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](#_Toc54275914)

[1.1背景介绍 3](#_Toc54275915)

[1.2研究目标及意义 3](#_Toc54275916)

[2 研究现状与相关技术分析 3](#_Toc54275917)

[2.1 研究现状 3](#_Toc54275918)

[2.2 相关技术分析 4](#_Toc54275919)

[2.2.1 攻击检测技术 4](#_Toc54275920)

[2.2.2 攻击响应技术 5](#_Toc54275921)

[2.2.3 云计算环境下的DDoS防御技术 6](#_Toc54275922)

[3 技术路线 7](#_Toc54275923)

[3.1 SDN网络架构 7](#_Toc54275924)

[3.2 Mininet虚拟组网 8](#_Toc54275925)

[3.3 FloodLight控制器 9](#_Toc54275926)

[3.4 sFlow代理 10](#_Toc54275927)

[3.5 OpenFlow协议 10](#_Toc54275928)

[3.6 模拟DDoS攻击 10](#_Toc54275929)

[4 小组成员分工及进度安排 12](#_Toc54275930)

[5 参考资料 12](#_Toc54275931)

## 1 选题背景

### 1.1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。

### 1.2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 研究现状与相关技术分析

### 2.1 研究现状

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。

### 2.2 相关技术分析

DDoS 防御一直是网络安全领域的研究热点，但至今仍然缺乏一种方法可以有效地杜绝DDoS 攻击的泛滥和危害。除了 DDoS 攻击隐蔽性的特点，目前整个因特网环境自身结构复杂、管理松散、子网间缺乏有效的合作，从而限制了各种防御机制的实施。从防御的过程来看，大致分为攻击检测和攻击响应 2 个步骤：首先，攻击检测是防范 DDoS 攻击的第一步，其主要任务是发现网络中的 DDoS 攻击，产生报警；其次，攻击响应将采取措施尽快恢复受害者正常工作能力，并进一步追踪溯源 DDoS 攻击的发起者。

#### 2.2.1 攻击检测技术

DDos检测策略主要可以分为源端检测、末端检测、中间网络检测以及混合分布式检测。

（1）源端检测。主要部署在用户本地网络的接入路由器，能够在源端及早地阻止攻击行为。但是这样存在一个问题，就是很多DDos攻击可能在不同区域发起，单一区域的攻击流量没有形成一定规模的话，可能很难被检测到。

（2）末端检测。这个机制运行在服务端，提高了检测精度，同时降低了部署开销，但又引入了处理滞后性的问题。

（3）中间网络检测。折中前两种策略，部署在传输路径中的路由器，建立多点流量检测分析机制，然而其部署成本和通信成本也随之增加。

（4）分布式检测。从集中式单点检测向分布式检测转变，是一种较为有效的方案。然而在构建分布式防御体系的过程中，仍然存在一定问题，例如节点间信任、通信负载等问题。

表2.1 攻击检测技术比较

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **检测机制** | **准确度** | **时效性** | **通信开销** | **部署成本** | **代表方案** |
| 源端检测 | 低 | 高 | 较低 | 较高 | MULTOPS、D-WARD |
| 末端检测 | 高 | 低 | 低 | 低 | IP Traceback、主动检测 |
| 中间网络检测 | 较高 | 较高 | 高 | 高 | 路由报文过滤 |
| 分布式检测 | 高 | 高 | 较高 | 较高 | ACC、StopIt |

