**Software Engineering and Applications** 软件工程与应用, 2020, 9(1), 1-6
Published Online February 2020 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2020.91001

Hans汉斯

# Review of DDoS Security in Software-Defined Networks

**Zhou Deng, Yangyu Zhang**

College of Software, SiChuan University, Chengdu Sichuan
Email: 15170047205@163.com

Received: Dec. 17th, 2019; accepted: Dec. 30th, 2019; published: Jan. 6th, 2020

## Abstract

**Software-defined network (SDN) provides a new network architecture that provides flexibility, scalability, and additional security. The control plane is separated from the data plane, the forwarding logic is handled by the switch, and the control logic is deployed in the centralized controller. Centralized control of the network can solve many security vulnerabilities and problems, but also brings new problems. This paper firstly introduces the architecture of SDN and the principle and characteristics of DDoS attack, analyzes and summarizes the characteristics of DDoS attack in each layer of SDN, and finally analyzes the existing detection scheme, and proposes the future research direction according to its shortcomings.**

## Keywords

**SDN, DDoS, Network Security**

# 软件定义网络中的DDoS安全研究综述

**邓　宙，张扬玉**

四川大学软件学院，四川　成都
Email: 15170047205@163.com

收稿日期：2019年12月17日；录用日期：2019年12月30日；发布日期：2020年1月6日

## 摘　要

**软件定义网络(SDN)提供了新型的网络体系结构，该体系结构提供了灵活性，可伸缩性和附加的安全性。控制平面和数据平面分离，转发逻辑由交换机处理，而控制逻辑则部署在集中式控制器中。网络的集中控制可以解决许多安全漏洞和问题，同时也带来了新的问题。本文首先介绍了SDN的架构及DDoS攻击原**

文章引用: 邓宙, 张扬玉. 软件定义网络中的 DDoS 安全研究综述[J]. 软件工程与应用, 2020, 9(1): 1-6.
DOI: 10.12677/sea.2020.91001

**理和特征，从SDN本身的结构发生DDoS攻击时的特点进行了分析归纳，最后对现有的防御方案进行了分析，针对其不足提出未来的研究方向。**

## 关键词

**SDN，DDoS，网络安全**



## 1. 引言

软件定义网络(SDN)在学术界和行业中都越来越流行，通过将控制逻辑与转发设备分离，SDN 可以抽象底层基础结构，并为管理员提供虚拟网络层操作系统，以更好地利用和控制其网络。因此，SDN 正在成为数据中心等大规模网络的领先技术，尽管 SDN 为网络带来了各种迷人的功能和巨大的希望，但它也引入了严重的潜在漏洞和威胁性，在 SDN 技术暴露的众所周知的漏洞中，分布式拒绝服务(DDoS)攻击是由集中控制逻辑引起的主要威胁，随着越来越多的企业将其应用程序转移到 SDN，可以肯定的是，SDN 将遭受传统和新型 SDN 专用 DDoS 攻击的热潮。面对这种不可避免的趋势，有必要对 SDN 各层中的 DDoS 攻击进行全面的分析研究。

本文首先对软件定义网络的主要特点和架构以及 OpenFlow 的特点进行了说明，然后指出了 DDoS 的特点以及在 SDN 中发送 DDoS 所体现的特征，并进一步分析并归纳了在 SDN 中防御 DDoS 的典型方法的优劣性，最后对未来的研究方向的趋势做出了展望。

## 2. 软件定义网络定义概述

### 2.1. 软件定义网络

在传统的 IP 网络中，用于协议计算的控制平面与报文数据转发的数据平面同处在同一台设备中，它必须同时操作 5000 多种分布式协议来促使整个网络变得智能化，一旦加入了一种新的网络协议，那么所有的网络设备必须同时做出相应的变化，而实际上，一种新的协议的落实需定义网络(SDN)就应运而生了。

