# 频域过滤 DoS 攻击方法的研究

吴志军 张 东
(中国民航大学通信工程系 天津 300300)

**摘 要**：拒绝服务 DoS(Denial of Service)攻击已逐渐成为全世界网络最严重的威胁之一。其攻击方式主要通过连续发送大量的数据包，耗尽网络资源，造成连接阻塞。该文采用数字信号处理的方法对 DoS 攻击进行分析，并针对其因发送大量数据而具有较大能量的特点，设计参数 FIR 滤波器来滤除频谱中含有攻击流量的频率分量，提高 LAR(Legitimate traffic to Attacked traffic Ratio)，以便有更多的网络资源为用户提供正常的服务。

**关键词**：拒绝服务攻击；谱分析；离散傅里叶变换；滤波器
**中图分类号**：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2008)06-1493-03

# The Approach of Defending Against DoS Attack in Frequency Domain

Wu Zhi-Jun Zhang Dong
(*Department of Communication Engineering, Civil Aviation University of China, Tianjin* 300300, *China*)

**Abstract**: DoS (Denial of Service) attacks have become one of the most severe security threats to the global Internet increasingly. It makes the resources of Internet used up and incurs congestion by sending a large number of packages constantly. This paper proposes using signal processing method to analyze DoS attacks. Because of sending mass packages, it must have much more power. For this, the FIR filter is designed to filtering the illegitimate frequencies in frequency domain and the LAR (Legitimate traffic to Attacked traffic Ratio) is improved. Then much more resources and service can be supplied for the users.

**Key words**: DoS attack; Spectral analysis; DFT; Filter

## 1 前言

近些年 DoS(Denial of Service)攻击已成为网络安全的最严重的威胁。这是因为这种攻击往往很难防范，容易引起大量的服务中断，因而使得合法用户的服务请求被拒绝。尽管 DoS 攻击可以利用像服务器溢出的这种软件因素的弱点，但通常还是通过连续的发送大量的数据包来消耗那些提供服务的有限资源来实现攻击。这些有限的资源包括带宽、服务器 CPU 的处理能力、存储器等等。

一般防御 DoS 攻击的方法是在尽可能的接近攻击源的地方检测发现并且限制攻击流量，这样可以减轻攻击的损害程度。然而，攻击者可以通过控制流量大小以躲避流量检测措施。

由于 DoS 攻击是在一段时间内连续的发送大量的数据，因此其能量要远大于正常流量的能量。基于此点特征，本文探索了一种新的方法：利用频谱分析和滤波器对含有 DoS 攻击的数据流进行过滤，降低链路中的数据流量，同时提高 LAR(Legitimate traffic to Attacked traffic Ratio)。

目前，数字信号处理方法处理网络异常逐步成为热点和趋势，而且也已经取得了很多的成果，如利用 TCP 流周期性特点检测网络异常[1−4]、针对低速率 DoS 攻击的协作异常检测和防御方法[5−7]以积极于小波分析方法检测攻击[2]等等。其中，文献[5]提出的方法是从数据流的角度为出发点，将到达路由器的数据包与黑、白名单相比对后决定处理对策的防御方法。而本文提出的方法是经过频谱分析，使用功率谱密度 PSD(Power Spectral Density)展现正常流量与攻击流量能量上的差别，在频域直接利用参数 FIR 滤波器进行过滤，滤除包含攻击流量的频率分量，达到降低攻击流的能量效果。

## 2 频域分析及滤波原理

对到达路由器的 TCP 和 UDP 数据包按照 5ms 的间隔抽样，得到一个离散的时间序列 $x(n)$。根据 Nyquist 采样定理，可以得到其幅频特性。在这个过程中，取样也起到了低通滤波器的作用，消除了高频噪声。数据包的到达数目可以按照如下随机过程模型来表示：$\{x(t), t = n\Delta, n \in N\}$。其中 $\Delta$ 是一个常数，代表采样周期，在实验中是 5ms。$N$ 是全部的取样点数。$x(t)$ 是一个随机变量，表示在 $(t-\Delta, t)$ 间隔内到达路由器的数据包的数目。利用离散傅里叶变换 DFT (Discrete Fourier Transform)将时域序列转换到频域：

$$\mathrm{DFT}(x(n),k) = \frac{1}{N}\sum_{n=0}^{N-1} x(n) e^{-j2\pi kn/N},\ \ k = 0,1,\cdots,N-1 \quad (1)$$

2006-10-30 收到，2007-10-17 改回
国家自然科学基金委员会与中国民用航空总局联合资助项目(60776808)，国家空管委项目(GKG200702020)和中国民航大学科技启动基金(2006 年)资助课题

