DDoS in Lab 开题报告

刘德欣，马赢超，张煌昭，张一舟，张元玮

摘要—DDoS（分布式拒绝服务）作为一种网络攻击手段，其特点是原理简单，攻击方式较为简单，但难以防御，一旦成功后果往往十分严重。近年来如何有效地防御和进行 DDoS 攻击，已经成为网络安全领域的重要问题。本次大作业，将在情况较为简单的实验室环境下，对常见的 DDoS 攻击进行实现和防御，并在此基础之上，结合较新的工具和研究，尝试使用混合 DDoS 进行攻击并对其进行防御。实验在局域网实验室环境下进行，组员分作相互独立的两部分，分别扮演防御方和攻击方，对一网络服务器进行防御和 DDoS 攻击。通过本次实验，期望可以通过 DDoS 作为切入点，对于网络安全、分布式开发以及工业级工程实现进行较为深入的探究。

I. 小组成员

本次大作业小组，“起飞”（“Taking-Off”）小组，的成员包括（以下按姓名字母序排序）：刘德欣，马赢超，张煌昭，张一舟，张元玮。其中张一舟为小组组长。小组成员信息见脚注，GitHub 组见 TakingOffPKU[1]。

本次大作业所有源代码，将实时同步更新于 GitHub 开源平台[2]。本次报告使用 Overeaf L^AT_EX 在线平台编写[3]。

II. DDoS 原理

DDoS 攻击近几年在世界范围内频繁发生。最近也是规模最大的一次 DDoS 攻击，发生于 2018 年 3 月 1 日凌晨 1 时 15 分，黑客攻击者利用 MemCached 漏洞对世界最大的开源项目平台之一 GitHub 发起 DRDoS 攻击，峰值流量达到 1.35Tbps。为了对 DDoS 有一些较为具体的理解，本小组对其进行了一些调研。

下面将对 DoS 攻击（第II-A节），DDoS 攻击（第II-B节）及 DDoS 防御（第II-C节）的基本原理进行详细的说明。

A. DoS 原理

DoS（Denial of Service，拒绝服务）攻击，是一种简单的，易于实现的，但破坏力很强的网络攻击方式。其基本思想为使用暴力手段或利用网络协议的漏洞，强占网络服务器资源，从而使得网络服务器无法提供正常的网络服务，甚至是宕机。

网络服务器一般而言，会提供正常设计下的正常用户所需的资源以及其备份资源。而 DoS 攻击一般则会在攻击者主机发送大量无意义的请求，从而这些请求一旦获取了服务器资源（比如获取了服务器的 TCP 连接，或占用了服务器的网络带宽）就会使得资源被无意义地耗用。然而由于 DoS 攻击相比于正常网络用户的请求而言，通常都是突发的，通过短时间的大量无意义请求，耗尽服务器资源，从而使得服务器无法向正常用户提供服务，甚至是由于资源耗尽而宕机。

还有另一种 DoS 攻击往往更加巧妙，攻击者会利用网络协议的漏洞，精确地、频次较低地发送请求。这一类攻击往往更加难以防范，而其一旦成功，同样会对服务器造成致命打击。

一般而言，越暴力的 DoS 攻击越需要攻击者更多的网络资源（比如网络带宽），同时防御方更容易进行过滤防御；协议层级越高，设计越精巧的 DoS 攻击，需要攻击者的网络资源越少，给防御方的防御难度和压力也越大。

由于 DoS 攻击本身所具备的暴力性，攻击方往往需要很多的网络资源，比如更大的网络带宽，更快的读写速度，更高的并发度等，而这些必需要求很难在同一台主机上得到满足。因此，出现了 DDoS 的攻击方式，使得攻击者更为隐蔽，攻击的广度更大，力度更强。

按字母序排序，组长为张一舟。
刘德欣，1500017704，元培学院
马赢超，1400015999，光华管理学院
张煌昭，1400017707，元培学院
张一舟（组长），1500012933，信息科学技术学院
张元玮，1400013399，信息科学技术学院

[1]GitHub 组请见 https://github.com/TakingOffPKU，项目源码请见 https://github.com/TakingOffPKU/DDoS

