软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(5):1272−1280 [doi: 10.3724/SP.J.1001.2012.04068]

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

基于大偏差统计模型的 Http-Flood DDoS 检测机制及性能分析*

王 进[1,3], 阳小龙[1,2+], 隆克平[1,2]

[1](电子科技大学 光互联网及移动信息网络研究中心,四川 成都 611731)

[2](北京科技大学 计算机与通信工程学院,北京 100083)

[3](成都大学 网络中心,四川 成都 610106)

Http-Flood DDoS Detection Scheme Based on Large Deviation and Performance Analysis

WANG Jin[1,3], YANG Xiao-Long[1,2+], LONG Ke-Ping[1,2]

[1](Research Center for Optical Internet and Mobile Information Network, University of Electronic Science and Technology of China, Chengdu 611731, China)

[2](School of Computer and Communications Engineering, University of Science and Technology Beijing, Beijing 100083, China)

[3](Network Center, Chengdu University, Chengdu 610106, China)

+ Corresponding author: E-mail: yxl@uestc.edu.cn, http://www.uestc.edu.cn

Wang J, Yang XL, Long KP. Http-Flood DDoS detection scheme based on large deviation and performance analysis. *Journal of Software*, 2012,23(5):1272−1280. http://www.jos.org.cn/1000-9825/4068.htm

Abstract: This paper focuses on Http-Flood DDoS (distributed denial of service) attack and proposes a detection scheme based on large deviation statistical model. The detection scheme characterizes the user access behavior with its Web-pages accessed and adopts the type method quantizing user's access behavior. Based on this quantization method, this study analyzes the deviation of ongoing user's empirical access behavior from the website's priori one with large deviation statistical model, and detects Http-Flood DDoS with large deviation probability. This paper also provides preliminary simulation regarding the efficiency of the scheme, and the simulation results show that the large deviation of most normal Web surfers is larger than 10^{-36}, yet, the attacker's is smaller than 10^{-40}. Thus, this scheme is promising to detect Http-Flood DDoS. Specifically, the scheme can achieve 0.6% false positive and 97.5% true positive with detection threshold of 10^{-60}. And compared with the existing detection methods, this detection scheme can outperform them in detection performance. In particular, this scheme can improve the true positive ratio 0.6% over the transition probability based detection scheme with the false positive below 5%.

Key words: IP network; distributed denial of service (DDoS); large deviation

摘 要: 针对 Http 洪泛 Web DDoS(distributed denial of service)攻击,提出了一种检测机制.该机制首先采用型方法量化处理用户访问的网页序列,以得到用户访问不同网页的实际点击概率分布;然后,利用大偏差统计模型分析了用户访问行为的实际点击概率分布与网站先验概率分布的偏差;最后,依据大偏差概率检测恶意 DDoS 攻击.对该机制的性能进行仿真,结果表明,正常用户的大偏差概率大于恶意攻击者,并且大部分正常用户的大偏差概率大于 10^{-36},

* 基金项目: 国家重点基础研究发展计划(973)(2012CB315905); 国家自然科学基金(60873263, 60932005, 61172048, 61100184); 教育部新世纪优秀人才计划(NCET-09-0268); 四川省青年科技基金(09ZQ026-032); 成都市科技局项目; 成都大学校基金(2010XJZ35)

收稿时间: 2011-04-13; 定稿时间: 2011-06-20

而大部分恶意攻击者的大偏差概率则小于 10^{-40}.由此,该机制能够有效地检测 Http 洪泛 Web DDoS 攻击,当检测门限设置为 10^{-60} 时,其有效检测率可达 97.5%,而误检率仅为 0.6%.另外,将该机制与基于网页转移概率的检测方法进行性能比较,结果表明,该检测机制的检测率优于基于网页专业概率的检测机制,并且在误检率小于 5%的情况下,该机制的检测率比现有检测机制提高 0.6%.

关键词: IP 网络;分布式拒绝服务;大偏差

中图法分类号: TP393 **文献标识码:** A

分布式拒绝服务攻击(DDoS)常通过大量消耗受害服务节点的各种资源(如带宽、CPU 及主存储器),使其对该节点的正常服务请求无法响应或延迟响应.因此,DDoS 攻击目前被视为 IP 网络持续服务能力的主要威胁之一.由于现在越来越多的网络服务或信息以 Web 方式提供,因此,Web 服务器自然成了各种 DDoS 攻击的首选目标.另外,当前 DDoS 攻击技术门槛低且攻击工具不断推陈出新,使得 Web DDoS 攻击成本很低,且非常容易得手.因此,当前 Web 网站的安全形势越来越严峻,不断有 DDoS 的重大攻击事件报道.例如,2009 年 7 月,韩国的一些政府、商业网站遭到了最为严重的 DDoS 攻击,据统计,此次攻击事件给韩国造成至少 76 亿韩元的经济损失[1].

