第33卷 第16期 计 算 机 工 程 2007年8月
Vol.33 No.16 Computer Engineering August 2007
·安全技术· 文章编号：1000—3428(2007)16—0139—03 文献标识码：A 中图分类号：TP393

基于流连接信息熵的DDoS攻击检测算法

赵继俊，胡志刚，张 健
(中南大学信息科学与工程学院，长沙 410083)

摘 要：分析了分布式拒绝服务(DDoS)攻击的特点，提出了流连接信息熵的定义，并通过对流连接信息熵时间序列的分析，采用非参数CUSUM算法进行DDoS攻击检测。该检测方法对固定IP、端口号随机变化的DDOS攻击有比较好的检测效果。实验结果证明，该方法能够以较高的精确度及时地检测出DDoS 攻击行为。

关键词：分布式拒绝服务攻击；相关数据包；流连接信息熵；非参数CUSUM算法

DDoS Attacks Detection Algorithm Based on Flow Connection Entropy

ZHAO Ji-jun, HU Zhi-gang, ZHANG Jian
(School of Information Science & Engineering, Central South University, Changsha 410083)

【Abstract】 On the basis of analyzing the features of distributed denial of service (DDoS) attacks, flow connection entropy time series analysis is proposed. It uses non-parametric CUSUM algorithm to complete the detection task of DDoS attacks. It minimizes the average delay of detection for a given false alarm rate. It has better detection effect on the fixed source IP and random destination ports's DDoS. Experimental result demonstrates this model can detect DDoS attack as early as possible with high detection accuracy.

【Key words】 DDoS attack; correlational packet; flow connection entropy(FCE); non-parametric CUSUM algorithm

1 概述

分布什拒绝服务攻击(DDoS)，是一种分布式的、协作的大规模拒绝服务攻击，能在一定时间内，彻底使被攻击的网络丧失正常服务功能。随着DDoS攻击软件的出现，如Trinoo,TFN,TFN2K等，发起DDoS攻击变得更加容易，许多著名的网站，如Yahoo, Amazon及CNN等都曾因DDoS攻击导致网站关闭[1]。因此，防御DDoS攻击在网络安全中就显得尤为重要。

总体上，DoS攻击和DDoS攻击都使用同一种方法，即用大量的垃圾数据包来堵塞网络，使得网络终端过于繁忙，超出了其正常运行的范围，使其不能完成正常的服务。这种攻击很难防御，因为它在网络层和传输层上消耗资源，在这两个层上很难验证一个访问是善意的还是恶意的。近期的研究表明，目前的DDoS攻击采用随机欺骗源地址、目的端口的数据包，这就掩饰了攻击的真实来源，使得过滤更加困难，也需要更加高级的业务建模技术。

防御DDoS攻击已成为一个非常活跃的研究领域[2]。文献[3]中的算法只能用于检测SYN FLOOD攻击，而对于其他的Dos/DDos攻击则无法检测；文献[4]运用了网络流量的自相似性特性进行分析；文献[5]对源IP地址过滤来检测防御DDoS攻击。以上的研究从不同方面对DDoS攻击进行了研究，但也存在各自的缺陷，需要有一定的先验知识，难于区分突发正常流量。文献[6]运用熵的方法对网络流量进行检测，根据在网络截获的数据包的源IP地址的数量变化特征，用统计方法来计算总体能量的变化特征，检测网络的异常。这种方法适合检测分布式的拒绝服务攻击，但对源IP地址比较固定的攻击效果不好。

基于对上述算法的研究，本文提出了一种分析网络流连接信息熵时间序列，运用非参数CUSUM算法统计一个特征量，实现了DDoS攻击检测。该方法不需要了解攻击细节，能有效区分正常的流量增加与DDoS攻击所导致的流量增加，对于固定IP、端口号随机变化的DDOS攻击有比较好的检测效果。

2 DDoS 攻击分析

DDoS攻击的基本过程如图1。攻击主机通过长时间准备，入侵大量攻击从机，并在从机上安装守护进程(Daemon)，当攻击从机接受到攻击命令后，首先攻击从机向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息，因为地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就始终没有被释放。当服务器等待一定的时间后，连接会因超时而被切断，攻击从机会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽，甚至导致系统崩溃。

