软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(8):2058−2072 [doi: 10.3724/SP.J.1001.2012.04237]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

DDoS 攻击检测和控制方法*

张永铮[1], 肖 军[1+], 云晓春[1], 王风宇[2]

[1](中国科学院 信息工程研究所,北京 100029)

[2](山东大学 计算机科学与技术学院,山东 济南 250101)

DDoS Attacks Detection and Control Mechanisms

ZHANG Yong-Zheng[1], XIAO Jun[1+], YUN Xiao-Chun[1], WANG Feng-Yu[2]

[1](Institute of Information Engineering, The Chinese Academy of Sciences, Beijing 100029, China)

[2](School of Computer Science and Technology, Shandong University, Ji'nan 250101, China)

+ Corresponding author: E-mail: xiaojun@iie.ac.cn

Zhang YZ, Xiao J, Yun XC, Wang FY. DDoS attacks detection and control mechanisms. *Journal of Software*, 2012,23(8):2058−2072 (in Chinese). http://www.jos.org.cn/1000-9825/4237.htm

Abstract: The Distributed denial of service (DDoS) attack is a major threat to the current network. Based on the attack packet level, the study divides DDoS attacks into network-level DDoS attacks and application-level DDoS attacks. Next, the study analyzes the detection and control methods of these two kinds of DDoS attacks in detail, and it also analyzes the drawbacks of different control methods implemented in different network positions. Finally, the study analyzes the drawbacks of the current detection and control methods, the development trend of the DDoS filter system, and corresponding technological challenges are also proposed.

Key words: DDoS; detection; control

摘 要: 分布式拒绝服务(distributed denial of service,简称 DDoS)攻击是当今互联网的重要威胁之一.基于攻击包所处网络层次,将 DDoS 攻击分为网络层 DDoS 攻击和应用层 DDoS 攻击,介绍了两类攻击的各种检测和控制方法,比较了处于不同部署位置控制方法的优劣.最后分析了现有检测和控制方法应对 DDoS 攻击的不足,并提出了 DDoS 过滤系统的未来发展趋势和相关技术难点.

关键词: DDoS;检测;控制

中图法分类号: TP309 **文献标识码**: A

分布式拒绝服务(distributed denial-of-service attack,简称 DDoS)攻击是当今互联网最重要的威胁之一.DDoS 攻击是指攻击者通过傀儡主机,消耗攻击目标的计算资源,阻止目标为合法用户提供服务.Web 服务器、DNS 服务器为最常见的攻击目标,可消耗的计算资源可以是 CPU、内存、带宽、数据库服务器等,Amazon,eBay,Yahoo,Sina,Baidu 等国内外网站都曾受到 DDoS 攻击.DDoS 攻击不仅可以实现某一个具体目标,如 WEB 服务器或 DNS 服务器的攻击,而且可以实现对网络基础设施的攻击,如路由器等.利用巨大的攻击流量,可以使攻击目

* 基金项目: 国家自然科学基金(61070185); 国家高技术研究发展计划(863)(2007AA010501, 2009AA01Z431)
收稿时间: 2011-04-29; 修改时间: 2011-11-17; 定稿时间: 2012-03-27; jos 在线出版时间: 2012-05-21
CNKI 网络优先出版: 2012-05-21 15:26, http://www.cnki.net/kcms/detail/11.2560.TP.20120521.1526.001.html

标所得的互联网区域网络基础设施过载,导致网络性能大幅度下降,影响网络所承载的服务.近年来,DDoS 攻击事件层出不穷,各种相关报道也屡见不鲜[1−4].比较典型的事件如 2009 年 5 月 19 日发生的暴风影音事件[5].该事件导致了中国南方六省电信用户的大规模断网,预计经济损失超过 1.6 亿元人民币,其根本原因是由于服务于暴风影音软件的域名服务器 DNS pod 遭到黑客的 DDoS 攻击而无法提供正常域名请求.由此可见,针对 DDoS 攻击的检测和控制的研究工作具有重要的理论意义和实际价值.

DDoS 的蓬勃发展有如下原因:

- 大量的操作系统漏洞使得攻击者可以控制大量的僵尸主机,构建大规模僵尸网络;
- 网络规模的不断扩大,使得僵尸网络的规模越来越大;
- 大量的攻击工具降低了发动攻击的技术门槛,大大降低了攻击的技术难度;
- 随着微电子技术和网络技术的不断发展,终端主机的计算能力不断增强,接入带宽不断提高,每台僵尸主机能够以更高的速率发送攻击包;
- 互联网在设计之初缺乏对安全问题的周详考虑,只关注对数据包的迅速转发;
- 互联网在功能上是一个哑铃型的结构,中间网络只负责数据转发,而把安全事件的检测和控制功能完全交由客户端来完成,网络本身不具备对网络攻击的检测和处理能力;
- 此外,经济利益的驱动是 DDoS 攻击频繁发生的重要因素.

依据攻击包的地址有效性、攻击速率等属性,Mirkovic 等人[6]对网络层 DDoS 攻击进行了详细分类,但分类仅局限于网络层 DDoS 攻击.近年来,基于应用层数据包的 DDoS 攻击越来越频繁,并有取代传统网络层 DDoS 攻击的趋势.在网络层 DDoS 攻击无法取得满意效果时,攻击者往往会采用应用层 DDoS 攻击[7]来实现攻击意图.与网络层 DDoS 攻击不同,应用层 DDoS 攻击首先与攻击目标建立 TCP 连接,在连接建立后,发送 HTTP 请求消耗攻击目标的资源.本文将 DDoS 攻击分为网络层 DDoS 攻击和应用层 DDoS 攻击,在此基础上,介绍 DDoS 攻击的检测和控制方法.

本文第 1 节对网络层 DDoS 攻击的检测和控制技术进行介绍和分析.第 2 节对应用层 DDoS 攻击的检测和控制技术进行介绍和分析.第 3 节对现有控制方法进行比较,提出 DDoS 过滤系统的未来发展趋势和相关技术挑战.第 4 节进行总结.

1 网络层 DDoS 攻击检测和控制

网络层 DDoS 攻击会引起流量、不同协议类型数据包数量分布、同协议不同种类数据包数比例、访问源地址数量及分布、数据包头信息等多方面上的变化,并可导致链路拥塞和数据传输时延大幅增加.现有网络层 DDoS 检测方法大都基于上述几个方面统计值的变化.

1.1 网络层DDoS攻击检测

1.1.1 基于流量变化的检测方法

DDoS 攻击最明显的特征就是流量的大幅度增加,基于流量变化检测 DDoS 也是最常见的方法.

与最常见的基于单链路流量检测 DDoS 攻击相比,基于全网流量变化检测 DDoS 攻击,能有效降低网络流量波动导致的检测误差.罗华等人提出了基于网络全局流量异常特征,检测 DDoS 攻击的方法,通过对全网或运营商网络中的 OD(origin-destination)对(或流,或者节点)之间的流量进行测量[8],构建网络流量矩阵,基于链路中攻击流的相关性,将流量矩阵分解为异常流量空间和正常流量空间,利用异常流量的相关特征检测出攻击.

Chen 等人采用 CAT(change-aggregation tree)机制[9]对流经同一个 ISP 网络中的路由器流量进行协同分析,根据路由器每个接口的流量分布情况发现流量异常,流量异常报警信号发送给 CAT 构建服务器,由 CAT 构建服务器对报警信号进行协同分析融合处理,实现对攻击的快速、准确识别.

TCP 协议承载了互联网中的大部分业务,并且 TCP 协议规定数据接收方需向数据发送方进行传输确认,因而某一网络节点或某一网段的 TCP 数据包数量比例在统计意义上是稳定[10],如果该比例值发生较大的变化,则认为发生了 DDoS 攻击.通过统计计算各子网的进出 TCP 包数比例,可以发现被攻击子网地址.

在骨干网层面检测 DDoS 攻击一直是研究的难点.Yuan 等人提出了采用 Cross-Correlation 和 Weight Vector 方法分析骨干网节点流量[11],检测 DDoS 攻击的方法.此方法能够有效检测多种攻击,如恒速流量攻击、增速流量攻击、Pulsing 攻击或 TCP-Target 攻击等.

DDoS 攻击发生时,在骨干网层面上及时发现被攻击地址对网络安全应急响应具有重要意义.基于 DDoS 攻击会导致流量大幅度增加的特征[12],Sekar 等人提出了一种两级 DDoS 检测机制,能够及时发现被攻击地址.采用 Snmp 测量路由器接口流量,并与历史流量数据进行比对,能够发现流量的异常变化,然后利用 Netflow 信息,提取被攻击地址.

