ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.10, October 2007, pp.2613−2623
DOI: 10.1360/jos182613

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

基于源目的IP地址对数据库的防范DDos攻击策略*

孙知信[1,2+], 李清东[1]

[1](南京邮电大学 计算机学院,江苏 南京 210003)

[2](南京邮电大学 计算机技术研究所,江苏 南京 210003)

Defending DDos Attacks Based on the Source and Destination IP Address Database

SUN Zhi-Xin[1,2+], LI Qing-Dong[1]

[1](College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

[2](Institute of Computer Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

+ Corresponding author: Phn: +86-25-85198095, Fax: +86-25-83492859, E-mail: sunzx@njupt.edu.cn

Sun ZX, Li QD. Defending DDos attacks based on the source and destination IP address database. *Journal of Software*, 2007,18(10):2613−2623. http://www.jos.org.cn/1000-9825/18/2613.htm

Abstract: This paper proposes a scheme to defend distributed denial of service attacks (DDos) based on the source and destination IP address database. The scheme establishes the source and destination IP address database (SDIAD) by observing the normal traffic and storages SDIAD in a three dimension Bloom Filter table. Then this paper cumulates and analyses the new pair of source and destination IP address based on the slide non-parametric cumulative sum (CUSUM) algorithm to detect the DDos attacks quickly and accurately. The secheme updates SDIAD by using a delayed update policy to keep SDIAD timely, accurate and robust. This secheme is mainly applied in the edge router and it can detect the DDos attacks efficiently either the edge router or the last-mile router is the first-mile router. The simulation results display that the secheme do a good performance in detecting DDos attacks.

Key words: Ddos (distributed denial of service attacks); router; non-parametric CUSUM; bloom filter

摘 要: 提出了一种基于源目的IP地址对数据库的防范分布式拒绝服务攻击(distributed denial of service attacks,简称DDos)攻击策略.该策略建立正常流量的源目的IP地址对数据库(source and destination IP address database,简称SDIAD),使用扩展的三维Bloom Filter表存储SDIAD,并采用改进的滑动窗口无参数CUSUM(cumulative sum)算法对新的源目的IP地址对进行累积分析,以快速准确地检测出DDos攻击.对于SDIAD的更新,采用延迟更新策略,以确保SDIAD的及时性、准确性和鲁棒性.实验表明,该防范DDos攻击策略主要应用于边缘路由器,无论是靠近攻击源端还是靠近受害者端,都能够有效地检测出DDos攻击,并且有很好的检测准确率.

关键词: 分布式拒绝服务攻击;路由器;无参数CUSUM算法;bloom filter

中图法分类号: TP393 **文献标识码**: A

* Supported by the National Natural Science Foundation of China under Grant No.60572131 (国家自然科学基金); the Key Technologies R&D Program of Jiangsu Province of China under Grant No.BE2007058 (江苏省科技攻关项目); the Scientific Research Foundation of ZTE and Huawei Corporation of China (中兴及华为基金); the Scientific Development Foundation of Government of China (南京市科技发展计划); the Scientific Research Foundation of NUPT of China under Grant Nos.NY206008, NY206050 (南京邮电大学攀登计划及青蓝计划)

Received 2006-06-05; Accepted 2006-11-13

分布式拒绝服务攻击(Dos/DDos)是指有人恶意地对网络进行干扰,使服务受到一定的影响,严重的可以造成巨大的经济损失.Yahoo,eBay,Amazon.com,E*Trade,ZDnet,Buy.com,FBI,DoubleClick Inc 等网站都遭受过其攻击[1−3].近年来,DDos(distributed denial of service attacks)攻击的频率和方式都呈上升的趋势[4],并且出现了攻击强度更大的高分布式拒绝服务攻击(highly distributed denial of service attack,简称HDDos)和反射式拒绝服务攻击(distributed reflection denial of service attacks,简称DRDos)[5].Gibson研究团体认为[6],目前,DDos攻击将大幅度增加(据Gibson估计为每星期 4 000 次),这将使互联网因为成百上千的DDos攻击而降低速度.

DDos 攻击一般有两个目的:消耗主机资源和恶意占用网络带宽.目前的保护机制主要是根据协议类型和端口号等在网关进行丢包.这种方式的致命缺点是区分正常流量和攻击流量的准确率不高.还有另一种称为“flash crowd”的流量,即很多合法用户同时访问一个网络服务,造成流量的突然增加,这与 DDos 攻击在流量统计上有相似的地方,更加难以区分.

目前,有很多文献研究如何防范 DDos 攻击.但是,这些策略应用在 HDDos 和 DRDos 攻击上效果并不明显,并且容易混淆 DDos 攻击流量和“flash crowd”流量.DDos 攻击一般采用假冒源 IP 地址的策略,对于 DRDos 攻击,虽然它使用合法的 IP 地址,但对于受害者来说,这些 IP 地址大多数都是“新”的,即受害者在以前并没有与该地址进行过通信.基于这样的本质特征,就形成本文防范 DDos 攻击的一种新策略.根据已建立好的合法源目的 IP 地址历史数据库,在路由器上对新出现的 IP 地址对采用滑动窗口无参数 CUSUM(cumulative sum)算法进行累积和分析,达到检测和过滤 DDos 攻击的目的.