经过 DFT 变换，就可以从另外一个角度来观察分析序列的特性。

TCP流中数据包的数目具有守恒的原则，具体表现在其周期性上，即：在网络的任意节点上出现一个TCP流的数据包，经过RTT(Round Trip Time)时间间隔，在此节点还将出现一个属于相同TCP流的数据包[1]。为了把此特征具体化，可以使用自相关函数，如下式：

$$R_{xx}(\tau,t)=E[x(t)x(t+\tau)] \tag{2}$$

然而在实际中，使用功率谱密度PSD观察周期性更为直接、有效。PSD函数实际上就是序列自相关函数的DFT变换：

$$S_x(f)=\sum_{k=-\infty}^{\infty}R_{xx}(k)e^{-j2\pi kf} \tag{3}$$

由于目前缺乏对随机过程完整的数学描述，本文方法使用PSD估计代替真实的PSD。在本实验中使用的Yule-Walker现代谱估计方法，方便地克服了像Welch方法这种经典估计算法的谱分辨率低的缺点。

然后比较正常流量和带有攻击流量的能量分布，用FIR数字滤波器滤除掉的包含攻击的频率分量。所谓数字滤波器，就是用有限精度算法实现的离散时间线性非时变系统。FIR数字滤波器的设计问题就是要所设计的FIR数字滤波器的频率响应 $H(e^{j\omega})$ 去逼近所要求的理想滤波器的响应 $H_d(e^{j\omega})$。从单位取样响应序列来看，就是使所设计滤波器的 $h(n)$ 逼近理想单位取样响应序列 $h_d(n)$。本实验中采用窗函数法设计FIR滤波器，也叫傅里叶级数法[8]。

## 3 实验方法及结果分析

在本文实验中，使用一台计算机产生单个的 TCP 流持续发送数据包至预先设置好的目标。在此期间，取其中两段固定时间同时使用另一台计算机作为攻击源，连续地向目标发送一个包含大量数据包的 UDP 流。在目标计算机将收到的数据包以 5ms 为间隔作抽样统计，产生时域序列，如图 1 所示。

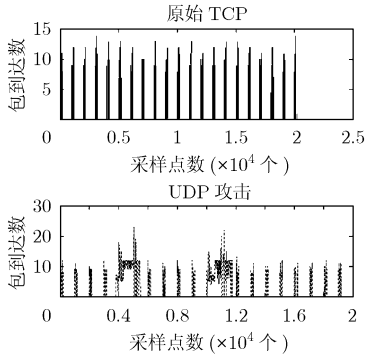


图 1 正常 TCP 和包含 UDP 攻击的统计流量对比

将得到的序列作 DFT 变换到频域，经过谱估计，统计序列的 PSD 如图 2 所示，可以看到包含 UDP 攻击的流能量要明显高于正常的 TCP 流能量，特别是在[0，1]区域内。据此，有理由相信进行滤波，滤除攻击的频率分量，就可以减轻 DoS 攻击。

图 3 是利用窗函数法所设计的 FIR 滤波器的幅频特性，滤波器只允许所需要的频率分量，亦即是正常流量所包含的频率分量通过。经过滤波后，在图 4 中将流量滤除前后的频谱作比较，显而易见，滤波后包含 UDP 攻击频率成分得到了很好的抑制，大部分正常 TCP 流不包含的频率分量，几乎被全部滤除，允许通过的都是正常流量合理的频率分量。而在[0，10]频段中，由于设计的滤波器过渡带性能的原因，因此未能过滤完全，还残留有小部分攻击流量的频率分量。换个角度，再从时域对过滤效果作更为直观的检验。观察图 5，在两个 UDP 攻击的时间段里，UDP 攻击数据包数目有了很大改善，与未经过滤前相比，数量大幅下降，这样便降低了链路中异常流量，有更多的资源为合理流量提供服务。