Shrew(pulsing)DDoS 利用了 TCP 协议重传的时间特性,根据 TCP 重传时间间隔,在较短时间内高速发送攻击包,消耗攻击目标缓冲区,导致大量 TCP 包被丢弃.TCP 包依据重传规则,过一定时间后重传数据包,此时,攻击主机再次发送攻击包消耗缓冲区.利用较少的攻击流量,攻击者即可获得较好的攻击效果,且不易被检测.Chen 等人提出一种 Shrew DDoS 攻击的识别机制[13].该方法对多个路由器流量的协同分析,计算流量采样序列的自相关序列,并利用傅里叶变换(discrete Fourier transform)将自相关序列转换为频域,由于其低频域的功率谱密度(power spectrum density)比正常流量要高,因而可以检测到 shrew DDoS 攻击.Sun 等人也提出了一种分布式的 DDoS 攻击检测方法[14],利用动态 Time Warping 方法,能够准确地检测出 Shrew DDoS 攻击.

1.1.2 基于同协议不同类型数据包数比例

流入一个地址的流量与流出流量在无攻击情况下成一定的比例.与正常流不同,攻击主机向攻击目标发送大量数据包,攻击目标不对攻击数据包作响应或由于拥塞,响应数据包较少.MULTOPS 基于这一特点[15],通过统计进出子网的数据包数检测 DDoS 攻击,并能够根据流量变化分布状况及时调整检测粒度,实现对攻击目标的细粒度定位.

TCP SYN Flood 攻击利用了 TCP 协议的漏洞,是最常见的 DDoS 攻击形式.操作系统每接收到一个 TCP/SYN 包,会发送 SYN-FIN 回应请求,并为这个连接请求分配一个单独的内存空间,直到接收到 SYN/ACK-FIN,才释放这个空间.攻击者发送大量的 SYN 包,并且不对 SYN-FIN 包作回应,以此来消耗攻击目标的内存空间.可见,攻击发生时,流入攻击主机的 SYN-FIN 包数和流出的 SYN/ACK-FIN 包数差异较大[16].对一个网段流进的 SYN-FIN 包和流出的 SYN/ACK-FIN 包数进行统计,能够有效地发现 SYN Flood 攻击主机.此方法能够在边界路由器上实现,在检测 SYN Flood 攻击的同时,实现了对攻击源定位.在上述检测方法的基础上,结合了非参数累加和(non-parametric cumulative sum)策略的检测方法能够适用于不同监测点[17],检测方法更加鲁棒,且计算开销更低.

不同的 DDoS 攻击方式,攻击目标的返回数据包类型也不同.Backscatter 方法基于这一特点[18],检测并统计全网范围内的 DDoS 攻击.结果表明,攻击规模和持续时间成重尾分布.

DiDDem(distributed denial-of-service detection mechanism)是一个两级的分布式 DDoS 检测机制[19].PF(pre-filter)检测节点在其所处路由器的流量增加时,提取流量分析是否攻击发生,如果发生,则向 C^2(command and control)服务器报警,C^2 服务器对比之前的流量,结合别的 C^2 服务器信息对报警信息进行判断,并作出控制反馈.

1.1.3 基于源地址数量及分布变化

为了隐藏攻击,DDoS 攻击者可以降低攻击速率,使攻击流量速率接近正常访问速率,以此增加检测难度.但在 DDoS 攻击时,访问 IP 数量大幅度增加是攻击的一个明显特征[20],且此特征无法隐藏.基于这个特征,利用机器学习,结合 Non-Parametric Change Detection Scheme,能够有效地检测 DDoS 攻击,特别是攻击源地址分布均匀的 DDoS 攻击.文献[21]采用新源地址出现速率作为攻击是否发生的依据,并采用了 Sequential Nonparametric Change Point Detection 方法改进检测精度;同时,通过访问流数量变化,实现对 Flash Crowd 和 DDoS 攻击的有效区分.

伪造源地址 DDoS 攻击发生时,源地址的流数量熵值和目标地址流数量熵值均会发生较大变化[22].大量流汇聚导致目的地址的熵值大幅度下降,而攻击流的均匀使得源地址熵值会有所增加.通过训练出的阈值,可以检测 DDoS 攻击.

当无攻击发生时,对某一目标地址访问的源地址分布是稳定的[23],且通常成簇.而 DDoS 攻击发生时,源地址的分布趋于离散.根据这一特性,Wang 等人提出了通过计算相邻时间滑动窗口内数据包的相关系数,识别 DDoS 攻击的方法.

1.1.4 基于数据包头统计信息的变化

攻击时,除了包数、源地址分布异常以外,数据包头信息统计分布也与正常情况不同.攻击者可以伪造某一方面信息,如源地址采用合法用户地址,却难以伪造包头的所有信息.熵和卡方检验(chi-sequare)是两种常用的统计方法[24],能够有效地计算特征分布变化.通过这两种方法计算数据包头部信息分布,如包长、协议等,与无攻击时的计算值进行比对,可以有效地检测出攻击.此外,为了降低计算开销,可以对数据包进行采样计算.

当攻击者采用较低的攻击速率隐藏攻击时,通过流量检测低速 DDoS 攻击,如 Shrew DDoS 攻击,效果不佳.但是 DDoS 攻击发生时,数据包头信息分布均会发生明显的改变[25].无论是高速流量攻击还是低速流量攻击,在一定的统计时隙内,攻击目标地址出现频率均会显著增加,源地址分布更加离散,攻击数据包的目的端口和源端口通常固定不变或随机变化.熵能够有效衡量流量特征的改变[26],选择源地址、目的地址、源端口、目的端口计算熵值.如果地址和端口分布比无攻击时集中,则熵值低于正常情况的熵值,反之高于正常情况的熵值,因而能够有效地检测高速和低速 DDoS 攻击.

传统的入侵检测方法采取误用检测的思路,根据已知攻击指纹识别攻击,因而无法检测新类型攻击.针对网络层攻击,文献[27]采取了异常检测的思路,如果行为与正常行为模型偏离,则可能为攻击.构建的入侵检测系统包含了数据包头异常检测器(packet header anomaly detector,简称 PHAD)和应用层异常检测器(application layer anomaly detector,简称 ALAD).PHAD 负责监测数据链路、网络层和传输层;ALAD 负责监测传统的用户行为,如 HTTP,FTP 或 SMTP.

现有的大部分 DDoS 检测方法采用入侵检测的思路进行 DDoS 检测,出现了即使检测到攻击,也无法准确判断该过滤何种数据包的问题.文献[28]构建朴素贝叶斯分类器进行 DDoS 攻击检测,并设计了 TCP 和 UDP 的分类器模型,可以判断异常数据包类型.该方法的不足在于,当攻击采用正常访问进行攻击时,无法获得满意的检测效果.

基于攻击时数据包长度分布异于正常情况,文献[29]提出了一个两级机制的 DDoS 防御系统,第 1 级为 DDoS 攻击检测,第 2 级为异常流识别.

1.1.5 基于链路拥塞和时延测量

DDoS 发生时,流量往往超过路由器等网络设备的处理能力,导致端到端的时延增加,因而时延变大也是 DDoS 攻击的特征之一.

由于监测点无法获取所有链路的时延,因而只能通过推算的方法获取无法测量的链路信息.文献[30]对网络进行端到端的测量,包括时延、包计数等,利用极大似然估计推算网络内部链路的特征分布,并采用自组织映射(SOM)神经网络对链路特征进行学习,建立起网络链路特征活动轮廓,并建立检测阈值,从而实现对异常现象的检测,并且能够将异常定位到具体的链路.

Passive 检测依赖于捕获的数据包及特征,在攻击发生初期,passive 检测精度不高.为了避免这种不足,文献[31]提出了在 SYN Flood 攻击下的主动检测方法.通过测量与 Source IP 的时延来判断是否发生了攻击.同时,如果存在大量未完成的 TCP 三次握手,则很可能发生了 SYN Flood 攻击.但 TCP 半连接可能由 TCP/SYN Flood 攻击导致,也可能由网络拥塞导致.为了判断是否为攻击所导致,选择一些地址,发送不同的 TTL 包,使 Router 发送 ICMP 包来推断时延,如果时延正常,则可以判断为 SYN Flood 攻击.此方法在攻击开始阶段具有很好的精度,但攻击严重时效果不佳,其原因是测量时延的数据包由于拥塞,很可能被丢弃而无法返回.

