辑架构的角度,可以将 SDN 技术特点归纳为以下三个方面:

集中性。将控制面从交换机中分离出来,以控制器集中控制网络设备,实现全局策略,从而简化了网络设备,通过统一标准的南向接口和虚拟化技术,实现统一管理、控制和维护不同厂家的设备。

可编程性。控制面向上向应用层提供可编程接口 API,网络配置、路与策略、安全策略等都以应用

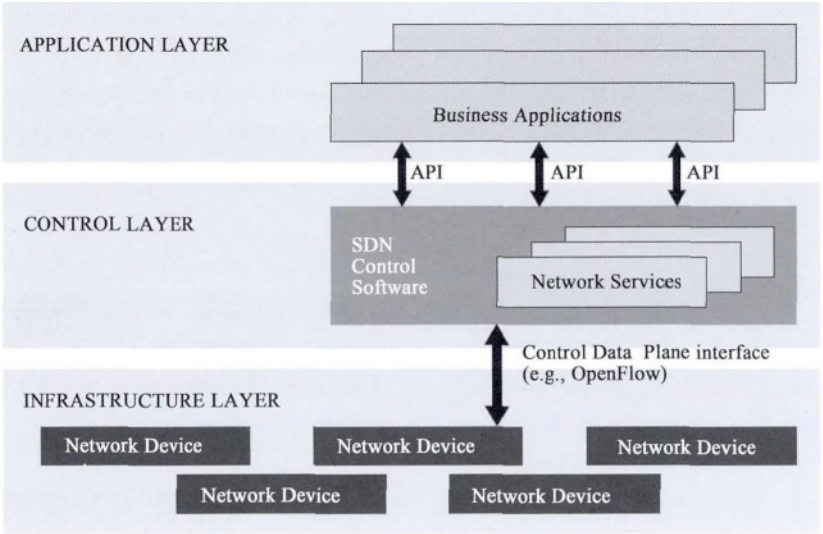

图 1　SDN 逻辑架构

软件的方式部署在控制器，网络配置变得更加的多样化，可以快速的开展各种新型的业务，进行新业务实验。可编程性使得网络变得更加的智能，实现了对网络设备更加灵活的管理，简化业务流程，提高网络灵活性，降低设备要求。

开放性。SDN 是一个开放的平台，现如今流行的几个 SDN 方案均是开源的。SDN 的可编程能力使得用户的个性化业务得到前所未有的支持，为网络开发人员和运营商提供了一个全新的业务开发平台[7]。

1.2 SDN 面临的安全挑战

然而，SDN 管理集中性、可编程性、开放性这些技术特点，虽然带来了很多好处，同时，在安全方面，也带来了新的特有的挑战。

(1) 控制层面挑战。管理集中性使得网络配置、网络服务访问控制、网络安全服务部署等都集中在 SDN 控制器上。攻击者一旦实现对控制器的控制，将造成网络服务的大面积瘫痪，影响控制器覆盖的整个范围。由于 SDN 网络的可编程性、开放性，SDN 控制器安全防护的重要性远大于传统网络中网管系统的安全。所以围绕控制器的攻防是 SDN 自身体系安全中最关键的节点，例如，在 OpenFlow 交换机流表中不存在的初始流信息将通过集中的控制器进行处理，虽然控制器可能并不是某次分布式拒绝服务攻击的直接目标，但大量的初始流量将使控制器的负载急剧上升；攻击者向控制器发送多个服务请求并且所有请求的返回地址都是伪造的直到控制器因过载而拒绝提供服务[8]。

(2) 应用层面的挑战。可编程性使控制器向应用层提供大量的可编程接口，这个层面上可能会带来很多安全威胁。例如向应用层的应用中植入蠕虫木马程序等达到窃取网络信息更改网络配置占用网络资源等目的，从而干扰控制面的正常工作进程影响网络的可靠性和可用性；利用某些接口实现拒绝服务攻击、进行网络窃听等。

(3) 开放性也给 SDN 带来很多安全隐患。安全和网络的应用插件都具备一定的规则写入权限，随着应用的复杂化，多个应用之间会出现安全规则冲突，从而造成网络管理混乱、安全规则被绕过、服务中断等现象；第三方应用或插件可能带有恶意功能、未声明功能、安全漏洞等多种风险[9]。如表 1 所示，综合分析了 SDN 技术特点、优势和安全威胁。

表 1 SDN 技术特点/优势/安全威胁对比

SDN 技术特点/优势/安全威胁	优势	安全威胁
管理集中性	管理方便，运营灵活，简化网络设备，统一、高效的管理和维护。	面临严重安全威胁，是攻击者攻击的重点中的重点，面临认证、授权等欺骗，拒绝服务等攻击。
可编程性	灵活配置，多业务支持易于更新升级，功能更加完善，提高网络运行效率。	可能带来 API 接口滥用，恶意软件，利用某些接口进行网络窃听，拒绝服务攻击等。
开放性	支持个性化定制，支持业务快速创新，易于推广，结构透明，使其成为学术界产业界热点。	第三方应用或插件可能带有恶意功能、安全规则冲突、未声明功能、安全漏洞等多种风险。

