

DDoS 攻击原理及防御方法分析

曾文权¹, 向友君², 尚敏¹

(1. 广东科学技术职业学院 计算机工程技术学院, 广东 广州 510640;

2. 华南理工大学 电子与信息学院, 广东 广州 510640)

摘 要:DDoS(分布式拒绝服务)攻击是目前对互联网的安全稳定性带来较大威胁的攻击形式之一, 给各电信运营商、互联网服务商、金融企业等一大批重要的互联网用户带来严峻挑战。因此, 对其攻击机理以及防御方法的研究近年来引起了人们的普遍关注。为了寻求有效应对 DDoS 攻击的防御策略, 探讨了 DDoS 攻击的原理、分类, 并对目前一些主流的防御方法进行了深入研究, 分析和比较了各自所具有的优缺点。提出了采取大范围分布式防御、多技术融合、主动防御的应对方法和建议。

关键词:分布式拒绝服务; 互联网安全; 防御系统

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2009)07-0156-03

Analysis of Principle and Defense of DDoS Attacks

ZENG Wen-quan¹, XIANG You-jun², SHANG Min¹

(1. School of Computer Engineering & Technology, Guangdong Institute of Science & Technology, Guangzhou 510640, China;

2. School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510640, China)

Abstract: DDoS (distributed denial of service) attacks are currently on the Internet security threat to the stability of the larger form of attack, to the telecom operators, Internet service providers, financial firms, such as a large number of Internet users with important challenges. Therefore, the mechanism of their attack and defense methods in recent years has aroused widespread concern. In order to seek an effective response to DDoS attacks on the defense strategy, discusses the principle of DDoS attacks, classification, and presents some of the mainstream of defense in-depth research, analysis and compared with their respective advantages and disadvantages. Finally, take the large-scale distributed defense, multi-technology integration, active defense response methods and recommendations.

Key words: distributed denial of service; Internet security; defense system

0 引言

近几年,随着互联网中僵尸网络的日益泛滥和“黑客经济产业”的逐渐形成,使得 DDoS^[1]攻击已经成为当前互联网中存在的最常见、危害性最大的攻击形式之一。尤其是受到商业竞争、经济勒索、政治情绪等因素的驱动,DDoS 攻击越来越呈现出组织化、规模化、商业化的特点,攻击频率也大有愈演愈烈之势,给各类互联网用户和服务提供商带来了业务中断、系统瘫痪等严重后果,严重威胁到互联网和相关应用系统的安全

稳定运行。

如何有效地防御 DDoS 攻击,长期以来一直是互联网安全领域的一个难点和热点。由于 DDoS 攻击常常采用合法的数据包形式,并利用大量分布式的僵尸主机,控制端也常常借助多级跳板加以隐蔽,给防御工作带来了极大的挑战。虽然目前也出现了多种防御手段^[2],从部署防火墙,IDS 设备,到利用接入路由器的过滤限速功能,以及后来的黑洞技术,虽然在不同的程度起到一定的防御效果,但始终未能有效消除 DDoS 攻击对于正常互联网业务的影响。

1 DDoS 攻击原理及分类

1.1 DDoS 攻击基本原理

DDoS 攻击^[3]是攻击者通过控制大量的主机(俗称肉鸡),同时对被攻击发起流量攻击,由于肉鸡数量庞

收稿日期:2008-11-17;修回日期:2009-03-04

基金项目:广东省自然科学基金项目(04010589)

作者简介:曾文权(1978-),男,湖北通城人,讲师,硕士,研究方向为网络性能及网络安全;尚敏,教授,硕士,研究方向为网络安全、智能控制。

大,汇集到被攻击目标网络的攻击流可以达到几十 G,其巨大的流量足以将 Internet 上任何网站站点淹没,造成被攻击目标停止网络服务。典型的分布式拒绝服务攻击网络结构如图 1 所示。