1.1.6 基于行为分析

文献[32]采用 CUSUM 方法来检测攻击,对 TCP SYN Flood 攻击的检测仍然基于三次握手的完成情况.为了区分是伪造固定地址攻击(或采用了真实地址)、伪造子网地址攻击,还是随机伪造地址攻击,采用了 Bloom Filter 来统计源地址分布情况.

DDoS、蠕虫和病毒(垃圾)邮件是影响骨干网安全的 3 个主要因素,三者在行为模式上有明显区别:DDoS 表现为多个地址向一个 IP 地址发送数据[33];蠕虫表现为一个 IP 地址向多个 IP 地址,通过一个或多个端口发送数据包;病毒邮件则是一个地址,通过 25 端口向多个 IP 地址发数据包.3 种行为模型称为威胁兴趣关系(threats interestedness relation,简称 TIR)模型,通过对源地址、目的地址、端口进行监控,构建 TIR 树,可识别 3 种攻击.

DDoS 攻击通常由僵尸网络发动,而蜜罐是捕获僵尸程序的重要手段.通过分析僵尸程序和僵尸网络控制者发送的命令,能够实现对 DDoS 攻击的提前检测,并且能够准确地获取 DDoS 攻击类型等信息[34].

正常的 TCP 流与其数据往返时间 RTT(round-trip time)具有极强的时间相关性,而攻击流不具备这样的特征[35].基于这一特征,可有效区分攻击流和正常流.Cheng 采用谱(spectral)分析,以一个固定时隙内到达数据包数为输入,计算信号的功率谱密度(power spectral density),可以区分攻击流和合法流.

攻击流由 Bot 程序生成,由于 Bot 程序不易随意改变,因而生成的攻击流比较相似,具有相同的攻击样式.基于信息论方法,计算流之间的距离,有助于识别攻击流[36].通过计算流中数据包的分布行为,能够有效区分攻击流和正常流.

1.2 网络层DDoS攻击控制

基于控制设备部署位置,网络层 DDoS 攻击控制可以分为攻击源端控制(source)、中间层控制(intermediate)、攻击末端控制(victim or end)和采用新的网络协议和网络体系结构进行控制.

1.2.1 攻击源端控制

在攻击源端进行控制,能够阻止攻击流进入骨干网,并且在攻击源端便于做 traceback 和调查攻击主机.同时,由于流量较小,边界路由器可以有足够的计算能力执行检测和控制.

当攻击发生时,攻击主机发出大量的数据包,而流入数据包较少.D-WARD[37,38]基于流入流出的流量比率、连接数量、包速率等信息,将主机行为与正常行为模型进行比较,如果偏离正常行为,则认为主机可疑或者为攻击主机,对其进行流量控制.此方法的不足在于无法有效应对慢速 DDoS 攻击.同时,由于 ISP 无法从部署攻击控制设备中获益,攻击源端控制策略往往无法实施.

1.2.2 中间层控制

中间层控制策略可分为过滤,Traceback 和 Pushback3 类.

1.2.2.1 中间层过滤

中间层过滤是指路由器基于可利用的鉴别信息,实现对数据包的过滤,或者单纯基于流量信息做限速控制.

通过数据包携带身份认证信息,是一类鉴别数据包源地址真伪的方法.PI(path identification)策略让数据包携带其所通过路径的指纹[39],被攻击目标可有效鉴别伪造数据包.相同路径的数据包应有相同的路径标识,伪造数据包虽然可以伪造源地址,但由于与真实数据包经过的路径不同,路由器所写指纹也不同,因而仍然能够识别出伪造攻击包.PI 方法不需要路径上所有的路由器均为数据包写指纹,并且 PI 是一种轻量级的控制策略.Stackpi 方法进一步发展了 PI 方法[40],并采用了 Stack-Based 标记方法和 Write-Ahead 策略,弥补了覆盖路由器数量不足的缺点,并且大大提高了性能.

在 DDoS 攻击发生时,上游路由器进行流量控制也是一种常见的 DDoS 控制策略.在攻击发生时,被攻击目标向上游路由器发出控制指令和控制参数[41].路由器采取令牌桶方法控制流量,路由器间的流量分配采取了 k 级 Max-Min 策略,并且采取了反馈控制策略动态调整流量控制参数.

骨干层上流量过滤的一个难点在于无法准确获知网络的流量大小和流量分布状况.文献[42]利用分布于全网各点的 IDS 检测网络局部状况,各 IDS 之间共享网络局部状况信息,构建全网流量状况并进行流量过滤,IDS 间的合作大大提高了检测和过滤的准确性.

在一定时间内流过某一链路的数据包头信息在统计上符合一定规律;而在攻击发生时,大量的伪造数据包会导致统计值发生变化.基于这一假设,Packetscore[43]利用贝叶斯分布计算数据包合法性,如果合法性计算结果大于训练出的合法性阈值,则丢弃数据包.此方法可在骨干层实现,能够有效过滤伪造地址 DDoS 攻击流量,但对新出现的合法流量具有较高的误报率;此外,对采用合法地址的攻击具有较高的漏报率.

互联网的 Power-law 特性,使得部署较少的路由器就能过滤大部分网络流量.文献[44]基于这一特性,提出了基于路由器的分布式数据包过滤方式,指明了网络层基于路由器的分布式过滤的应用前景.

ION(indirection-based overlay network)要求攻击者无法获取客户端的连接信息和网络架构,然后,攻击者可以利用这一条件对连接通过的网络节点进行攻击,实现攻击目的.为了避免这一弱点,客户端可以选择一些网络节点(路由器)进行传输[45],使攻击者看来这些网络节点是随机选择的,从而无法选择合适的网络节点进行攻击.同时,在客户端和节点间进行 Session 协商,节点仅保证完成协商的客户端通讯,对未进行协商的节点,丢弃其数据包或者进行流量控制.

除了在路由器上实现流量控制和过滤以外,在 ISP 内部建立流量清洗中心也是一种解决策略[46],且清洗中心机制更灵巧,能够执行复杂的过滤策略,同时能够避免骨干核心路由器承受巨大的计算开销.构建清洗中心的难点在于攻击检测、攻击目标识别,以及待清洗流量引入清洗中心和完成清洗后,重新注入互联网的路由问题.

在一个节点发生流入流量过大时,可以通知邻近节点和路由器进行限流[47].Backwork-Propagation 和 On-Off 控制策略能够反复调整许可的流量速率,发送给邻近节点或路由器,通过临近节点实现对攻击的控制.这种方法本质上是一种协同的限流策略,并不对流量类型作区分,也不识别攻击流量,因而不能有效保护合法流量.

攻击包均有 Bot 程序生成,因而攻击包头通常有相同的特性,如包长、标志位相同,或者端口均随机生成.文献[48]采用重心原理对数据包进行聚类,在一定的欧式距离范围内对基于目的地址的 IP 流样本相应字段进行聚类,动态提取攻击流重心作为攻击特征,并将特征传给 Netflow 进行过滤.该方法的不足在于仅能处理攻击方式简单、攻击特征明显的攻击.

1.2.2.2 Traceback

Traceback[49]策略在攻击发生时能够定位数据包源地址,并且可用于攻击后续追踪和攻击场景重现.在伪造地址 DDoS 攻击发生时,基于 Traceback 策略,被攻击主机根据数据包所打路由器标记,可以分析得到数据包所经过的路由器,从而定位对攻击地址或攻击主机所在子网.路由器采用了概率打包策略为流经的数据包做标记,攻击主机需通过多个同一个路径上的数据包,重现出整条路径.此方法的不足在于,如果路径上的一个路由器被攻击者攻陷,那么该路径就无法重现.

Advanced Marking Scheme 和 Authenticated Marking Scheme[50]具有较低的网络和路由器开销,在大规模 DDoS 攻击下,仍然具有较低的路径构造计算开销;同时,路径构造准确性也大为提高.而且,即使路径上的某一个路由器被攻击者控制,Authenticated Marking Scheme 也能够保证其他路由器标记不会被其更改.