为了能够有效地防范 Web DDoS 攻击,国内外学者纷纷就此进行了深入研究.文献[2,3]分析了目前 DDoS 攻击的研究现状,指出 Bandwidth-Flood Web DDoS 攻击和 SYN-Flood Web DDoS 攻击是目前最典型的 DDoS 攻击.对此,文献[4–8]分别提出了相应的检测和抵御方法.然而,为了逃避检测,目前一些攻击者采取了更隐蔽、更复杂的攻击方式,其中典型的有 HTTP 洪泛 Web DDoS 攻击(简称 Http-Flood).该攻击对 Web 服务造成的危害很大:它可以模拟正常用户浏览网页的行为,向 Web 服务器发送大量的 HTTP Get 请求,耗尽 Web 服务器资源,使其无法响应其他正常用户的服务请求.其隐蔽性主要体现在如下两个方面:一方面,它能够产生与正常用户请求序列相似的页面或对象请求序列;另一方面,它在攻击中仅需占用很少的带宽,其攻击流量常淹没于其他正常流量之中.因此,与其他攻击相比,对 Http-Flood 攻击进行有效检测的难度更大.

本文围绕 Http-Flood Web DDoS 攻击问题,提出一种解决方法.首先,我们通过对用户访问行为进行分析发现,正常用户通常只访问他们感兴趣的网页,并且他们对该网站的兴趣点相对比较固定,例如,一些用户喜欢该网站的体育版,而另一些用户则喜欢它的娱乐版.伴随着大量用户的不断访问,服务器网页的受欢迎程度表现出了高度不对称性,一些网页由于访问量大而变成“热门”网页,而另一些网页则由于访问量少而变成“冷门”网页.Web 网页文件点击率分布服从 Zipf 分布,呈现高度不对称性,即大多数访问集中于少数热门的文件,一般情况下,30%的文件得到了 60%~80%的请求数[9].因此,正常用户访问过程中表现出的主要特点是:访问热门网页较多,而访问冷门网页较少.然而,由于恶意 DDoS 攻击者对网站的内容信息不了解,它们通常只能通过随机获取网页方式访问该网站,这也使得它们的访问行为表现出了极大的随机性.因此,正常用户和恶意攻击者在访问方式上不同,这也为本文检测 DDoS 攻击奠定了基础.基于此,本文提出一种 Http-Flood Web DDoS 攻击检测机制.该机制采用网站先验点击概率分布描述了不同网页内容的受欢迎程度,它是大量正常用户访问行为的集中体现.因此,对于单一正常用户,其访问行为的实际点击概率分布与网站先验点击概率分布极为相似,而恶意攻击者的随机访问行为产生的实际点击概率分布与网站先验点击概率分布则相差较大.为了准确地刻画用户实际点击概率分布与服务器网页先验点击概率分布的偏差,本文运用大偏差统计模型对两者的偏差建模,并依据大偏差概率值检测恶意攻击.最后,通过仿真对本文的检测机制进一步验证,结果表明,该机制能够有效地检测 Http-Flood Web DDoS 攻击.另外,由于服务器网页文件先验点击概率分布是大量正常用户访问行为的集中体现,这使得恶意攻击者很难获取该特征信息并破解该检测机制.

1 相关工作

为了抵御 Http-Flood 攻击,文献[10]采用预先认证机制,其主要思路是:当用户会话请求到达时,服务器从本地图片库中随机抽出一张图片(图片上包含失真的数字和字符)要求用户辨认,并且依据辨认结果来确定该用户是否是恶意攻击者.该检测机制能够有效工作的前提条件是:恶意攻击者(如僵尸网络)无法正确辨认失真的字

符和数字,而正常用户能够正确辨认.然而依据文献[11]分析结果,该机制检测条件存在严重漏洞,目前一些恶意的僵尸机器采用合适的图形匹配算法也能准确辨认出失真的数字和字符,进而破解该检测机制;另外,该机制在用户正常访问网页过程中引入了预先认证,这不但给正常用户访问造成很多麻烦,而且还给正常用户访问带来额外延时.文献[12]也采用预先认证机制抵御 Http-Flood 攻击,它与文献[10]的区别在于认证机制不同.它是通过加密服务器端口信息隐藏应用服务程序,并采用 JavaScript 的脚本方式对正常用户进行密钥分发.该检测机制的主要不足在于它的密钥分发方式容易遭到破解(恶意攻击者只需安装 JavaScript 解析器就可以成功破解该检测机制),而且它同样也会给正常用户访问带来额外延时.

