软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2013,24(6):1263−1273 [doi: 10.3724/SP.J.1001.2013.04274]

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

# 一种基于 Web 群体外联行为的应用层 DDoS 检测方法*

王风宇[1], 曹首峰[2], 肖 军[3], 云晓春[2,3], 龚 斌[1]

[1](山东大学 计算机科学与技术学院,山东 济南 250101)

[2](国家计算机网络应急技术处理协调中心,北京 100029)

[3](中国科学院 信息工程研究所,北京 100029)

通讯作者: 王风宇, E-mail: wangfengyu@sdu.edu.cn

**摘 要**: 由于攻击者采用各种技术手段隐藏攻击行为,DDoS 攻击变得越发难以发现,应用层 DDoS 成为 Web 服务器所面临的最主要威胁之一.从通信群体的层面分析 Web 通信的外联行为特征的稳定性,并提出了一种应用层 DDoS 检测方法.该方法用 CUSUM 算法检测 Web 群体外联行为参数的偏移,据此来判断 DDoS 攻击行为的发生.由于外联行为模型刻画的是 Web 通信群体与外界的交互,并非用户个体行为,所以攻击者难以通过模仿正常访问行为规避检测.该方法不仅能够发现用户群体访问行为的异常,而且能够有效区分突发访问和应用层 DDoS 攻击.模拟实验结果表明,该方法能够有效检测针对 Web 服务器的不同类型的 DDoS 攻击.

**关键词**: 应用层 DDoS;Web 群体;外联行为;CUSUM

**中图法分类号**: TP309 **文献标识码**: A

中文引用格式: 王风宇,曹首峰,肖军,云晓春,龚斌.一种基于 Web 群体外联行为的应用层 DDoS 检测方法.软件学报,2013,24(6):1263−1273. http://www.jos.org.cn/1000-9825/4274.htm

英文引用格式: Wang FY, Cao SF, Xiao J, Yun XC, Gong B. Method of detecting application-layer DDoS based on the out-linking behavior of Web community. Ruan Jian Xue Bao/Journal of Software, 2013,24(6):1263−1273 (in Chinese). http://www.jos.org.cn/1000-9825/4274.htm

## Method of Detecting Application-Layer DDoS Based on the Out-Linking Behavior of Web Community

WANG Feng-Yu[1], CAO Shou-Feng[2], XIAO Jun[3], YUN Xiao-Chun[2,3], GONG Bin[1]

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

[2](The National Computer Network Emergency Response Technical Team Coordination Center of China, Beijing 100029, China)

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

Corresponding author: WANG Feng-Yu, E-mail: wangfengyu@sdu.edu.cn

**Abstract**: Distributed denial of service (DDoS) attacks have become more and more difficult to detect due to various hiding techniques that have been adopted. Application-Layer the DDoS attack is becoming a major threat to the current network. This paper analyzes the stability of out-linking behavior on the level of Web community and proposes an approach for detecting application-layer DDoS aimed at Web server. CUSUM is used to detect the offset of out-linking parameters and determine the attack occurring. Rather than the individual behavior, out-linking parameters are about the group behavior of Web community, so it is difficult to circumvent detecting by simulating normal accesses. This approach can not only detect the anomaly of accessing behavior, but can also distinguish flash crowd and application-layer DDoS. The results of simulated experiments show that this approach can detect various types of DDoS attacks aiming at Web servers effectively.

**Key words**: application-layer DDoS; Web community; out-linking behavior; CUSUM

* 基金项目: 国家自然科学基金(60803142); 山东省科技攻关计划(2010GGX10117)
收稿时间: 2011-06-02; 定稿时间: 2012-05-29

Web 服务是互联网中最广泛的应用类型,然而,由于其重要的社会和商业价值,Web 服务器同时也成为互联网中最主要的被攻击目标.分布式拒绝服务攻击(distributed denial-of-service attack,简称 DDoS)是 Web 服务器所面临的最重要的威胁之一,DDoS 攻击是指攻击者通过傀儡主机发送大量请求,消耗攻击目标的资源,阻止目标为合法用户提供服务.可消耗的资源可以是 CPU、内存、带宽、数据库服务器等.近年来,针对 Web 服务的 DDoS 攻击可谓层出不穷[1−4],Amazon,Yahoo 和 Baidu 等国内外著名网站都曾受到 DDoS 攻击,造成了重大的经济损失.

DDoS 攻击技术的发展可以简单地归结为两个阶段.早期的 DDoS 攻击方式属于网络层攻击,以消耗攻击目标的带宽资源为目标,如 ICMP Flooding 和 SYN Flooding 等.针对网络层 DDoS 攻击的检测和控制进行了很多研究[5],已经能够有效地对其加以控制.然而,为了规避不断完善的 DDoS 检测和控制技术,达到理想的攻击效果,攻击者也不断改进其攻击技术,采用更加复杂的攻击方式.随着 Internet 应用的复杂度和系统带宽的不断提高,CPU、I/O 带宽、数据库带宽等应用资源取代网络资源成为 Web 服务新的瓶颈.因此,在网络层 DDoS 攻击难以奏效的情况下,攻击者逐渐将目标从网络带宽转向了服务器计算资源,从而出现了应用层 DDoS 攻击.通过建立正常连接,向目标服务器提交大量合法服务请求,应用层 DDoS 攻击能够大量消耗服务器计算资源以阻塞正常访问,如 HTTP Flooding.由于攻击端与被攻击目标建立正常 TCP 连接,并发送表面上合法的请求,传统的网络层 DDoS 攻击检测方法不再适用.目前,研究人员主要从两个层面检测应用层 DDoS 攻击.大部分研究从访问数据流层面进行观察,即分析 Web 服务器日志或用户请求报文序列,建立正常用户访问行为模型,从而发现攻击异常[6−8]或识别出偏离正常行为的访问数据流[9−14].由于需要对报文载荷或者 Web 服务日志进行深度分析,所以计算负担较重.另外,有的研究人员从主机行为测试的角度进行研究,即根据客户端对测试的反应来判断该客户端是否攻击傀儡机[15,16],由于需要对所有客户端发送测试请求,处理负担重,且会对客户端造成干扰.