上述方法均是基于传输路径上路由器所打标识,构建出数据包流经的路径,但是由于数据包源地址真伪无法确定,因而不能实现对数据包源地址的追踪.基于哈希的 IP Traceback 方法使用了原路径分离机制(source path isolation engine)实现了对源地址的追踪[51],同时采用 Bloom Filter 策略,大大降低了内存消耗.Yu 等人根据提出了一种基于流分布熵进行 traceback 的方法[52].在无攻击时,计算路由器的流分布熵进行训练,基于训练值和当前熵计算结果检测攻击.在检测到攻击后,识别异常的上游路由器,通知其识别与之连接的上游路由器.如此循环,直到找到攻击目标.该方法没有通过标注数据包来重构攻击路径,而是采取了根据流分布熵识别上游攻击路由器的思路,因而避免了数据包标注的一些缺点,如可扩展性弱、标注易被篡改、存储开销和路径重构计算开销大等.该方法的不足在于无法有效处理低速率 DDoS 攻击.

1.2.2.3 Pushback

在 Pushback[53]策略下,在攻击发生时,被攻击目标发出 Pushback 信息,通知其邻近路由器监控进入流量,并进一步将 Pushback 信息传给临近路由器.如此逐次传播 Pushback 信息,完成对拥塞的控制.但一个路由器的接口往往连接了多个路由器,只能识别异常流量来自某一个端口,而无法准确判断异常流量来自哪一个路由器.另一方面,如果攻击流量在各个路由器分布较均匀,则识别异常路由器的效率较低,且识别难度也大为增加.选择性 Pushback[54]策略针对上述两个问题,按概率对数据包打标记,标识其通过的路径和数据包源头,可以有效地辨别伪造包并实施过滤.选择性 Pushback 策略能够有效过滤攻击流量,保护合法流量,其不足在于无法识别真实地址或伪造子网地址的攻击攻击包.

1.2.3 攻击末端控制

攻击末端控制是最普遍的控制措施,能够最有效地识别攻击和过滤攻击流量;此外,部署者也能获益.

对访问地址的流量进行检测是一类常见的控制方法.通过学习正常访问行为,建立正常访问行为模型[55],监测每个访问地址的包速率,并与包速率阈值进行比较,可发现可疑地址.同时,按照可疑度进行服务时间排队,可疑度越小,获得的服务时间就越长.文献[56]对超过阈值的IP地址进行屏蔽,阻止其数据包进入系统,同时对包速率未超过阈值但数据包总数较多的地址进行限流,同时还采用Syn Cookie方式判断伪造地址.

对一个攻击目标而言,由于网络路径不会频繁改变,因而从同一个网段数据包的TTL一般是固定的[57].由于攻击者无法获取数据包跳数信息,因而伪造数据包达到攻击目标时,TTL值与正常情况不符.通过训练,可建立一个C类IP子网的跳数表,在攻击发生时,根据收到数据包的TTL值还原初始TTL,判断其是否符合初始TTL值规范,因此进行伪造数据包识别.

Low-Rate DDoS利用了TCP协议重传的时间特征,无需发生大量的数据包,攻击比较隐蔽.RTO随机化方法使TCP协议重传时间随机化[58],可有效降低Low-Rate DDoS的攻击效果.此外,探测网络的状态并获取Low-Rate DDoS攻击的周期性,也能抵抗Low-Rate DDoS攻击.文献[59]通过信号处理方法分析Low-Rate攻击流和正常访问流,发现Low-Rate DDoS攻击在低频范围分布较广.基于这一特征,可对流的数据包进行采样分析,如果其频率符合Low-Rate DDoS攻击流特征,则对其进行过滤.

在攻击发生时,可以调节返回TCP包中的WIN对客户端进行流量控制[60].正常客户端会对调整作出反应并相应地降低发送速率,而攻击主机则会尽最大能力发动攻击.因而攻击端会忽略调节信息,发送速率保持不变.通过此方法,能够区分攻击主机和正常客户端.

对一个服务器而言,以前访问的用户往往还会再次出现,在DDoS发生时,为这些用户提供服务,能够有效地抵御攻击.基于历史IP的过滤方法(history-IP filtering)基于这一原理[61],根据正常访问源地址出现的频率和相应的数据包数构建了IP地址数据库,并且采用滑动窗口进行过期地址淘汰.在DDoS攻击发生时,依据IP地址数据库提供服务.

Serwadda等人研究了在多种DDoS攻击下[62],服务器、路由器请求调度策略保护合法流量的效果.该工作对设计更鲁棒、更灵活的调度策略具有参考价值.

1.2.4 新的体系结构和协议

协议漏洞和当前互联网缺乏对安全事件的有效控制能力,均是DDoS攻击频繁发生的重要原因.采取更安全的协议,或者采用新的网络体系结构,能够有效地提高对DDoS攻击的过滤能力,或者能够阻止某些DDoS攻击的发生.

攻击者可以利用一些网络协议的漏洞发动攻击,以较小的攻击代价造成攻击目标无法承受的代价.最典型的协议攻击是TCP SYN Flood攻击和碎包攻击(fragmented packet).伪造源地址DDoS攻击是另一种利用协议漏洞攻击的例子,利用了当前网络无法验证源地址真实性的漏洞.研究者已提出了一些高安全性的协议,让客户端完成安全性测试或者身份验证后再提供服务[63],或者利用SYN Cookie[64],完成TCP连接后再提供服务.

如果能够鉴别数据包源地址的真伪,则能有效地控制伪造源地址这一类DDoS攻击,极大地提高网络的安全性.但当前,互联网的路由器并不能获得信息鉴别数据包源地址的真实性.SAVE(source address validaty enforcement procotol)协议通知路由器一个数据包的路径信息[65],路由器建立源地址簇对应的路由器接口信息表,验证源地址真实性.但是网络拥塞会导致数据包路径变更,如SAVE的接口信息表不能及时更新,必然会产生大量的误报.同时,SAVE方法会消耗路由器大量的计算能力,在网络负载较大时,会影响服务器对数据包的及时转发.

DDoS攻击源自于任何主机,可以在任何时候向任何目标发送数据,如果客户端必须获得其通信对象的许可,则可有效阻止DDoS攻击[66].服务器给许可客户端提供令牌,客户端在数据包中携带令牌,合法性验证节点分布在网络中,对流经自己的流量进行合法性识别,并丢弃非法流量.同时,服务器也可进行请求合法性验证.此方法可在网络骨干层对流量进行有效控制,避免了攻击终端计算能力有限的不足.

ITS(implicit token scheme)让数据包携带 Token 来鉴别数据包的真实性[67],Token 信息包含了数据包的部分信息,如源地址、TTL、IP 等,以及所经过的路由器信息.携带正确 Token 的数据包被转发到目标地址,而携带非法 Token 的数据包会被 Perimeter 路由器丢弃.ITS 对客户端透明,不需要修改现有协议,对路由器的计算开销不高,不会产生误报.

如何使合法用户在攻击者中还能获得较好的性能,是另一类 DDoS 攻击的处置思路[68].Rewire 是一种 Survive Overlay 类型的网络结构,能够检测网络状况,并基于应用层性能要求动态调整合法用户与服务器间的链路,保证服务器为合法用户提供高性能服务.Rewire 兼顾了链接性能、服务性能和灵活性,并且具有较低的计算复杂性.

总体而言,新的网络体系结构通过鉴定数据包的真伪(携带路径信息),或者让数据包携带真伪认证信息,或者给合法用户派发请求发送许可来实现对 DDoS 攻击流量过滤或攻击阻止.然而,网络系统结构往往不具有应对多种攻击的能力,如只能应对伪造地址攻击,并且,新型网络体系结构需要对现有网络进行较大的修改,ISP 需要进行较大的投入,同时,大量的通信协议、客户端和服务器端软件和系统都需要进行修改,因而,新的网络体系结构一直没有得到应用.此外,新型网络体系结构往往对骨干网路由器的计算能力要求较高,会进一步加重核心路由器的计算负担.

2 应用层 DDoS 攻击检测和控制

2.1 应用层DDoS攻击检测

与网络层 DDoS 攻击不同,应用层 DDoS 攻击在网络层表现正常,当前网络层 DDoS 攻击的检测方法不适用于应用层 DDoS 攻击,需要从应用层进行分析和检测.应用层 DDoS 攻击导致访问流量大幅度增加,与 Flash Crowd[69]极为相似,应用层 DDoS 攻击的检测研究主要是如何区分这两者.

Flash crowd 和应用层 DDoS 攻击具有如下几点不同[70]:

- 在 Flash Crowd 发生时,大量的地址 Cluster 重复出现,而 DDoS 攻击时,会出现大量新的地址 Cluster;
- 在 Flash Crowd 时,与正常访问相比,每个用户对应的请求数变小,而 DDoS 时则变大;
- Flash Crowd 的访问地址分布不均匀,而 DDoS 攻击时,访问地址分布比较均匀;
- 在文件请求方面,Flash Crowd 时被请求文件呈 Zipf-like 分布,而 DDoS 时则集中在少数文件.