DDoS攻击通常采用对目标主机的某个端口请求大量的服务或对目标主机的多个端口请求服务，以消耗目标主机的资源。为了隐藏攻击者的真实位置，DDoS攻击在实施过程中会随机伪造攻击数据包的源IP地址，或者使用大量的反射服务器，这会引起网络流量的某些特性发生改变。所以，同时综合考虑源IP地址、目的IP地址、目的端口号这些参量，研究彼此数据包的相关性，就可以有效地检测DDoS攻击。

作者简介：赵继俊(1981－)，男，硕士研究生，主研方向：网络安全；胡志刚，博士后、教授、博士生导师；张 健，讲师、博士研究生
收稿日期：2006-10-18 **E-mail：**captainstag@163.com

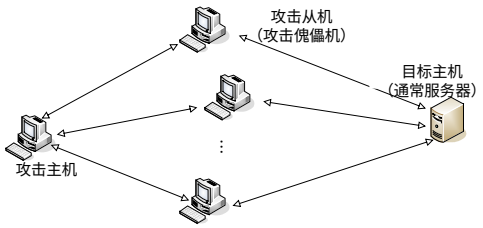


图 1　典型 DDoS 攻击示意图

3　检测算法

本文的检测算法是在因特网上统计数据包头的一些信息。通过在核心路由器上或提供服务的服务器的监视器，监视到达数据包的源 IP 地址、目的 IP 地址、目的端口号等信息，然后统计单位时间内的流连接信息熵这个统计量，通过更进一步计算熵值分布，来测量这个熵值分布的随机性。如果出现一个较大的阶跃，就认为可能预示着一个 DDoS 攻击。下面给出能够反映 DDoS 攻击所导致的流量特性变化的流连接信息熵(FCE)的定义：

定义 1 R={p_1,…,p_i,…,p_j}为IP数据包集合，其中数据包元素为三元组形式，即p_i=(s_i,d_i,$port_i$)其中，s_i,d_i,$port_i$分别表示数据包i的源IP地址、目的IP地址、目的端口号。若p_1,…,p_i,…,p_j的源、目的IP地址及目的端口号均相同，则称其为一组相关数据包，称集合R为相关数据包集合。相关数据包集合内元素个数至少为 1[7]。

定义 2 假设单位时间网络流量内的数据包集合为P={p_1,p_2,…,p_M},其内相关数据包集合为Q={Q_1,Q_2,…,Q_N},|Q_i|表示集合Q_i中数据包的数量;对集合Q中相同|Q_i|的数据包再次聚集，得到集合D={D_1,…,D_i,…,D_K}，其中，D_i表示有i个数据包彼此相似的集合。

假设某网络流中数据包的源、目的IP地址及目的端口如图 2 所示，根据源、目的IP地址及目的端口进行聚合后的对应关系如图 3 所示。此网络流的数据包集合为{p_1,p_2,p_3,p_4,p_5,p_6,p_7,p_8}，根据定义 1 相关数据包集合有R_1={p_1,p_2},R_2={p_3},R_3={p_4,p_5},R_4={p_6,p_7,p_8}。根据定义 2，|R_3|=2，|R_2|=1；再次聚集后的集合D={D_1,D_2,D_3}，其中，D_1={R_2}；D_2={R_1,R_3}；D_3={R_4}。D_1表示彼此不相关的数据包集合；D_2表示有两两相关的数据包彼此相似的集合。

