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。

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。针对不同的待攻击对象，又可按照攻击方式分为诸如ICMP泛洪攻击、UDP泛洪攻击、ACK反射攻击、TCP泛洪攻击、DNS泛查询攻击等。其中ICMP泛洪攻击是最基本也是最能体现DDoS本质的攻击方式，本实验初步计划使用该种攻击方式来构造DDoS攻击。

### 1.2 研究目标及意义

## 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/)