基于 Document Populairty 来可区分应用层 DDoS 攻击和 Flash Crowd[71],Flash Crowd 对应的 Aggregate Access Behavior 熵无明显变化,而 DDoS 对应的熵值有较大下降.此外,概率测量的方法(variation metric 和 bheattacharyya metric)也可来区分 DDoS 攻击和 Flash Crowd[72].

2.2 应用层DDoS攻击控制

应用层 DDoS 攻击控制的研究主要集中在如何区分攻击流和正常流,主要分为基于测试的方法(测试客户端是否具有正常的行为能力)和基于行为模型的方法.

2.2.1 基于测试的识别方法

图灵测试[73]能够有效区分攻击者和正常访问者.由于合法用户能够正确地完成测试,而攻击主机不具备完成测试的能力,因而可以准确区分两者.但是,图灵测试往往会干扰访问者对服务器的正常访问.为了区分正常访问者和攻击 Robot,文献[74]也采用图灵测试方法,将行为探测程序传到客户端,分析是否有鼠标移动等正常用户行为;同时,分析用户的访问请求是否符合正常浏览的行为模式,判断是正常用户还是 Yu 在 CAT 方法的基础上[75]提出了一种抵御 DDoS 攻击的 Heimdall 结构,弥补了 CAT 方法对合法流量保护不够的不足,本质上仍然是一种图灵测试的方法.测试生成器部署于攻击目标上,攻击目标将生成的测试和测实验证结果发送到中间路由器.在接收到新连接请求后,中间路由器并不立即执行请求转发,而是给请求发起者发送测试,如果请求发起者能够完成测试,则视为正常访问,将连接请求转发给连接目标(攻击目标),未完成测试则不予转发.此方法同样大大增加了骨干路由器的计算负担,并且对服务器、路由器和客户端均需进行修改.

文献[76]提出一种 Speak-up 方法来抵御应用层 DdoS.与以往降低攻击流量或削弱攻击者行为能力的过滤方法相反,Speak-up 方法让所有客户端均提高发送速率.攻击者为了达到较好的攻击效果,通常采用尽最大能力发动攻击,并且会忽视攻击对象对发送速率的控制,所以能够增加发送速率的均为合法用户,通过此方法能够区别合法访问和攻击行为.

2.2.2 基于行为模型的识别方法

攻击流由固定的程序生成,与正常访问流相比,攻击流之间呈现明显的相似性[77],利用这一特点可实现对 DDoS 攻击流和 Flash crowd 流的区分.

基于请求的动态变化、请求的语义和是否具备对可视对象的处理能力这 3 个可用于区分正常访问行为和程序行为的特征[78],Oikonomou 等人构建了正常行为模型,用来区分攻击 Bot 和正常访问者.

Ranjan 等人根据 Session 的参数[79],包括 Session 建立速率、Requests 的请求速率和 Requests 请求对系统资源的消耗,把应用层 DDoS 攻击分为 Request flooding 攻击、asymmetric workload 攻击和 repeated one-shot 攻击.基于这 3 种攻击,提出了一种 Session 可疑度计算模型,依据 Session 可疑度大小进行请求转发.构建合法用户行为模型需要基于系统日志来获取请求对 CPU、带宽以及磁盘等资源的消耗,但系统日志并不易获得,并且在服务器进行更新后,无法及时获得新请求的资源消耗.

文献[80]结合多种异常检测技术可检测多种应用层攻击,如 SQL 注入、缓冲区溢出攻击等.该方法以服务器日志为输入,计算请求查询的异常指数.此方法针对查询进行研究,但没有针对应用层 DDoS 攻击进行检测;并且,以日志为输入进行分析,限制了该方法的应用范围.

Yu 等人结合 K-means Clutering 异常检测方法和 Offense 方法识别攻击端[81],并过滤应用层 DDoS 攻击,但该方法无法有效抵御慢速的应用层 DDoS 攻击.

Xie 等人提出了一种基于用户浏览行为的统计异常检测[82],根据 Web 页面的链接特性和各级 Cache 对用户请求的响应,采用了隐马尔可夫模型描述服务器端观察到的用户访问行为.如果一个用户的访问行为偏离了正常用户的行为特征,则认为此用户为攻击端.此方法的不足在于训练和计算过程比较繁琐,且计算复杂度较高.

肖军等人基于应用层 DDoS 攻击请求的生成方式[83],将应用层 DDoS 攻击分为 5 类,分析并比较了应用层 DDoS 攻击会话与正常访问会话的不同之处,提出了访问行为属性和会话异常度模型.基于异常度模型,能够有效识别应用层 DDoS 攻击会话,并分析了常见转发策略(FCFS、最小异常度优先和 Round Robin)与异常度模型结合时各自的转发性能.此方法能够在服务器外实现对应用层 DDoS 攻击会话的识别,且具有较低的计算开销.

3 控制策略比较和未来发展

3.1 不同部署位置控制策略分析比较

攻击源端控制是指在攻击源所在的子网内或者该子网接入的路由器进行流量控制.通常采用的方法有依据数据包的子网地址进行过滤(如果数据包源地址不属于本地网络,则边界路由器将进行丢弃),或者客户端在发送数据包前向一个认证服务器提交发送请求,只有获得许可的客户端才能发送数据包.攻击源端控制的优点在于,能够最大限度地降低攻击危害,在攻击数据包进入骨干网前就可以进行控制;同时,可利用的计算资源足够多.其不足在于需要边界路由器的配合,由于 ISP 无法从对攻击的控制中获益,攻击源端控制往往无法实施;同时,对复杂攻击的检测和控制效果不佳.

网络骨干层控制是指在检测出突发流量后,由骨干层路由器或专门的流量清洗中心对流量进行限制、过滤和清洗,能在攻击流量到达攻击目标前实现对流量的过滤.有如下几类方法:

- 被攻击端将流量调控信息发送给骨干路由器,骨干路由器对流量作限制.此方法能够有效降低服务器的负载,其不足在于,无法区分攻击流量和合法流量,无法有效保护合法流量.
- 基于清洗中心的策略则是在检测到攻击发生后,由骨干路由器将流量注入清洗中心,在过滤后,将清洗过的流量回注进网络.此方法过滤策略比较灵活,且能够处理较大的攻击流量,其不足在于实现机制比较复杂.

- 另一类控制方法是 pushback 策略,在检测出攻击后,靠近攻击目标的路由器向上游路由器发出流量控制信息,上游路由器对流量进行控制,最后在靠近攻击源端进行流量限制.

由于检测准确和便于部署等优势,攻击终端控制最常见.现有的网络安全设备和机制大都属于攻击终端控制,如防火墙、Syn Cokie 等.攻击终端控制能够实现较复杂的控制机制,但由于攻击者可利用的计算资源远远大于攻击目标能利用的计算资源,并且攻击规模较大时,攻击过滤设备往往成为被攻击的目标,丧失对目标服务器的保护能力,因而攻击终端控制通常不具备对大规模攻击的有效控制能力.

表 1 为 3 种部署位置控制策略的比较.

Table 1 Comparison between control mechanisms of different positions

表 1 不同位置控制策略的比较

	攻击源端	骨干层过滤	攻击终端过滤
检测灵敏度	低	中等	高
部署难度	难以广泛部署	难度高,费用高	易于部署
优点	能有效抵御伪造源地址攻击,能最早控制攻击	能处理各种攻击,且有足够的计算能力	灵活,过滤性能好
不足	难以广泛部署,不能有效处理真实地址 DDoS 攻击	需要 ISP 配合	处理能力有限

可以看出,攻击源端控制方式通常仅对伪造源地址 DDoS 攻击有较好的防御效果,无法应对当前众多的攻击方式.同时,由于部署者无法获益而无法得到广泛的部署.攻击终端控制方式由于相对较低的开销、高检测灵敏度和灵活的处理策略,虽然受到处理能力的限制,仍然是主要的部署方式.骨干层过滤方法具有较强的控制能力,可以处理各类攻击,但是控制粒度往往较低,不能完成细粒度控制,且大大增加了骨干层路由器的计算负担;此外,还需要 ISP 的配合才能得以实施.