[2]本次大作业源码可通过以下 git 命令获得，
git clone git@github.com:TakingOffPKU/DDoS.git

[3]本报告源码可通过以下 git 命令获得，
git clone https://git.overleaf.com/15642711mpgntxxpnxdn

no Project

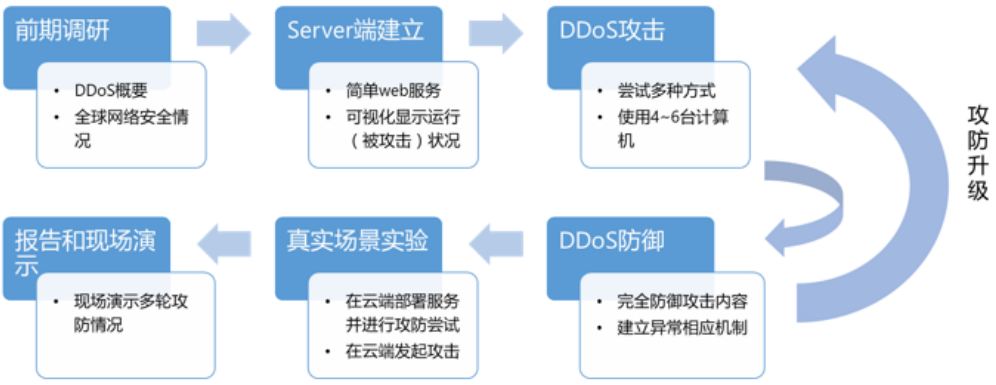

图 1. 项目流程。前期工作包括前期调研，Server 端 Web 服务器实现，被攻击情况可视化实现；实验内容为 2 到 3 轮的 DDoS 攻防练习，DDoS 攻击方使用 4-6 台计算机采取多种攻击方式对服务器端进行攻击，DDoS 防御方于服务器端过滤和防御攻击行为并建立异常响应机制；实验后期将场景扩展为真实场景，将攻击方和服务器均部署于云端并尝试与云端发起攻击；最终成果展示以现场演示的方式进行。

B. DDoS 原理

DDoS（Distributed Denial of Service，分布式拒绝服务）攻击，将单主机的 DoS 攻击分配给若干个主机，攻击者并不亲自发起攻击，而是利用其控制的僵尸网络中的同时发起 DoS 攻击。DDoS 攻击的攻击者更为隐蔽，攻击力度更强，对于攻击者的网络资源要求相对更低。

僵尸网络（Botnet）中，具有一个或多个攻击者，攻击者利用病毒等手段，攻破其余主机，从而形成一个一对多的控制网络。攻击者隐藏于僵尸网络背后，通过僵尸网络发起网络攻击。

下面对几种典型的 DDoS 攻击方式进行介绍。

SYN Flood 利用 TCP 协议三次握手的漏洞发起攻击。TCP 协议中三次握手分别为客户端发送 SYN，服务器端回复 SYN+ACK，客户端回复 ACK，当服务器端发送 SYN+ACK 后将预分配该 TCP 连接所需资源，该资源只有在连接失败或连接断开时才会释放，判断连接失败的条件往往是连接超时，通常被设置为几秒甚至几十秒；当服务器端 TCP 资源不足时则将拒绝其余所有 SYN。攻击方利用这一漏洞，伪造不存在的 IP 发送 SYN，由于该 IP 不存在，不可能回复 ACK，因此服务器的 TCP 资源将在几秒钟内被大量的假 TCP SYN 占用直至耗尽。

DNS Flood 针对网络中的 DNS 服务器发起攻击。DNS 服务通过 UDP 层之上的 DNS 层实现，因此攻击方于 UDP 层伪造 IP 和端口，DNS 层伪造 ID 和待解析的域名，通过暴力发起 DNS 请求，耗尽 DNS 服务器的 CPU 等资源。

HTTP Flood 模仿正常用户的网页行为对 HTTP 层发起攻击。网络安全厂商很难对正常用户的请求和攻击者伪造的攻击请求进行分辨，因此往往只能针对某个产品或某次攻击进行防御，而很难在不影响用户体验的前提下进行通用的防御。HTTP Flood 一旦成功，连锁反应很强，从 Web 前端服务器，到业务后端，甚至更后端的数据库服务器的压力都将增大，其中任何一台崩溃宕机，都将导致整个网络服务崩溃。

慢速连接攻击是一种反其道而行之的攻击方式，其避免暴力发送请求从而规避流量过滤，通过利用协议漏洞和巧妙设计，对网络服务进行攻击。其中 Slowloris 攻击针对 HTTP 协议漏洞进行慢速连接攻击。HTTP 协议中规定了客户端发送结束的标志，在收到这一标志前且没有超时时连接不会中断。攻击方发起攻击时，发送 HTTP 头为 Keep-Alive 的请求，使得连接不会断开，之后每隔几十秒或几分钟发送一小段关键数据至服务器端，最终耗尽服务器 TCP 资源。