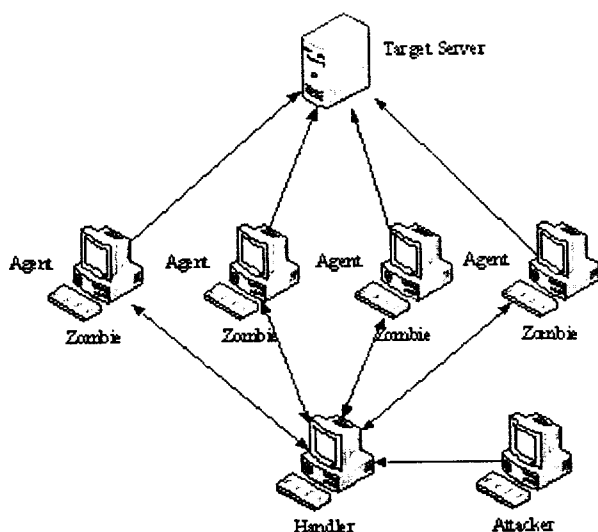


图 1 典型分布式拒绝服务攻击网络结构图

发动 DDoS 攻击时,攻击者在 Attacker(客户端)操纵攻击过程。每个 Handler(主控端)是一台已被入侵并运行了特定程序的系统主机,每个主控端主机能够控制多个 Agent(代理端),每个代理端也是一台已被入侵并运行特定程序的系统主机,每个响应攻击命令的代理端会向被攻击目标主机发送拒绝服务攻击数据包。

从目前来看,绝大多数的 DDoS 攻击所采取的攻击形式无外乎这几种方式:

(1)制造大流量无用数据,造成通往被攻击主机的网络拥塞,使被攻击主机无法正常和外界通信;

(2)利用被攻击主机提供服务或传输协议上处理重复连接的缺陷,反复高频地发出攻击性的重复服务请求,使被攻击主机无法及时处理其它正常的请求;

(3)利用被攻击主机所提供服务程序或传输协议的本身实现缺陷,反复发送畸形的攻击数据引发系统错误的分配大量系统资源,使主机处于挂起状态甚至死机。

1.2 DDoS 攻击的分类

DDoS 攻击的分类方法^[4]多种多样,按照 DDoS 攻击工具的自动化程度,可以分为手动攻击、半自动化攻击和全自动化攻击;按照 DDoS 攻击的攻击速率,可以分为持续稳定攻击和动态变化攻击;其中,最常见的是根据攻击所采用的方式进行分类,可分为以下几类:

1)带宽消耗型:制造超大流量导致被攻击目标的网络拥塞,从而无法提供正常的网络服务,包括 smurf、

ICMP flood、udp flood 等。特点是分布式攻击、攻击流量从 Internet 会聚到目标网络,占用大量带宽。

2)服务器资源消耗型:发送大量网络访问请求,导致目标服务器资源过载,无法响应正常用户请求,包括 TCP-SYN flood、DNS query flood 以及其它特定网络服务(如 QQ、联众)的海量服务请求。特点是攻击流量和正常用户流量特征基本相同,都遵循 TCP/IP 协议或私有协议,很难对非法流量进行识别和过滤。

3)TCP/IP 协议栈漏洞利用型:利用操作系统或应用系统 TCP/IP 协议栈实现的漏洞,包括 teardrop、land 等,特点是只需通过构造一个或少量数据包就可以导致对方服务死锁。目前大部分系统对此类攻击已经免疫,防火墙等网络安全设备可以对该类攻击进行识别、过滤。

当然 DDoS 攻击的手段不止这些,但 DDoS 攻击的主要特征始终都是通过占用某种资源从而使得业务中断或者服务器资源过载,进而达到拒绝服务的攻击目的。

2 常见的防御方法分析

随着 DDoS 攻击对互联网带来的影响日益严重,对于 DDoS 防御方法^[5]的研究目前已成为一个越来越多人关注的热点,业界也出现了多种不同的防御方法,以下通过对一些主流的防御手段的分析,来探讨其中存在的一些值得进一步完善的问题。

