软件定义网络中DDoS的检测与防护

专业班级：J通信工程1402 学生姓名：陆信宇

指导教师：蒋中秋 职称：讲师

摘要

软件定义网络(SDN)是一种新型的网络架构，代表了网络在未来的发展趋势。与传统网络相比，SDN的数据控制平面分离，并且网络可编程，这使得SDN架构下的网络变得更加灵活可控。Distributed Denial of Service(DDoS)，分布式拒绝服务攻击一直都是网络安全领域中难以攻克的问题之一。本文对基于SDN网络的DDoS攻击的检测与防护进行研究。

首先，本文分析了相比于传统网络，SDN网络的优势以及存在的问题，在宏观上建立SDN网络的架构模型。其次阐述DDoS的不同攻击方式以及相应的流量特征。然后基于此流量特征提出一种基于流量监控的源IP攻击检测与防护方案。最后基于此方案设计仿真实验验证方案可行性。

实验结果表明：该方案能够基于不同的业务流量特征，通过修改流量阈值等参数，动态灵活的检测DDoS攻击并且做出相应的防护措施。

关键词：软件定义网络 SDN OpenFlow DDoS 分布式拒绝服务攻击 攻击检测 攻击防护

Detection and Protection of DDoS in Software-defined Networks

Abstract

Software-defined network (SDN) is a new type of network architecture that represents the future development of the network. Compared with the traditional network, the SDN's data control plane is separated and the network is programmable. This makes the network under the SDN architecture more flexible and controllable. Distributed Denial of Service (DDoS), Distributed Denial of Service (DDoS) attacks have always been one of the most difficult problems to overcome in the field of network security. This paper studies the detection and protection of DDoS attacks based on SDN networks.

First of all, this paper analyzes the advantages and existing problems of the SDN network compared with the traditional network, and establishes the architecture model of the SDN network on a macro level. Secondly, the different attack methods of DDoS and the corresponding traffic characteristics are described. Then based on this traffic characteristics, a source IP attack detection and protection scheme based on traffic monitoring is proposed. Finally, based on this scheme, the simulation experiment is designed to verify the feasibility of the scheme.

Experimental results show that this scheme can dynamically detect DDoS attacks and make corresponding protection measures by modifying parameters such as traffic threshold based on different service traffic characteristics.

Key words：Software-defined network SDN OpenFlow DDoS Distributed Denial of Service detection protection

1. 绪论
   1. 课题研究背景与研究现状

在传统的网络架构中，数据平面和控制平面是紧耦合的，分布式的。扁平状的网络架构使得网络的控制节点分布在每一台网络设备(路由器/交换机)中。尽管如OSPF、EIGRP等动态路由协议可以动态学习路由，减少了手工配置转发规则的配置量，但这样的动态学习其实是不可控的。随着网络规模的扩大，网络的管理和维护将变得越来越困难，代价也越发的高昂。而且网络遇到变动或者遭到攻击的时候，不能快速感知并及时作出调整，以至于收敛时间过长而导致网络服务中断。

可编程能力弱则是传统网络的另一缺陷。尽管如Cisco、华为等网络设备供应商都提供了一套独立且功能丰富的接口来满足当前网络的需要，但随着网络功能需求的增长，这样的模式已经使得网络变得越来越臃肿，难以灵活管理。而且新协议的开发需要时间，这就导致网络功能的扩展受了到极大限制。

软件定义网络(SDN)的出现和发展，在某种程度上解决了上述传统网络的问题。与传统网络相比，SDN的数据平面和控制平面是分离的。控制平面从传统的网络设备中剥离出来，集成到可以纵观全网的控制器。这种控制平面集中的模式，能够更加灵活的调度网络流量。SDN的可编程性使得网络功能能够得到快速部署，极大的提高了网络的可扩展能力。