与文献[10,12]不同,文献[13,14]则采用群测理论(group testing)来检测 Http-Flood 攻击.它们都是以采用最少次数的测验来找到群体中的异类.文献[13]将所有用户分为不同组,通过观察每组中的平均请求响应时间来确定该组中是否存在恶意攻击者;文献[14]则通过观察每组中用户的平均请求速率来确定该组中是否存在恶意攻击者.群测理论检测异常的前提条件是:异常个体的存在能够导致测试结果呈阳性.然而在实际网络环境中,一个恶意攻击者发起的攻击通常还不足以严重影响服务器性能,也不会导致群测结果呈阳性.显然,群测理论有效工作的前提条件与 Http-Flood 攻击的实际环境不符,这将大大降低检测灵敏度,进而严重影响该方法的检测有效性.

此外,文献[15]还从类似“竞拍”的角度,提出了一种称为 Speak-Up 的 Http-Flood 攻击检测机制.该文献假定恶意攻击者由于实施 DDoS 攻击而消耗了自身大部分接入带宽,而正常用户则有足够的空闲带宽可供利用.由此,在服务器受到攻击时,Speak-Up 以带宽为“筹码”,要求所有用户“竞拍”获得服务,鼓励所有用户提高发送速率.由于恶意攻击者的发送速率已经达到其上限,因此无法再响应服务器的鼓励,而正常用户则能够通过不断增加发送速率来响应服务器.最终,Speak-Up 依据“竞拍”结果决定最终服务对象.由于正常用户增加的发送速率大于恶意攻击者,因此正常用户“竞拍”得到了服务器提供的服务,而恶意攻击者则被拒绝服务.然而,该检测方法存在如下两个问题:(1) 一些硬件性能比较差的用户(如接入带宽较低)由于自身原因无法再增加流量,而被误认为恶意攻击者;(2) Http-Flood 攻击者由于只占用了很少的带宽,也能够再增加流量,而被误认为正常用户.因此,Speak-Up 需要进一步对这两个问题进行处理.

鉴于上述检测方法存在不少缺陷,很多学者试图利用用户访问行为特征来检测 Http-Flood Web DDoS 攻击,其研究已取得了一些积极的进展.文献[16]对 Http-Flood 攻击行为特征进行建模,它认为恶意攻击者的请求速率通常比较高,而且它们几乎没有访问该网站的历史记录.基于这些特征,该文献采用一种启发式拓扑计算方法,提取现有访问用户的 IP 地址特征,与该特征不符的用户即被视为恶意攻击.由于该方法只是针对恶意攻击特征建模,因此它仅能检测特征已知的 Http-Flood Web DDoS 攻击,却不能检测其他未知特征的 Http-Flood 攻击;而且由于它采用 IP 地址特征检测恶意攻击,容易产生误检.文献[17–20]提出了基于正常用户访问行为特征的检测方法.其中,文献[17,18]分别对正常用户会话的一些统计特征(如请求到达间隔、会话负载模式等)进行建模,然后基于这些统计特征来检测 Http-Flood 攻击.然而,这些统计特征容易被恶意攻击者模仿,并且这些统计特征值是否平稳对对它们的检测效果影响较大.实际上,它们是否平稳还需要进一步论证.文献[19,20]采用隐马尔可夫(HsMM)模型分别描述了正常用户访问行为和网页点击率的小时间尺度变化.其中,文献[19]将服务器网页表示为 HsMM 状态、用户请求网页到达服务器端的网页内嵌对象数量近似表示 HsMM 状态持续时间,对正常用户浏览不同网页的逻辑关系建模.然而,这一点与正常用户浏览行为不符,这将严重影响检测性能.文献[20]采用服务器网页点击率分布向量表示 HsMM 状态,并依据训练后的 HsMM 模型识别 DDoS 攻击事件与 flash-crowd.检测恶意攻击.然而,该检测方法中 HsMM 样本空间对训练数据得到 HsMM 样本空间,而 HsMM 模型的样本空间是否完备还需要进一步验证,这同样也会严重影响 Http-Flood 检测性能.由于现有基于用户访问行为的检测模型自身依然存在一些问题,Http-Flood 攻击检测还需要进一步研究.