对于 DDoS 这种大规模网络攻击,如果能在主干网络对其进行及时检测和控制,可以避免攻击对基础网络带宽的冲击,从而有效降低负面影响.然而,当前的应用层 DDoS 攻击检测方法的复杂度高且需要细节数据,只适合于部署在被攻击端.因此,本文以设计一种可部署于骨干网络的应用层 DDoS 攻击检测方法为目标.在主干网络检测应用层 DDoS 攻击主要面临两方面的挑战:一,投入大量计算资源对 Web 通信应用层数据进行解析不可行;二,互联网采用动态路由策略,同一用户的访问数据可能经过不同的路径,这导致在一个监测点不能观察到完整的通信数据.因此,需要开辟新的途径研究应用层 DDoS 攻击检测方法.通过对主干网络数据集的分析发现,访问 Web 服务器的部分用户同时也会和其他计算机通信,而且对于特定 Web 服务器,其用户群体的外联行为表现出了较强的稳定性.本文以 Web 通信群体的外联行为特征为基础,利用 CUSUM 方法检测外联特征参数的异常变化,能够及时发现应用层 DDoS 攻击并准确将其与 Flash Crowd 进行区分.

本文第 1 节介绍相关技术研究.第 2 节给出 Web 通信群体提取方法及相关定义,并分析 Web 通信群体的外联特征.第 3 节分析不同形式的 DDoS 攻击对外联行为参数的影响,提出一种基于 Web 通信群体外联特征的 DDoS 检测方法.第 4 节通过模拟实验对检测方法进行评估.第 5 节分析该检测方法的特点,并和相关检测方法进行比较.最后一节对全文进行总结.

## 1 相关研究

在网络层 DDoS 攻击难以达到效果的情况下,应用层 DDoS 攻击成为近年来攻击者常用的手段,给 Web 服务构成了极大威胁.应用层 DDoS 攻击提交的是表面合法的应用请求,虽然会导致访问流量或用户数量大幅度增加,但又与 Flash Crowd 极为相似.因此,原来的基于网络层或传输层特征的检测方法在对付应用层 DDoS 攻击方面显得无能为力,如何阻截应用层 DDoS 攻击成为近年来网络安全领域新的研究热点.

攻击检测是对抗应用层 DDoS 的第 1 步,应用层 DDoS 攻击检测的一个难点在于区分 DDoS 和 Flash Crowd,当前,检测应用层 DDoS 的主要途径是利用访问数据聚合特征的偏移.Jung 等人[6]深入分析了应用层 DDoS 和 Flash Crowd 的区别: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.Xie 等人[7]基于 Document Popularity 来区分应用层 DDoS 攻击和 Flash Crowd,Flash Crowd 对应的聚合访问行为的熵不会产生明显变化,而在 DDoS 攻击下聚合访问行为的熵会有较大下降.Li 等人[8]则用混合测度(total variation 和 Bhattacharyya 系数相结合)来检测流分布的偏移,从而区分 DDoS 攻击和 Flash Crowd 访问.

在检测的基础上,需要识别出攻击端或攻击流,并对其访问数据加以控制.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.Yu 等人[9]利用这一特点,用 Sibson 距离来测量流之间的相似程度,实现对 DDoS 攻击流和 Flash Crowd 流的区分.基于请求的动态变化、请求的语义和具备对可视对象处理能力这 3 个正常访问的特征,Oikonomou 等人[10]构建了正常行为模型,用来区分攻击傀儡机和正常访问者.Ranjan 等人[11]根据 session 的参数,包括 session 建立速率、请求的速率和请求消耗,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,并依据 session 可疑度进行请求转发.Yu 等人[12]结合 *K*-means Clustering 异常检测方法和 Offense 方法识别攻击端,但无法有效抵御慢速的应用层 DDoS 攻击.Xie 等人[13]提出了一种基于用户浏览行为的统计异常检测,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.肖军等人[14]基于应用层 DDoS 攻击请求的生成方式,提出了访问行为属性和会话异常度模型,以识别应用层 DDoS 攻击会话.这一类方法根据用户访问行为的统计特征来识别 DDoS 攻击流,需要深入分析系统日志或报文载荷,从数据获取和计算复杂度的角度来考虑,只适合部署于被攻击端网络.

识别应用层 DDoS 攻击流的另一途径则是利用主机对测试的反应.为了区分正常访问者和攻击傀儡机,Park 等人[15]采用图灵测试,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傀儡机.Walfish 等人[16]提出了一种 Speak-up 方法来抵御应用层 DDoS,与以往减慢或削弱攻击者的过滤方法相反,Speak-up 方法让所有客户端提高发送速率,但攻击者为了达到较好的攻击效果,通常采取尽最大能力攻击原则,在攻击开始时就会采用最大发送速率,所以增加发送速率的均为合法用户,因此能够识别合法流量.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,所以主机测试方法可以准确地区分两者,但同时,也往往会干扰访问者对服务器的正常访问.