1 相关性研究

目前的绝大多数检测DDos攻击的策略[7−13]在靠近受害者端的网络比较容易实施,随着与受害者距离的增加,检测就变得比较困难,而且在准确率上都会有所降低.当DDos攻击的分布式程度越高,上面所引用的方法在检测准确率上也就越低.此外,基于流量分析的策略[11,14,15]在检测过程中无法准确地区分DDos攻击流量和“flash crowd”流量.而一种好的检测策略必须尽可能地靠近源端,靠近攻击流量发起的网络,尽早地检测出攻击并过滤掉攻击流量,以免造成网络带宽的浪费,并且,这种策略要能够准确地区分DDos攻击流量和“flash crowd”流量.

文献[16]提出一种通过监测新的源IP地址在Δ时间内出现的个数的机制来判断是否有攻击发生,在一次带宽攻击过程中,这些IP地址对于受害者来说大多是新的,这种特征与“flash crowd”中表现出来的是不同的,这种策略也被用于过滤攻击流量.Bloom Filter算法[17]的最初目的是研究一组给定信息之间的关系,在 20 世纪 80 年代它被用于减少访问磁盘不同文件的次数[18,19].文献[20]中发展Bloom Filter算法为Counting Bloom Filter,文献[21,22]做了一些将Counting Bloom Filter算法应用到DDos防范方面的工作,它们对不同IP地址的流量数据使用Counting Bloom Filter算法进行计数统计,以发现那些超出门限的流量,进而检测出DDos攻击.

CUSUM 算法是在统计过程控制中常用的算法,它可以检测到一个统计过程均值的变化.在文献[23]中,使用非参数 CUSUM 算法来检测 DDos 攻击,减少了漏报率和误报率,并且消耗较少的计算机资源.文献[24]中提出了矩阵式的多统计量 CUSUM 算法,应用于核心路由器,有较高的检测准确率.文献[25]提出了基于攻击流量特征聚类的特征提取算法,能够有效地进行过滤,减少攻击包传播的危害,保护有限的网络资源.但这些算法在检测攻击结束时刻的延迟比较大.

综上所述,现有的防范 DDos 攻击方法做了很多有益的工作,但在检测准确率或检测速度等方面都存在一定的不足.因此,本文提出了一种基于源目的 IP 地址对数据库的防范 DDos 攻击策略.本文使用扩展的三维 Bloom Filter 表存储 SDIAD(source and destination IP address database),以节省存储空间和提高查找效率,并采用改进的滑动窗口无参数CUSUM算法对新的源目的IP地址对进行累积分析,以快速而准确地检测出DDos攻击.

2 策略描述

研究表明,现在的DDos攻击都是高分布式和高源IP地址伪装的(通过随机函数产生IP地址)[26,27],在一次

DDos攻击中,只有 0.6%~14%的IP地址是在以前出现过的[26].Jung[26,27]发现,在一次正常的“flash crowd”中,大约有 82.9%的IP曾经发送过请求.对网络流量的统计发现,网络中出现的IP地址有很大的概率在一定时期内重复出现,这就隐含着可以根据历史IP来检测异常的出现,本文即基于这样的策略.

设A_{normal},A_{flash},A_{attack}分别代表正常情况下、发生“flash crowd”情况下和发生DDos攻击情况下的数据包个数,A_{normal},B_{flash},B_{attack}分别代表正常情况下、发生“flash crowd”情况下和发生DDos攻击情况下的新出现的IP地址个数.文献[6,27]指出,当观察点靠近受害者的网络时,有

$$A_{normal}<<A_{flash}\approx A_{attack} \tag{1}$$

$$B_{normal}<B_{flash}<<B_{attack} \tag{2}$$

当观察点靠近攻击者的网络时,有

$$A_{normal}\approx A_{flash}\approx A_{attack} \tag{3}$$

$$B_{normal}\approx B_{flash}<B_{attack} \tag{4}$$

上面的公式指出,当发生DDos攻击时,所观察到的新IP地址的增加是显著的,SIM(source IP address monitoring)机制就基于这种特征来检测DDos[16].本文防范DDos攻击的策略就是基于上面的网络本身所固有的特征,因此,无论是靠近攻击源端还是靠近受害者端,都能够有效地检测出攻击.本文的策略主要包括两个部分:源目的IP地址历史数据库(SDIAD)的建立与更新和基于滑动窗口无参数CUSUM算法的检测机制.SDIAD包括离线训练和在线自我学习更新两部分.

离线训练将合法的 IP 地址添加到数据库中,离线是确保这些 IP 地址数据不包括 DDos 攻击成分.在线更新将保证 SDIAD 的及时性.网络是一个复杂的实体,总会不停地有主机增加进来也会有新的 IP 地址增加进来,就需要保持对 SDIAD 的更新.当检测到 DDos 攻击时,在线学习机制必须挂起,以免将恶意的 IP 地址添加到数据库中.为此,采用三维的 Bloom Filter 表来存储 SDIAD.在检测时,采用滑动窗口无参数 CUSUM 算法(slide non-parametic CUSUM)统计在Δ时间内的进入流量和在此期间新 IP 地址对出现的个数,当它们超过一定的阈值时,则表明有攻击发生.前者主要用于检测一些低分布式的使用合法 IP 地址进行的拒绝服务攻击,而后者根据新 IP 地址对出现的异常可以检测到那些高分布式和反射式拒绝服务攻击.我们的系统主要定位于边缘路由器,对于边缘网络,它比骨干网络有着相对稳定的源目的历史 IP 地址数据库,这将有利于攻击检测,确保了检测的准确率,系统架构如图 1 所示.