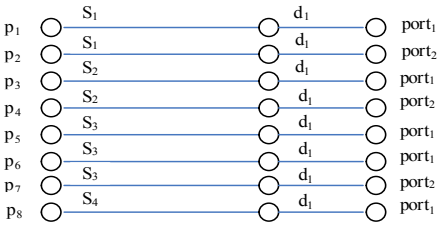


图 2　数据包源、目的地址及目的端

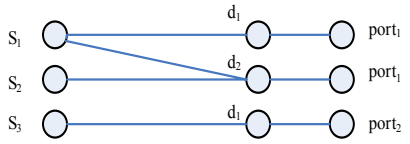


图 3　聚合处理后的对应关系

定义 3 时间间隔⊿t内相关数据包x_i出现的频率近似为该x_i的出现概率p(x_i)，所以某段连续报文流的信息熵(FCE):

$$H(X)=-\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$$

其中，p(x_i)为数据包x_i在时间间隔⊿t内出现的概率。

结合上述分析及定义 2 可以看出，DDoS 攻击会引起网络流的FCE异常增加。当然，合法的访问用户的增加也会使 FCE 增大，但合法用户在一定的时间段内的请求服务方式是单一的，或者请求服务的数量是有限的，而且其D_1类型的数据包不会增加得非常显著，这就是其与DDoS攻击行为的　不同。

4　基于非参数 CUSUM 决策算法

CUSUM(Cumulative Sum)算法通常用于检测一个统计过程均值的变化。通常CUSUM需要随机序列的参数模型，以便可以用概率密度函数来监控序列。但因特网是一个动态而复杂的实体，其业务模型的理论结构是一个复杂的问题，因而，一个主要的难题是如何模拟随机序列{W_n}，而非参数CUSUM算法不是具体的模型，更适合于分析因特网[8]。非参数CUSUM算法的主要思想是：累积明显比正常运行情况下的平均水平高的{W_n}值。该算法的优点之一是，能以连续方式监控输入的随机变量，从而达到实时检测。

本文的目的是通过监控测⊿t时间间隔内的FCE来实现DDoS攻击的检测。设W_n代表在时间间隔⊿t内的熵值。为了尽可能在攻击发生的早期实现实时检测，需要把序列{W_n}转换成以下的连续函数的形式：

$$W_n = a + \xi_n I(n < m) + (h + \eta_n) I(n \geq m) \quad (1)$$

其中，$E(W_n)=a$；$\xi = \{\xi_n\}_{n=1}^{\infty}$；$\eta = \{\eta_n\}_{n=1}^{\infty}$是两个随机序列；$E(\xi_n) = E(\eta_n) \equiv 0$，$h \neq 0$。

$I(H)$是一个指示器函数，当H条件满足时函数取值为 1，不满足则为 0。对于序列{W_n}，若其均值在m点存在一个由a到$a+h$的阶跃变化，则表明序列值发生了突变，需要寻求一个算法以连续的方式检测出步长至少为h的序列值变化，确定相应的跃点(m点)。本文采用了非参数的CUSUM算法[8]，通过累加明显超过正常情况下随机序列均值的变化量来检测网络通信量的异常变化，它的优点在于连续方式检测，能够实现低误警率情况下的实时检测，及时发现DDoS攻击行为；另外这种检测方法实现简单，无须建立一个较为复杂的网络通信量正常或异常模型。

假设在网络流量比较大的时间段内实施该算法，W_n在网络通信量正常情况下，其值接近于平稳。为了满足非参数的CUSUM算法的要求，需要将式(1)作进一步转换，即$Q_n=W_n-\sigma$，当$a'=a-\sigma$，$h>>\sigma$; σ是依据特定的网络环境计算的偏移值，通过这个偏移值将序列{W_n}在正常情况下的均值转换为负数，而当发生异常时才使序列值变为正数，从而适用于无参数的CUSUM算法。

$$Q_n = a' + \xi_n I(n < m) + (h + \eta_n) I(n \geq m) \quad (2)$$

其中，$a'<0$；$-a'<h<1$。

根据非参数的CUSUM算法，随机序列{Q_n}产生负数均值φ，当攻击发生时，Q_n将突变到正数($h+a'>0$，为攻击发生时序列{Q_n}增长的最小值)，此时将此序列的正值进行累加、负值忽略，当某一时刻的累加值超过了指定的阈值，便可以判定DDoS发生；当网络通信量正常时，{Q_n}序列值多为负数或非连续的小值正数，累加数值不会超过各自阈值。此时算法进一步转换为计算式(3)的问题。值得注意的是，h是攻击发生时均值增长的最小值，它并不是算法中攻击检测的　阈值。