## 2 Web 通信群体外联特征分析

### 2.1 相关定义

互联网中每一个用户会根据其兴趣爱好或使用目的的不同加入(或被加入)不同的通信群体.通信群体指的是相互通信关系密切且具有相同的负载特征的一组主机的集合.Web 服务器和访问该服务器的客户端共同构成一个 Web 通信群体.部分客户端在访问 Web 服务器的同时,会与 Web 通信群体之外的主机节点通信,我们把这些外部主机节点称做外联节点,客户端和外联节点之间的连接称做外联.我们进一步把外联节点分为多外联节点和单外联节点,如果有多个 Web 客户端连接到某外联节点,那么该节点是该 Web 群体的多外联节点,这类节点通常包括由同一网站的其他服务器、关联密切的其他网站;如果只有一个 Web 客户端连接到某外联节点,那么该节点是该 Web 群体的单外联节点,通常由用户的个体访问行为产生.

### 2.2 Web通信群体外联行为测量

从主干网络的海量通信数据中测量 Web 通信群体,是我们首先面对的问题.由于 Web 通信群体在较高的层次上进行聚合,可以以较低的计算和存储代价把相关数据提取并表达出来.当出现目的地址为指定 Web 服务器 IP 地址且目的端口为 80 的 SYN 报文时,为该 Web 服务器增加一个客户端,该客户端和该 Web 服务器的后续通信报文不再记录.如果发现报文的源地址或目的地址属于某 Web 服务器的客户端,而通信另一方不是该 Web 服务器,则增加一条外联边,属于该外联边的后续报文亦不再记录.图 1 是从 CAIDA-OC48[17]数据集中随机选取的一个小型 Web 通信群体的联通图,测量时间段长度为 1 分钟,该图用 Graphviz[18]生成.Web 通信群体联通图是一

个无向图,图中连接最多的核心点是Web服务器,圆点表示连接到Web服务器的客户端,圆环表示客户端外联的主机,相同IP地址的主机不会在图中重复出现.

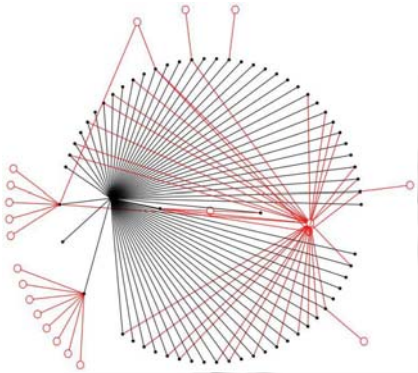


Fig.1 Link graph of Web community

图1 Web 通信群体联通图

### 2.3 外联行为特征分析

我们基于两个不同来源的网络数据集进行分析:一个是CAIDA-OC48[17],2003年4月24日采集于美国某大型ISP的OC48链路,共1小时的数据;一个是WIDE-TRANSIT[19],2009年3月29日采集于日本一条150Mbps跨太平洋主干链路,每个报文截取前96字节,共24小时的数据.

对于规模较大的Web通信群体,外联现象是普遍存在的.我们从两个数据集中分别抽取了10个在1分钟时间段中客户端数量大于50的Web通信群体,统计了其中的客户端数量CN、与单外联节点连接的客户端数量*CN_SLN*、与多外联节点连接的客户端数量*CN_MLN*,见表1.统计结果表明,从主干网络层面观察,外联行为是热点Web通信群体中较为普遍存在的一种现象,基于外联特征检测DDoS攻击适用于大部分Web服务器.外联通信的产生有多种原因,主要有:

a) 规模较大的网站都会根据内容或负载将网页分布在不同的服务器和虚拟机,这就导致主页的链接或者内嵌对象指向了网站的其他IP地址;

b) 大多数主页都有指向其他网站的链接,例如广告链接或者引用链接;

c) 用户在浏览网页的同时也在进行其他网络通信活动,例如浏览主页的同时在进行P2P下载.

特定Web服务器的用户群体的访问行为具有统计意义上的稳定性:一方面,对于特定网站,用户群相对稳定,大部分用户浏览行为具有一定的相似性;另一方面,网站服务器设定是相对固定的,网站内容的分布也相对稳定.当然,从骨干网络层面观察到的用户行为也存在一些不确定性,网络中的各级代理(proxy)、用户浏览器的高速缓存会对用户的HTTP请求做出响应,在骨干网络层面可能观察不到用户的完整浏览行为,但这里我们关注的是Web群体的统计行为,并非个体用户的准确行为,Web代理和缓存的影响已经被计入其中,不会对我们的检测策略造成影响.

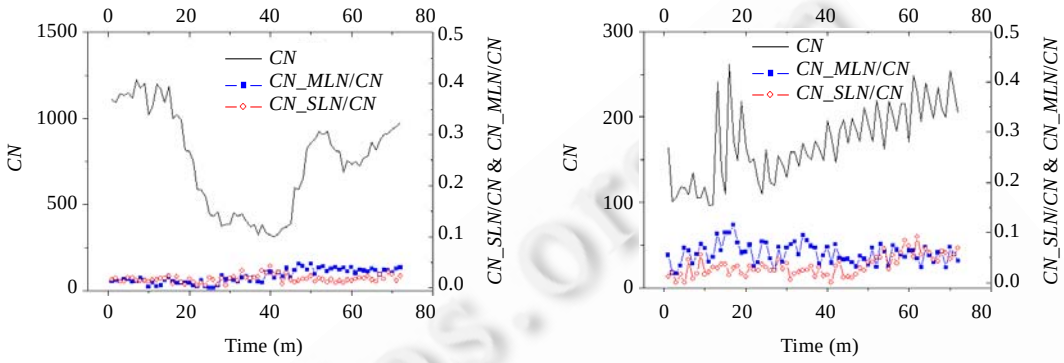
**Table 1** Out-Link statistics of Web community

**表1** Web群体外联统计

| 数据集 | *CN* (max/min/avg) | *CN_SLN* (max/min/avg) | *CN_MLN* (max/min/avg) |
|---|---|---|---|
| CAIDA-OC48 | 806/88/320 | 156/47/93 | 52/5/18 |
| WIDE-TRANSIT | 1110/60/343 | 262/2/58 | 50/3/12 |