尽管与传统网络相比，SDN有着巨大的优势，但是SDN本身也存在一定的问题。例如SDN控制器的接口还未标准化，这就导致各大控制器厂商之间的设备不能很好的兼容。控制平面集中导致单点问题严重，如果控制器被打死，那么整个网络将陷入瘫痪，这也导致控制器成为DDoS攻击的主要目标。SDN的受攻击平面广，SDN的三层架构(应用层，控制层，数据层)中任何一层都有遭受DDoS攻击的可能。

无论是在传统网络中还是SDN网络中，安全问题一直都是研究的热点。其中分布式拒绝服务(DDoS)攻击则是最严重的的安全威胁之一。随着云计算技术的不断发展，DDoS破坏性也呈几何级增长。内容分发网络(CDN)提供商Akamai调查发现DDoS攻击的年增长率高达125%。

在传统网络中，根据攻击的TCP/IP层次不同，DDoS攻击主要有两种类型，分别是以网络为中心的DDoS攻击和应用层为中心的DDoS攻击。以网络为中心的DDoS攻击主要目标是网络设备和带宽，通过海量的垃圾数据打满目标带宽，导致正常流量堵塞，达到使目标对外提供的服务中断的目的。以应用层为中心的攻击主要目标是目标服务器，通过不断的发送垃圾请求来消耗服务器的资源，导致服务器对外提供的服务性能受到巨大影响。

而在SDN网络中，攻击者可以针对SDN的三个不同层面进行攻击。针对控制层的攻击有攻击时间短，流量大的特点，在短时间内使控制器失效，从而导致控制器控制的网络区域瘫痪。针对数据层的攻击有流量低，持续时间长，难以检测区分等特点，攻击者往往控制傀儡主机伪装成合法用户，使用低速的流量慢慢消耗目标主机资源。

* 1. 课题研究意义

SDN自从2009年被提出以来，短短10年不到的时间，就迅速得到业界的认可，即使是Cisco这样的传统网络设备供应商中的佼佼者也不得不去拥抱SDN。国内外的芯片厂商也推出了支持OpenFlow的芯片。使得SDN商业化得到了积极推进。随着时代向智能化的方向发展，全球接入互联网的设备急剧增多，传统的网络架构已经很难适应当前的网络需求。随着国内各大企业的业务逐渐向云上迁移，对于SDN的研究和完善必然会如火如荼的进行。

虽然SDN得到了众多IT企业巨头的青睐，几乎代表了网络未来发展的趋势，但是SDN的安全体系还处于初级阶段，对于DDoS这种老牌的攻击手段还没有一个很完善的解决方案。各大云计算厂商所采取的解决方案主要有路由黑洞和流量清洗两种，然而都是治标不治本，前者会误杀正常流量，后者的代价又过于高昂。所以，如何在SDN网络中有效的抑制DDoS攻击是网络安全领域的一个重点研究课题。

本次毕业设计的重点有两个方面，分别是SDN这种新型的网络架构思想以及在这种新型网络架构中的DDoS攻击的检测和防护。通过开发DDoS监控程序，部署在SDN网络中，能够根据不同类型的DDoS攻击，实时的监控并分析异常流量，并将分析的结果以web页面的方式呈现出来。程序主体使用Python编写，用户可以在页面中查看当前网络中的实时流量情况，可根据业务情况动态调整报警阈值。

* 1. 论文的结构安排

论文主要章节内容安排如下：

第1章：绪论，分析介绍SDN网络中DDoS攻击的国内外研究现状以及研究的意义。

第2章：分析介绍SDN网络架构，归纳总结DDoS的不同攻击方式以及现有的检测和防护方案。

第3章：介绍基于流量监控的源IP攻击检测与防护方案，给出算法流程图与分析过程。

第4章：仿真实验，简要介绍实验过程中使用到的工具软件，详细分析基本的仿真环境搭建、代码实现以及最终的实验结果。

第5章：总结全文，并提出未来可研究的方向。

* 1. 论文符号规定

1. 软件定义网络(SDN)与DDoS攻击
   1. 软件定义网络

软件定义网络(SDN)最早诞生于斯坦福大学的Clean Slate课题。相比于传统网络，主要有两个方面的改进，一是网络的数据平面和控制平面分离，二是网络可编程。通过控制器的集中控制和网络可编程，可以大大提高网络功能部署的灵活性。本节主要介绍SDN的模型架构以及相比传统网络，SDN的优势。