$$\psi_n = S_n - \min_{1 \leq k \leq n} S_k \quad (3)$$

其中，$S_k = \sum_{i=1}^{k} Q_i$；$S_0 = 0$。

Ψ_n作为检测的统计特征，为降低检测的在线运行消耗，使用非参数CUSUM算法的递归版本，表示如下：

$$\psi_n = (\psi_{n-1} + Q_n)^+ \tag{4}$$

其中，x^+表示当$x>0$ 时x^+等于x，当x≤0 时x^+为 0。一个较大的Ψ_n值(超过对应的阈值)意味着网络中存在攻击行为。Ψ_n表示$\{Q_n\}$正序列值的累加。当$\Psi_{tN} \geq N$时意味着在t_N时刻统计量发生跃变，网络正遭受分布式拒绝服务攻击。基于⊿t时间间隔内的FCE的决策函数描述如下：

$$W_N(\psi_n) = \begin{cases} 0 & \psi_n \leq N \\ 1 & \psi_n > N \end{cases} \tag{5}$$

其中，N是攻击检测的阈值；$W_N(\Psi_n)$表示在时间n时，若为 1 则意味着$\Psi_n > N$，表示有攻击行为发生；若为 0，表示网络通信量正常。参考文献[9]，将目标检测时间定为可以到达的最小值 5s，即$\tau_N = m+5$；取$|a|=0.05$，$h=0.1$，得到

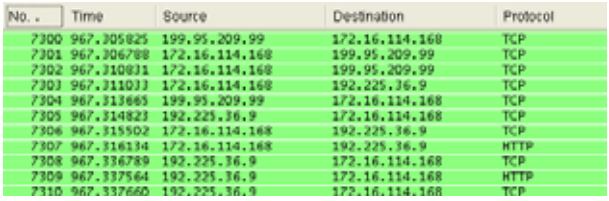
$$\rho_N \to \gamma = \frac{1}{h-|a|} = \frac{1}{0.1-0.05} = 20$$

$$N = \frac{(\tau_N - m)^+}{\rho_N} = \frac{(m+5-m)}{20} = 0.25$$

其中，ρ_N是标准化的检测时间；m是攻击发起时刻；$a(a<0)$是正常运转中$\{Q_n\}$的均值；$h-|a|$是当攻击发生时$\{Q_n\}$均值的较底边界。

5 性能评估

本文实验数据使用了MIT 林肯实验室的 2000 年分布式拒绝服务攻击数据集LLDOS1.0 [10]。为了使实验数据更具一般性，在攻击数据集的基础上增加了背景流量，背景流量取自MIT 1999 年的数据集。通过TcpDump获取的数据集如图 4 所示。假设攻击通信流量的速率是稳定的，攻击周期为 40s，这个阶段监视器上获得的FCE的变化情况如图 5 所示。



No.	Time	Source	Destination	Protocol
7300	967.305825	199.95.209.99	172.16.114.168	TCP
7301	967.306788	172.16.114.168	199.95.209.99	TCP
7302	967.310031	172.16.114.168	199.95.209.99	TCP
7303	967.311033	172.16.114.168	192.225.36.9	TCP
7304	967.313665	199.95.209.99	172.16.114.168	TCP
7305	967.314823	192.225.36.9	172.16.114.168	TCP
7306	967.315502	172.16.114.168	192.225.36.9	TCP
7307	967.316134	172.16.114.168	192.225.36.9	HTTP
7308	967.336789	192.225.36.9	172.16.114.168	TCP
7309	967.337564	192.225.36.9	172.16.114.168	HTTP
7310	967.337660	192.225.36.9	172.16.114.168	TCP