下面我们就从上述角度对Web群体的外联行为进行统计,观察其稳定性.样本数据取自于WIDE-TRANSIT数据集,从2009年3月30日0点开始到3月30日24点一天的时间,每小时截取一组15分钟的数据,并以5分钟为时间段提取客户端数量超过50的Web通信群体.我们从中随机选取了两个Web通信群体*Server-A*和

*Server-B*,统计了其中的客户端数量 *CN*、与单外联节点连接的客户端数量 *CN_SLN* 以及与多外联节点连接的客户端数量 *CN_MLN*.图 2 是两个通信群体中 *CN*,*CN_MLN*/*CN* 和 *CN_SLN*/*CN* 随着时间的变化曲线.可以看出,虽然客户端数量随着时间有较大的变化,但与多外联节点连接的客户端比例、与单外联节点连接的客户端比例都相对稳定,没有随着客户端数量的波动而产生相应的变化.




(a) *Server-A* (b) *Server-B*

Fig.2 Stability of out-linking behavior

图 2 外联行为的稳定性

## 3 DDoS 攻击检测方法

### 3.1 DDoS攻击与外联行为的相关性

为了选定有效的行为特征参数和检测方法,我们先对常见的应用层 DDoS 攻击形式进行分析,找出其在 Web 通信群体的外联特征上的体现.为了规避攻击检测,应用层 Web DDoS 攻击采用了不同的攻击形式.肖军等人[14]对应用层 DDoS 攻击进行了分类.依据攻击主机提交请求的真实性,把应用层 DDoS 攻击分为真实 URL 请求攻击和伪造 URL 请求攻击(forged URL flood).真实 URL 攻击请求可进一步分为重复使用单一 URL 请求(single URL flood)攻击、重复使用多个 URL 请求(multi-URL flood)攻击、基于页面链接随机选择 URL 请求(random URL flood)攻击以及为了更好地隐藏攻击者,利用已有合法 session 的请求,按照 session 中各个请求的间隔时间和请求顺序反复提交请求(session flood)进行攻击.

无论攻击者采用哪种 DDoS 攻击形式,一般都是以固定的 Web 服务器 IP 地址为目标.因此,傀儡主机在攻击过程中的通信数据由两部分组成:向目标主机发送的攻击报文,傀儡主机的真正用户的个体访问行为.而用户的个体访问行为通常能够形成单外联节点,很少会构成 Web 群体的多外联节点.因此,当攻击发生时,Web 群体的客户端数量会大量增加,与单外联节点连接的客户端数量近似于按比例增加,而与多外联节点连接的客户端数量却基本不会增加.用序列$\{x_n\}$表示不同时间段内访问多外联节点的客户端数量与客户端总数的比值,$\{C_n\}$表示客户端总数,$\{M_n\}$表示访问多外联节点的客户端数量,假设从 $n$+1 时段发生了攻击,攻击端数量为 $S_{n+1}$,正常客户端数量为 $R_{n+1}$ 则有

$$x_n = \frac{M_n}{C_n} \tag{1}$$

$$x_{n+1} = \frac{M_{n+1}}{C_{n+1}} = \frac{M_{n+1}}{R_{n+1} + S_{n+1}} \tag{2}$$

当然,我们也不能排除有的攻击者为了更好地模仿正常访问行为而保留了部分外联访问请求.这类访问行为除了导致 Web 群体客户端数量大幅增加,也会显著增加访问多外联节点的客户端的数量,用 $L$ 表示访问多外联节点的攻击端的数量,则有

$$x_{n+1}=\frac{M_{n+1}+L_{n+1}}{R_{n+1}+S_{n+1}} \tag{3}$$

理论上,访问多外联节点的客户端数量与客户端总数的比值变化是不确定的,受到攻击端外联访问行为的发生频率和测量的时间间隔等因素的影响,但实际过程中,测量时间段的长度通常足以使客户端的外联访问行为在每个时间段内出现,即访问多外联节点的客户端比例显著增大.

然而,如果由于某些原因恰巧出现 $L/S$ 近似于 $M/R$ 的情况,则序列$\{x_n\}$在发生攻击的情况下不会发生偏移,也就无法检测 DDoS 攻击,发生漏判.理论上,这种情况出现的概率近似为 $1/C_n$,即正常客户端的数量越大,未发生偏移的概率越小.更进一步,我们可以转而采用更细粒度的行为参数,用序列$\{x_{k,n}\}$表示 $n$ 时段第 $k$ 个多外联节点的客户端的数量与客户端总数的比值,即

$$x_{k,n}=\frac{M_{k,n}}{C_n},k=1,2,3,...,n=1,2,3\ldots \tag{4}$$

统计表明,该序列同样具有相对稳定性,我们可以根据 Web 服务的规模选择 $m$ 个序列进行统计观察,只要有一个序列发生明显偏移,就可以判断攻击的发生.此时,在发生攻击的情况下,$m$ 个序列均没有偏移发生的概率大幅降低,近似为

$$F=\frac{1}{(C_n)^m},m=1,2,3,...,n=1,2,3... \tag{5}$$

对于大规模 Web 服务,这种检测方案可以使漏判的概率达到很低的水平.另外,外联行为数据需要在主干网络或边界网络测量,而且在主干网的不同位置测得的数据也会有所不同.因此,在攻击大型网站时,攻击者试图通过模仿外联访问行为隐藏攻击是相当困难的.无论从多外联节点的个体层面进行检测,还是从多外联节点的总体层面进行检测,其原理是一样的,因此,本文后面部分只从多外联节点的总体层面进行分析和实验.