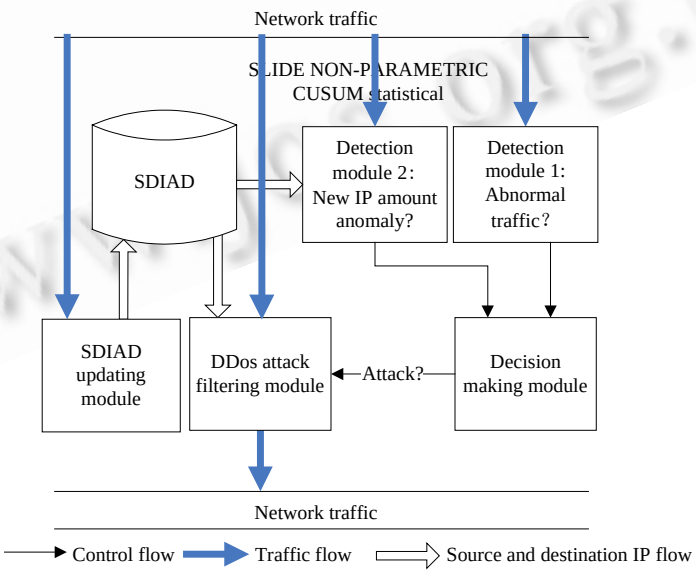

Fig.1 System structure

图 1 系统构架图

3 源目的 IP 地址对数据库(SDIAD)

本文采用扩展的三维 Bloom Filter 表来存储庞大的源目的 IP 地址对信息,主要考虑到源目的 IP 地址对存储、存储空间要求以及查找和计算效率等方面的要求.

定义 1. $SD_i=\{SD_1^i, SD_2^i, \ldots, SD_{n_i}^i\}$,$SD_i$表示在第$i$天所记录到的合法源目的IP地址对,并记$|SD_i|=n_i$.

定义 2. $F^k=\{f_1,f_2,\ldots,f_k\}$.

F^k表示从第 1 天到第k天所记录的达到一定频率的合法源目的IP地址对,并记$|F^k|=m_k$.

定义 3. $A=\{a_1,a_2,\ldots,a_x\}$.

A 表示在一次 DDos 攻击中所出现的源目的 IP 地址对.正常流量的源目的 IP 地址对绝大多数都在以前出现过,而 DDos 攻击流量的源目的 IP 地址则很少,因此有下面的公式:

$$\left|\cup\sum_{i=1}^{k}SD_i\right|<\sum_{i=1}^{k}n_i<|A| \tag{5}$$

显然有$F^k\subseteq\cup\sum_{i=1}^{k}SD_i$,如果以$k$天的源目的IP地址数据记录作为计算新源目的IP地址对出现个数,并记$F=F^k$为常用的合法的源目的IP地址对,则有$P_{normal}=\dfrac{|F\cap S_j|}{|S_j|}$.

P_{normal}表示第j天正常流量的源目的IP地址对在常用的合法的源目的IP地址对中所占的比例;$P_{ddos}=\dfrac{|F\cap A|}{|A|}$,$P_{ddos}$表示一次DDos攻击流量的源目的IP地址对在常用的合法的源目的IP地址对中所占的比例;对于P_{normal}和P_{ddos},理想情况下有$P_{normal}=1$,$P_{ddos}=0$.此时,对DDos攻击检测的准确率为 100%.

定义 4. $Set_{RDIAD}=\left|\cup\sum_{i=j}^{k}SD_i\right|$,$k>=j$,$Set_{RDIAD}$表示在一段时间内(第$j$天到第$k$天)所记录到的合法的源目的IP地址对的集合,SDIAD 即用于存储这样的集合.

在定义 2 中提到"达到一定频率的合法源目的 IP 地址对"这一说法,对于频率大小的衡量标准,使用下面两个规则:

规则 1. $R_1(d)$,表示在SDIAD中至少出现过d天的源目的IP地址对的集合.

规则 2. $R_2(u)$,表示在SDIAD中至少有过u个IP包数据交换的源目的IP地址对集合.

在本文中,联合使用规则 1 和规则 2,记$F=R_1(d)\cap R_2(u)$,表示在规则 1 和规则 2 的约束下所得到的常用的合法的源目的IP地址对集合.SDIAD的存储采用上面提到的Bloom Filter表,Bloom Filter算法设置一个由k个独立hash函数组成的$k\times m$的表结构[17],每个hash函数独立地计算k位的hash值a_{ij}并映射到存储空间为m位的对应位置上去,如图 2 所示.

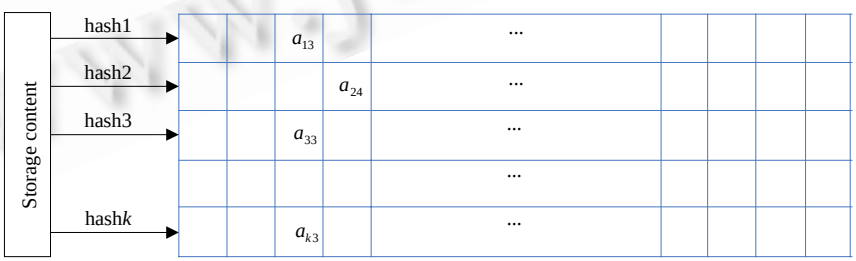

Fig.2 The $k\times m$ hash table

图 2 $k\times m$ 的 hash 映射表

这里,要存储的是源目的IP地址对,并且还要存储在一段时间间隔d天内所有合法的源目的IP地址对.因此,在上面的二维$k\times m$ Bloom Filter表的基础上,还要加上一维——时间,即三维的Bloom Filter存储表$k\times m\times d$.考虑IP

地址本身的*A*,*B*,*C*类特征和源目的IP地址对,共 64 位,这里将其分成 8 位一组,即k=8,m<=2^8,并取m=2^8.此时,hash 映射退化为简单的一一映射,存储空间的要求为 $8\times 2^8\times d$位.