图 4 TcpDump 获取的数据集

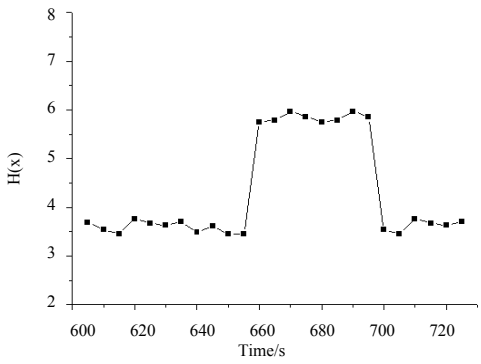


图 5 对于模拟的 DDoS 攻击的 FCE

假设Σ代表单位时间⊿t 的网络数据包总数；Ω代表单位时间⊿t 时间内的异常数据包。当源 IP 地址固定时，目的端口号随机时的 DDoS 攻击用 CUSUM 算法检测的实验结果如图 6 所示。

在实验中模拟测试不同的Σ值和不同的Ω值。针对图 4 中的DDoS攻击，当Ω_1=20 时，在攻击后的前 10s未能检测到DDoS攻击，直到第 15s累积和才超过阈值，即检测出DDoS攻击；当Ω_2=30 时候，在攻击发生后的第 1 个⊿t(5s)时间内就检测到DDoS攻击。实验证明当异常数据包增大时，检测时间明显缩短。

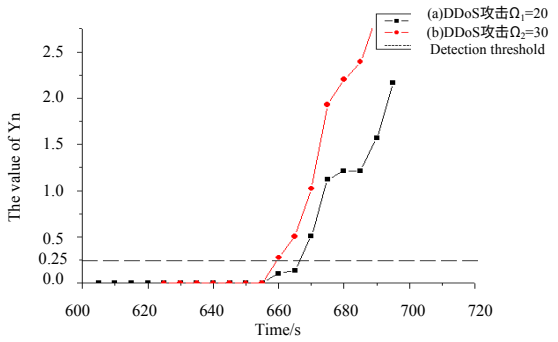


图 6 对于模拟的 DDoS 攻击的检测结果

6 结束语

本文分析了 DDoS 攻击的特点，定义了 FCE 的概念，并提出了基于 FCE 时间序列 CUSUM 算法的 DDoS 攻击检测新方法，实现了 DDoS 攻击自动检测。实验结果证明了该方法对 TCP 类型的 DDoS 攻击检测的有效性及准确性。但对于 ICMP 等类型的 DDoS 攻击还需要进一步设计数据包异常的判定规则。后续的研究包括：使用其他的在线或离线数据集进一步试验；将本检测方法扩展到其他类型的异常检测中。

参考文献

1 Lau F, Rubin S H, Smith M H, et al. Distributed Denial of Service Attacks[C]//Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Nashville. 2000.

2 Moore D, Voeker G M, Savage S. Inferring Internet Denial-of-Service Activity[C]//Proceedings of USENIX Security Symposium. 2001.

3 Wang H N, Zhang D L, Kang G S. Detecting SYN Flooding Attacks[C]//Proc. of INFOCOM'02. 2002.

4 Xiang Y, Lin Y, Lei W L, et al. Detecting DDOS Attack Based on Network Self-similarity[C]//Proc. of IEEE Int'l Conf. on Communications. 2004.

5 Tao Peng, Leckie C, Ramamohanarao K. Defending Against Distributed Denial of Service Attack Using Selective Pushback[C]// Proceedings of the 9th IEEE International Conference on Telecommunications, Beijing, China. 2002.

6 Feinstein L, Schnackenberg D, Balupari R, et al. Statistical Approaches to DDoS Attack Detection and Response[C]//Proc. of the DARPA Information Survivability Conf. and Exposition. 2003.

7 孙钦东, 张德运, 高 鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报, 2005, 28(5).

8 Tao Peng, Leckie C, Ramamohanarao K. Proactively Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring[C]//Proceedings of the 3rd International IFIP-TC6 Networking Conference. 2004.

9 林 白, 李 鸥. 基于序变化检测的 DDoS 攻击检测方法[J]. 计算机工程, 2005, 31(9).

10 MIT Lincoln Laboratory. 2000 DARPA Intrusion Detection Scenario Specific Data Sets[EB/OL]. (2003-10-21). http://www.ll.mit.edu/ IST/.