西南大學

本科课程论文（设计）

题　目 基于 SDN 的 DDoS 攻击检测与防御方法

学　　院	人工智能学院
专　　业	智能科学与技术
年　　级	2020 级
学　　号	222020335220177
姓　　名	严中圣
课　　程	计算机网络
指 导 教 师	钟明洋
成　　绩	

2023 年 5 月 13 日

基于 SDN 的 DDoS 攻击检测与防御方法

严中圣
西南大学人工智能学院，重庆 400715
zhongshengyanzy@foxmail.com

摘要： DDoS 攻击是网络安全领域中的重要问题之一，而 SDN 技术的出现为 DDoS 攻击的检测和防御提供了新的思路和手段。本文利用 mininet 平台模拟 SDN 架构进行网络流量监测研究，通过 SDN 架构实时监控流量信息的变化，并对 DDoS 攻击做出及时处理，实现了高效的 DDoS 攻击检测和精准的攻击源定位，有效地提高了网络安全防御能力。

1. 引言

分布式拒绝服务攻击 (DDoS) 是一种通过同时向目标网络中发送大量伪造的流量，导致目标网络服务不可用的攻击方式。DDoS 攻击对全球范围内的各种类型的网络造成了严重的威胁，从小型网络到政府和金融机构的大型数据中心都可能成为攻击目标。DDoS 攻击的主要目的是使网络服务不再响应，从而导致网络的瘫痪。这种攻击对于企业和组织而言，可能会带来严重的经济损失和信誉问题。

目前，DDoS 攻击的检测和防御成为网络安全领域的重点研究问题之一。然而，传统的检测和防御方法通常是基于网络流量的规律性和特征的预测和分析，因此难以准确地识别 DDoS 攻击。此外，传统的 DDoS 防御方法往往需要较大的硬件投资和监控系统来检测网络中潜在的压力点，因此具有比较高的成本。

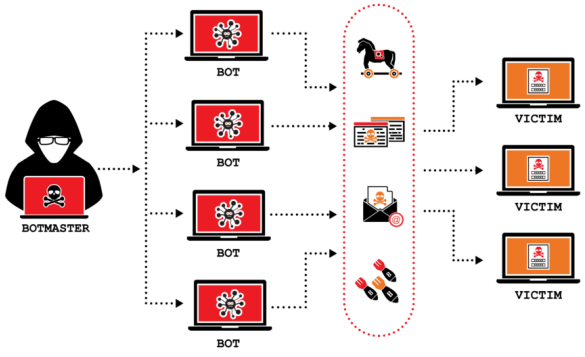


图 1: DDoS 攻击示意图

随着 SDN 技术的不断发展，越来越多的研究者开始探索基于 SDN 的 DDoS 攻击检测与防御方法。使用 SDN 技术进行流量控制和数据包分析，可以更加精细地分析 DDoS 攻击流量，准确地识别攻击源并进行切断，从而降低 DDoS 攻击的威胁。本文利用 mininet 平台模拟 SDN 架构进行网络流量监测研究，通过 SDN 架构实时监控流量信息的变化，深入挖掘网络流量中的潜在威胁，通过检测源地址和流量控制等方式，实现了高效的 DDoS 攻击检测和准确的攻击源定位。

2. 相关介绍

2.1 DDoS 攻击

分布式拒绝服务攻击 (DDoS)，是一种通过网络对系统或服务进行攻击的方式，致使系统或服务无法正常提供服务，或导致系统瘫痪。DDoS 攻击是一种袭击目标系统或服务的方式，它会占用网络带宽、系统资源和网络设备。本文中模拟使用的是 Ping Flood DDoS 攻击，这是一种最常见的 DDoS 攻击方式之一，它利用 ICMP 请求（Ping）向受害者发送大量伪造的网络数据，从而阻止受害者服务器的响应和服务，该攻击方式通常需要大量的机器共同协作实施，因此被称为分布式 Ping Flood 攻击。