设 SD_j^i 的源地址为 $S_{jA}^i . S_{jB}^i . S_{jC}^i . S_{jD}^i$,目的地址为 $D_{jA}^i . D_{jB}^i . D_{jC}^i . D_{jD}^i$, S_{jA}^i 在三维Bloom Filter存储表的映射为a_{kmd},其中,k=1,m= S_{jA}^i +1,d=i,其他 S_{jB}^i , S_{jC}^i , S_{jD}^i , D_{jA}^i , D_{jB}^i , D_{jC}^i , D_{jD}^i 的映射也类似,则SDIAD建立如图 3 所示.

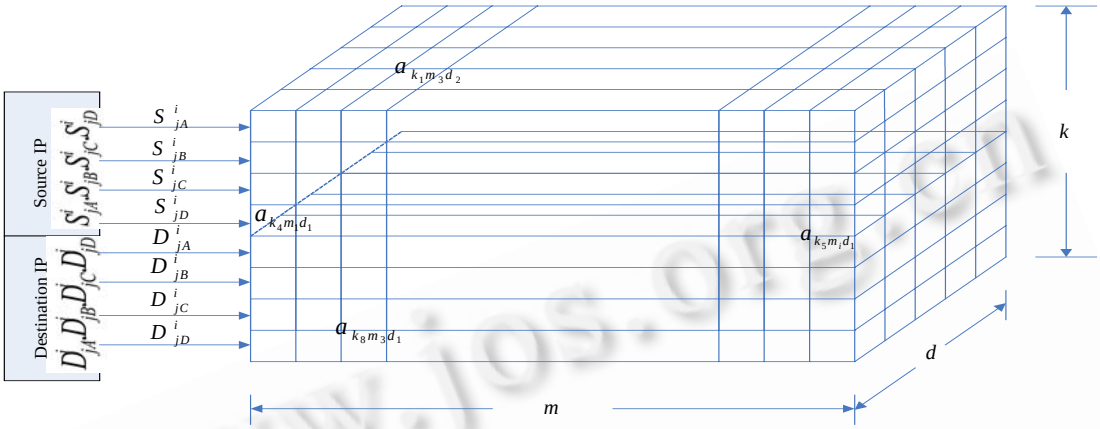

Fig.3 The storage space frame of SDIAD with the 3-dimensional Bloom Filter

图 3 SDIAD 三维 Bloom Filter 表存储空间图

4 SDIAD 更新策略

因特网是一个动态而复杂的不断变化的实体,这就要求 SDIAD 必须不断地进行自我更新,确保 SDIAD 中的源目的 IP 地址对是最近一段时间内记录到的.在本文中,采用先验规则 2 和延迟更新策略,即首先记录下满足规则 2 的新的源目的 IP 地址对.因为此时还不知道该地址对是否是攻击流量的地址对,所以延迟等待一定的时间,当确认无攻击发生时,就将等待的新的源目的 IP 地址对添加到 SDIAD 中去.

另一方面,SDIAD 只保存 *d* 天的源目的 IP 地址对,对于新一天的 IP 地址对必须进行循环更新操作.综合上述两点,更新策略描述如图 4 和图 5 所示.

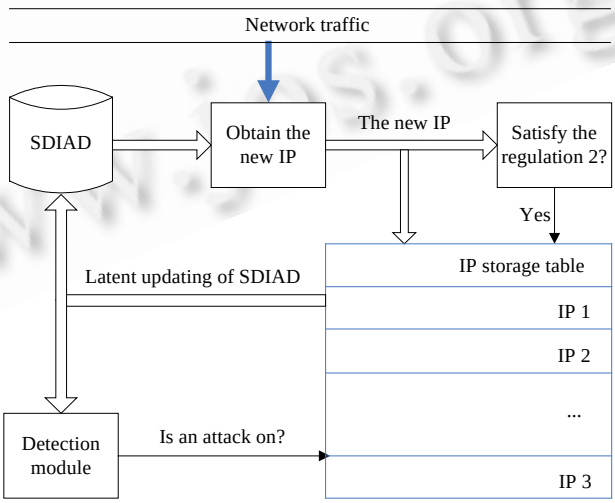

Fig.4 The latency updating strategy of SDIAD

图 4 源目的 IP 地址对延迟更新策略图

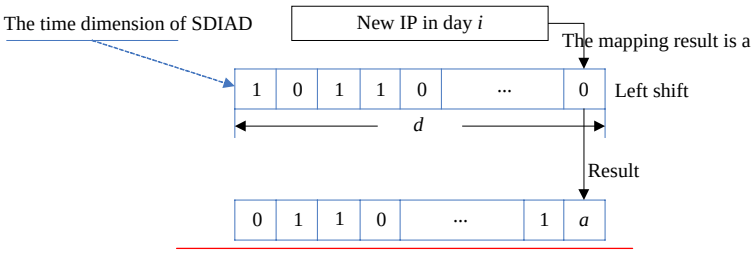

Fig.5 The updating of SDIAD

图 5 SDIAD 循环更新策略图

在图 4 中,SDIAD 更新模块部分不断地从网络流量中获取新的源目的 IP 地址对,并将其缓存在一个记录表里.当 DDos 检测模块检测到攻击时,就将缓存表里的源目的 IP 地址对清空(大部分可能为攻击地址);反之,则将这些地址对加入到 SDIAD 中去.在图 5 中,当记录新一天的 IP 地址对时,首先将所有保存的源目的 IP 地址对信息都进行 d 维上的左移操作,删除最早一天的记录信息,并空出新的空间来记录新一天的源目的 IP 地址对信息.

