单位代码 **10006**  

课程名称 **高等计算机网络**

分 类 号 **TP311.1**

****

开题报告

基于SDN的DDoS攻击防御实现

|  |  |
| --- | --- |
| 学院名称 | 计算机学院 |
| 团队成员 | 温雅楠SY2006345 |
| 团队成员 | 武仕沛ZY2006357 |
| 团队成员 | 王宇翔ZY2006160 |

2020年 10 月20日

目录

[1 选题背景 3](#_Toc54107357)

[1.1 背景介绍 3](#_Toc54107358)

[1.2 研究目标及意义 3](#_Toc54107359)

[2 相关工具及技术分析 3](#_Toc54107360)

[2.1 SDN网络架构 3](#_Toc54107361)

[2.2 Mininet虚拟组网 3](#_Toc54107362)

[2.3 FloodLight控制器 3](#_Toc54107363)

[2.4 sFlow代理 3](#_Toc54107364)

[2.5 OpenFlow协议 3](#_Toc54107365)

[3 小组成员及分工 3](#_Toc54107366)

[4 参考资料 3](#_Toc54107367)

## 1 选题背景

### 背景介绍

分布式拒绝服务攻击（Distributed Denial of Service）就是利用大量合法的分布式服务器对目标发送请求，从而导致正常合法用户无法获得服务。通俗点讲就是利用网络节点资源如：IDC服务器、个人PC、手机、智能设备、打印机、摄像头等对目标发起大量攻击请求，从而导致服务器拥塞从而无法对外提供正常服务。历史上这种攻击方式已经出现了很多次，导致很多的大型网站都出现了无法访问的情况，这样不仅仅会影响用户的正常使用，同时造成的经济损失也是非常巨大的。

不同于其他恶意篡改数据或劫持类攻击，DDoS简单粗暴，可以达到直接摧毁目标的目的。另外，DDoS的技术要求和发动攻击的成本很低，只需要购买部分服务器权限或控制一批现存网络设备即可，而且攻击速度很快，攻击效果可观。另一方面，DDoS具有攻击易防守难的特征，服务提供商为了保证正常客户的需求需要耗费大量的资源才能和攻击方进行对抗。

下面分别从DDoS攻击和防御两个角度，谈谈目前的抗衡机制是怎样的，通过分析防御一方的不足，进而引出基于SDN的DDoS防御原理、优势和过程。

DDoS按照攻击对象的不同，可分为对网络带宽资源攻击、系统攻击和应用攻击。网络带宽资源攻击，顾名思义即通过占用、消耗目标网络的上下行网络带宽，进而使得正常的网络请求或响应被阻塞在网络环境中。系统攻击，这部分攻击对象主要是特定的网络协议，利用网络协议的工作特点定制攻击方案，如针对TCP的三次握手工作模式，可通过发送大量的“半连接”请求来实现占用目标主机的内存、CPU资源等。应用攻击，这一类攻击往往针对服务器后端应用，通过发送大量的后端服务请求包来达到迅速消耗目标服务器的资源，DNS攻击就属于这一种。

从防御角度来说，本质上都是基于资源较量和规则过滤的智能化系统，常用的防御手段包括资源隔离、用户规则、智能分析和资源对抗。除了最后一种防御手段是通过“硬接”攻击来达到保护服务器外，其余三种都是通过设置过滤规则来进行防范的，只不过是在不同协议栈层次上来进行保护。真实环境下，黑客会混合多种攻击方式，使得DDoS攻击具有难识别、难过滤和高效的特点。另外，网络设施核心部件存在周期长，协议更新缓慢，使得DDoS攻击不用变通就可长期有效。随着网络应用层出不穷，DDoS攻击也变得多元化，难以通过一套通用的规则过滤掉所有的攻击。

然而，SDN的出现有效的解决了传统防御模式下所无法应对的问题。基于控制与转发分离这样的架构，使得网络能够更全面的掌握全局信息，这为分析、排查攻击流提供了基础。另外，通过下发流表来控制网络设备的转发过程，使得应对DDoS攻击更加迅速、便捷。软件定义网络另一个较为核心的功能在于可以动态定制不同设备的处理功能，这使得原本难以变通的协议体系栈变得更加灵活，从而能够从容的应对不同种类的DDoS攻击。

### 研究目标及意义

本实验通过在虚拟网络环境中模拟ICMP泛洪，实现初步的DDoS攻击，通过建立SDN体系架构并配置控制器和下发流表，实现DDoS防御，从而对SDN的工作过程、核心原理有一个完整的认识。后期通过进一步实现更加多元化的DDoS攻击和定制防御机制，以发掘SDN更多的价值潜力。

## 2 相关工具及技术分析

### 2.1 SDN网络架构

### 2.2 Mininet虚拟组网

### 2.3 FloodLight控制器

### 2.4 sFlow代理

### 2.5 OpenFlow协议

## 3 小组成员及分工

## 4 参考资料

[[DDoS 攻击与防御：从原理到实践]](https://blog.csdn.net/wangyiyungw/article/details/80537891)

[[Mininet 安装及可视化操作]](https://blog.csdn.net/AsNeverBefore/article/details/78916645)

[[常用SDN控制器安装部署之Floodlight篇]](https://www.sdnlab.com/2909.html)

[[SDN-LAB实验平台]](https://www.sdnlab.com/experimental-platform/)

[[sFlow流量监控之DDoS防御]](https://www.sdnlab.com/sflow-ddos/)