混合 DDoS 攻击将上述的攻击方式进行组合，从而进行更为复杂的 DDoS 攻击。

C. DDoS 防御原理

下面对在第II-B节中介绍的几种典型的 DDoS 攻击方式的防御原理进行介绍。

SYN Flood 防御，通过反向探测进行，通过建立 SYN Cookie，实现白名单过滤，从而验证 IP 真伪，过滤虚假流量，使得假 TCP SYN 无法占用 TCP 资源。

DNS Flood 防御，通过使用缓存，减少 DNS 解析时间来对 DNS 攻击进行缓解；同时可以通过过滤丢弃以及回复特殊响应使得客户端确认重发的机制进行防御。

ICP Project

表 I
各时间节点任务

时间节点	任务	参与成员
第一周	建立服务器端 Web 服务	马赢超
	经典的 DDoS 攻击实现	张煌昭, 张一舟
	经典的 DDoS 防御实现	刘德欣, 张元玮
第二周	混合 DDoS 攻击实现	张煌昭, 张一舟
	混合 DDoS 攻击的防御的实现	刘德欣, 马赢超, 张元玮
第三周	对前沿 DDoS 攻击方式及防御方式的调研	张煌昭
	服务器端部署至云端并对防御尝试升级	刘德欣, 马赢超
	DDoS 攻击部署至云端并尝试实现较前沿的攻击方式	张一舟, 张元玮
第四周	服务器端负载和资源可视化展示	马赢超, 张元玮
	展示效果优化	所有人

HTTP Flood 防御，通过缓存技术，减少单次 HTTP 请求处理时间来进行缓解，同时可以通过部署 CDN 节点进行防御。

慢速连接攻击防御，限制 HTTP 传输的最大许可时间，同时对报文内容进行精确识别，判断攻击行为。

面对混合攻击防御时，需要综合上述防御手段，进行灵活的 DDoS 防御。

III. 项目内容及分工

本次大作业将在实验室环境中模拟实现 DDoS 攻击和防御。预期使用一台计算机作为服务器端，提供 Web 或数据库等网络服务，其余若干处于同一局域网环境下的计算机扮演僵尸网络，由攻击者控制向服务器计算机发起 DDoS 攻击，预期攻击成功后，服务器端将无法再提供任何网络服务。防御者则可以在服务器端使用任何方式，在尽量不影响正常用户使用的前提下对 DDoS 攻击进行防御。

整个项目内容分作三部分，如图 1所示：1) Web 服务器开发和部署；2) DDoS 攻击方僵尸网络程序开发、改进和部署；3) DDoS 防御方防御程序开发、改进和部署。其中第 2) 和第 3) 部分的攻防练习将于实验过程中进行迭代，即攻击方首先对没有防御的服务器发动第一轮攻击，成功后防守方针对攻击行为进行第一轮防御，之后攻防双方再进行第二轮甚至第三轮攻防。

预计第一轮攻防使用第II-B节和第II-C节中介绍的 SYN Flood，HTTP Flood 和慢速连接的攻击和防御方法进行攻防。第二轮攻防使用混合方法，并配合 IP 池等方法进行攻防。如果时间条件允许的情况下，第三轮攻防将对当前安全领域前沿研究中出现的 DDoS 攻防方法进行剖析和实现。最后，将会在条件允许的前提下，将 Web 服务部署至云端，并尝试对其进行攻击。

对应上述实验内容，小组成员分工如下，1) Web 前端服务器开发和部署，由马赢超完成；2) DDoS 攻击的实现和部署，由张煌昭和张一舟完成；3) 服务器端 DDoS 防御的实现和部署，由刘德欣，马赢超和张元玮共同完成。

IV. 时间节点

预计本次大作业需要 4 周的时间完成，以周为单位的各个时间节点的任务及参与成员如表 I所示。

第一周，建立并部署服务器 Web 服务器，对第II-B节和第II-C节中经典的的 DDoS 攻击方式进行实现，并对服务器端的攻击和防御。

第二周，进行混合 DDoS 攻击和防御的实现，并对比现有开源 DDoS 攻击工具。

第三周，完善先前实验，对目前较为前沿的攻击和防御方式进行调研并尝试实现，将实验部署于云端真实环境，尝试进行攻击和防御。

第四周，准备展示，服务器端负载的可视化实现，并对实验室环境（局域网下）和真实环境（云端下）下的展示效果进行优化。

预计中期成果展示时完成混合 DDoS 攻击和防御，项目截止时完成上述全部内容。

Project