5 滑动窗口无参数 CUSUM 算法检测

前面提到,CUSUM算法用于检测一个统计过程均值的变化,但CUSUM算法需要一个随机序列的参数模型,以便可以用概率密度函数来监测序列.而无参数CUSUM算法[28]不是具体的模型,它的主要思想是累积比正常运行情况下的平均水平要更高的值.这一算法更适合于分析因特网,它能够以连续方式监测随机变量,从而达到实时检测的目的.

定义 5. 随机序列$\{X_n\}$表示在Δ时间内出现的新的源目的IP地址对个数,在正常情况下,X_n值很小且较为固定,设$E(X_n)=\alpha$.如图 6 所示,其中,h为平均攻击强度,m为发起攻击的时刻.

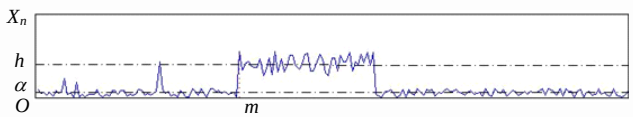

Fig.6 X_n

图 6 序列X_n

非参数CUSUM算法的一个假设条件是随机序列的均值在正常情况下为负,当有变化发生时变为正,这样,在没有丢失任何统计特征的情况下,$\{X_n\}$就被转换为一个负的随机序列.

定义 6. 随机序列$\{Z_n\}$,其中,$Z_n=\Phi-\beta$.对于给定的网络环境,参数β是常数,它可以帮助产生均值为负的随机序列Z_n,以便$\{Z_n\}$所有的负值不会随时间而累积.当攻击发生时,Z_n会突然变得很大并且为正,通过累积具有正值的Z_n来显示攻击发生与否.如图 7 所示,其中,h为平均攻击强度,m为发起攻击的时刻.

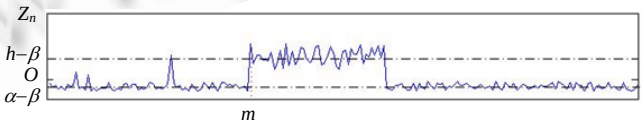

Fig.7 Z_n

图 7 序列Z_n

定义 7. Z_n的累积值y_n,$y_n=S_n-\min_{1\le k\le n} S_k$,其中,$S_0=0$,$S_k=\sum_{i=1}^{k} Z_i$.为了提高计算效率,有下面的递归定义:

$$y_n=(y_{n-1},Z_n)^+ \tag{6}$$

$y_0=0$,其中,x^+当$x>0$ 时就等于x,否则等于 0.当y_n超越一定的门限N时,就表明检测到统计特性的变化,即发生了攻

击,其值累积得越大,表明攻击越强.如图 8 所示,N为攻击检测门限,m为攻击发起时刻,τ_m为检测到攻击的时刻.

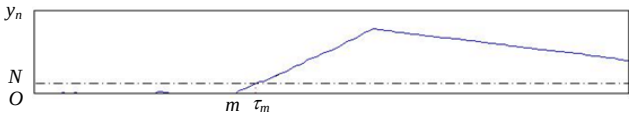

Fig.8 Non-Parametic CUSUM sequence y_n

图 8 无参数CUSUM算法序列y_n

上面描述的是一种检测随机序列$\{Z_n\}$有没有统计特性变化的无参数CUSUM算法,在应用到本文中检测源目的IP地址对的统计特性变化时,在攻击结束的下延,由于开始累积了很高的y_n值,导致在攻击停止之后y_n值下降得很慢,这对于检测攻击停止的时刻会有很大的延迟,由图 7 可以明显地看出这一点.另一方面,考虑到时间和统计特征的相关性,已经过去很久的参数Z_k对当前统计特性的判断影响比较小.例如,前一次攻击所统计的Z_n值对新的一次攻击的y_n值的累积效应应该移除.尽管y_n值随着时间的推迟也能回到一个正常值,但这是一个缓慢的过程,对于检测攻击的灵敏度有很大的影响.因此,在本文中采用滑动窗口无参数CUSUM算法来检测统计特性的变化.滑动窗口无参数CUSUM算法的y_n值只累积一定窗口时间内的Z_n值.

定义 8. 窗口时间T,共包含有k个Δ时间,则滑动窗口累积函数y_n如下:

$$y_n=\begin{cases}\sum_{i=1}^{n}(Z_i)^+, & n<k\\ \sum_{i=n-k+1}^{n}(Z_i)^+, & n\ge k\end{cases} \tag{7}$$

同样,我们有如下的递归定义:

$$y_n=\begin{cases}y_{n-1}+(Z_n)^+, & n\le k\\ y_{n-1}+(Z_n)^+-(Z_{n-k})^+, & n>k\end{cases} \tag{8}$$

y_0=0,y_n即表示在窗口时间T内出现的新的源目的IP地址对的个数.如图 9 所示,其中,N为攻击检测门限,m为攻击发起时刻,τ_m为检测到攻击的时刻,从该图中也可以看出,在攻击停止之后,y_n下降得很快.