软件定义网络(SDN)的起源最初是在 2006 年由 Clean State 团队作为学术实验开始的，在 2008 年，由 Mckeown 教授正式提出了 SDN 的概念，SDN 作为一种新兴起的网络体系结构[1]，它的控制平面和数据平面是分离的，网络智能和状态在逻辑上是集中地，底层网络基础结构则是从应用程序中抽象出来的[2]，而这样做的好处是使得整个网络根据不断变得流量需求来进行配置和部署，这恰恰是当前网络所不存在的。根据 ONF 的定义，SDN 可分为三层结构，图 1 展示了它的体系结构。

应用层：处于 SDN 体系结构的顶层，为软件开发者提供了开放性可编程的接口，让其可以根据用户的特定需求，进行软件的私有化定制，并且可以让网络管理者通过配置来更灵活地掌控并配置网络。

控制层：SDN 的核心层，它的核心组件是由集中式控制器组成，这些控制器负责管理整个业务流，通过编程来对路由、流、数据包做出转发丢弃决策。

基础设施层：也被称为数据平面，该层主要由交换机和路由器等转发设备组成，按照控制层下发的流的转发策略来对流进行转发。

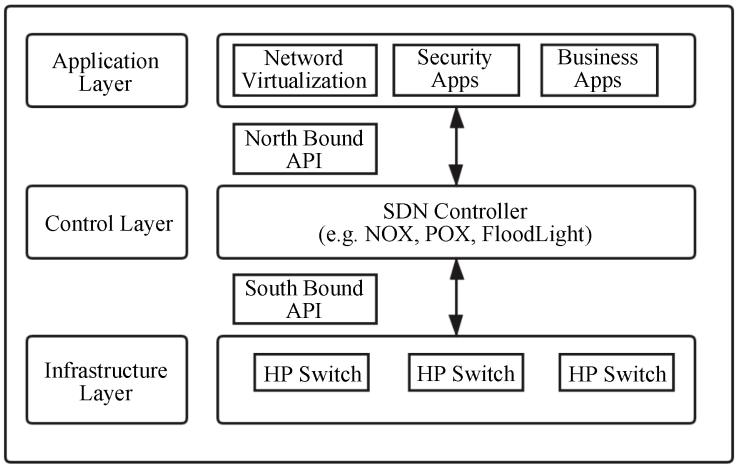


**Figure 1.** Basic SDN architecture
**图 1.** SDN 结构图

### 2.2. OpenFlow

OpenFlow 协议作为一种规范，实现了 SDN 的南向接口[2] [3] [4]。该协议构成的要素有 OpenFlow 控制器、交换机、交换机与控制器之间通道建立的链接，以及交换机中的流表，如图 2 所示。当交换机收的新的数据包时，首先会根据流表的顺序来进行匹配，如果匹配成功，就会执行流操作中的相关动作，如果匹配失败，则将消息(PacketIn)转发到控制器，以查询有关新流的信息。控制平面会制定新的路径转发策略，并向交换机发送消息(PacketOut)，以安装新流程的规则。

## 3. 分布式拒绝服务攻击(DDoS)概述

### 3.1. DDoS 攻击原理

分布式拒绝服务攻击主要是攻击者利用数量较多的恶意用户来伪造大量的虚假请求来发送到受害端，使得受害端的网络或者系统资源被耗尽，从而无法为合法的用户提供正常的网络服务，导致正常用户的体验下降。随着大数据的兴起，互联网的规模日益趋大，出于各种各样的利益目的，DDoS 攻击发生的频率及规模也逐渐变大，并且 DDoS 的目标也不是单一的服务器，如图 2 所示。