* + 1. SDN的模型架构

SDN的基本模型架构如图2.1所示。从上到下共有三层，分别是业务层(应用层)、控制层、转发层(基础设施层)。







业务应用

业务层

API API API



网络服务

SDN Controller

控制层

控制—转发通信接口

网络设备

网络设备

网络设备

网络设备

网络设备

转发层

图2.1 SDN基本架构

1. 业务层：业务层也称应用层，不同的业务通过控制层提供的北向API与控制层进行通信，从而使得网络管理人员能够根据所管理的网络的需要灵活的控制网络流量。在传统网络中，由于网络功能都是由网络设备供应商进行开发并集成到各自的网络设备中的，所以在传统网络中，网络功能的可扩展性很差，成本高。而在SDN中，由于控制层提供了足够的API供开发调用，使得网络功能的扩展变得十分方便。而且由于这些API是与平台无关的，并不依赖于特定的硬件设备，所以网络功能的可移植性很高，大大推进了计算机网络的发展。
2. 控制层：控制层在逻辑上集中，是SDN的核心组成部分。SDN的核心之一就是控制平面与数据平面解耦。在传统网络中，其实控制层和数据层已经是分离的，但是在物理上两者依然是封装在一个硬件设备中，这就导致网络扩展变得很不方便。在SDN中，控制层面从转发设备中完全或者部分抽取出来，在远端单独部署，使得控制层与数据层分离，网络结构更加清晰。另外，SDN网络中，底层转发设备(路由器、交换机)不需要关心邻居是谁，不需要通过OSPF等动态路由协议建立邻居关系，它们仅仅具有数据转发功能，转发行为由远端的控制器通过下发流表进行控制。控制层通过控制—转发通信接口(南向接口，主要是OpenFlow)与底层网络硬件转发设备通信，通过北向API与上层应用进行通信，目前主流的控制器：Cisco等传统网络设备供应商联合开发的开源控制器OpenDayLight、ONF主导的开源控制器ONOS、斯坦福大学提出的第一款控制器NOX以及其Python重写的衍生版POX、FloodLight、Ryu、Beacon等。
3. 转发层：转发层也叫基础设施层。是SDN三层结构的最底层，由具有转发功能的硬件或者软件组成。该层的设备仅仅具有转发功能，不需要理解网络通信协议。转发层设备根据控制器下发的流表规则处理数据流。
   * 1. SDN的优势
4. 数据控制平面分离：控制平面拥有全网的拓扑信息以及设备状态信息，可以灵活控制网络流量。
5. 网络可编程：随着网络规模的扩大，网络功能的不断完善，企业业务逻辑也变得更加复杂多样，频繁的业务变动使得传统网络越来越难以满足企业需求，SDN开放的控制平面屏蔽了底层转发设备的差异，可以灵活智能的部署网络应用。
   1. 分布式拒绝服务攻击

分布式拒绝服务攻击是当前网络安全领域中比较突出的问题。攻击者通过病毒程序感染控制大量主机。被感染的主机称为僵尸主机，由僵尸主机组成的网络称为僵尸网络。然后由攻击者发送攻击指令，被控制的僵尸主机向被攻击的服务器发送大量非法请求，从而达到消耗目标服务器资源，使得目标所提供的服务中断的目的。