应用层 DDoS 检测的一个关键问题是能够区分应用层 DDoS 与突发访问(flash crowd).突发访问是由大量正常用户集中访问产生的,同样会产生用户数量突然大量增加的现象,但与 DDoS 攻击不同,突发访问中大量增加的用户伴随着正常比例的外联访问行为,因此公式(1)中的$\{x_n\}$不会出现异常变化.以图 2(a)为例,在 40 分钟~50 分钟这段时间,用户数量增加了 1 倍多,但外联行为比例 $CN\_MLN/CN$ 序列表现平稳,即$\{x_n\}$没有发生异常变化.

综合以上分析,我们可以分别检测序列(公式(6))的向上偏移,$\{x_n\}$的向上偏移表示有带有外联访问行为的攻击发生,$\{y_n\}$向上偏移则可能发生了无外联访问或外联访问比例很低的 DDoS 攻击.

$$x_n=\frac{M_n}{C_n},y_n=\frac{C_n}{M_n},n=1,2,3... \tag{6}$$

### 3.2 CUSUM算法

CUSUM 算法属于变化点检测方法中的序贯检测法,可以检测到一个统计过程均值的变化.CUSUM 算法基于这一事实:如果有变化发生,随机序列的概率分布也会改变.由于因特网是一个动态变化的复杂实体,所以我们选择非参数 CUSUM 算法进行检测.该算法与具体的网络业务模型无关,能够适用于不同的网络场景,在以往的攻击检测方法中多有采用且取得了较好的效果[20−23].

设 $x_1,x_2,\ldots,x_t$ 为独立的 $N(0,1)$同分布,$x_{t+1},x_{t+2},x_{t+3}$ 为独立的 $N(\delta,1)$同分布(其中,$t$+1 是未知变点),对于给定检测时序 $x_1,x_2,\ldots,x_n$,令 $v=t+1(v<n)$,假设 $t=\infty$的对数似然统计量为

$$A_n=\max_{1\leqslant v\leqslant n}A_{n,v}=\max\left\{\delta\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right)\right\} \tag{7}$$

如果我们检测的为向上偏移,即$\delta>0$,则上述对数似然统计量等价于

$$Z_n=\max_{1\leqslant v\leqslant n}\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right) \tag{8}$$

为便于计算,降低在线检测的开销,我们使用非参数 CUSUM 算法的递推公式(其中,用不定参数 $k$ 代替$\delta/2$):

$$Z_n=\max\{0,Z_{n-1}+x_n-k\},n=1,2,3,\ldots \quad (9)$$

如果事先选择一个阈值 $h>0,Z_{n-1}\leqslant h$ 说明前 $n-1$ 个检测值的均值没有发生偏移,检测对象为正常状态.若某个 $Z_n>h$,则检测对象发生了异常.

### 3.3 基于CUSUM的DDoS攻击判定

前面我们分析了 Web 通信群体的外联行为特征以及 DDoS 攻击在外联特征上的表现.特定 Web 通信群体中,与多外联节点连接的客户端数量 $M$ 与客户端总数 $C$ 的比值序列$\{x_n=M_n/C_n\}$和$\{y_n=C_n/M_n\}$可以作为我们进行 DDoS 攻击检测的依据.无论攻击者采用哪一种应用层 DDoS 攻击形式,其中一个比值会显著增长,可以用 CUSUM 算法进行检测.

对于 DDoS 攻击检测,误报率和检测时间是两个主要的性能衡量标准,需要尽可能降低误报率并缩短检测时间,但这两个目标又是冲突的,需要在它们之间进行折衷.由前面分析可知,非参数 CUSUM 算法中可以通过选择参数 $k$ 和 $h$ 实现误报率和检测时间之间的平衡.选择的 $k$ 越大,在$\{Z_n\}$中出现正值的可能性就越小,因而累积到一个较大的值来发现攻击的可能性越小.$h$ 是攻击门限,$h$ 越大,误报率越低,但检测时间越长.为了更好地适应网络环境的复杂性和动态性,我们采用文献[21]中提出的一种改进的 CUSUM 算法,向上偏移的递推公式为

$$Z_n=\max\{0,Z_{n-1}+x_n-\delta_n-d\},n=1,2,3,\ldots \quad (10)$$

其中,$\delta_n$ 为$\{x_n\}$的指数加权移动平均 EWMA,$d$ 是使 $Z_n$ 在正常情况下小于 0 的偏移值,$\delta_n$ 的计算方法如下:

$$\delta_n=(1-\alpha)\delta_{n-1}+\alpha x_n,\delta_0=x_0 \quad (11)$$

为了既能适应网络的动态变化,又不会导致漏报率的提高,EWMA 系数$\alpha$的取值较小,范围为 0.01~0.03.根据攻击导致$\{x_n\}$的抖动情况,可以设定

$$d=\mu\delta_n,h=\lambda\delta_n \quad (12)$$

式中的参数$\mu$可以通过实际数据的统计获得;而参数$\lambda$值的确定则稍微复杂,不同的攻击会导致特征值的不同程度的偏移,$\lambda$的值取决于用户对误报率的容忍范围,以及用户期望的检测时间.如果令$\lambda$=2,则可以在不多于 4 个时间间隔内检测到偏移程度达到均值的 50%以上的攻击,而在不多于 20 个时间段内检测到偏移程度达到均值的 10%以上的攻击.由于 Web 业务量随着时间的变化而变化,所以需要系统能够根据参数$\mu$和$\lambda$实时地得到适合当前业务量的 $h$ 和 $d$.