#### 2.2.2 攻击响应技术

攻击响应的最基本技术包括报文过滤、速率限制、攻击容忍和攻击溯源 4 个方面。

（1）报文过滤技术针对地址欺骗的 DDoS 攻击，通过检测报文源 IP 地址真实性并过滤源地址欺骗报文进行防御。

（2）速率限制通过抑制可疑攻击流的发送速率，避免大量报文拥塞链路或淹没攻击受害者。

（3）攻击容忍的目的是缓解 DDoS 攻击对目标系统的影响，尽可能地维持系统服务的继续进行，但本身并不能阻止 DDoS 攻击。

（4）攻击溯源的作用是追踪发起 DDoS 攻击的真正攻击者，为攻击响应机制提供真实的攻击源位置及攻击路径信息。

表2.2 攻击响应技术比较

|  |  |  |  |
| --- | --- | --- | --- |
| **攻击响应技术** | **优点** | **缺点** | **代表方案** |
| 报文过滤 | 过滤通过地址欺骗的 DDoS 攻击，保护正常用户流量 | ①无法防御利用真实主机和 IP 地址的攻击；②对检测的精确度依赖较高；③大规模攻击时负载较高 | 分布式报文过滤、路径标识 |
| 速率限制 | 能够避免大量报文拥塞链路，保障攻击情况下的系统正常运行 | ①需要大规模部署；②可能对正常用户造成影响 | Pushback、最大最小公平限流 |
| 攻击容忍 | 尽可能维持系统的正常运行和用户的使用，为反攻措施争取时间 | ①本身不能阻止 DDoS 攻击；②需要大量的系统资源开销以维持服务正常运行 | Honeynet、负载均衡 |
| 攻击溯源 | 追踪攻击的发起者进行主动防御，从根源上抑制攻击产生 | ①需要大规模部署；②需要利用空间有限的报文头信息进行标记；③利用大量路由器存储数据分组信息 | Packet marking、Logging |

#### 2.2.3 云计算环境下的DDoS防御技术

随着云计算技术的应用和发展，针对云环境的DDoS攻击也在显著增长。

很多大型的云服务提供商都针对性地提出了防御产品，例如Amazon CloudWatch、阿里云盾等。主要防御策略是将传统网络中的DDoS攻击防御手段经过适当改进，应用在云计算环境中。然而效果却并不理想。

为满足云环境下的特定应用需求，相关研究提出了云特定的DDoS防御策略。例如：

（1）攻击检测方面，文献[10]利用 Netflow 协议对数据流量进行采集，并通过自我学习的方式进行 DDoS 攻击检测。

（2）文献[11]结合云计算灵活部署和多租户的特性，提出了资源限定条件下的基于虚拟机的 DDoS 系统检测机制。

（3）在攻击响应方面，文献[12]提出了使用 fast-flux 群智网络解决云环境下的 DDoS 攻击，在遭受 DDoS 攻击时，该网络会自动调整结构，从而保证提供高质量的服务。

（4）文献[13]则提出按需安全体系结构，根据云环境下用户的个性化 DDoS 防御需求提供不同的防御服务。

然而云计算领域仍然存在很多隐患和问题没有解决：

（1）现有云平台的按需自助服务使攻击者可以在短时期内构建大规模僵尸网络发动 DDoS 攻击；

（2）云计算保证很多缺乏安全防御的移动设备可以轻松访问云服务，为黑客攻击埋下隐患；

（3）云计算使用“即用即付”计费模型，从而导致攻击者将其对云数据中心的 DDoS 攻击转移至针对使用云服务用户的 EDoS（economicdenial of sustainability attack）攻击。

综上，现有的DDoS防御机制仍存在难以检测，响应不及时，处理不灵活的问题。因此，本项目提出了基于SDN的DDoS防御系统，通过SDN控制器的收集，可以做到全局信息的掌控，达到分布式收集效果的同时，解决了节点间的信任问题，同时极大地降低成本。另外，由于有了网络全局信息，使得算法在分析报文时更加准确，保障了正常用户访问的同时，避免非法报文的入侵。最后，通过软件定义的方式，能够更加灵活的制定过滤规则，使其在应对不同种类的DDoS攻击时更加灵活。

## 3 技术路线

### 3.1 SDN网络架构

软件定义网络（SDN）是一种控制与转发分离并可直接编程的网络架构，利用分层的思想，SDN将数据与控制相分离。在控制层，包括具有逻辑中心化和可编程的控制器，可掌握全局网络信息，方便运营商和科研人员管理配置网络和部署新协议等。在数据层，包括哑的交换机（与传统的二层交换机不同，专指用于转发数据的设备），仅提供简单的数据转发功能，可以快速处理匹配的数据包，适应流量日益增长的需求。两层之间采用开放的统一接口（如OpenFlow等）进行交互。如下图是SDN的体系架构图。