2 Web 用户访问行为描述及其基于型方法的度量

假定用户访问序列记为 $S\triangleq\{s(t)\in\Omega|t=1,2,\ldots,n\}$,其中,$s(t)$表示 t 时刻用户访问的网页;Ω表示网页集合并记为

$\Omega=\{p_1,p_2,\ldots,p_M\}$,$|\Omega|=M$.正常用户在访问过程中常依据主观判断来点击他们感兴趣的链接,并且不同点击行为之间是近似独立的.因此,本文将用户的访问过程用独立同分布随机过程来描述,其中,用户的每一次点击行为 $s(t)$表示一个随机变量且服从网站先验点击概率分布,其样本空间是整个网页集合.

为了准确地刻画用户访问行为特点,本文运用型方法度量用户访问行为,得到它们的实际点击概率分布,其中,文献[21]中对型定义如下:

假定序列 $x_1,x_2,\ldots,x_n$ 为来自集合$\chi=\{a_1,a_2,\ldots,a_{|\chi|}\}$的 n 个样本构成的序列,它的型记为 P_x(也称经验概率分布)是χ中的每个元素在该序列中出现次数的相对比例(对任意的 $a\in\chi$,$P_x(a)\triangleq N(a|x)/n$),其中,$N(a|x)$表示元素 a 在序列 x 中出现的次数.

由上述型定义可知,型描述了不同样本在随机序列中的发生概率.因此,型方法能够有效地刻画本文检测机制中用户访问行为特点,很好地刻画用户访问不同网页的兴趣特征.

依据上述型定义,用户 $S\triangleq\{s(t)\in\Omega|t=1,2,\ldots,n\}$的实际点击概率分布度量记为

$$\varepsilon_n^S=(\varepsilon_n^S(p_1),\varepsilon_n^S(p_2),\ldots,\varepsilon_n^S(p_M)) \tag{1}$$

其中,$\varepsilon_n^S(p_i)=\frac{1}{n}\times N(p_i)$,$N(p_i)$表示网页 p_i 被用户 S 访问的次数.因此,用户的实际点击概率分布反映了他对不同网页的感兴趣程度.

由于本文采用用户访问的目标网页序列描述它的访问行为,因此如何获得网页表示信息也至关重要.文献[20]观察服务器端用户请求序列,并依据请求到达间隔将请求对象分组,每组表示一个网页.由于服务器端观察到的用户请求序列中通常包括目标页面的主请求(页面框架)和若干内嵌对象(如图片或声音文件)的请求,受一些因素(如代理缓存)的影响,不同用户即使访问相同网页,所产生的请求序列也可能不相同,由此获得的网页表示信息不准确.文献[18]通过网络蜘蛛获取网页内容并分析网页组织结构得到网页表示信息,尽管该方法能够获得准确的网页信息,但频繁爬取网页会对服务器造成严重负担.我们通过大量的观察发现,用户点击网页链接时所产生的主页面请求总是会到达服务器端,其中,这些主页面包括*.php,*.(s)htm(l),*.cfm,*.php,*.asp(x),*.jsp以及*.txt 等类型网页对象.由此,本文依据这些主页面标示信息识别网页,既能准确表示网页,又不会对服务器造成严重负担.

3 Http-Flood Web-DDoS 攻击检测

本节首先从随机过程角度描述 Web 用户访问行为,采用型方法度量用户访问行为;然后阐述基于大偏差统计模型的 Http-Flood 检测机制,并给出该检测机制的实现流程.

基于上一节建立的用户访问行为描述及其度量方法,本节将构建一种有效的 Http-Flood 攻击检测方法.正常用户经常是带着明确的信息获取目的和需求去访问相应网页,其访问行为具有较强的主观倾向性(例如常访问一些热门网页);而恶意攻击者则与之相反,它们只是随机地访问网页.正常用户和恶意攻击在访问方式上的巨大差别直接造成了他们在访问网站过程中的实际点击概率分布差异较大.因此,本文采用大偏差统计模型量化分析了正常 Web 用户与恶意攻击访问行为的实际点击概率分布的区别,并依据得到的大偏差概率检测 Http-Flood 攻击.