## 4 实验评估

为了验证检测算法,我们用网络数据集进行了模拟实验.模拟数据由背景数据和攻击数据组成.从 CAIDA-OC48[17]数据集中截取 2004 年 4 月 24 日 0 点 0 分起共 15 分钟的数据,并从中选择客户端数量较多的 Web 服务器(20 秒内客户端数量超过 20)作为备用攻击目标.原始数据作为背景数据,攻击数据则由大量傀儡机按照指定的攻击模式生成,并混杂到背景数据中.

根据文献[14]对应用层 DDoS 攻击的分类和我们的检测方法的特点,实验中采用了几种代表性的攻击模式,见表 2.单个傀儡机采用两种发送攻击报文的速度,其中,快速发送的速率为 10pps,常速发送的速率则按照报文的原始时间间隔发送.*A* 模式循环发送固定的请求,*B* 模式则在 *A* 模式的基础上按一定比例插入了外联请求.在构造 *C* 和 *D* 模式的攻击数据时,从原始数据中选择一个被攻击 Web 服务器的客户端,截取一段请求报文序列(包含一个完整 session),*C* 模式删除其中夹杂的外联访问请求,而 *D* 模式中则按比例保留其中的部分外联请求.每个傀儡机都按照指定的模式和速度发送预先设定的报文.

**Table 2** Attack mode

**表 2** 攻击模式

| 攻击模式 | 构成 | 发送速度 | 外联 |
|---|---|---|---|
| *A* | 1 request | Rapid | No |
| *B* | *n* requests | Rapid | 1 in *n* |
| *C* | 1 session (*n* requests) | Normal | Deleted |
| *D* | 1 session (*n* requests) | Normal | Reserved |

前面的分析表明,影响检测效果的主要因素有两个:在一个检测时间段内出现傀儡机的数量 $S$ 和有外联行为傀儡机的比例$\omega$.其中,$S$ 受到傀儡机的总数和攻击报文发送速度两个因素的影响,$\omega$会受攻击报文发送速度和攻击报文中外联报文的比例的影响.前面已经设定了快速发送和常速发送两种速度模式,因此我们把参与攻击的傀儡机的总数 $N$ 和外联报文的比例$\sigma$作为评估我们的检测方法有效性的参数.

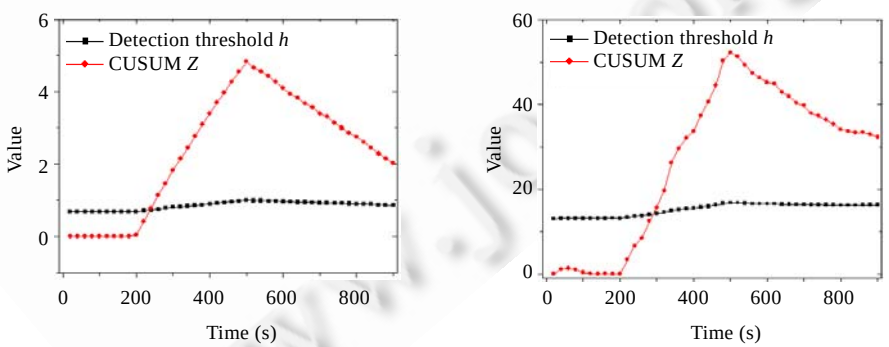
首先,我们观察傀儡机的数量对检测效果的影响.$B$ 模式的外联比例设定为 1/20;$C$ 模式则选择一个客户端,从它发向 Web 服务器的请求中截取一个报文序列;$D$ 模式则在 $C$ 模式的基础上保留其间少量外联请求,外联比例亦设定为 1/20.攻击端在第 200 秒开始发起攻击,持续 5 分钟,按照 $A$,$B$,$C$,$D$ 这 4 种模式向 Web 服务器发起攻击.傀儡机数量分别设定为 100,200,400 和 800,每次选用一种攻击模式攻击一台 Web 服务器.实验中,根据不同服务器的特征值序列确定$\delta_0$和$\mu$的值,$\lambda$则统一设定为 3,检测时间段长度为 20 秒.表 3 是选取 5 台 Web 服务器的平均检测结果,其中,检测时间是指从攻击开始到发现攻击所用的时间段的个数(未检测到的情况按攻击持续时间计,本实验中为 15 个时间段).其中,用 100 台傀儡机以 $A$ 模式和 $B$ 模式发起的攻击未能被检测到,其他攻击均在 5 分钟的攻击期间被检测到,在攻击强度(傀儡机数量)较小时,$A$ 和 $C$ 模式攻击的检测时间有所延后.

**Table 3** Detection performance and number of attack slaves

**表 3** 傀儡机数量与检测性能

| 攻击节点数 | 检测概率 (%) | | | | 检测时间 (时间段数量) | | | |
|---|---|---|---|---|---|---|---|---|
| | *A* | *B* | *C* | *D* | *A* | *B* | *C* | *D* |
| 100 | 80 | 100 | 80 | 100 | 8.7 | 1 | 8.7 | 1 |
| 200 | 100 | 100 | 100 | 100 | 5.6 | 1 | 5.6 | 1 |
| 400 | 100 | 100 | 100 | 100 | 3.5 | 1 | 3.5 | 1 |
| 800 | 100 | 100 | 100 | 100 | 2.2 | 1 | 2.2 | 1 |

同时,为了验证采用的 CUSUM 算法的有效性,我们给出了部分检测过程中$\{Z_n\}$的变化.图 3(a)是 200 台傀儡机用 $D$ 模式对某 Web 服务器进行攻击的检测结果,其中,$\{Z_n\}$是序列$\{x_n\}$的 CUSUM 累积和.图 3(b)是 200 台傀儡机用 $A$ 模式对某 Web 服务器进行攻击的检测结果,其中,$\{Z_n\}$是序列$\{y_n\}$的 CUSUM 累积和.图中同时给出了检测门限 $h$ 的变化曲线.同样的攻击强度(傀儡机数量)下,$D$ 模式导致特征值产生较大程度的偏移,在一个时间段内就检测到了攻击;而 $A$ 模式下傀儡机数量相对于客户端总数相对较小,因此特征值相对于均值偏移较少,用了多个时间段才检测到.