3.2 当前现状、未来发展趋势和技术挑战

3.2.1 当前现状

快速发展的网络技术、不断扩大的网络规模和不断增加的操作系统漏洞使得僵尸网络的规模不断扩大,如 conficker 僵尸网络的主机规模已达到了千万级,相应地,攻击者可轻易发动攻击流量达数 10G 的 DDoS 攻击.如此大规模的攻击流量对 DDoS 过滤设备的安全性、实时处理能力和可扩展性提出了更高的要求.此外,shrew DDoS 攻击和应用层 DDoS 攻击技术的兴起大大增加了攻击过滤的难度,对流量剥离技术提出了严峻的挑战.

在攻击检测方面,由于攻击流量汇聚,攻击末端检测具有最好的检测精度,并且检测延迟最小;攻击源端和骨干层检测往往只能通过流量变化进行,误报率高.除了基于单一数据来源的检测手段以外,部分研究者也关注融合多数据来源的检测方法,如 Choi 等人提出的一种 DDoS 防御模型[84],通过多种信息的融合检测 DDoS 攻击,如 C&C 服务器信息、边界路由器信息、骨干网信息、僵尸网络通信信息等,但该工作未对多种信息的融合方法做详细介绍.

在攻击过滤方面,当前主流的攻击目标端控制策略受限于可利用的计算能力限制,已无法满足大规模 DDoS 攻击过滤的要求.攻击端控制策略主要受限于攻击类型,对真实地址攻击往往不具有较好的过滤效果.骨干层过滤主要问题在于过滤精度低,通常不对攻击包和合法包作区分;此外,骨干层过滤策略也大大增加了骨干路由器的计算负担.新型网络体系结构需要对现有网络进行较大的修改,ISP 需要进行较大的投入.同时,大量的通信协议、客户端和服务器端软件都需要相应地进行修改,因而难以推广.

3.2.2 未来发展趋势和技术挑战

未来的 DDoS 控制需兼顾检测灵敏度、过滤准确性、大流量处理能力等多方面的因素.

接入端的安全设备由于计算能力的限制,不能有效处理大流量的 DDoS 攻击,可在骨干层部署 DDoS 过滤设备.虽然骨干路由器具有较高的计算能力,但其优势在于数据包转发和流量控制,不宜执行较繁琐的流量过滤.可采用流量清洗中心策略,在不同的 ISP 内部署流量清洗中心,在攻击发生时,骨干路由器进行分光,将流量注入流量清洗中心进行清洗,在清洗完成后进行回注.

在攻击检测方面,由于攻击流量的汇聚,与攻击源端和网络骨干层检测相比,攻击末端检测具有最高的灵敏度.可以在信息系统部署的安全设备中增加攻击检测和报警功能,在检测到流量变化或者访问行为异常后,向部署于骨干层的 DDoS 过滤系统发出报警,由 DDoS 过滤系统进行攻击类型识别、攻击流量注入、攻击流量过滤和攻击流量回注.此外,大量的信息系统或者中小网站并没有部署防火墙等网络安全设备,因此,DDoS 攻击过滤系统可以在骨干层进行 DDoS 攻击检测,在发现 DDoS 攻击后再确定攻击目标.

在应用前景方面,上述策略无须对现有网络结构进行大幅度修改,DDoS 攻击过滤系统对网络用户透明,网络用户无须对现有的协议和应用程序进行修改;此外,ISP 可将 DDoS 攻击检测和攻击流量过滤以安全服务的形式提供给信息系统、门户网站,当前已有 ISP 开始规划、构建并部署这样的过滤系统.

构建上述 DDoS 控制系统,主要面临如下技术挑战:

1) DDoS 攻击类型识别技术.当前已有的 DDoS 检测和过滤往往针对某一具体攻击类型,如 Syn flood 等,在 DDoS 攻击类型识别方面的研究较少.
2) 流量清洗系统.首先,流量清洗系统应具备高速流量采集功能,能够实时捕获骨干路由器分光的流量;此外,流量清洗系统应处理各种类型 DDoS 攻击的能力,能够有效清洗各种类型的攻击流量.如何有效融合多个过滤模块,与流量清洗系统的处理性能紧密相关.
3) 骨干大流中无检测目标的 DDoS 攻击检测.无安全设备的信息系统无法及时上报攻击信息,通过骨干网流量变化发现 DDoS 攻击,是解决无固定检测目标 DDoS 过滤的前提;在检测到 DDoS 攻击后,通过骨干层流量分布变化发现 DDoS 攻击目标,是无目标 DDoS 攻击过滤的另一个重要问题.
4) 攻击流识别技术.精确过滤攻击流量的前提是对攻击流的准确辨别.随着攻击手段的不断提高,攻击流识别的难度越来越大,简单地依赖包速率、包数等指标识别攻击流具有较大的识别误差,需研究新的攻击流识别方法.

4 结束语

提高计算机用户的安全意识,是抵御 DDoS 攻击的最简便有效的方法.及时弥补操作系统漏洞,更新网络安全设备和软件,能够有效地检测恶意软件、降低操作系统被感染的几率,进而减小 DDoS 攻击发生的规模.

DDoS 攻击是当前互联网安全的最重要威胁之一,但是大量的研究并没有产生行之有效的控制措施.本文将 DDoS 攻击分为网络层 DDoS 攻击和应用层 DDoS 攻击.在此基础上介绍了这两类 DDoS 攻击的检测和控制方法.分析了各类 DDoS 攻击控制的不足之处,并分析了当前 DDoS 攻击防御现状,提出了过滤系统未来的发展趋势和相关的技术挑战.期望能够推动国内对这一问题的关注和认识.

References:

[1] http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html
[2] http://www.highbeam.com/doc/1P2-25571545.html
[3] http://www.wired.com/dangerroom/2009/06/activists-launch-hack-attacks-on-tehran-regime/
[4] http://www.0577s.com/News/NewsShow-4071.html
[5] http://net.chinabyte.com/519DNS/
[6] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 2004,34(2):39−54. [doi: 10.1145/997150.997156]
[7] http://news.netcraft.com/archives/2004/09/16/latest_mydoom_ddos_targets_symantec.html
[8] Luo H, Hu G, Yao X. DDoS attack detection based on global network properties of network traffic anomaly. Computer Applications, 2007,27(2):314−317 (in Chinese with English abstract).
[9] Chen Y, Hwang K. Collaborative change detection of DDoS attacks on community and ISP networks. In: Proc. of the IEEE Int'l Symp. on Collaborative Technologies and Systems (Special Sessions on Collaboration Grids and Community Networks). Las Vegas, 2006. 401−410. [doi: 10.1109/CTS.2006.27]

[10] Zhuang X, Lu K, Wang L, Lu J, Li O. A detecting method of DDoS attacks based on traffic statistics. Computer Engineering, 2004, 30(22):127−129 (in Chinese with English abstract).

[11] Yuan J, Mills K. Monitoring the macroscopic effect of DDoS flooding attacks. IEEE Trans. on Dependable and Secure Computing, 2005,2(4):324−335. [doi: 10.1109/TDSC.2005.50]

[12] Sekar V, Duffield N, Merwe JVD, Zhang H. LADS: Large-scale automated DDoS detection system. In: Proc. of the USENIX Annual Technical Conf. Santa Clara, 2006. 171−184.

[13] Chen Y, Hwang K, Kwok Y. Collaborative defense against periodic shrew DDoS attacks in frequency domain. http://gridsec.usc.edu/files/TR/ACMTISSEC-LowRateAttack-May3-05.pdf

[14] Sun H, Lui JCS, Yau DKY. Defending against low-rate TCP attacks: Dynamic detection and protection. In: Proc. of the 12th IEEE Int'l Conf. on Network Protocols. Berlin, 2004. 196−205.

[15] Gil TM, Poletto M. MULTOPS: A data-structure for bandwidth attack detection. In: Proc. of the 10th Usenix Security Symp. Washington, 2001. http://thomer.com/mit/multops_usenix2001.pdf

[16] Wang H, Zhang D, Shin KG. Detecting SYN flooding attacks. In: Proc. of the IEEE Infocom. New York, 2002. http://www.cs.wm.edu/~hnw/paper/attack.pdf [doi: 10.1007/ 11599463_44]

[17] Wang H, Zhang D, Shin KG. Change-Point monitoring for the detection of DoS attacks. IEEE Trans. on Dependable and Secure Computing, 2004,1(4):193−208. [doi: 10.1109/TDSC.2004.34]

[18] Moore D, Shannon C, Brown DJ, Voelker GM, Savage S. Inferring Internet denial-of-service activity. ACM Trans. on Computer System, 2006,24(2):115−139. [doi: 10.1145/1132026.1132027]

[19] Haggerty J, Berry T, Shi Q, Merabti M. DiDDeM: A system for early detection of TCP SYN flood attacks. In: Proc. of the IEEE Globecom. Dallas, 2004. 2037−2042. [doi: 10.1109/INFCOMW.2009.5072099]

[20] Peng T, Leckie C, Ramamohanarao K. Proactively detecting distributed denail of service attacks using source IP address monitoring. In: Proc. of the 3th Int'l IFIP-TC6 Networking Conf. LNCS 3042, Athens, 2004. 771−782. [doi: 10.1007/978-3-540-24693-0_63]

[21] Peng T, Leckie C, Ramamohanarao K. Detecting distributed denial of service attacks by sharing distributed beliefs. In: Proc. of the 8th Australasian Conf. on Information Security and Privacy. LNCS 2727, Wollongong, 2003. 214−225.