鉴于本文方法的出发点为能量差异，使用能量比值作为评价指标较为直观。将单个 TCP 流作为正常流量，将单纯

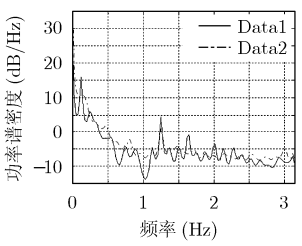


图 2 正常 TCP 和包含 UDP 攻击的流量 PSD 对比

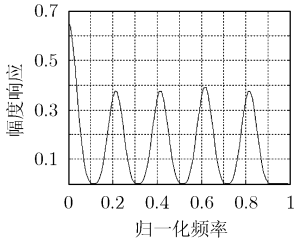


图 3 FIR 滤波器特性曲线

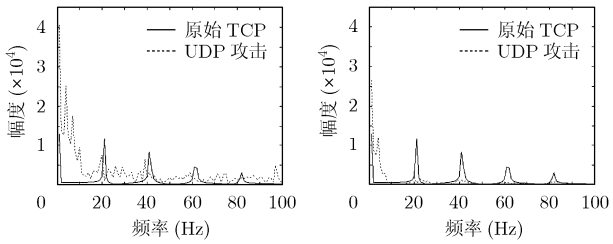


图 4 过滤前后的频谱对比

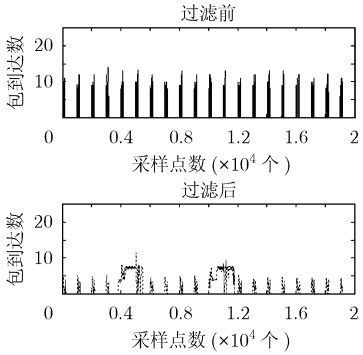


图 5 时域中含 UDP 攻击流量过滤前后的比较

的 UDP 流作为攻击流量，分别计算两者能量，再求比值，即 LAR，如表 1 所示。结果显示，过滤前后 LAR 提高大约 10dB 左右，说明 FIR 数字滤波器的过滤对于 DoS 攻击能够起到明显减轻的作用，使得链路保持通畅，为用户提供正常的服务。

**表 1 过滤前后的效果对比(单位：dB)**

| | 过滤前 | 过滤后 |
|---|---|---|
| LAR | −19.3121 | −10.8417 |

在文献[2]中，针对 DDoS 攻击主要采用的是黑、白名单比对法。而本文所提出的是使用滤波器。由实验结果显示，黑、白名单比对法的检测准确度概率为 82.6%，本文方法采用 LAR 作为技术指标，抑制了攻击数据流的能量，相对而言即是提高正常数据流的能量，过滤前后提高了将近 10dB。在前者方法中，若想要通过降低判决门限来提高正常流量的通过率，有一定的困难，因为降低门限后误判率会随之增加，使更多攻击流量被当作正常流量而通过，这是一对矛盾因素。相比之后，后者改进提高的机会更大，滤波器性能越好，滤除的攻击频率成分越彻底，攻击与正常流量的能量差距就越大。就两种方法的思路而言，后者的思想要比前者简单，在发现了含有攻击的多余能量后，直接地滤除其频率成分，同时也节省了前者的名单存储开销和进行对照比较的时间。所需要考虑多一些的是在滤波器的设计与过滤方面上。在实际中，对于 DFT 变换、谱分析和滤波器的设计均可以采用 DSP 来实现，设计出独立的模块设备，这样可以大大发挥硬件的优势，提高了处理速度，节约了时间，从而降低路由器或者目标终端检测和防御网络异常的负担。

## 4 结束语

本文提出在频域使用滤波器的方法来防御 DoS 攻击，思路简单，利用 DSP 处理速度快的特点，节约时间，并具有明显降低攻击能量的作用，保证链路的通畅。同时本文利用现有的实验环境加以验证，对于将来能够使用滤波技术解决 DoS 攻击提供了一个新的思路，做了探索和铺垫。

在接下来的工作中，要在 FIR 滤波器的设计上寻求突破，尝试其他的设计方法考虑降低运算量，减小滤波器过渡带和阶数，来提高其性能。同时，将实验进一步复杂化，增加多 TCP 流，并加入背景流量作为噪声。最终目标是设计空间滤波器组应用于真实的网络环境。

## 参 考 文 献

[1] Cheng Chen-Mou, Kung H, and Tan Koan-Sin. Use of spectral analysis in defense against DoS attacks. Proceedings of IEEE GLOBECOM, Taipei, China, 2002: 2143−2148.

[2] Barford P, Kline J, Plonka D, and Ron A. A signal analysis of network traffic anomalies. Proceedings of ACM SIGCOMM Internet Measurement Workshop, Marseilles, France, 2002: 71−82.

[3] Ferguson P and Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, May 2000.

[4] Barford P and Plonka D. Characteristics of network traffic flow anomalies. Proceedings of ACM SIGCOMM Internet Measurement Workshop, San Francisco, CA, November 2001: 5−17.

[5] Chen Yu, HWang Kai, and Kwok Yu-KWong. Collaborative defense against periodic shrew DDoS attacks in frequency domain. Technical Report TR 2005-11, ACM Trans. on Information and System Security, 2005.

[6] Chen Yu, Hwang Kai, and Kwok Yu-Kwong. Filtering of shrew DDoS attacks in frequency domain. Proceedings of the The IEEE Conference on Local Computer Networks 30th Anniversary, November 15−17, 2005: 786−793.

[7] Feinstein L, Schnackenberg D, Balupari R, and Kindred D. Statistical approaches to DDoS attack detection and response. DARPA Information Survivability Conf. and Exposition (DISCEX'03), Washington, 2003: 303−314.

[8] 薛年喜. Matlab在数字信号处理中的应用. 清华大学出版社, 2003: 227−233.

吴志军：　男，1965 年生，教授，博士后，研究方向为网络信息安全.

张　东：　男，1982 年生，硕士，研究方向为网络信息安全.