大偏差统计模型刻画了定义在集合Γ上的一系列概率向量的收敛特性,即当$\varepsilon\to0$ 时,Γ上的概率序列$\{\mu_\varepsilon\}$的收敛行为.假定随机变量 X,它的样本空间记为 $A\triangleq\{a_1,a_2,\ldots,a_M\}$、初始概率分布记为$\mu\triangleq\{\mu(a_1),\mu(a_2),\ldots,\mu(a_M)\}$,$\mu$是一个 M 维概率单纯形,即它满足:

$$\mu\in M_1(A)\triangleq\{r\in R^M\mid r_i\in[0,1],i=1,\ldots,M,\sum_{i=1}^M r_i=1\} \tag{2}$$

定义在该样本空间A上的独立同分布随机变量序列记为 $Y\triangleq\{Y_1,Y_2,\ldots,Y_N\}$,其中,$Y_i$服从该样本空间的初始概率分布$\mu$.通过实际观察,可以得到它在该样本空间上的实际概率分布记为 ε_n^Y.

$$\varepsilon_n^Y=(\varepsilon_n^Y(a_1),\varepsilon_n^Y(a_2),\ldots,\varepsilon_n^Y(a_M)) \tag{3}$$

其中,

$$\varepsilon_n^Y(a_i)=\frac{1}{n}\sum_{j=1}^{n}1_{a_i}(Y_j),i=1,...,M \tag{4}$$

$1_{a_i}(Y_j)$ 表示事件 $Y_j=a_i$ 的发生函数,定义为

$$1_{a_i}(Y_j)=\begin{cases}1, & Y_j=a_i\\ 0, & Y_j\neq a_i\end{cases} \tag{5}$$

由于 Y_j 服从样本空间 A 的初始概率分布 μ,因此,随机变量序列 Y 在该样本空间 A 上的概率测度 ε_n^Y 与 μ 不一致这一事件($\varepsilon_n^Y\neq\mu$)属于稀有事件,按照 Sanov 定理,这类稀有事件发生的概率是可以计算的.

Sanov 定理[22]. 设 $X_1,X_2,\ldots,X_n$ 为 *i.i.d*~$Q(x)$,记 P 为全体概率分布,若 $E\subseteq P$,则

$$Q^n(E)=Q^n(E\cap P)\leqslant(n+1)^{|\chi|}2^{-nD(P^*\|Q)} \tag{6}$$

其中,P^*是在相对熵意义下 E 中最接近于 Q 的分布.另外,若集合 E 是自身内部的闭包,则

$$\frac{1}{n}\log Q^n(E)\to -D(P^*\|Q) \tag{7}$$

Sanov 定理建立了 *i.i.d* 随机序列 Y 在样本空间 A 上的概率测度与该样本空间的初始概率分布之间的关系,假定 $D(P\|Q)$为 P 与 Q 之间的相对熵,则随机序列 Y 在样本空间 A 上的概率测度为 P 这一事件的概率为 $e^{-nD(P\|Q)}$.

基于上述大偏差统计模型,本文分析了用户访问行为的实际点击概率分布与网站先验概率分布的偏差.网站先验概率分布是大量正常用户访问行为的集中统计结果,它反映了不同网页内容的受欢迎程度.因此在无偏情况下,用户访问行为的实际概率分布应与网站先验概率分布一致.然而实际情况并非如此,它们之间由于一些主观因素影响,常存在一定的偏差.依据 Sanov 定理,在满足先验概率分布的条件下,用户访问行为的实际点击概率分布与网站先验概率分布不一致事件属于稀有事件,可以采用大偏差统计模型计算该稀有事件的发生概率.两者偏差越大,其大偏差概率值越小.大偏差概率计算方法如公式(8)所示.

$$\Pr[\varepsilon_n^S]\simeq e^{(-nH(\varepsilon_n^S|\mu))} \tag{8}$$

其中,$H\left(\varepsilon_n^S/\mu\right)$ 表示正常用户访问行为的实际点击概率分布 ε_n^S 与网站特征概率分布 μ 之间的相对熵,如公式(9)所示.

$$H\left(\varepsilon_n^S/u\right)\triangleq\sum_{i=1}^{M}\varepsilon_n^S(p_i)\log\frac{\varepsilon_n^S(p_i)}{\mu(p_i)} \tag{9}$$

相对熵 $H\left(\varepsilon_n^S/\mu\right)$ 描述了用户访问行为的实际点击概率分布与网站特征概率分布间的距离,即两个概率分布序列的相似性. $H\left(\varepsilon_n^S/\mu\right)$ 越大,说明用户 S 的访问行为的实际点击概率分布 ε_n^Y 与网站特征概率分布越相似;反之,则说明两者差异越大.大偏差统计模型说明,在满足先验概率分布情况下,用户 S 的访问行为的实际点击概率分布 ε_n^Y 与网站先验概率分布偏差较大属于稀有事件,这类事件发生的概率非常小.由于正常用户的访问行为的实际概率分布与网站的特征概率分布相似,而恶意攻击者由于通过随机访问网页,它的访问行为的实际概率分布与网站特征概率分布差异较大,按照大偏差理论,正常用户的大偏差概率远大于恶意攻击.由此,我们依据大偏差概率值检测 Http-Flood 攻击.