Ping Flood DDoS 攻击利用 ping 命令实现，它在网络上广泛使用以检测计算机和网络的通信。Ping Flood 攻击向目标服务器发送大量的 ping 请求，并且在服务器响应时发送更多的请求。随着请求的不断增加，服务器最终无法正常响应请求，无法为合法用户提供服务，并可能导致网络设备和带宽资源被瓶颈。Ping Flood DDoS 攻击通常采用分布式的方式进行，攻击者可以通过控制大量系统和设备，并通过 Botnet 等方式将请求分散到多个主机上，从而增加攻击的规模和强度。

2.2 SDN 架构

SDN(Software Defined Network，软件定义网络) 是一种新兴的网络架构，基于该架构，网络控制平面（control plane）和数据转发平面（data plane）被物理

上分离开来。SDN 中的网络设备只负责数据转发，并通过 OpenFlow 协议将数据转发行为反馈给 SDN 控制器。SDN 架构的核心思想是将网络中的路由器、交换机等设备的数据转发和控制功能分离开来，将网络控制平面集中到一个名为 SDN 控制器的中心化控制器中。SDN 控制器可以通过控制平面接口（如 OpenFlow）管理网络中所有硬件设备，根据 SDN 网络的模型和策略实现数据包的转发和流量控制。

在 SDN 架构下，网络管理人员可以通过 SDN 控制器的相关工具和 API 来对网络进行管理和监控，包括网络拓扑、设备配置、访问控制、流量工程等。SDN 技术可以对网络进行灵活的流量控制和优化，例如实现网络流量的负载均衡，统计网络流量和设备性能指标，优化路由路径等。SDN 架构的优势主要体现在以下几个方面：

- 简化管理：SDN 架构通过集中式控制和管理，简化了网络管理的复杂性，减少了大量的手动配置和管理工作。
- 更灵活的流量控制：SDN 架构中的 SDN 控制器可以动态地管理网络设备的数据转发，可以快速应对网络的变化，例如改变流量的路由路径，对网络拓扑进行调整等，从而避免网络的拥堵和流量泛滥。
- 更好的安全性：SDN 架构的中心化控制器可以对网络设备进行统一的访问控制和审计，通过流量控制和权限管理等手段防止网络中的攻击和威胁。

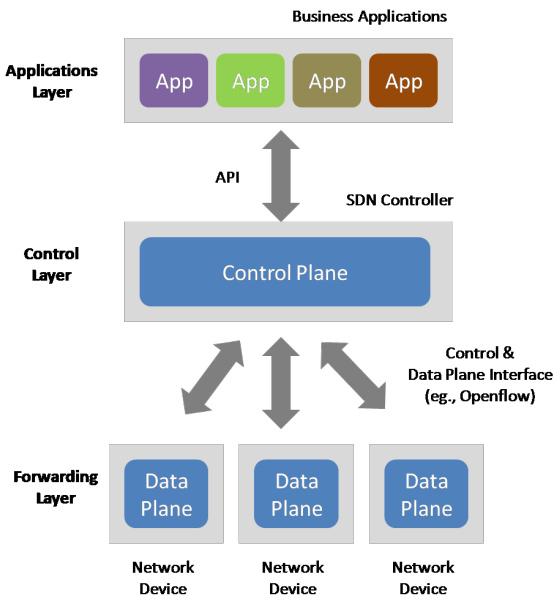


图 2: SDN 架构示意图

总的来说，SDN 架构是一种全新的、灵活的网络控制方式，为网络管理和安全提供了更加高效的方式。

3. 基于 SDN 的 DDoS 攻防模拟实验

3.1 实验环境

为了便利模拟真实环境中的网络操作与架构，本次实验基于 Ubuntu 操作系统下的 mininet 网络仿真 SDN 平台。同时我们采用 ryu 控制器作为 SDN 控制器；利用 postman 进行 API 调试，对流表进行相关操作；利用适用于高速交换网络中的监控软件 sFlow 实时监控在 DDoS 攻击下流量信息的实时变化。具体环境如下：

