ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.4, April 2009, pp.930–941
doi: 10.3724/SP.J.1001.2009.03302

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

一种基于小波特征提取的低速率 DoS 检测方法*

何炎祥+, 曹 强, 刘 陶, 韩 奕, 熊 琦

(武汉大学 计算机学院,湖北 武汉 430079)

A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform

HE Yan-Xiang+, CAO Qiang, LIU Tao, HAN Yi, XIONG Qi

(School of Computer Science, Wuhan University, Wuhan 430079, China)

+ Corresponding author: E-mail: yxhe@whu.edu.cn, http://cs.whu.edu.cn/yxhe/

He YX, Cao Q, Liu T, Han Y, Xiong Q. A low-rate DoS detection method based on feature extraction using wavelet transform. *Journal of Software*, 2009,20(4):930–941. http://www.jos.org.cn/1000-9825/3302.htm

Abstract: LDoS (low-rate denial-of-service) attacks are stealthier and trickier than the traditional DDoS (distributed DoS) attacks. According to the characteristic of periodicity and short burst in LDoS flows, a detection system DSBWA (detection system based on wavelet analysis) against LDoS attacks has been designed and implemented based on feature extraction using wavelet transform. The proposed system, focusing on the number of arriving packets at the monitoring node, extracts five feature indices of LDoS flows through wavelet multi-scale analysis of network traffic. Then a synthesis diagnosis is made by a trained BP neural network. Once the attack is verified, the information related to attackers can be obtained by locating malicious pulses. Simulation results in NS-2 show that the scheme DSBWA, capable of detecting the variants of LDoS attack, achieves high detection rate with low computation cost, and hence has good practical value.

Key words: LDoS (low-rate denial-of-service) attack; wavelet analysis; feature extraction; BP neural network

摘 要: 低速率拒绝服务攻击(low-rate denial-of-service,简称LDoS)比传统的DDoS(distributed DoS)攻击更具隐蔽性和欺骗性,依据其周期性脉冲突发特点,设计实现了一种基于小波特征提取的 LDoS 检测系统 DSBWA(detection system based on wavelet analysis).该系统以到达检测节点的数据包数目为研究对象,通过小波多尺度分析,结合LDoS 的攻击规律提取 5 个特征指标,在此基础上采用 BP 神经网络进行综合诊断.一旦检测出 LDoS 攻击,系统定位攻击脉冲数据的到达时刻以获得攻击者的相关信息.NS-2 模拟实验结果表明,DSBWA 具有高检测率和低误警率,并且能够检测出 LDoS 变种攻击,消耗计算资源少,具有良好的实用价值.

关键词: LDoS 攻击;小波分析;特征提取;BP 神经网络

中图法分类号: TP393 **文献标识码**: A

低速率拒绝服务攻击(low-rate denial-of-service,简称 LDoS)是一种新型的 DoS 攻击[1],它利用网络协议或系统中适应性机制的安全漏洞,通过向目标发送周期性脉冲攻击流,导致受害端服务性能降低.尽管 LDoS 没有传统洪泛式 DDoS(distributed DoS)的攻击效果,不会导致受害端完全拒绝服务,但其只需发送少量攻击数据包就

* Supported by the National Natural Science Foundation of China under Grant Nos.60642006, 60773008 (国家自然科学基金)
Received 2007-05-30; Accepted 2008-03-10

可以极大地降低服务质量,以此获得了更高的攻击效率.LDoS 攻击者大部分时间保持沉默,只有在短暂的活动时间段内才发送高强度脉冲流,这一间歇性攻击特点使得攻击流的平均数据率与合法用户无太大区别,传统 DoS 检测方法对其难以奏效,这给网络安全带来了新的挑战.