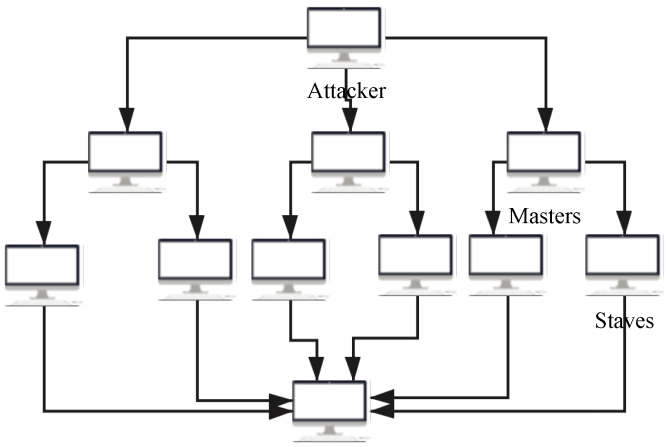


**Figure 2.** Schematic of DDoS attack
**图 2.** DDoS 攻击原理图

### 3.2. DDoS 攻击分类

由于参照的标准不同，DDoS 攻击划分的形式多种多样[5] [6] [7] [8] [9]，本文则是根据带宽消耗和资源消耗来进行划分。

1) 带宽消耗类

这这类攻击的特点是攻击者通常是利用协议的漏洞，然后针对漏洞形成畸形的数据包发送到主机，然后导致主机的 CPU，I/O 等系统资源被耗尽，从而导致其无法提供正常服务。

2) 资源消耗类

这类攻击的重点通常都是利用 TCP，UDP，ICMP 和 DNS 协议数据包而发起的，特点是攻击者向主机在短时间内发送大量的数据包或者是恶意放大流量来耗尽链路的带宽，它可以分为洪泛攻击和放大攻击。洪泛攻击包括 UDPFLOOD 和 ICMPFLOOD 等，而放大攻击包括 DNS 反射攻击。

### 3.3. SDN 中的 DDoS 攻击

#### 3.3.1. OpenFlow 流重载

OpenFlow 交换机的特点是在当收到未知数据包时，会想控制器发送请求信息，来获得新的流匹配规则。但是每个流规则都是有自己严格的生命周期的，一旦超过，则会被另外的流规则所取代。

攻击者恰恰是利用这一特性，生成新的陌生数据包，控制器会为这些新的数据包下发新的流匹配规则，交换机存储流表项的空间有限，这些新的流匹配规则会取代旧的规则，这时，正常的数据包匹配的流规则由于没有空间存储，则会被丢弃。目前，商用的交换机最多可以匹配 2000 个流规则。

#### 3.3.2. OpenFlow 通道拥塞

OpenFlow 交换机内部维护着一个较小的三态内容寻址内存器(TCAM)，在数据包匹配流表规则的时候，一旦没有匹配到，交换机会将数据包的头部作为 Packet-In 消息发送到控制器，并将其剩下一部分存储到 TCAM 中，但是它的空间是有限的，一旦 TCAM 已满，交换机则会把整个数据包都当做 Packet-In 消息发送，由于交换机与控制器之间的安全通道带宽是有限的，最终会导致整个通道拥塞， 这样合法的用户数据也无法获得服务。

#### 3.3.3. 控制器过载

控制器作为 SDN 中的核心，有着集中控制的有点同时也容易造成单点故障，这恰恰是 DDoS 攻击的首选目标。当大量的假流进入网络时，控制器就会收到许多虚假的“Packet-In”消息，控制器的有限资源将会被耗尽，从而导致整体架构性能降低，甚至瘫痪。

## 4. SDN 中的 DDoS 防御

DDoS 对于网络安全的影响越来越大，在 SDN 环境中进行 DDoS 缓解正处于研究和探索阶段，大多数的研究都是在借鉴了传统网络中的检测防御方案的基础上，针对 SDN 的独有特性来进行一系列探索修改。本节就是针对 SDN 中的 DDoS 攻击的防御机制做出介绍分析。