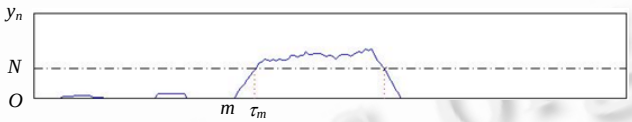

Fig.9 Slide non-parametic CUSUM sequence y_n

图 9 滑动窗口无参数CUSUM算法序列y_n

定义 9. 攻击检测判决函数:

$$d_N=\begin{cases}0, & y_n\le N\\ 1, & y_n>N\end{cases} \tag{9}$$

N为攻击检测的门限,当$y_n>N$时表明攻击已经产生.

衡量一个攻击检测机制有几项指标:检测延迟时间、误检率和漏检率.然而,这几项指标又是互相制约的,Slide non-parametic CUSUM 算法通过设置恰当的β,N 和 T 参数值来达到它们之间的平衡.设 h 为Δ时间内攻击所发送的平均新的源目的 IP 地址对数,Slide non-parametic CUSUM 算法窗口滑动时间 $T=k\times\Delta$,则有:

攻击开始检测延迟:

$$D_1=\frac{N}{h-\beta}\times\Delta \tag{10}$$

攻击结束检测延迟:

$$D_2=\left(k-\frac{N}{h-\beta}\right)\times\Delta,\text{其中},k>\frac{N}{h-\beta} \tag{11}$$

由上面的公式可知,攻击强度 h 越大,则攻击开始检测延迟越短,攻击结束检测延迟越长;检测门限 N 越大,则攻击开始检测延迟越长,攻击结束检测延迟越短.此外,N 值越大,误检率越小,漏检率越大,反之亦然.另一方面,参数的选取是与实际的网络环境密切相关的.若取 β=0.5,h=2,N=10,Δ=1s,k=10,即 $T=k\times\Delta$=10s,则有:

$$D_1=\frac{N}{h-\beta}\times\Delta=6.7(\text{s}),$$

$$D_2=\left(k-\frac{N}{h-\beta}\right)\times\Delta=3.3(\text{s}).$$

6 策略比较

文献[16,29]提出的使用源 IP 地址检测 DDos 攻击策略,由于仅仅考虑到源 IP 地址,只能从单个网络的范围内来限定合法的访问.即,就同一个网络来说,该网络中的两个目的 IP 地址拥有完全相同的合法源 IP 地址集.这是不合理的,也在一定程度上降低了检测的准确率.

设IAD_s,IAD_d分别表示靠近攻击者端和受害者端的合法源IP地址数据库,则在靠近攻击者端检测的时候,只要是非伪造的源IP地址都会属于IAD_s,也就是合法的,这给HDDos和DRDos攻击的检测带来了困难;在靠近受害者端检测时,只要源IP地址属于IAD_d,而IAD_d的范围很大,这也会降低DDos检测的准确率.

而本文的策略基于源目的 IP 地址对,虽然也定位于边缘路由器,但它却在单个连接上来限定合法的访问,对不同的目的 IP 地址,它们有着不同的合法源目的 IP 地址对集,显然,这种机制提高了攻击检测的准确率.

设$SDIAD_s$,$SDIAD_d$分别表示靠近攻击者端和受害者端的合法源目的IP地址数据库,在检测时,无论靠近攻击者端还是受害者端,我们的策略都会同时检测源和目的IP地址在$SDIAD_s$或$SDIAD_d$中的合法性,这极大地缩小了IP地址合法性的检测范围,对于HDDos和DRDos的检测同样也有效,提高了检测的准确率.

7 系统仿真

本系统采用DAPAR(defense advanced research projects agency)入侵检测数据集[30]来对文中基于源目的历史IP地址的防范DDos攻击策略进行仿真.在仿真中,首先建立SDIAD,我们用正常的DAPAR流量对文中的检测引擎进行训练,通过对其中源目的IP地址对的处理,这里一共建立了 14 天的源目的历史IP地址对数据记录.并且计算常用的合法源目的IP地址对集合F,根据上面建立的SDIAD,分别计算$F=R_1(d)$,$F=R_2(u)$(参考第 3 节的规则 1 和规则 2),并设Set_R为规则R所参考的所有源目的IP地址集合.