本文检测机制包括两个阶段:特征提取阶段和检测阶段.在特征提取阶段,以无攻击情况下的网站访问日志(包括大量正常用户访问记录,如图 1 所示)为样本,分析提取网站的网页集合以及网站先验概率分布.在已知各网页被访问的次数条件下,本文采用最大似然方法估计网站先验概率分布.假定观察得到每个网页被访问次数分别为 $x_1,x_2,\ldots,x_N$,网站先验概率分布记为 $P=(p_1,p_2,\ldots,p_N)$,则本文最大似然估计的对数似然函数为

$$\ln P=x_1\ln p_1+x_2\ln p_2+\ldots+x_N\ln\left(1-\sum_{i=1}^{N-1}p_i\right) \tag{10}$$

运用 SciPy 中的 linalg 模块即可计算得到网站先验概率分布 $P=(p_1,p_2,\ldots,p_N)$.

在检测阶段,分析每个到达用户的访问网页序列,采用型方法计算它的实际点击概率分布,并采用公式(8)、公式(9)大偏差概率计算方法得到该用户大偏差概率.最后,依据大偏差概率值进行检测.

源 IP 地址	日期	方法	请求对象	协议	返回代码	大小	用户代理
X.X.X.X	13/Sep/2009:06:32:27	GET	/favicon.ico	HTTP/1.1	200	7 178	Mozilla/4.0
X.X.X.X	13/Sep/2009:06:32:27	GET	/images/spacer.gif	HTTP/1.1	200	43	Mozilla/4.0
X.X.X.X	13/Sep/2009:06:32:27	GET	/images/index/logoname.gif	HTTP/1.1	200	13 202	Mozilla/4.0
X.X.X.X	13/Sep/2009:06:32:28	GET	/	HTTP/1.1	200	44 354	Mozilla/4.0
X.X.X.X	13/Sep/2009:06:32:28	GET	/images/index/logoright.jpg	HTTP/1.1	200	3 339	Mozilla/4.0

Fig.1 Sample of Web access log

图 1 网站访问日志样本

4 Http-Flood Web-DDoS 检测性能分析

本文以某大学门户 Web 网站为例,拟对所提出的 Http-Flood 攻击检测机制进行性能分析和评估.由于目前尚无有关 Http-Flood Web DDoS 攻击数据可供利用,因此,本文通过随机访问网页集合中的网页模拟 Http- Flood 攻击,得到了模拟攻击实验数据.本文模拟仿真中的参数见表 1.

Table 1 Parameters in performance evaluation

表 1 模型性能评估中的相关参数

名称	数值
网页数量	3 230
正常用户请求数	750 000
正常会话数	6 558
攻击会话数	10 000
攻击会话长度	Uniform (20,1000)

首先,在特征提取阶段,通过分析 Web 网站的日志,得到该网站网页集合,并且依照公式(10)最大似然估计方法计算得到该网站的先验点击概率分布,如图 2 所示,其中,横坐标表示网页序列,纵坐标表示页面点击概率.由于特征提取阶段的样本日志来自大量正常用户访问,我们假定这些访问能够遍历整个网页集合,由此得到的网页集合是完备的.

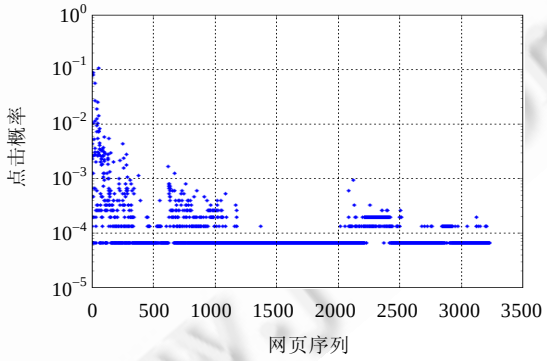


Fig.2 Priori click probability distribution of the website

图 2 网站先验点击概率分布

图 2 描述了该网站中不同网页在近一段时间内被访问的受欢迎程度,其中,热门网页的点击概率远大于冷门网页,而且热门网页的数量相对较少,仅占网站页面总量的很小部分.接下来,我们以图 2 所示的网站先验点击概率为基准,依据公式(9)、公式(10)计算所有会话(包括正常用户和恶意攻击)的大偏差概率.如图 3 所示为其大

偏差累积概率分布,其中,横坐标表示大偏差概率,纵坐标表示累计概率分布.由图 3 可以看出,大部分正常用户的大偏差概率值大于 10^{-36},而大部分恶意攻击的大偏差概率值则小于 10^{-36}.由此可以初步看出,本文检测机制能够识别正常 Web 用户与恶意攻击.若将检测门限设置为 10^{-60},则采用该机制可以检测 97.5%的 Http-Flood 恶意攻击,而仅有 0.6%的误检率.