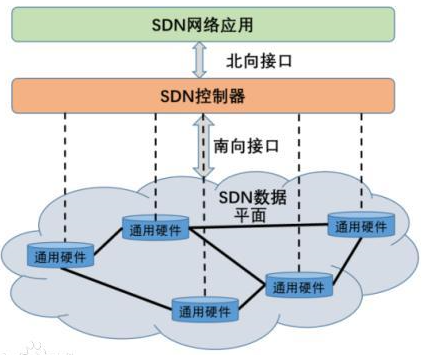


图3.1 SDN体系架构

从上图可以看到自下而上分为三个平面：

1. 数据平面(基础设施层)：数据平面由交换机等网络通用硬件组成，各个网络设备之间通过不同规则形成的SDN数据通路连接。

2. 控制平面(控制层)：这控制平面包含了逻辑上为中心的SDN控制器，它掌握着全局网络信息，负责各种转发规则的控制。

3. 应用平面(应用层)：包含着各种基于SDN的网络应用，用户无需关心底层细节就可以编程、部署新应用。

除了三个平面还有两个接口非常重要：

1. 南向接口(Southbound Interface或D-CPI)：位于数据平面和控制平面之间，具有统一的通信标准，主要负责将控制器中的转发规则下发至转发设备，最主要应用的是OpenFlow协议。

2. 北向接口(Northbound Interface或A-CPI)：位于控制平面与应用平面之间，上层的应用程序通过北向接口获取下层的网络资源，并通过北向接口向下层网络发送数据。没有统一的通信接口，它允许用户根据自身需求定制开发各种网络管理应用

### 3.2 Mininet虚拟组网

Mininet是一个强大的网络仿真平台，通过这个平台可以创建一个包含主机，交换机，控制器和链路的虚拟网络。基于SDN的实验，在真实网络中进行相关的网络实验有一定难度，Mininet采用轻量级的虚拟化技术使得系统可以和真实网络相媲美。Mininet可以很方便地创建一个支持SDN的网络：host就像真实的电脑一样工作，可以使用ssh登录，启动应用程序，程序可以向以太网端口发送数据包，数据包会被交换机、路由器接收并处理。同时，Mininet可以运行在多种操作系统上（windows\linux\Mac OS）,具有很强的系统兼容性。

### 3.3 FloodLight控制器

Floodlight是目前主流的SDN控制器之一，控制器作为SDN网络中的重要组成部分，能集中地灵活控制SDN网络，为核心网络及应用创新提供了良好的扩展平台。

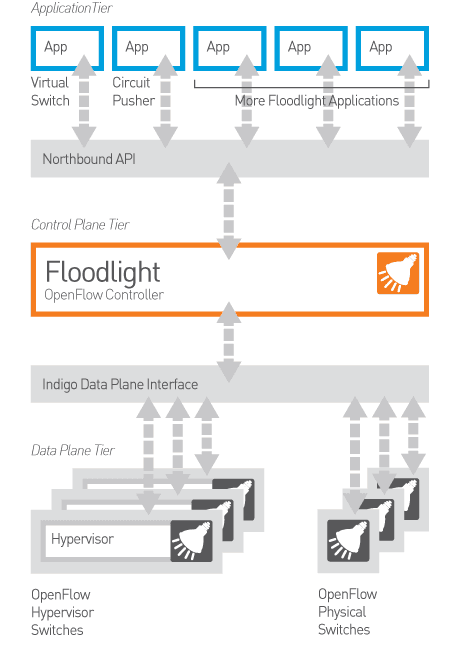


图3.2 Floodlight控制器工作流程

Floodlight控制器还实现了一套控制和查询开放流网络的通用功能，其上的应用实现了不同的功能，以解决网络上不同的用户需求。如下图下图显示floodlight controller、module application以及rest application之间的关系。floodlight controller部分主要有这几个关键模块：模块管理、设备管理、拓扑管理和路由、链路发现。