* + 1. DDoS的攻击类型

由于DDoS攻击的目的是消耗目标资源，中断目标提供的服务，所以根据攻击消耗的资源类型可以将攻击分为以下几种类型

1. 带宽资源消耗型攻击：该攻击的目的是打满目标主机的带宽，使得目标主机带宽资源耗尽，无法对外提供正常服务。通常有直接攻击和反射型攻击两种。直接攻击是攻击者控制大量僵尸主机对目标直接发起大流量攻击，利用带宽资源的不对等，耗尽目标带宽，但是此种攻击不易隐藏攻击源。反射攻击是攻击者伪装成被攻击服务器的IP，向网络中的路由器、DNS服务器等设备发送大量请求数据，当这些设备收到请求数据时，会将响应数据发送给被攻击的服务器，使得被攻击服务器被大量响应数据淹没，服务中断。反射型攻击相比直接攻击，不但能够隐藏攻击者的真实地址，还能够对攻击流量进行放大，因为响应数据通常要比请求数据大的多，所以攻击者只需要发送少量的请求流量，就可以让被攻击者遭到巨大响应流量的攻击。
2. 系统资源消耗型攻击：该攻击的目的是打满目标主机的系统资源，包括CPU、内存、磁盘IO等。比较常见的系统资源消耗型攻击是SYN FLOOD攻击。正常情况下客户端向服务端发送SYN包，客户端进入SYN\_SEND状态；服务端收到客户端的SYN包后，会回复一个SYN+ACK包，同时进入SYN\_RECV状态；客户端收到服务端的回复后，向服务端发送ACK报文确认，客户端服务端都进入ESTABLISHED状态，至此正常连接建立完成。在SYN FLOOD攻击中，攻击者控制大量僵尸主机在短时间内向服务器发送大量SYN包请求建立TCP连接，而服务器能够维护的连接数是有限的，这就导致正常的请求连接无法建立。
3. 应用服务资源消耗型攻击：该攻击利用服务器处理请求能力有上限，通过发送需要消耗大量资源的请求来耗尽服务器资源，从而达到中断服务的目的。例如攻击者控制大量僵尸主机向被攻击服务器发送大量数据查询的报文，服务器每处理一个查询请求，就需要对后台数据库做一次查找，当大量的垃圾请求占满数据库资源时，将导致后台数据库宕机。
   * 1. DDoS的危害性

随着IT行业的发展，资源性能的不断提供，尤其是云计算时代的到来，使得DDoS攻击变得更加凶猛，危害更大。在公有云中，攻击者可以在短时间内创建出庞大的高资源僵尸网络，对攻击对象发起超大流量的DDoS攻击，对企业生产造成巨大破坏。就连技术实力雄厚的GitHub，也遭到了有史以来最严重的DDoS攻击，峰值流量达到了1.35Tbps。

* + 1. 现有的检测和防护方案

由于DDoS攻击的巨大破坏性，业界已经提出了很多检测与防护的解决方案。

论文[]根据流包数中位值、流字节数中位值、对流比、端口增速、源IP增速在内的5个流量特征，采用优化的KNN算法对所选的流量特征进行异常检测，识别率较高，误报率较低。

论文[]提出基于熵值算法的DDoS检测方法。在SDN的控制层使用该算法判断攻击，在转发层处理流表，结合ACL和流量管理，使用OpenFlow协议实现策略，提高了检测率，降低了误报率，能够快速响应。

论文[]采用SDN+BGP FLOWSPEC技术，精确控制丢弃异常攻击流量，保护正常流量正常转发，而且成本低廉，性能高。

* 1. 小结

1. 基于流量监控的源IP攻击检测与防护方案
   1. 方案模型

方案模型如图3.1所示。

转发层

检测层

物理层

流量转发

流量过滤

流量特征分析

流量阈值检测

网络接口

流量方向

图3.1 检测防护方案模型

本方案分为三个层次，共有三个核心模块，分别是流量阈值检测模块、流量特征分析模块和流量过滤模块。数据流进入网络接口，经过流量阈值检测模块，出现异常流量则进入流量特征分析模块，再通过流量过滤模块过滤异常流量，最后转发正常流量。