(a) $D$ 攻击模式 (b) $A$ 攻击模式

Fig.3 Sensitivity of attack detection

图 3 攻击检测灵敏度

其次,我们观察外联请求比例对检测效果的影响.前面的分析表明,有外联行为的傀儡机的比例越接近正常用户的比例,攻击检测越困难.我们选择了两个 Web 通信群体进行实验.为了方便地控制攻击参数,这里采用 $B$ 攻击模式,傀儡机的数量设定为 200,攻击持续时间仍然是 5 分钟,检测时间段长度是 20 秒.实验中,攻击数据设定不同的外联请求比例,图 4 是检测时间与攻击数据外联访问比例的关系,横轴为 $\log(1/\sigma)$,$\sigma$为外联比例;纵轴为

检测到异常所用的时间段的数量.在曲线上升阶段,是用$\{x_n\}$序列检测到异常;在曲线下降阶段,是用$\{y_n\}$序列检测到异常.可以看到,对于每台 Web 服务器,都有一段非敏感区域,需要较多时间段才能检测到,甚至在限定的 20 个时间段内检测不到攻击,发生漏报.这是由于在一个检测时间段内,傀儡机中发生外联行为的比例和背景数据中的比例相近,特征值序列偏移较小.在前面,我们已经针对这种情况进行了分析,并指出,通过对多个多外联节点分别进行单点检测,可以有效地避免这种漏报的发生.

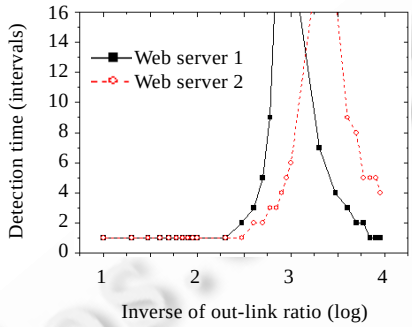



Fig.4 Detection time vs. ratio of out-linking packet

图 4 检测时间与外联报文比例的关系

## 5 讨论与比较

从网络层行为观察不到异常行为,而从应用层进行行为观察又要付出较重的计算代价,这造成了应用层 DDoS 攻击检测和控制研究中难以调和的矛盾.当前的网络流量监控和攻击检测多从 3 个层面进行观察:报文(packet)层、流(flow)层和主机(host)层.随着研究的深入,这 3 个层面特征的描述能力渐渐地难以满足需求.以往主要的应用层 DDoS 攻击检测和过滤方法都是聚焦于流层面的行为,如文献[6−14]所提出的方法,要解决矛盾需要从新的层面进行观察.本文创新性地从 Web 通信群体的层面进行观察,根据 Web 群体行为的偏离推断应用层 DDoS 攻击的发生.与以往的工作相比,本文是在一个更高的层面上进行行为观察,好处是:1) 数据聚合程度高,处理复杂度大幅度降低;2) 行为模型涉及范围扩大,通过模仿正常行为规避检测的难度加大.近年来,已经有研究者从通信群体的层面进行了网络流量研究.Aiello 等人[24]从兴趣群体(community of interesting,简称 COI)的层面进行观察,分析了不同应用类型的兴趣群体在大小和构成方面的稳定性.Iliofotou 等人[25]提出了用流量分散图 TDG(traffic dispersion graphs)来描述主机在网络范围的互动行为,即通信群体行为,并基于 TDG 进行了 P2P 流量的识别和分类[26].与本文的工作不同,以往在通信群体层面的研究多从特征分析的角度进行研究,尚未应用于攻击检测.

本文工作中采用了 CUSUM 算法来检测行为参数的偏移.作为一种有效的变异点检测算法,CUSUM 在网络攻击检测中被广泛采用.文献[20]用 CUSUM 算法检测 SYN 报文和 FIN 报文比例的偏离,并据此判断 DDoS 攻击的发生;文献[21]用改进的 CUSUM 算法 M-CUSUM 对路由器输入/输出端口流量的绝对差与和之比进行统计,实时地监控其均值的偏移情况;文献[22]中则监测未确认的报文段个数与总报文段个数的比值,并用 CUSUM 算法判断 DDoS 攻击的发生;文献[23]用非参数 CUSUM 算法监测网络流量的异常变化.以往的工作主要是以流量的变化或协议比例的变化为依据检测网络层 DDoS 攻击.虽然同样采用了 CUSUM 算法来检测变异点,但本文是以 Web 群体外联行为特征为依据检测应用层 DDoS 攻击,所依据的特征不同,目标也不同.之所以选择了 CUSUM 算法,是因为该算法既可以及时发现参数的突变,也能够通过累积发现渐变过程,可以很好地满足对外联参数监测的需求.

## 6 总 结

应用层 DDoS 攻击采用的是表面合法的请求,且容易与 Flash Crowd 混淆,因此是近期网络安全检测中的难点之一.不同于以往的研究,本文从通信群体外联行为的层面研究检测 Web DDoS 攻击的方法.通过对公开的网络数据集的分析,发现了 Web 通信群体的外联行为的普遍性以及外联客户端数量与客户端总数之间的相关性,并分析了不同形式的 DDoS 攻击在 Web 通信群体外联行为特征上的体现.在特征分析的基础上,我们进一步采用 CUSUM 算法检测特征值序列的偏移,从而判断攻击的发生.