- CPU: 12th Gen Intel(R) Core(TM) i9-12900K
- OS: Ubuntu 18.04 LTS
- Tools: floodlight 1.2, mininet 2.3.0, Sflow-RT 3.0
- Java 1.8.0, Apache Ant 1.10.13

3.2 实验模拟过程

首先基于 mininet 仿真 SDN 平台搭建网络拓扑，如下图所示：

```
sudo mn --controller=remote, ip=127.0.0.1,
    port=6653 --topo=single, 3
```

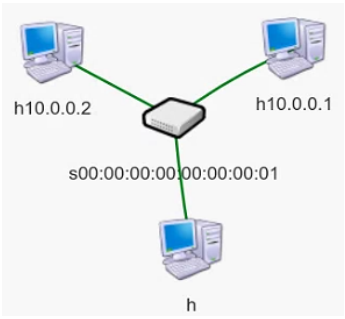


图 3: 拓扑结构网络搭建

3.2.1 DDoS 攻击模拟

首先在虚拟交换机配置 sFlow Agent，以便 sFlow Collector 获取流量信息进行分析和呈现。

```
sudo ovs-vsctl -- --id=@sflow create sflow
    agent=eth0 target=\"127.0.0.1:6343\"
    sampling=10 polling=20 -- -- set bridge
     s1 sflow=@sflow
```

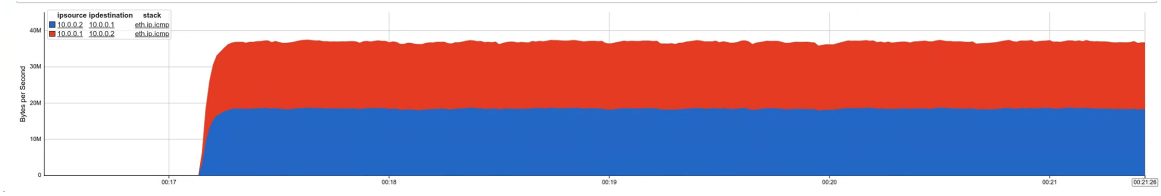
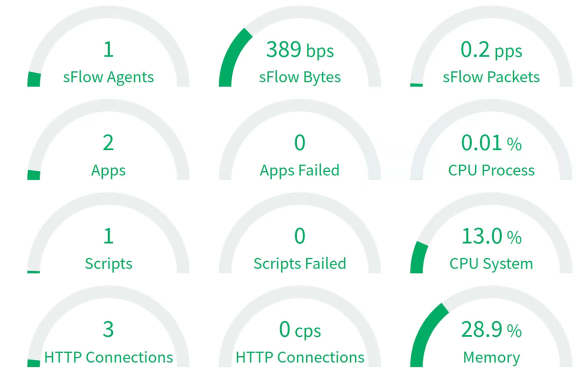
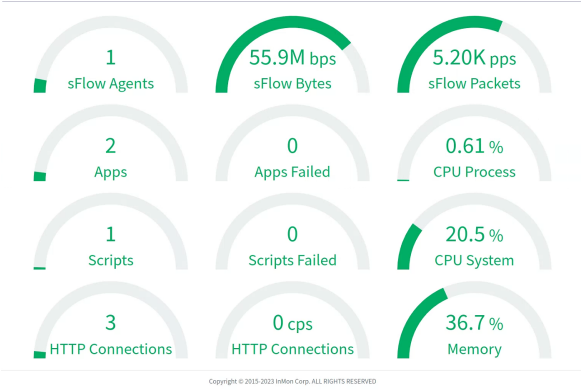


图 4: DDoS 攻击期间交换机流量



(a) DDoS 攻击前流量监测



(b) DDoS 攻击期间流量监测

然后切换到 mininet 控制台窗口，打开 Host1 和 Host2 的终端，并在 Host1 上启动一个 http 服务：

```
mininet> xterm h1 h2
python -m SimpleHTTPServer 80&
```