2.1 客户端防御设备

客户端防御设备^[6]主要指通过在客户端部署防火墙、IPS(入侵防护系统)等一些防御设备来防护 DDoS 攻击,这也是早期所采用的一种最为传统的防御手段。通常会串联在被攻击目标之前的位置,当攻击发生的时候,对攻击流量进行封堵过滤。

由于这类 CPE 客户端防御设备的位置处于网络路径下游远端,不能为从运营商到企业边缘路由器的访问链路提供足够的保护,从而无法保证企业网的出口链路部分免受 DDoS 攻击的危害,一旦出口链路被 DDoS 流量堵塞,防火墙、IPS 等下游的防御设备将失去抵御作用。其次,由于防火墙、IPS 这类设备通常通过过滤一些具有攻击特征的数据包来实现保护,而 DDoS 攻击包很多时候采用的是合法数据报文形式,因此可以逃过防火墙、IPS 的检测机制。另外,由于这类设备都是串联在攻击目标之前,对 DDoS 攻击数据包的处理也会耗费其大量的性能资源,因此,这类客户端设备自身也很容易成为 DDoS 攻击的对象。

2.2 端口访问控制

这种方法是运用路由器的 ACL(访问控制列表)

功能提供对 DDoS 攻击的防御。ACL 是路由器最基本的一项安全功能,基本所有的路由设备都支持该功能。通过 ACL,不仅可以实现所需要的网络访问控制策略,还可应用于路由的再分配等。为了防御 DDoS 攻击,通过在互联网的接入层或汇聚层对 IP 网用户上网流量实施一定的端口过滤策略,在不影响用户正常访问 Internet 的前提下,对常见的网络蠕虫端口及 DDoS 工具端口进行过滤,对于防御一般常见的 DDoS 攻击可以起到一定作用。

但其最大问题是如果攻击来自于互联网,将很难去制作面向源地址的访问列表,因为源地址出处带有很大的随意性,无法精确定位,唯一能做的就是就面向目的地址的 ACL,把面向这个服务器的访问控制量列出来,将所有请求连接的数据包统统扔掉,这样做反而达到了攻击者的目的。另外,采用这种方式,也无法识别一些利用虚假攻击源和针对应用层的 DDoS 攻击类型。

2.3 CAR 流量限速

CAR(约定访问速率)^[7]是指允许某一网络设备严格地限制流入或流出某一接口流量数量的一种技术,利用这种流量限制技术,可以对所有 IP 流量或只对某几类 IP 流量使用 CAR 流量限速。通过在互联网上利用 CAR 流量限制功能可以减轻 DDoS 攻击对网络或系统造成的一些冲击,特别是对一些 flood 形式的大流量型攻击,如常见的 TCP-SYN flood、ICMP flood、UDP flood 等攻击类型。

同 ACL 相比,流量限速的优点是能够有效避免过大的攻击流量造成网络的拥塞或系统的瘫痪。但主要的问题是其在限制非法用户的网络攻击流量同时,也限制了正常的访问流量,会对合法业务的正常运行带来一定程度的影响。

2.4 黑洞路由

黑洞路由^[8]是近年来运营商经常采用的一种防御 DDoS 攻击的技术,如图 2 所示,当攻击流量到达网络边缘设备 PE 路由器的时候,通过一台触发路由器 (Trigger Router) 向所有 PE 路由器发送 BGP 更新信息,从而控制 PE 路由器对这些流量进行丢弃,也即将其转发到一个“路由黑洞”,从而保护整个网络和其他主机不受影响。

这种方式同 ACL 方式相比,可以大大减少攻击发生时的维护工作量,而且对路由器的性能影响较小,适合对大规模针对特定 IP 或 IP 段的 DDoS 攻击。但其缺点是不能对所牵引的数据包进行区别处理,只能全部丢弃,使得合法用户也被拒绝了,从而造成间接的 DDoS 攻击。