### 4.1. 流表重载防御

Dao 等人提出了一种基于源 IP 过滤的检测方案[10]，该方法选取了源 IP 地址、地址统计计数器、用户平均连接数(k)、最小数据包统计数(n)等 4 个参数作为检测依据，来对正常流量和攻击流量进行一个分类，如果源 IP 地址建立的连接数小于 k，并且每个连接发送的数据包小于 n，那么它就认为该连接为 DDoS 连接，然后控制平面会针对该地址下发丢弃规则策略到交换机。该技术优点在于可以快速的对恶意的流

量进行删除，但是同时可以能容易造成误判让用户丢弃正常的数据。

Xu 等人提出了一种交换机空间智能管理框架，它可以再流表重载之前作出响应[11]。它主要包含三个模块流表的状态收集模块、流预测模块、流删除模块，它的工作原理是流表状态收集模块将在、周期时间 T 获取流表的状态信息，并计算出当前交换机中缓存区的剩余空间，然后流量预测模块预测下一采样周期到达交换机的新流数。如果剩余空间小于预计的数量，则主动流条目删除模块将删除在将来的时期最不可能匹配的流条目，以提供更多的空间来插入新的流条目。另一方面，如果下一周期中新流的预测数量太大，则当流的可能性值超过网络管理员预先设置的阈值时，主动流条目删除模块将评估表溢出的可能性，该框架可以调用某些速率限制策略来防止表溢出的发生，缺陷在于它并没有对其作出响应策略。

### 4.2. OpenFlow 通道防御

Lu Y 等人提出了一种结合 OpenFlow 和 sFlow 的检测方法[12]，该方法流收集模块、异常流量检测模块、清洗模块构成，主要通过 sFlow 的报文收集能力，来减少交换机和控制器之间的报文交互，从而减少带宽。

Gao 等人提出了一种用于 SDN/OpenFlow 网络的独立于协议的防御框架[13]，它主要由 4 个功能模块组成，分别是攻击检测模块、表丢失工程模块、数据包过滤器和流规则管理模块，攻击检测模块会持续的监视网络状态，一旦检测到 DDoS，其他 3 个平时空闲的模块被激活，在 DDoS 发生时表丢失工程模块会安装保护规则将流量分流到邻居交换机，从而减少控制器和受害者交换机之间的带宽。

### 4.3. 控制器防御

Zhang 等人提出了一种多层队列方法(MLFQ)，允许队列动态的扩展和聚合，从而达到网络中的交换机和主机之间强制公平的共享控制器资源[14]，它的基本实现的思路是：当网络中的请求正常时，控制器只利用少数几个队列来进行处理，一旦超过阈值时，就会额外的在维护多个子队列用来处理请求，当请求的数量小于阈值时，临时增加的队列将重新聚合，虽然实验证明了它可以有效的隔离泛滥的请求，但是当攻击的流量太大并且持续时间较长时，它维护起来将会变的很麻烦。

Braga 提出了自组织映射(SOM)一种神经网络机制来控制控制器流量[15]，用来对网络中的流量进行分类。它具有三个模块：流收集模块，特征提取模块和分类器模块。流特征提取模块会从流量中提取每流包的平均数、每流平均比特数、每流平均时长、对流比、单流增长速率等六个特征，然后配合机器学习的方法，进行训练分析最后达到检测效果。实验结果显示该算法的检测效果很好，但是在特征提取和训练学习上面花费较长的时间开销，影响了控制器的处理速率。

## 5. 结语

随着 SDN 应用的发展，SDN 网络的安全问题受到了越来越多的重视，而 DDoS 则是它主要问题之一。本文主要简单介绍了 SDN 及 DDoS 的背景，DDoS 攻击对软件定义网络威胁，最后分析了针对 SDN 结构中的不同的防御方案，讨论了其优劣性。尽管到目前为止，研究学者已经提出了许多防御机制，但是仍然存在一些挑战需要解决，从分析中可以看出在设计 SDN 的安全防御方案时，结合人工智能、深度学习将是未来研究的方向。

## 参考文献

[1] 张朝昆, 崔勇, 唐骞骞, 吴建平. 软件定义网络(SDN)研究进展[J]. 软件学报, 2015, 26(1): 64-72.