接下来进行 DDoS 模拟攻击，在 mininet 终端中执行

```
h2 ping -f h1
```

即模拟 h2 对 h1 的 Ping Flood DDoS 攻击。攻击期间流量监测见图 4 与图 5。可以看出当，命令执行后，监测的传输流量剧增，CPU 占用和内存占用也大幅度增加。

3.2.2 DDoS 攻击防御

在监测到流量异常之后，需要利用 RYU 控制器向 OpenFlow 交换机下发流表，抑制攻击流量。流表是交换机进行转发策略控制的核心数据结构。交换机芯片通过查找流表项来决策进入交换机网络的数据包执行适当的处理动作。下发一条流表则好比一条指令，告诉交换机收到数据包之后该做什么。由于先前的 DDoS 采用的 Ping Flood 攻击，因此我们需要下发流表，将攻击流抵消掉。在静态流表下发之后，可以发现流量迅速下降，h2 向 h1 泛洪的数据包被迅速地完全 Drop。

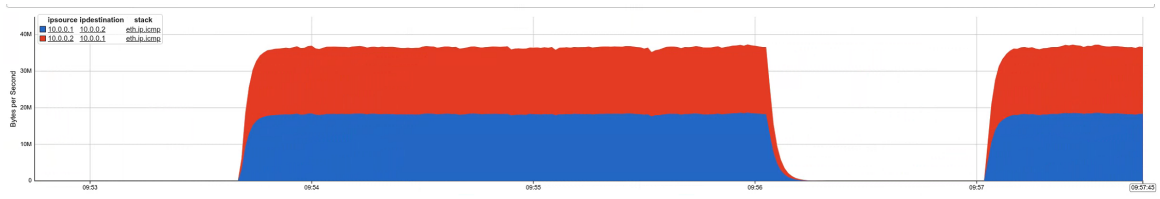


图 5: 下发流表后的流量监控

4. 总结

本文基于 mininet 平台模拟仿真 SDN 架构研究 DDoS 的攻击和防御，为真实网络监控提供一定的借鉴意义。利用 sFlow 来实时监控传输流量信息的变化，并实时显示网络流量以得到更加直观的结果。对于传统网络的部署，是无法做到像 SDN 那样可以实时监控

端口传输流量信息的。利用 SDN 架构的网络拓扑结构，以中央控制的方式部署网络结构相较于传统的网络部署方式更加具有防御性，对抑制 DDoS 攻击更加有效。通过 SDN 技术，我们可以对网络流量进行实时监控与提取分析，并能够及时的对流量进行调整比如 QoS，负载均衡，DDoS 流量过滤等，具有丰富的实践意义。

参考文献

[1] Nunes B A A, Mendonca M, Nguyen X N, et al. A survey of software-defined networking: Past, present, and future of programmable networks[J]. IEEE Communications surveys & tutorials, 2014, 16(3): 1617-1634.

[2] 陈润泽, 杨亚如, 阮方鸣等. 一种基于 SDN 的 DDoS 攻击防御方法 [C], 中国电子学会电磁兼容分会. 第 27 届全国电磁兼容学术会议论文集.[出版者不详],2021:76-80.DOI:10.26914/c.cnkihy.2021.056482.

[3] 钱振勇. 基于 mininet 平台模拟 SDN 架构对 DDoS 的研究 [J]. 电脑与电信,2021(07):60-63.DOI:10.15966/j.cnki.dnydx.2021.07.015.

[4] Bawany N Z, Shamsi J A, Salah K. DDoS attack detection and mitigation using SDN: methods, practices, and solutions[J]. Arabian Journal for Science and Engineering, 2017, 42: 425-441.

[5] Mousavi S M, St-Hilaire M. Early detection of DDoS attacks against SDN controllers[C]//2015 international conference on computing, networking and communications (ICNC). IEEE, 2015: 77-81.