1.3 SDN 安全加固的建议

针对 SDN 引入的新安全威胁，相应的防护建议策略包括但不限于以下几个方面：

在控制器层面，在控制器入口处部署流量清洗设备，防止大规模流量攻击造成拒绝服务；使用分布式多控制器方案，当某一台控制器受到攻击或者发生故障，马上自动选择其他控制器代替其功能，使得网络不会因为控制器故障而产生大面积瘫痪；部署安全代理，由于控制策略都是应用程序实现的，对应用程序进行漏洞检测和安全加固，可以在一定程度上缓解控制器安全问题；制定一系列严密的授权、访问控制、安全管理等规则赋予使用者一定的管理权限。

在应用层层面，制定一系列安全准入规则，对应用提供的服务以及需要控制器提供的接口等进行鉴定，负责任的应用才允许成为 SDN 中合法的应用[9]；利用可编程接口针对目前存在的安全威胁，利用已有的技术对安全威胁进行监控和排除；应用软件认证机制，例如自信任管理方法确保交换机的安全。

其他的，设计实现安全服务和网络服务之间、安全服务之间等接口的安全标准；慎重开放 API(Application Programming Interface) 接口，开放之前做好安全分析；设计精巧的算法及优先级政策，以避免安全策略冲突或被绕过。

2 SDN 安全技术及应用

随着 SDN 技术的不断发展，基于 SDN 的技术

不断出现,其中重要一个方向便是将传统网络设备与 SDN 技术结合[9]。

图 2　基于 SDN 增强型网络安全设计示意图

SDN 将网络控制功能转移到专用 SDN 控制器上,由它负责管理和控制虚拟网络和物理网络的所有功能,鉴于 SDN 有这些特点与优势,并将 SDN 技术与传统安全设备有机结合。如图 2 所示,基于 SDN 增强型网络安全设计示意图,利用 SDN 控制调度方面的优势,结合传统安全设备如防火墙、路由器、IDS(Intrusion Detection Systems) 、IPS(Intrusion Prevention System) ,利用 SDN 技术实现更深层次的数据包分析、网络监控和流量控制,基于 SDN 增强型网络安全设计将是今后网络安全研究的一个重要方向。

基于此背景,本文提出一种基于 SDN 技术抵抗 DDoS 的设计。如图 3 所示,由一台 SDN 控制器(可通过编程实现) 、防火墙、交换机、IDS、用户计算机构成。控制器与交换机、防火墙、IDS 通过软件连接。抵抗 DDoS 攻击思路为: 当突发大规模攻击流量由互联网进入防火墙后,触发 IDS 预警,IDS 将报警信号以及攻击特征情况发送给 SDN 控制器,控制器接收报警,下发指令至防火墙,更改防火墙配置,减少攻击流量,同时下发流表更改指令至 OpenFlow 交换机,更改流表匹配项设置,丢弃攻击数据包。