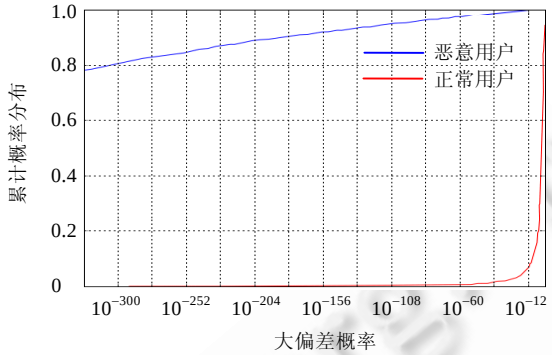


Fig.3 Large deviation probability distribution of normal user and attackers

图 3 正常用户和恶意攻击者累计大偏差概率分布

为了更加全面地评价本文检测机制性能,本文采用 ROC(receiver operating characteristic)曲线分析检测模型的动态检测性能[23].ROC 曲线描述了检测模型在不同检测门限条件下检测率与虚警率之间的折中关系,检测率 TP(true positive)与虚警率 FP(false positive)分别定义如下:

$$TP \approx \frac{\text{positives correctly classied}}{\text{total positives}},$$

$$FP \approx \frac{\text{negatives incorrectly classied}}{\text{total negatives}}.$$

按照文献[23]中提出的 ROC 曲线计算算法,我们计算得到了本文检测机制的 ROC 曲线.另外,我们将本文的检测机制与文献[18]中基于网页转移概率的检测机制进行性能比较,如图 4 所示为比较结果.为了方便标示,本文的机制简称为 LD(large-deviation based Http-Flood detection method),文献[18]算法简称为 TP(transition probability based detection method).

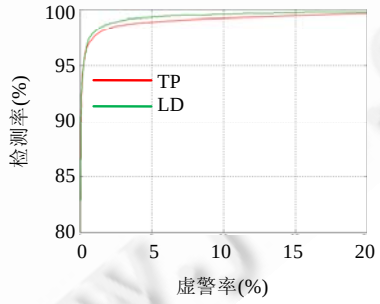


Fig.4 Performance comparison of LD-ADD and TP in term of ROC metric

图 4 LD-ADD 与 TP 的 ROC 性能比较

由图 4 可以得出,本文的检测机制能够实现低误检率和高检测率.同时,本文机制的性能也优于文献[18]的检测机制,其中,在相同虚警率的要求下,本文算法能够实现比文献[18]算法更高的检测率.

5 结 论

本文以 Http-Flood Web DDoS 攻击检测为核心问题,提出一种检测机制.首先,通过对大量正常 Web 用户访问行为观察,得到了正常用户与恶意攻击的访问行为的重要区别:他们访问不同网页的点击概率分布不同.基于此,本文采用型方法量化分析用户访问的目标网页序列,得到了用户访问不同网页的实际点击概率分布;然后,运用大偏差统计模型对正常用户与恶意攻击者的访问行为区别建模,即采用大偏差统计方法分析用户访问行为实际点击概率分布与网站先验点击概率分布的偏差;最后,依据其大偏差概率进行检测.仿真结果表明,本文的检测机制能够有效检测 Http-Flood 攻击,并且在低误检率条件下可以实现较高的检测率.

致谢 在此,我们向对本文的工作给予支持和建议的同行表示感谢.