记 $\Phi=\frac{|F|}{|Set_R|}$ 为常用的合法源目的 IP 地址集合 F 占整个参考的源目的 IP 地址结合的百分比,有如图 10 和图 11 所示的Φ分布:

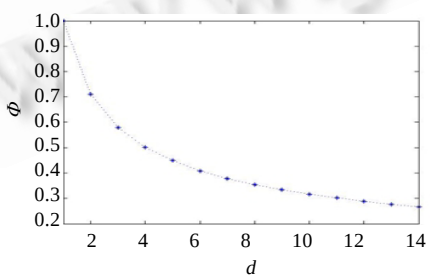

Fig.10 Φ of $R_1(d)$

图 10 $R_1(d)$的Φ分布图

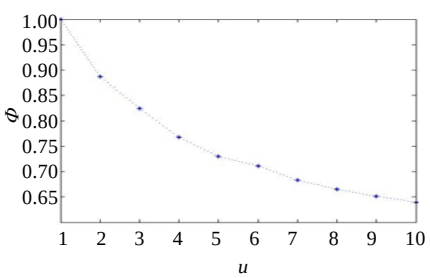

Fig.11 Φ of $R_2(u)$

图 11 $R_2(u)$的Φ分布图

下面使用 DAPAR 数据集里的 DDos 攻击数据对我们的策略进行检测.在仿真中,取滑动窗口无参数 CUSUM 算法的相关参数为Δ=1s,k=20,即 $T=k\times\Delta$=20s,判决门限 N=40;Δ=1s,k=20,即 $T=k\times\Delta$=20s,判决门限 N=40;并取不同的 d 值和 u 值来进行仿真,检测结果见表 1~表 3.仅检测源 IP 地址的策略结果见表 4~表 6.

从表中的数据对比可以看出,我们的策略无论在攻击者端还是在受害者端都有很好的检测效率,在受害者端的检测效率优于攻击者端,主要是由于Dos攻击的分布式特性,在攻击者端攻击流量是分布式的,只有在受害者的网络这些流量才会汇聚.与文献[16,29]中仅基于源IP地址的策略相比较,本文的策略有更高的检测准确率和更短的检测延迟.其中,d值和u值的选取与检测引擎的性能参数密切相关.当d=2 或u=5 时,系统在检测准确率和检测延迟方面都有一个较好的平衡点.另一方面,当我们采用联合规则,即$F=R_1(d)\cap R_2(u)$时(其中, d=2,u=5),仿真结果与d=2 或u=5 的结果差不多,这主要是因为集合$R_1(2)$和集合$R_2(5)$有很大一部分是相同的,此外还会与实际的流量数据有关.

Table 1 The detection results based on different values of d

表 1 取不同 d 值时的系统检测效率

d	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
1	0	0	6.7	15.7	12.3	13.3	8.1	7.2
2	1.1	0.7	2.3	9.3	11.8	12.8	8.9	7.5
3	4.1	1.1	0	6.7	11.2	12.2	9.4	7.7
4	11.7	11.7	0	0	9.8	10.1	10.8	9.4

Table 2 Detection results based on different values of u

表 2 取不同 u 值时的系统检测效率

u	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
1	0	0	6.7	15.7	12.3	13.2	8.1	7.4
2	0	0	5.3	9.3	12.1	12.6	8.2	7.3
3	0	1.1	5.3	6.7	11.7	12.1	8.7	7.7
4	1.1	1.1	3.7	6.7	11.5	11.9	8.8	8.1
5	1.1	4.1	2.3	2.3	11.6	11.5	8.6	8.2
6	1.1	4.1	2.3	0	11.5	11.6	8.5	8.9
7	4.1	11.7	0	0	10.6	10.6	10.1	9.7

Table 3 Detection results when d=2, u=5

表 3 d=2,u=5 时的系统检测效率

(d,u)	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
(2,5)	1.1	4.1	2.3	2.3	12.1	12.3	8.2	8.1

Table 4 The detection results based on different values of d

表 4 取不同 d 值时的系统检测效率

d	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
1	0	0	15.7	23.1	13.3	14.7	10.3	9.2
2	0	0	15.3	15.7	12.7	13.2	11.1	9.4
3	1.1	0	9.3	15.7	11.9	12.2	11.4	10.1
4	5.3	5.3	6.7	6.7	10.8	11.5	12.7	11.5

Table 5 Detection results based on different values of u

表 5 取不同 u 值时的系统检测效率

u	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
1	0	0	23.1	31.9	13.1	14.3	9.3	8.8
2	0	0	23.1	31.9	12.7	13.2	10.1	9.1
3	0	0	15.7	15.7	12.1	12.1	10.3	9.6
4	4.1	1.1	13.2	15.7	11.7	11.9	10.6	10.3
5	4.1	4.1	9.3	9.3	11.7	12.0	11.1	10.7
6	7.6	4.1	9.3	9.3	10.3	11.2	11.7	11.2
7	7.6	5.3	9.3	9.3	9.5	10.9	11.9	12.4

Table 6 Detection results when d=2, u=5

表 6 d=2,u=5 时的系统检测效率

(d,u)	Rate of false alarm (%)		Rate of missed alarm (%)		Average detection latency of attack outset (s)		Average detection latency of attack ending (s)	
Detection position	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker	Near to victim	Near to attacker
(2,5)	4.1	4.1	9.3	9.3	12.7	12.1	8.02	8.5

8 结论和未来工作

本文提出了一种基于源目的历史 IP 地址对的 DDos 攻击检测方法,检测引擎采用 Slide non-parametric CUSUM 算法统计不在集合 F 里面的地址对的个数,并以此来判决 DDos 攻击发生与否,有很高的准确率和灵敏度.此外,SDIAD 一方面可以用来检测攻击,另一面还可以根据 SDIAD 来进行包的过滤,在检测到 DDos 攻击之后启动,将那些非法的源目的地址对之间的包丢弃.

