单位代码 **10006**  

课程名称 **高等计算机网络**

分 类 号 **TP311.1**

****

中期报告

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 11 月24日

目录

[1. 研究内容 3](#_Toc57111052)

[2. 已完成工作 3](#_Toc57111053)

[3. 关键技术与难点 4](#_Toc57111054)

[4. 作业分工与进度安排 4](#_Toc57111055)

## 研究内容

分布式拒绝服务攻击（DDoS）通过大量合法分布式节点对服务器发送请求，从而淹没服务器临近链路带宽或耗尽服务器本身计算资源，最终使正常用户无法获得服务器的响应。

由于现行网络本身具有分布式的特点，因此在面对DDoS攻击时，往往难以及时协调一致的进行响应。通常分布式的网络设备是不具备状态的，也很难进行集中管理以记录状态，因此在收到转发包时，直接采取查表的方式进行转发，而不对数据流进行分析，这就给DDoS攻击流留有可乘之机。因此，当网络检测到DDoS攻击时，被攻击服务器临近链路已经被消耗了大量带宽，且服务器也已经收到了大量非法的请求。可见传统的网络在面临该攻击行为时，其反制措施往往有一定后滞性。

传统的采用分布式协议的网络如不能如期对DDoS攻击进行有效的防御，那么便考虑集中控制式的网络模型。因此，本实验采用SDN网络模型，结合mininet搭建起虚拟网络环境，控制器采用FloodLight，控制器和交换机之间采用OpenFlow协议传输报文和下发流控制规则，网络流量监视器采用sFlow进行监控。

本实验的工作可以分为两大部分，一是通过在mininet中搭建虚拟网络环境，并结合FloodLight开发，通过源码级的调试，来测试诸如控制器模块、报文交换模块、链路发现模块、拓扑管理模块和转发模块，进而对控制器有一个全面而详细的认识，并结合网络流量监测工具sFlow对网络流量进行实时监控，通过设置转发规则并查看前后流量变化，从而对SDN网络架构及其工作流程有一个宏观的认识。

另一部分的工作内容在于DDoS的攻防对抗上，正如前文所述，DDoS攻击可分为两大类，一是对服务器临近链路带宽的占用，二是对服务器本身计算资源的耗费。因此，这部分工作重点就在于如何设计攻击流量以达到占用链路带宽和耗尽服务器计算资源的效果，以及设计相应的算法或者逻辑规则，并部署到控制器上，针对这二者攻击，起到良好的防御效果。

## 已完成工作

2.1环境搭建

2.2模块设计与实现

2.3实验设计与结果分析

## 关键技术与难点

3.1 FloodLight核心组件与工作流程

3.2伪造攻击源占用链路带宽

3.3链路带宽占用解决方案

3.4服务器计算资源占用

3.5链路节点请求过滤算法

## 作业分工与进度安排