[22] Ehrlich WK, Futamura K, Liu D. An entropy based method to detect spoofed denial of service (DoS) attacks. Telecommunications Modeling, Policy, and Technology (Operations Research/Computer Scicence Interfaces Series), 2008,44:101−122. [doi: 10.1007/978-0-387-77780-1_6]

[23] Wang Z, Wang X. DDoS attack detection algorithm based on the correlation of IP address analysis. In: Proc. of the 2011 Int'l Conf. on Electrical and Control Engineering (ICECE). Yichang, 2011. 2951−1954. [doi: 10.1109/ICECENG.2011.6057035]

[24] Feinstein L, Schnackenberg D, Balupari R, Kindred D. Statistical approaches to DDoS attack detection and response. In: Proc. of the DARPA Information Survivability Conf. and Exposition. Washington, 2003. 303−314.

[25] Lakhina A, Crovella M, Diot C. Mining anomalies using traffic feature distributions. In: Proc. of the ACM SIGCOMM. Philadelphia, 2005. 217−228. [doi: 10.1145/1080091.1080118]

[26] Kumar K, Joshi RC, Singh K. A distributed approach using entropy to detect DDoS attacks in ISP domain. In: Proc. of the Int'l Conf. on Signal Proceeding, Communications and Networking (ICSCN). Chennai, 2007. 331−337. [doi: 10.1109/ICSCN.2007.350758]

[27] Mahajan R, Bellovin SM, Floyd S, Ioannidis J, Paxson V, Shenker S. Controlling high bandwidth aggregates in the network. ACM Computer Communication Review, 2002,32(3):62−73. [doi: 10.1145/571697.571724]

[28] Vijayasarathy R, Raghavan S, Ravindran B. A system approach to network modeling for DDoS detection using a naïve Bayesian classifier. In: Proc. of the 3th Int'l Conf. on Communication Systems and Networks (COMSNETS). Bangalore, 2011. 1−10. [doi: 10.1145/571697.571724]

[29] Liu H, Sun Y, Valgenti V, Kim M, TrustGuard: A flow-level reputation-based DDoS defence system. In: Proc. of the 2011 IEEE Consumer Communications and Networking Conf. (CCNC). Las Vegas, 2011. 287−291. [doi: 10.1109/CCNC.2011.5766474]

[30] Sun H, Fang B, Zhang H. DDoS attacks detection based on link character. Journal of Communications, 2007,28(2):88−93 (in Chinese with English abstract).

[31] Xiao B, Chen W, He Y, Sha EH. An active detecting method against SYN flooding attack. In: Proc. of the 11th IEEE Int'l Conf. on Parallel and Distributed Systems. Fukuoka, 2005. 709−715. [doi: 10.1109/ICPADS.2005.67]

[32] Chen W, Yeung DY. Defending against TCP SYN flooding attacks under different types of IP spoofing. In: Proc. of the Int'l Conf. on Networking, Systems, Mobile Communications and Learning Technologies. Washington, 2006. 38.

[33] Gu R, Yan P, Zou T, Yang J. An adaptive Internet backbone traffic anomalies detection algorithm based on frequent pattern mining. Computer Science, 2006,33(9):76−80 (in Chinese with English abstract).

[34] Weiler N. Honeypots for distributed denial of service attacks. In: Proc. of the 11th IEEE Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Pittsburgh, 2002. 109−114.

[35] Cheng CM, Kung HT, Tan KS. Use of spectral analysis in defense against DoS attacks. In: Proc. of the IEEE Globecom. Taipei, 2002. 2143−2148.

[36] Yu S, Zhou W, Doss R. Information theory based detection against network behavior mimicking DDoS attacks. IEEE Communications Letters, 2008,12(4):319−321.

[37] Mirković J, Prier G, Reiher P. Attacking DDoS at the source. In: Proc. of the 10th Int'l Conf. on Network Protocols (ICNP). Paris, 2002. 312−321.

[38] Mirković J. D-WARD: Souce-end defense against distributed denial-of-service attacks [Ph.D Thesis]. Los Angeles: University of California Los Angeles, 2003.

[39] Yaar A, Perrig A, Song D. Pi: A path identification mechanism to defend against DDoS attacks. In: Proc. of the IEEE Symp. Security and Privacy. Oakland, 2003. 93−107. [doi: 10.1007/978-3-540-30582-8_84]

[40] Yaar A, Perrig A, Song D. Stackpi: New packet marking and filtering mechanism for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communications, 2006,24(10):1853−1863. [doi: 10.1109/JSAC.2006.877138]

[41] Yau DKY, Lui CS, Liang F, Yam Y. Defending against distributed denial-of-service attacks with man-min fair server-centric router throttles. IEEE/ACM Trans. on Networking, 2005,13(1):29−42. [doi: 10.1109/TNET.2004.842221]

[42] Zhang G, Parashar M. Cooperative defense against DDoS attacks. Journal of Research and Practice in Information Technology, 2006,38(1):69−84.

[43] Kim Y, Lau WC, Chuah MC, Chao HJ. Packetscore: Statistics-Based overload control against distributed denial-of-service attacks. In: Proc. of the IEEE INFOCOM. Hong Kong, 2004. 2594–2604. [doi: 10.1109/INFCOM.2004.1354679]

[44] Park K, Lee H. On the effective of router-based packet filtering for distributed DoS attack prevention in power-law Internets. In: Proc. of the SIGCOMM. San Diego, 2001. 15–26. [doi: 10.1145/964723.383061]

[45] Stavrou A, Keromytis AD. Countering DoS attacks with stateless MultiPath overlays. In: Proc. of the ACM CCS. Alexandria, 2005. 249–259.

[46] Agarwal S, Dawson T, Tryfonas C. DDoS mitigation via regional cleaning centers. Sprint ATL Research Report, RR04-ATL-013177, Berkeley: University of California, 2004. [doi: 10.1145/1102120.1102153]

[47] Xiong Y, Liu S, Sun P. On the defense of the distributed denial of service attacks: An on-off feedback control approach. IEEE Trans. on System, Man and Cybernetics, 2001,31(4):282−293. [doi: 10.1109/3468.935045]

[48] Sun Z, Tang Y, Zhang W, Gong J, Wang R. A router anomaly traffic filter algorithm based on character aggregation. Journal of Software, 2006,17(2):295−304 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/295.htm [doi: 10.1360/jos170295]

[49] Burch H, Cheswick B. Tracing anonymous packets to their approximate source. In: Proc. of the 14th USENIX Conf. on System Administration. New Orleans, 2000. 878−886. http://static.usenix.org/event/lisa2000/burch/burch_html/

[50] Song DX, Perrig A. Advanced and authenticated marking schemes for IP traceback. In: Proc. of the IEEE INFOCOM. Anchorage, 2001. 878−886. [doi: 10.1109/INFCOM.2001.916279]

[51] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer WT. Hash-Based IP traceback. In: Proc. of the 2001 Conf. on Applications, Technologies, Architectures and Protocols for Computer Communication. San Diego, 2001. http://www.cs.cmu.edu/~srini/15-744/papers/p1-snoeren.pdf [doi: 10.1145/383059.383060]

[52] Yu S, Zhou W, Doss R, Jia W. Traceback of DDoS attacks using entropy variations. IEEE Trans. on Parallel and Distributed Systems, 2011,22(3):412−425.

[53] Ioannidis J, Bellovin SM. Implementing Pushback: Router-Based Defense Against DDoS Attacks. AT&T Labs Research, 2001.

[54] Peng T, Leckie C, Ramamohanarao K. Defending against distributed denial of service attacks using selective pushback. In: Proc. of the 9th IEEE Int'l Conf. on Telecommunications. Beijing, 2002. 411−429.