在以后的工作中,SDIAD 的建立仍然是一个重点,一个有效的 SDIAD 是检测引擎的关键.可以考虑采用新的规则来建立常用的合法源目的IP地址对.例如建立一次完成的TCP连接的地址对才是合法的等等.另一方面,如何将该策略推广到骨干路由器上去,由于骨干网络更加复杂,不断动态变化这一特征更加明显,因此可以考虑将 SDIAD 应用到分布式的骨干网络环境中去,在各个路由器不同的 SDIAD 之间交换源目的历史 IP 地址对信息等.

References:

[1] CNN. Immense network assault takes down yahoo. 2000. http://www.cnn.com/2000/TECH/computing/02/08/yahoo.assault.idg/index.html

[2] CNN. Cyber-Attacks batter Web heavyweights. 2000. http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html

[3] Hicks M. DDoS attack knocks out DoubleClick Ads. 2004. http://news.bbc.co.uk/1/low/business/3713174.stm

[4] CNN. Denial-of-Service attacks on the rise? 2002. http://www.cnn.com/2002/TECH/internet/04/09/dos.threat.idg/index.html

[5] Paxson V. An analysis of using reflectors for distributed denial-of-service attacks. Computer Communication Review, 2001, 31(3):38−47.

[6] Gibson S. Distributed reflection denial of service. 2002. http://grc.com/dos/drdos.htm

[7] Savage S, Wetherall D, Karlin A, Anderson T. Network support for IP traceback. IEEE/ACM Trans. on Networking, 2001,9(3): 226−237.

[8] Song DX, Perrig A. Advanced and authenticated marking schemes for IP traceback. In: Proc. of the IEEE INFOCOM 2001. http://paris.cs.berkeley.edu/perrig/projects/iptraceback/triptrace.ps.gz

[9] Belenky A, Ansari N. IP traceback with deterministic packet marking. Communications Letters, 2003,7(4):162−164.

[10] Ioannidis J, Bellovin SM. Implementing pushback: Router-based defense against DDoS attacks. In: Proc. of the Network and Distributed System Security Symp. 2002. http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/ioanni.pdf

[11] Mahajan R, Bellovin SM, Floyd S, Ioannidis J, Paxson V, Shenker S. Controlling high bandwidth aggregates in the network. Technical Report, AT&T Center for Internet Research at ICSI (ACIRI) and AT&T Labs. Research, 2001.

[12] Bellovin S. The ICMP traceback message. Internet Draft, IETF, 2000. draft-bellovin-itrace-05.txt. http://www.research.att.com/?smb

[13] Wu SF, Zhang LX, Massey D, Mankin A. Intension-Driven ICMP trace-back. Internet Draft, IETF, 2001. draft-wu-itrace-intension-00.txt

[14] Yau DKY, Lui JCS, Feng L, Yeung Y. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Trans. on Networking, 2005,13(1):29−42.

[15] Khorashadi-Zadeh H. A novel approach to detection high impedance faults using artificial neural network. In: Proc. of the 39th Int'l, Vol.1. 2004. 373−376.

[16] Tao P, Leckie C, Ramamohanarao K. Detecting distributed denial of service attacks using source IP address monitoring. 2004. http://www.ee.mu.oz.aupgradtaopresearchdetection.pdf

[17] Bloom B. Space/Time trade-offs in hash coding with allowable errors. Communications of the ACM, 1970,13(7):422−426.

[18] Gremillion LL. Designing a bloom filter for differential file access. Communications of the ACM, 1982,25(9):600−604.

[19] Mullin JK. A second look at bloom filters. Communications of the ACM, 1983,26(8):570−571.

[20] Fan L, Cao P, Almeida J, Broder AZ. Summary cache: A scalable wide-area web cache sharing protocol. IEEE/ACM Trans. on Networking, 2000,8(3):281−293.

[21] Chan EYK, Chan HW, Chan KM. IDR: An intrusion detection router for defending against distributed denial-of-service (DDoS) attacks. In: Proc. of the 7th Int'l Symp. on Parallel Architectures. IEEE, 2004. 581−586.

[22] Kim YH, Lau WC. Packetscore: Statistical-based overload control against deistributed denial-of-service attacks. In: Proc. of the IEEE INFOCOM. 2004. http://www.ieee-infocom.org/2004/Papers/54_2.PDF

[23] Wang HN, Zhang DL, Shin KG. Detecting SYN flooding attacks. INFOCOM, 2002,3:1530−1539.

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

[25] Sun ZX, Tang YW. Router anomaly traffic filter algorithm investigation 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

[26] Houle KJ, Weaver GM, Long N, Thomas R. Trends in denial of service attack technology. Technical Report, CERT and CERT Coordination Center, 2001.

[27] 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 Word Wide Web Conf. 2002. http://nms.lcs.mit.edu/papers/flash-crowds02.pdf

[28] Bassevilleand M, Nikiforov IV. Detection of Abrupt Changes: Theory and Application. Prentice Hall, 1993.

[29] Tao P, Leckie C, Ramamohanarao K. Protection from distributed denial of service attacks using history-based IP filtering. Communications, 2003,1(1):482−486.

[30] MIT Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific datasets. 2000. http://www.ll.mit.edu/IST/

附中文参考文献:

[24] 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

[25] 孙知信,唐益慰.基于特征提取的路由器异常流量过滤算法研究.软件学报,2006,17(2):295−304. http://www.jos.org.cn/1000-9825/17/295.htm

孙知信(1964－),男,江苏南京人,博士,教授,主要研究领域为计算机网络与安全,计算机仿真,软件工程.

李清东(1981－),男,硕士生,主要研究领域为计算机网络与安全.