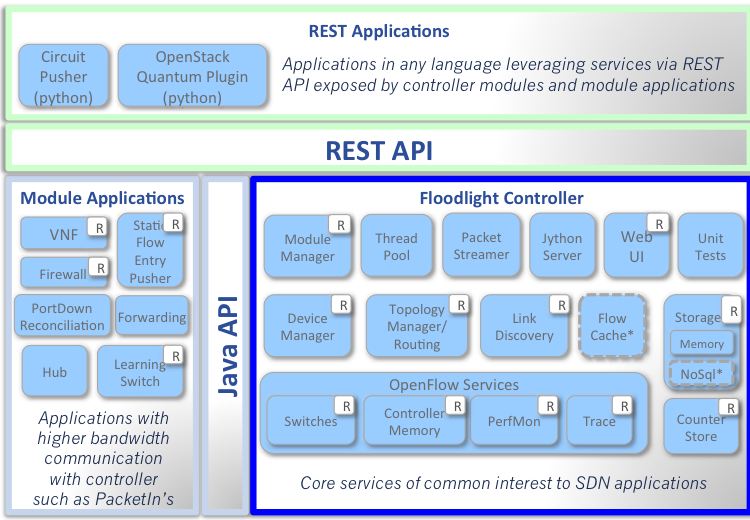


图3.3 Floodlight控制器架构

### 3.4 sFlow代理

sFlow是一种用于监控数据网络上交换机或者路由器流量转发状况的技术。sFlow系统包括若干sFlow Agent（内嵌于交换机或者路由器等转发设备）以及一个核心的sFlow Collector。sFlow Agent通过特定的采样技术获取网络设备上的流量转发统计并实时地通过sFlow数据报文发送到Collector，Collector作为远端服务器，负责对sFlow报文分析、汇总、生成流量报告通，帮助网络管理员有效的获知网络中的流量情况。

### 3.5 OpenFlow协议

OpenFlow是控制器和交换机之间的标准协议，openFlow最基本的特点是基于流（Flow）的概念来匹配转发规则，每一个交换机都维护一个流表（Flow Table），依据流表中的转发规则进行转发，而流表的建立、维护和下发都是由控制器完成的。针对北向接口，应用程序通过北向接口编程来调用所需的各种网络资源，实现对网络的快速配置和部署。东西向接口使控制器具有可扩展性，为负载均衡和性能提升提供了技术保障。

### 3.6 模拟DDoS攻击

主要的DDoS攻击主要包括以下7个攻击方式，通过对其原理进行了解和掌握的前提下，生成相应的DDoS攻击，作为模拟输入。

（1）SYN Flood攻击

SYN- Flood攻击是当前网络上最为常见的DDoS攻击，也是最为经典的拒绝服务攻击，它利用了TCP协议实现上的一个缺陷，通过向网络服务所在端口发送大量 的伪造源地址的攻击报文，就可能造成目标服务器中的半开连接队列被占满，从而阻止其他合法用户进行访问。

（2）ACK Flood攻击

ACK Flood攻击是在TCP连接建立之后，所有的数据传输TCP报文都是带有ACK标志位的，主机在接收到一个带有ACK标志位的数据包的时候，需要检查该 数据包所表示的连接四元组是否存在，如果存在则检查该数据包所表示的状态是否合法，然后再向应用层传递该数据包。如果在检查中发现该数据包不合法，例如该 数据包所指向的目的端口在本机并未开放，则主机操作系统协议栈会回应RST包告诉对方此端口不存在。

（3）UDP Flood攻击

常见的攻击是利用大量UDP小包冲击DNS服务器或Radius认证服务器、流媒体视频服务器。 100k pps的UDP Flood经常将线路上的骨干设备例如防火墙打瘫，造成整个网段的瘫痪。