利用模拟产生的网络攻击流量,我们对该 DDoS 检测方法进行了评估.根据 DDoS 攻击的分类,设计了 4 种不同的攻击模式,该检测方法在不同的攻击模式下均表现出了较好的检测性能,能够在较短的时间内检测到不同形式 DDoS 攻击的发生.同时,我们还通过变换外联报文的比例分析了算法所存在的盲区,并给出了有效的解决办法,即对多个多外联节点同时进行单点检测.该检测方法的优点在于不需要对报文载荷进行分析,只需要构造出 Web 群体联通图即可.与以往方法不同,该检测方法适合于在主干网络进行检测,可以及早对攻击加以遏制,降低攻击对基础网络所造成的冲击;而不能部署于被攻击端网络出入口,因为这里已经不能观测到通信群体的外联行为.

**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] 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]

[6] 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. 2002. [doi: 10.1145/511446.511485]

[7] Xie Y, Yu SZ. 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]

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

[9] Yu S, Thapngam T, Liu JW, Wei S, Zhou WL. Discriminating DDoS flows from flash crowds using information distance. In: Proc. of the 3th Int'l Conf. on Network and System Security. 2009. [doi: 10.1109/NSS.2009.29]

[10] Oikonomou G, Mirkovic J. Modeling human behavior for defense against flash-crowd attacks. In: Proc. of the IEEE Int'l Conf. on Communications. 2009. [doi: 10.1109/ICC.2009.5199191]

[11] Ranjan S, Swaminathan R, Uysal M, Nucci A, 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]

[12] Yu J, Li ZJ, Chen HW, Chen XM. A detection and offense mechanism to defend against application layer DDoS attacks. In: Proc. of the 3th Int'l Conf. on Networking and Services. 2007. [doi: 10.1109/ICNS.2007.5]

[13] Xie Y, Yu SZ. 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]

[14] 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):1−12 (in Chinese with English abstract).

[15] Park KS, Pai VS, Lee KW, Calo S. Securing Web service by automatic robot detection. In: Proc. of the Annual Conf. on USENIX 2006 Annual Technical Conf. 2006.

[16] 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. [doi: 10.1145/1159913.1159948]

[17] Shannon C, Aben E, Claffy KC, Andersen D, Brownlee N. The CAIDA OC48 traces dataset—<Apr 24, 2003>. 2011. http://www.caida.org/data/passive/passive_oc48_dataset.xml

[18] GraphViz. 2011. http://www.graphviz.org/

[19] WIDE-TRANSIT. 2011. http://mawi.wide.ad.jp/mawi/

[20] Wang HN, Zhang DL, Shin KG. Detecting SYN flooding attacks. In: Proc. of the IEEE Infocom 2002. 2002. [doi: 10.1109/INFCOM.2002.1019404]

[21] Sun ZX, Tang YW, Cheng Y. Router anomaly traffic detection based on modified-CUSUM algorithms. Ruan Jian Xue Bao/Journal of Software, 2005,16(12):2117−2123 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/2117.htm [doi: 10.1360/jos162117]

[22] Yan F, Chen YQ, Huang H, Yin XC. Detecting DDoS attack based on compensation non-parameter CUSUM algorithm. Journal of Communication, 2008,29(6):126−132 (in Chinese with English abstract).

[23] Lin B, Li O, Liu QW. DDoS attacks detection based on sequential change detection. Computer Engineering, 2005,31(9):135−137 (in Chinese with English abstract).

[24] Aiello W, Kalmanek C, McDaniel P, Sen S, Spatscheck O, Van der Merwe J. Analysis of communities of interest in data networks. In: Proc. of the Passive and Active Network Measurement Workshop 2005. LNCS 3431, Berlin: Springer-Verlag, 2005. [doi: 10.1007/978-3-540-31966-5_7]

[25] Iliofotou M, Pappu P, Faloutsoset M, Mitzenmacher M, Singh S, Varghese G. Network monitoring using traffic dispersion graphs (tdgs). In: Proc. of the 7th ACM SIGCOMM Conf. on Internet Measurement. 2007. [doi: 10.1145/1298306.1298349]

[26] Iliofotou M, Kim HC, Faloutsos M, Mitzenmacher M, Pappu P, Varghese G. Graph-Based P2P traffic classification at the Internet backbone. In: Proc. of the 28th IEEE Int'l Conf. on Computer Communications Workshops. 2009. [doi: 10.1109/INFCOMW.2009.5072151]

**附中文参考文献:**

[14] 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):1−12.

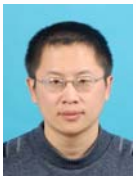
[21] 孙知信,唐益慰,程媛.基于改进 CUSUM 算法的路由器异常流量检测.软件学报,2005,16(12):2117−2123. http://www.jos.org.cn/1000-9825/16/2117.htm [doi: 10.1360/jos162117]

[22] 严芬,陈轶群,黄皓,殷新春.使用补偿非参数 CUSUM 方法检测 DDoS 攻击.通信学报,2008,29(6):126−132

[23] 林白,李鸥,刘庆卫.基于序贯变化检测的 DDoS 攻击检测方法.计算机工程,2005,31(9):135−137.

**王风宇**(1973－),男,山东龙口人,博士,副教授,CCF 会员,主要研究领域为网络安全,网络行为学.
E-mail: wangfengyu@sdu.edu.cn

**云晓春**(1971－),男,博士,教授,博士生导师,CCF 会员,主要研究领域为网络安全,互联网建模.
E-mail: yxc@hit.edu.cn



**曹首峰**(1980－),男,博士,主要研究领域为计算机网络信息安全.
E-mail: csf@cert.org.cn

**龚斌**(1964－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为高性能计算.
E-mail: gb@sdu.edu.cn

**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.
E-mail: xiaojun@iie.ac.cn