[55] Kargl F, Maier J, Weber M. Protecting Web servers from distributed denial of service attacks. In: Proc. of the 10th World Wide Web. Hong Kong, 2001. http://wwwconference.org/www10/cdrom/papers/pdf/p409.pdf [doi: 10.1145/371920.372148]

[56] Xu J, Lee W. Sustaining availability of Web services under distributed denial of service attacks. IEEE Trans. on Computer, 2003, 52(2):195−208. [doi: 10.1109/TC.2003.1176986]

[57] Jin C, Wang H, Shin KG. Hop-Count filtering: An effective defense against spoofed traffic. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington, 2003. http://www.eecs.umich.edu/techreports/cse/2003/CSE-TR-473-03.pdf [doi: 10.1145/948109.948116]

[58] Guirgues M, Bestavros A, Matta I. On the impact of low-rate attacks. In: Proc. of the IEEE Int'l Conf. on Communication. Istanbul, 2006. 2316−2321.

[59] Chen Y, Kwok YK, Hwang K. Filtering shrew DDoS attacks using a new frequency-domain approach. In: Proc. of the 1st IEEE Workshop on Network Security. Sydney, 2005. http://gridsec.usc.edu/files/TR/WoNS-2005.pdf

[60] Gao Z, Ansari N. Differentiating malicious DDoS attack traffic from normal TCP flows by proactive tests. IEEE Communications Letters, 2006,10(11):793−795.

[61] Peng T, Leckie C, Ramamohanarao K. Protection from distributed denial of service attacks using history-based IP filtering. In: Proc. of the IEEE Int'l Conf. on Communication. Anchorage, 2003. 482−486.

[62] Serwadda A, Phoha V, Rai I. Size-Based scheduling: A recipe for DDoS? In: Proc. of the 17th ACM Conf. on Computer and Communications Security (CCS). New York, 2010. 729−731.

[63] Leiwo J, Nikander P, Aura T. Towards network denial of service resistant protocols. In: Proc. of the 15th Int'l Informational Security Conf. Australia, 2000. 301−310.

[64] Bernstein DJ. Syn cookie. http://cr.yp.to/syncookies.html

[65] Li J, Mirkovic J, Wang M, Reiher P, Zhang L. SAVE: Source address validity enforcement protocol. In: Proc. of the IEEE INFOCOM. New York, 2002. http://lasr.cs.ucla.edu/save/save_to_infocom.pdf

[66] Anderson T, Roscoe T, Wetherall D. Preventing Internet denial-of-service with capabilities. SIGCOMM Computer Communication Review, 2004,34(1):39−44. [doi: 10.1145/972374.972382]

[67] Farhat H. Protecting TCP services from denial of service attacks. In: Proc. of the ACM SIGCOMM Workshops. Pisa, 2006. 155−160. [doi: 10.1145/1162666.1162674]

[68] Bu T, Norden S, Woo T. A survivable DoS-resistant overlay network. Computer Networks: The Int'l Journal of Computer and Telecommunications Networking, 2006,50(9):1281−1301. [doi: 10.1016/j.comnet.2005.06.010]

[69] Chen X, Heidemann J. Flash crowd mitigation via adaptive admission control based on application-level observations. ACM Trans. on Internet Technology, 2005,5(3):532−569. [doi: 10.1145/1084772.1084776]

[70] Jung J, Krishnamurthy B, Rabinovich M. Flash crowds and denial of service attacks: Characterization and implications for CDNs and Web sites. In: Proc. of the 11th IEEE Int'l World Wide Web Conf. Honolulu, 2002. 293−304. [doi: 10.1145/511446.511485]

[71] Xie Y, Yu S. Monitoring the application-layer DDoS attacks for popular Websites. IEEE/ACM Trans. on Networking, 2009,17(1): 15−25. [doi: 10.1109/TNET.2008.925628]

[72] Li K, Zhou W, Li P, Hai J, Liu J. Distinguishing DDoS attacks from flash crowds using probability metrics. In: Proc. of the 3th Int'l Conf. on Network and System Security. Gold Coast, 2009. 9−17. [doi: 10.1109/NSS.2009.35]

[73] Kandula S, Katabi D, Jacob M, Berger A. Botz-4-Scale: Surviving organized DDoS attacks that mimic flash crowds. In: Proc. of the 2nd Conf. on Symp. on Networked Systems Design and Implementation. Kyoto, 2005. 287−300.

[74] Park K, Pai V, Lee K, Calo S. Securing Web service by automatic robot detection. In: Proc. of the Annual Conf. on USENIX 2006 Annual Technical Conf. Boston, 2006. 255−260.

[75] Chen Y, Ku W, Sakai K, Decruze C. A novel DDoS attack defending framework with minimized bilateral damages. In: Proc. of the 7th IEEE Conf. on Consumer Communications and Networking Conf. (CCNC). Piscataway, 2010. 1−5.

[76] Walfish M, Vutukuru M, Balakrishnan H, Karger D, Shenker S. DDoS defense by offense. In: Proc. of the Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications. Pisa: ACM Press, 2006. 303−314. [doi: 10.1145/1151659.1159948]

[77] Yu S, Thapngam T, Liu J, Wei S, Zhou W. Discriminating DDoS flows from flash crowds using information distance. In: Proc. of the 3th Int'l Conf. on Network and System Security. Gold Coast, 2009. 351−356.

[78] Oikonomou G, Mirkovic J. Modeling human behavior for defense against flash-crowd attacks. In: Proc. of the IEEE Int'l Conf. on Communications. Dresden, 2009. 625−630.

[79] Ranjan S, Swaminathan R, Uysal M, Knightly E. DDoS-Shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Trans. on Networking, 2009,17(1):26−39. [doi: 10.1109/TNET.2008.926503]

[80] Kruegel C, Vigna G. Anomaly detection of Web-based attacks. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington, 2003. 251−261. [doi: 10.1145/948109.948144]

[81] Yu J, Chen H, Chen X. A detection and offense mechanism to defense against application layer DDoS attacks. In: Proc. of the 3th Int'l Conf. on Networking and Services. 2007. 251−261. [doi: 10.1109/ICNS.2007.5]

[82] Xie Y, Yu S. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors. IEEE/ACM Trans. on Networking, 2009,17(1):54−65. [doi: 10.1109/TNET.2008.923716]

[83] Xiao J, Yun XC, Zhang YZ. Defend against application-layer distributed denial-of-service attacks based on session suspicion probability model. Chinese Journal of Computers, 2010,33(9):1713−1724 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.01713]

[84] Choi Y, Oh J, Jang J, Ryou J. Integrated DDoS attack defense infrastructure for effective attack prevention. In: Proc. of the 2nd Int'l Conf. on Information Technology Convergence and Services (ITCS). Cebu, 2010. [doi: 10.1109/ITCS.2010.5581263]

附中文参考文献:

[8] 罗华,胡光岷,姚兴苗.基于网络全局流量异常特征的 DDoS 攻击检测.计算机应用,2007,27(2):314−317.

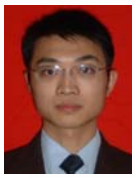
[10] 庄肖斌,芦康军,王理,芦建芝,李鸥.一种基于流量统计的 DDoS 攻击检测方法.计算机工程,2004,30(22):127−129.

[30] 孙红杰,方斌兴,张宏莉.基于链路特征的 DDoS 攻击检测方法.通信学报,2007,28(2):88−93.

[33] 顾荣杰,晏蒲柳,邹涛,杨剑锋.基于频繁模式挖掘的 Internet 骨干网攻击发现方法研究.计算机科学,2006,33(9):76−80.

[48] 孙知信,唐益慰,张伟,官婧,王汝传.基于特征聚类的路由器异常流量过滤算法.软件学报,2006,17(2):295−304. http://www.jos.org.cn/1000-9825/17/295.htm [doi: 10.1360/jos170295]

[83] 肖军,云晓春,张永铮.基于会话异常度模型的应用层分布式拒绝服务攻击过滤.计算机学报,2010,33(9):1713−1724. [doi: 10.3724/SP.J.1016.2010.01713]



张永铮(1978－),男,黑龙江哈尔滨人,博士,副研究员,CCF 会员,主要研究领域为网络安全.

云晓春(1971－),男,博士,教授,博士生导师,主要研究领域为网络安全,互联网建模.

肖军(1979－),男,博士,助理研究员,主要研究领域为 DDoS 攻击检测和过滤.

王风宇(1973－),男,博士,副教授,CCF 会员,主要研究领域为网络安全,网络行为分析.