[2] 左青云, 陈鸣, 赵广松, 邢长友, 张国敏, 蒋培成. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报, 2013, 24(5): 4-7.

[3] Hu, F., Hao, Q. and Bao, K. (2014) A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation. *IEEE Communications Surveys & Tutorials*, **16**, 2191-2204. https://doi.org/10.1109/COMST.2014.2326417

[4] Jia, Y., Xu, L., Yang, Y. and Zhang, X. (2019) Lightweight Automatic Discovery Protocol for OpenFlow-Based Software Defined Networking. *IEEE Communications Letters*, 1. https://doi.org/10.1109/LCOMM.2019.2956033

[5] 张永铮，肖军，云晓春，王风宇. DDoS 攻击检测和控制方法[J]. 软件学报, 2012, 23(8): 2065-2070.

[6] Zargar, S.T., Joshi, J. and Tipper, D. (2013) A Survey of Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, **15**, 2046-2069. https://doi.org/10.1109/SURV.2013.031413.00127

[7] Khattak, S., Ramay, N.R., Khan, K.R., Syed, A.A. and Khayam, S.A. (2014) A Taxonomy of Botnet Behavior, Detection, and Defense. *IEEE Communications Surveys & Tutorials*, **16**, 898-924. https://doi.org/10.1109/SURV.2013.091213.00134

[8] Sattolo, T.A.V., Macwan, S., Vezina, M.J. and Matrawy, A. (2019) Classifying Poisoning Attacks in Software Defined Networking. *IEEE International Conference on Wireless for Space and Extreme Environments*, Ottawa, 16-18 October 2019, 60-63. https://doi.org/10.1109/WiSEE.2019.8920310

[9] Radivilova, T., Kirichenko, L., Ageiev, D. and Bulakh, V. (2019) Classification Methods of Machine Learning to Detect DDoS Attacks. 10*th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications*, Metz, 18-21 September 2019, 209-210. https://doi.org/10.1109/IDAACS.2019.8924406

[10] Dao, N.-N., Park, J., Park, M. and Cho, S. (2015) A Feasible Method to Combat against DDoS Attack in SDN Network. *International Conference on Information Networking*, Cambodia, 12-14 January 2015, 309-311. https://doi.org/10.1109/ICOIN.2015.7057902

[11] Xu, J., Wang, L., Song, C. and Xu, Z. (2018) Proactive Mitigation to Table-Overflow in Software-Defined Networking. *IEEE Symposium on Computers and Communications*, Natal, 25-28 June 2018, 00719-00725.719-721. https://doi.org/10.1109/ISCC.2018.8538670

[12] Lu, Y. and Wang, M. (2016) An Easy Defense Mechanism against Botnet-Based DDoS Flooding Attack Originated in SDN Environment Using sFlow. *The* 11*th International Conference*, ACM, New York, 412-415. https://doi.org/10.1145/2935663.2935674

[13] Shang, G., Zhe, P., Bin, X., Aiqun, H. and Kui, R. (2017) Flood Defender: Protecting Data and Control Plane Resources under SDN-Aimed DoS Attacks. *IEEE Conference on Computer Communications*, Atlanta, 1-4 May 2017, 1-9. https://doi.org/10.1109/INFOCOM.2017.8057009

[14] Zhang, P., Wang, H., Hu, C. and Lin, C. (2016) On Denial of Service Attacks in Software Defined Networks. *IEEE Network*, **30**, 28-33. https://doi.org/10.1109/MNET.2016.1600109NM

[15] Braga, R., Mota, E. and Passito, A. (2010) Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow. *IEEE Local Computer Network Conference*, Denver, 10-14 October 2010, 408-415. https://doi.org/10.1109/LCN.2010.5735752