* + 1. 流量阈值检测模块

该模块主要用于流量检测，即实时监测每个OpenFlow交换机的接口流量。流量参数包括入接口字节速率(单位KB/s)、出接口字节速率(单位KB/s)，入接口包速率(pkgs/s)，出接口包速率(pkgs/s)。之所以包含包速率作为流量参数是因为DDoS攻击中可能存在数据包长度很小但是数据很多的情况。正常情况下，交换机接口的流量应该处于稳定状态，当遇到大规模DDoS攻击的时候，交换机接口流量将趋于饱和。

流量阈值可以自行设定，设定的阈值应该高于流量高峰期时的数值，避免由于误判而导致流量误杀。当接口流量大于设定阈值时，则初步判断可能遭到DDoS攻击，然后立刻进入流量特征分析模块进行流量特征分析。

* + 1. 流量特征分析模块

当流量阈值检测模块检测到异常流量时，将会进入该模块。该模块会启动抓包程序，通过抓取流经异常流量接口的指定数量的数据包，记录下抓包时间，分析包括源IP地址、目的IP地址、源端口、目的端口、数据包长度以及它们相应的统计数据，统计数据以源IP地址为键，其它元素为值，以键值对的形式保存。保证所存的数据中包含出现的所有源IP地址以及其对应的每一个目的IP地址、源端口、目的端口、数据包长度。统计数据数据结构如下：

{

sip1 : {

counts : xxx,

length : [length1, length2, length3,…],

dip : [dip1, dip2, dip3,…],

sports : [sport1, sport2, sport3,…],

dports : [dport1, dport2, dport3,…]

}

sip2 : {

…

}

}

根据统计数据，就可以判断DDoS攻击流量的源地址是否是随机生成的。

首先判断是否是随机源IP地址的DDoS攻击。众所周知，ipv4地址的数量有42亿之多，当攻击者利用随机生成的IP地址进行攻击的时候，IP地址的重复率会很低，同时源IP地址出现次数的平均值也会很低。由于抓取的数据包个数恒定，所以只要不同源IP地址个数占总的数据包个数的比例超过指定阈值，并且源IP地址出现次数的平均值低于指定阈值，则可判断正在遭受随机源IP的DDoS攻击。

如果不是随机源IP的DDoS攻击，则需要根据其它参数进行判断是否是固定源IP的DDoS攻击。针对每个源IP地址所需参数如下：

1. 数据包平均长度

数据包平均长度指的是相同源IP地址的数据包的平均大小。如果数据包平均长度低于或者高于正常阈值，则可判断该源IP为异常IP。

1. 目的IP变化速率

目的IP变化速率指的是相同源IP地址的数据包，每秒出现的目的IP地址(去重之后)数量。如果该参数高于正常阈值，则可判断该源IP为异常IP。

1. 目的IP最大速率

目的IP最大速率指的是

1. 源端口变化速率
2. 源端口最大速率
3. 目的端口变化速率
4. 目的端口最大速率

由于所抓取的数据包个数恒定，所以可以根据源IP地址出现的次数以及其对应元素出现的次数来计算出相应的变化速率，如果超出阈值，则判断为异常流量。最终筛选出异常流量交给流量过滤模块进行过滤。

* + 1. 流量过滤模块

流量过滤模块接收来自流量特征分析模块的流量。根据DDoS的攻击方式，有两种过滤方式

* 1. 流程分析
     1. 流程图

1. 仿真实验
   1. 仿真环境与工具介绍
      1. mininet仿真工具
      2. OpenDayLight控制器
      3. VMware虚拟机
      4. sflow网络监测工具
      5. Python开发环境
      6. Java开发环境
      7. hping3
   2. 环境搭建
   3. 仿真过程
   4. 仿真结果
   5. 代码分析
      1. 创建拓扑
2. 总结与展望