（4）ICMP Flood攻击

ICMP Flood 的攻击原理和ACK Flood原理类似，属于流量型的攻击方式，也是利用大的流量给服务器带来较大的负载，影响服务器的正常服务。

（5）Connection Flood攻击

利用真实的IP地址向服务器发起大量的连接，并且建立连接之后很长时间不释放，占用服务器的资源，造成服务器服务器上残余连接(WAIT状态)过多，效率降低，甚至资源耗尽，无法响应其他客户所发起的连接。

（6）HTTP Get攻击

这种攻击主要是针对存在ASP、JSP、PHP、CGI等脚本程序，并调用MSSQLServer、MySQLServer、Oracle等数据库的网站系 统而设计的，特征是和服务器建立正常的TCP连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用。

（7）UDP DNS Query Flood攻击

UDP DNS Query Flood攻击采用的方法是向被攻击的服务器发送大量的域名解析请求，域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成DNS服务器解析域名超时。

## 4 小组成员分工及进度安排

|  |  |  |
| --- | --- | --- |
| 成员 | 主要工作 | 备注 |
| 温雅楠 | 虚拟组网配置，sFlow代理配置 | 搭建网络环境，并能对网络设备的数据流进行采集和显示 |
| 武仕沛 | Floodlight控制器配置，配置下发流表 | 将控制器和组网连接，根据不同种类DDoS攻击设置相应规则处理 |
| 王宇翔 | DDoS攻击模拟 | 生成多种有效攻击方式，瘫痪网络 |

10月24日-11月8日：

在虚拟组网环境中搭建起SDN管理控制体系，并实现网络设备的配置和资源监管。

11月9日-11月15日：

基于简单的攻击模型，如ICMP泛洪，实现一个初步的DDoS攻击，通过设置转发规则，完成对此次攻击的防御。

11月16日-实验结束：

考察更多种类的DDoS攻击，分析其攻击原理，特点，并在系统中复现该攻击与防御模型。

## 5 参考资料

[1] <https://blog.csdn.net/wangyiyungw/article/details/80537891>.

[2] <https://blog.csdn.net/AsNeverBefore/article/details/78916645>.

[3] <https://www.sdnlab.com/2909.html>.

[4] <https://www.sdnlab.com/experimental-platform/>.

[5] <https://www.sdnlab.com/sflow-ddos/>.

[6] <http://blog.chinaunix.net/uid-20556054-id-3164909.html>.

[7] 陈飞,毕小红,王晶晶,刘渊.DDoS攻击防御技术发展综述[J].网络与信息安全学报,2017,3(10):16-24.

[8]Mattijs Jonker,Anna Sperotto,Roland van Rijswijk-Deij,Ramin Sadre,Aiko Pras. Measuring the Adoption of DDoS Protection Services[P]. Internet Measurement Conference,2016.

[9]Lukasz Apiecionek, Jacek M.Czerniak, Wojciech T.Dobrosieski. Quality of Services Method as a DDoS Protection Tool. Intelligent Systems 2014 pp 225-234

[10]Elaine Shi, Ion Stoica, David Andersen, Adrian Perrig. OverDoSe: A Generic DDoS Protection Service Using an Overlay Network. 2006-01, CMU-CS-06-114.

[11]RUKAVITSYN A, BORISENKO K, SHOROV A. Self-learningmethod for DDoS detection model in cloud computing[C]//IEEEYoung Researchers in Electrical and Electronic Engineering. 2017:544-547.

[12]WAHAB O A, BENTAHAR J, OTROK H, et al. Optimal loaddistribution for the detection of VM-based DDoS attacks inthe cloud[J]. IEEE Transactions on Services Computing, 1939,(99): 1.

[13]LUA R, YOW K C. Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network[J]. IEEE Network, 2011, 25(4):28-33.

[14]CHEN J, WANG Y, WANG X. On-demand security architecture forcloud computing[J]. Computer, 2012, 45(7): 73-78.