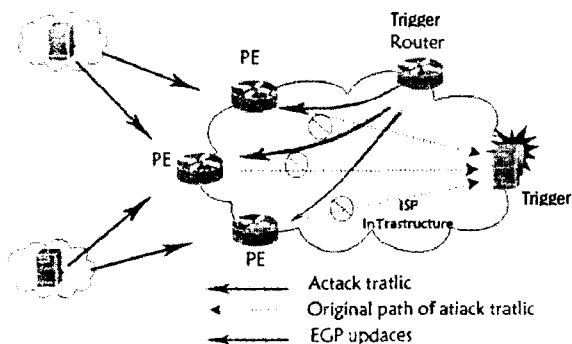


图 2 黑洞路由技术工作示意图

3 结束语

如何有效地防御 DDoS 攻击^[9],长期以来一直是互联网安全领域的一个难点和热点。根据常用防御方法的分析,需要从以下几个方面来改进:

(1) 加强多方合作,在网络骨干运营商之间,网络安全工作者之间以及用户与运营商之间加强合作,密切配合。DDoS 攻击主要特征之一就是分布式,较好的防御需要大范围分布式的共同防范。

(2) 现有的防御方法由于侧重点不同,具有各自的优缺点,如果能在环境允许的条件下将各种技术方法融合,多种措施并举,可能产生比单一方法更有效的防御结果。

(3) 传统的 DDoS 攻击防御方法只是被动的防御,主动防御是一种新思想,是以入侵检测系统、蜜罐系统以及计算机取证系统为主要组成部分,对保护网络实施主动防御、综合控制和联合防御,将对攻击者造成巨大的压力和威慑。

DDoS 攻击对于目前互联网的安全可用是个严峻的挑战,需要研究探索的道路还很长很长。

参考文献:

- [1] Mirkovic J, Martin J, Reiher P. A Taxonomy of DDoS attacks and DDoS defense Mechanisms [EB/OL]. 2002. <http://www.lasr.cs.ucla.edu/DDoS/>.
- [2] Glenn M. A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment [EB/OL]. 2003. <http://www.sans.org/reading-room/whitepapers/>.
- [3] Martin J. Denial of Service Attacks [DB/OL]. 2004. <http://www.securitydocs.com/library/2616>.
- [4] 崔永君, 张永花. 基于 DDoS 攻击的研究[J]. 计算机时代, 2007(3): 27-28.
- [5] 杨文静, 陈义平. 一种新的分布式 DDoS 攻击防御体系[J]. 现代电子技术, 2006(19): 54-57.

(下转第 162 页)

Leader 成员,需要的通信次数为: $\text{Number}(\text{队形转换表中元素的个数})$;

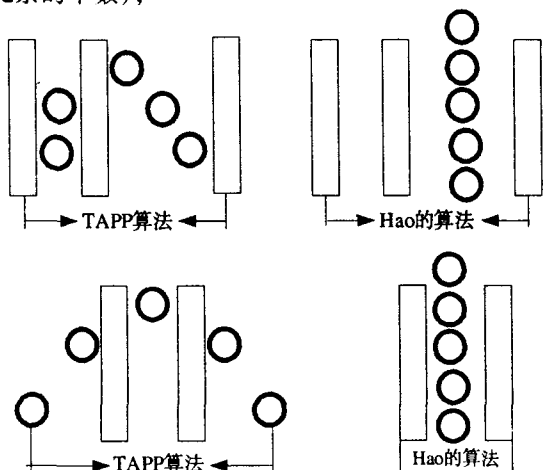


图 2 两种方法的结果比较

②队形转换表使团队中的非 Leader 成员清楚队形转换的结果,从而确保团队成员的行为一致,而 Hao^[2]的方法中每个成员都根据自己的局部信息来调整自己的位置,不知道队形的转换结果,容易导致成员的行为不一致,导致转换过程的混乱和相互等待。