References:

[1] http://world.kbs.co.kr/chinese/program/program_economyplus_detail.htm?No=1813

[2] Mirkovic J, Reiher P. A Taxonomy of DDoS attack and DDoS defense mechanisms. ACM Sigcomm Computer Communications Review, 2004,34(2):39−53. [doi: 10.1145/997150.997156]

[3] Sun ZX, Jiang JL, Jiao L. DDOS attack detecting and defending model. Journal of Software, 2007,18(9):2245−2258 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/18/2245.htm [doi: 10.1360/jos182245]

[4] Anderson T, Roscoe T, Wetherall D. Preventing Internet denial of service with capabilities. In: Proc. of the HotNets-II. 2003. 39−44. [doi: 10.1145/972374.972382]

[5] Yang XW, Wetherall D, Anderson T. A DoS-limiting network architecture. In: Proc. of the ACM SIGCOMM 2005, Vol.35. 2005. 241−252. [doi: 10.1145/1080091.1080120]

[6] Argyraki K, Cheriton DR. Scalable network-layer defense against Internet bandwidth-flooding attacks. IEEE/ACM Trans. on Networking, 2009,17(4):1284−1297. [doi: 10.1109/TNET.2008.2007431]

[7] Beaumont-Gay M. A comparison of SYN flood detection algorithms. In: Proc. of the 2nd Int'l Conf. on Internet Monitoring and Protection. 2007. [doi: 10.1109/ICIMP.2007.1]

[8] Ohsita Y, Ata S, Murata M. Detecting distributed denial-of-service attacks by analyzing TCP SYN packets statistically. In: Proc. of the IEEE Globecom. 2004. 2043−2049. [doi: 10.1109/GLOCOM.2004.1378371]

[9] Yu SZ. Macro behavior of Web workload. Pattern Recognition and Artificial Intelligence, 2005,18(1):31−37 (in Chinese with English abstract).

[10] Kandula S, Katabi D, Jacob M, Berger AW. Botz-4-Sale: Surviving organized DDoS attacks that mimic flash crowds. Technical Report, TR-969, MIT, 2004.

[11] Mori G, Malik J. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. In: Proc. of the Computer Vision and Pattern Recognition. 2003. 134−144.

[12] Srivatsa M, Iyengar A, Yin J, Liu L. A client-transparent approach to defend against denial of service attacks. In: Proc. of the 25th IEEE Symp. on Reliable and Distributed Systems (SRDS). 2006. 61−70. [doi: 10.1109/SRDS.2006.6]

[13] Xuan Y, Shin I, ThaiMT, Znati T. Detecting application denial-of-service attacks: A group-testing-based approach. IEEE Trans. on Parallel and Distributed Systems, 2010,21(8):1203−1216. [doi: 10.1109/TPDS.2009.147]

[14] Khattab S, Gobriel S, Melhem R, Mosse D. Live baiting for service-level DoS attackers. In: Proc. of the Infocom 2008. 2008. 682−690. [doi: 10.1109/INFOCOM.2008.43]

[15] Walfish M, Vutukuru M, Balakrishnan H, Karger D, Shenker S. DDoS defense by offense. In: Proc. of the ACM Sigcom 2006. 2006. [doi: 10.1145/1159913.1159948]

[16] 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 Int'l World Wide Web Conf. 2002. 252−262. [doi: 10.1145/511446.511485]

[17] Ranjan S, Swaminathan R, Uysal M, Knightly E. DDoS-Resilient scheduling to counter application layer attacks under imperfect detection. In: Proc. of the IEEE Infocom 2006. 2006. 1−13. [doi: 10.1109/INFOCOM.2006.127]

[18] Oikonomou G, Mirkovic J. Modeling human behavior for defense against flash-crowd attacks. In: Proc. of the IEEE ICC 2009. 2009. 1−6. [doi: 10.1109/ICC.2009.5199191]

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

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

[21] Cover TM, Thomas JA. Elements of Information Theory. New York: Wiley Interscience, 1991.

[22] Dembo A, Zeitouni O. Large-Deviations techniques and applications. 2nd ed., New York: Springer-Verlag, 1998.

[23] Fawcett T. ROC graphs: Notes and practical considerations for data mining researchers. Technical Report, HPL-2003-4, Palo Alto: HP Laboratories, 2003.

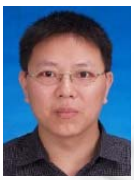
附中文参考文献:

[3] 孙知信,姜举良,焦琳.DDOS 攻击检测和防御模型.软件学报,2007,18(9):2245−2258. http://www.jos.org.cn/1000-9825/18/2245.htm [doi: 10.1360/jos182245]

[9] 余顺争.Web 负载流的宏观模式与识别.模式识别与人工智能,2005,18(1):31−37.

王进(1980－),男,宁夏银川人,博士生,讲师,主要研究领域为 IP 网络,计算机网络安全.

隆克平(1968－),男,博士,教授,博士生导师,主要研究领域为光互联网络技术,新一代网络理论与技术,无线信息网络,网络新业务与安全.



阳小龙(1971－),男,博士,教授,博士生导师,主要研究领域为宽带网络理论及技术,网络生存性,光互联网及交换技术,网络定位.