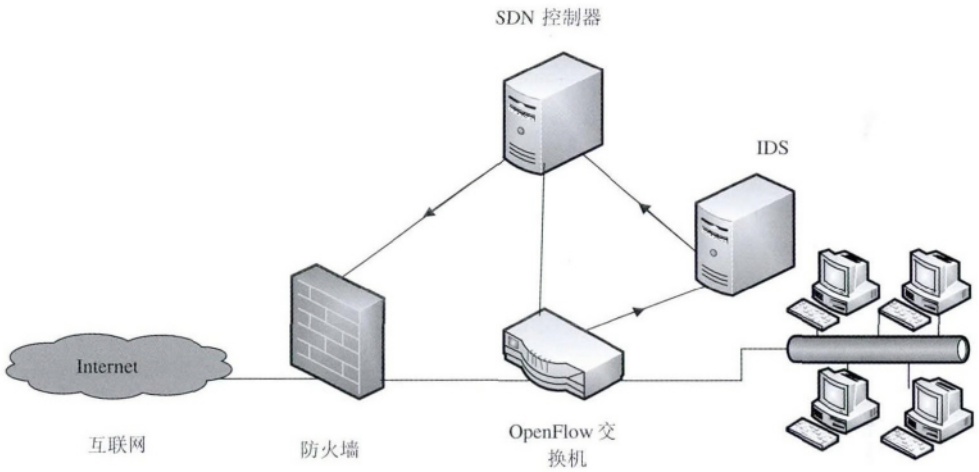

图 3　一种基于 SDN 技术抗 DDoS 的设计

这种将 SDN 技术和传统安全设备结合的技术,相比于传统的网络安全设备,具有很多的优势。首先,网络保护的全面性。传统的安全设备(如防火墙) 都仅部署在两个安全级别不同的网络边界,对同一个安全级别内部的攻击却束手无策; IDS 的预警不能够自动的更改其他安全设备的设置,各个安全设备之间不够协调,没有统一集中的安全策略。SDN 技术与传统的网络安全设备相结合,SDN 控制器通过管理网络设备,具备全局视图能力,可以以此制定全局的路由策略、安全策略,使得各个网络设备可以统一的控制器的管理下协调工作,各个设备相辅相成,使得安全漏洞变得更少。因此,它带来了全面性的安全保护。其次,网络安全是均衡的。众所周知,一个好的网络安全设计不应该出现明显短板。采用 SDN 技术的网络安全设计使得网络中没有明显的缺陷,将安全策略划分为多个等级,每个等级采取不同的安全策略,根据不同的路由策略在不同逻辑等级上实现转发。这样,使得网络安全策略有逻辑、有层次、有条理,不会出现“木桶效应”[10]。因此,它具有均衡性。再次,网络易于升级、维护。传统网络安全设备管理复杂,管理难度大,进行升级耗费周期长,需要厂商的参与。SDN 的集中控制与可编程性,使得这些问题得到解决。可以通过北向开放的 API 接口实现新的网络安全应用,安全策略的变更也仅需在控制器上编程即可,对病毒特征库、攻击特征库进行升级也仅需在控制器上进行,由于所有策略都是在控制器实现,相当于整个网络都升级到最新补丁。另外,如果某一节点出现问题或者被攻陷,SDN 控制器可以马上制定新的路由策略,绕开失效节点。所以,SDN 网络安全设计具备易于升级、易于维护的特性。

我们看到很多 SDN 网络安全设计的优势,这种

方法是对网络安全进行全新的探索。将 SDN 架构和传统的网络安全技术相结合，在 SDN 架构的基础上，将网络安全设备如防火墙、IDS、IPS 等部署在重要的网络位置，用 SDN 技术进行全局管理，使这两种方式相辅相成发挥各自最大效用。随着 SDN 技术的不断发展和网络安全设备功能不断强大，将 SDN 技术和传统网络安全设备相结合，可以让网络安全设备发挥出最大的效用，网络安全将会变得越来越可靠。

3 结 语

本文在现有研究基础上，提出一种基于 SDN 技术抗 DDoS 的设计，下一步工作为优化控制器调度算法，使得各部分协调工作，效率更高。SDN 的引入与发展，给互联网安全形势带来巨大而深刻的变化，既可以给网络安全设计带来新的思路，使网络安全设计更加自动化、全面化，同时自身的安全性面临了不可低估的挑战。本文在梳理 SDN 技术特点与面临的安全挑战，介绍 SDN 在安全方面的应用，提出一种基于 SDN 技术抵抗 DDoS 攻击的方法，以期为 SDN 的发展做出一些有益的探索。

参考文献:

[1] 编辑部. 大数据时代 [J]. 中国电子科学研究院学报，2013，01：31-35.

[2] MCKEOWN N，et al. OpenFlow：Enabling Innovation in Campus Networks [M]. ACM SIGCOMM Computer Communication Review，2008，38(2)：69-74.

[3] CHUNG S，et al. Software Defined Networks [J]. Communicationsns Magazine，IEEE，2013，51(2)：113.

[4] Open Networking Foundation (ONF) White Paper. Software Defined Networking：The New Norm for Networks. 2012.

[5] DAVY M，et al. A Case Expanding Open-flow SDN Developments on University Campus. [EB/OL]. [2013-08-15]. G-ENI report.

[6] 陶冶，张尼，张云勇，王肖梅. SDN 安全防护技术研究 [J]. 电信技术，2014(6).

[7] 袁广翔. 软件定义网络技术发展与应用研究 [J]. 现代电信科技，2013(4).

[8] 王淑玲，李季汉，张云勇等. SDN 架构及安全性研究 [J]. 电信科学，2013(3).

[9] 裘晓峰，赵粮，高腾. VSA 和 SDS：两种 SDN 网络安全架构的研究 [J]. 小型微型计算机系统，2013(10).

[10] 彭阳. 基于 OpenFlow 的网络安全技术研究 [J]. 物联网技术，2013(9).

作者简介

孙 鹏(1990—)，男，四川绵阳人，硕士，主要研究方向为网络安全，软件定义网络；

E-mail：sunpengjet@163.com

刘秋妍(1984—)，女，辽宁大连人，高级工程师，主要研究方向为无线通信组网与干扰和网络安全技术。

《中国电子科学研究院学报》编辑部诚聘审稿专家

为了更进一步完善稿件评审机制，提高稿件的评审质量及评审效率，缩短本刊出版时滞周期，确保具有原创性高质量学术水平的稿件及时发表，本刊编辑部现面向国内外诚聘本学科各领域审稿专家。

诚聘审稿专家的条件如下:

·具有博士学历、副教授及以上技术职称，具有良好的科研道德，处于本学科各研究领域的中青年专家、学者。

·熟悉并了解所从事研究领域国内外最新的研究状况及发展趋势。具有良好的专业英语水平，能熟练使用网络对评审的稿件进行文献的查新、检索。

·近年来在国外重要检索源刊或国内主要核心期刊上发表过数篇以上的学术性论文。

·有意从事兼职审稿工作，具有较高的学术造诣；对稿件的评审能做到认真负责、客观公正；能按本刊稿件评审要求及时返回审稿意见。

有意者请联系我编辑部，电话：68893411。