图 3 给出的是三个 Agent 构成的团队在经过障碍物时的运动轨迹。编号 3 的成员为团队中的 Leader 成员,团队成员在经过复杂障碍物时,队形由三角形队形变换为列队形,行进的过程中当环境满足三角形队形的要求时,又变为三角形队形。

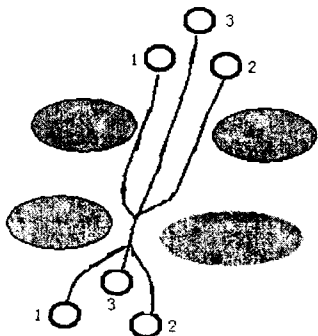


图 3 Agent 团队在经过障碍物时的运动轨迹

3 结束语

给出了一个保持 Agent 团队队形的路径规划算法

ATPP。ATPP 算法是一种集中式的全局规划方法,通过两步得到团队中所有自治实体的路径规划,分析与试验结果表明该算法是合理和有效的。用户可以根据任务的要求及自身需要,通过调整影响因子 k_1, k_2 的值,分别得到侧重距离和侧重队形的路径规划。队形转换表是根据环境特性得到的,用它来指导团队行进中的队形变换更合理,ATPP 算法改进了 Hao 的方法。与 Hogg^[6]方法相比,ATPP 方法减少了队形维持过程中需要的通信量,并且能够确保团队中每个非 Leader 成员在队形变换的过程中知道队形变换的结果,确保其行为一致,避免队形转换过程中的等待和混乱。

参考文献:

- [1] Kamphuis A, Overmars M H. Finding paths for Coherent Groups using Clearance[C]//Eurographics/ACM SIGGRAPH Symposium on Computer Animation, Copyright ACM SIGGRAPH / Eurographics. [s. l.]:[s. n.], 2004.
- [2] Hao Yongxing, Agrawal S K. Planning and control of UGV formations in a dynamic environment: A practical framework with experiments[J]. Robotics and Autonomous Systems, 2005, 51: 101-110.
- [3] 范莉丽,王奇志. 改进的生物激励神经网络的机器人路径规划[J]. 计算机技术与发展, 2006, 16(4): 19-21.
- [4] 易荣贵,罗大庸. 基于遗传算法的物流配送路径优化问题研究[J]. 计算机技术与发展, 2008, 18(6): 13-15.
- [5] 郑延斌. 团队 CGA 行进中的动态避障方法[J]. 计算机工程, 2005, 31(19): 23-25.
- [6] Hogg R W, Rankin A L, Romelitis S I, et al. Algorithms and sensors for small robot path following[C]//Proc 2002 IEEE Int Conf on Robotics and Automation. Washington D C: [s. n.], 2002: 3850-3857.
- [7] 谭民,王硕,曹志强. 多机器人系统[M]. 北京: 清华大学出版社, 2005.
- [8] Tabuada P, Pappas G J, Lima P. Motion Feasibility of Multi-Agent Formations[J]. IEEE Transactions on Robotics, 2005, 21(3): 387-391.
- [9] 王凤林. 坦克兵营连战胜教程[M]. 北京: 国防工业出版社, 1991.

(上接第 158 页)

- [6] 陈三堰,沈阳. 网络攻防技术与实践[M]. 北京: 科学出版社, 2006: 362-367.
- [7] 汤丹,匡晓红,蒋光和,等. 运营商抵御 DDOS 的安全解决方案[J]. 计算机工程与设计, 2006, 27: 4028-4032.
- [8] 忽海娜,冯浩,王中立. DDOS 攻击下高带宽聚类的控制[J]. 计算机技术与发展, 2008, 18(4): 155-157.
- [9] 尚占锋;章登义. DDOS 防御机制研究[J]. 计算机技术与发展, 2008, 18(1): 116-118.