针对 TCP 拥塞控制机制的 Shrew 攻击[1]是最早提出来的一种 LDoS 攻击,目前被广泛用于测试 LDoS 检测机制.Kuzmanovic 在 2003 年提出随机化端系统的最小超时等待时间,使攻击者无法准确估测出攻击数据流的发送时刻[1].虽然该措施有一定的缓解效果,但涉及 TCP 协议的修改,并且只能防范 Shrew 攻击,无法检测攻击的存在性.Sarat 和 Terzis 通过控制路由器队列缓冲区的大小,并配合适当的 AQM(active queue management)技术来过滤 LDoS 攻击流[2],但目前的 AQM 机制只适合于抑制持续时间较长的高速率流,对 LDoS 脉冲式攻击流的作用并不明显.Kwok 针对 LDoS 提出一种新的路由器队列管理方法——HAWK(halting anomaly with weighted choking)[3],但可能导致大量正常 TCP 数据流被误认为非法攻击流,误警率很高.Sun 通过自相关分析提取可疑数据流的周期特征,采用动态时间扭曲算法匹配特征,一旦检测出攻击就根据差额循环算法(deficit round robin,简称 DRR)进行带宽限制和资源保护[4,5].该方法需要对所有数据流进行同样的检测处理,计算和存储开销大;而且 DRR 并不针对 LDoS 攻击流,对合法流量影响较大.Chen 在流量频谱图的低频带进行假设检验以确定攻击的存在性[6].尽管该方法检测率较高,但只能报告当前分析窗内是否存在 LDoS 攻击,不能定位攻击数据包,且当攻击者伪造 IP 时,存储和计算开销很大,可能导致溢出错误.

结合 LDoS 的攻击规律,分析正常 Internet 流与 LDoS 攻击流的差异,我们提出了一种基于小波特征提取的 LDoS 检测方法 DSBWA(detection system based on wavelet analysis).该系统用信号处理的方法来分析网络流量,通过小波工具较好地缓解了合法用户背景流量对攻击特征提取的干扰;综合诊断器采用具有良好学习能力的 BP 网络实现,不仅能够准确检测标准 LDoS 攻击,而且对其变种攻击也有很好的效果.该方法以到达检测路由器的数据包数目为分析对象,消耗计算资源少,健壮性和可移植性较强.另外,利用小波系数模极大原理可以定位攻击数据包的到达时刻,进而找到攻击数据包,为追踪攻击源提供较准确的线索,具有很好的实际意义和应用价值.

本文第 1 节分析 LDoS 攻击原理.第 2 节提出一种基于小波分析的 LDoS 特征提取技术,作为检测方法的基础.在第 3 节设计 LDoS 检测系统 DSBWA,阐述各模块的工作原理.第 4 节给出实验结果,确定系统参数,分析系统性能.最后对全文进行总结并展望未来工作.

1 LDoS 攻击原理

虽然目前所提出的 LDoS 攻击方式多种多样[7,8],但其都是利用网络或端系统适应性机制在设计上的安全缺陷进行的攻击.适应性协议主要注重系统稳态的有效性和公平性,对其安全性考虑不多,尤其忽略了系统的暂态性能.LDoS 攻击者发起周期性脉冲攻击,使系统在失效和稳定两个状态间频繁切换,如图 1 所示,其中攻击参数包括攻击周期 T,脉冲持续时间 τ 和脉冲强度 δ.假设系统初态性能为 0,稳态(steady state)性能为 SS,失效状态(disabled state)性能为 DS,攻击开始后系统从稳态转入失效状态的时间为 t_1,从失效状态通过适应性机制恢复到稳定状态的时间为 t_2,适应性协议中 $t_2>>t_1$.一旦系统达到稳态 SS,攻击者发送攻击脉冲,受其影响,系统性能迅速降至 DS,此时停止攻击;等到系统经时间 t_2 缓慢恢复至稳态后,再发起下轮攻击,如此循环,系统始终无法保持稳定,性能大为降低.LDoS 攻击允许系统缓慢恢复,大多数情况下不会导致完全拒绝服务,其攻击效果不如传统 DDoS,但 LDoS 利用了适应性机制中存在的安全漏洞,更加彻底地做到了有的放矢,攻击效率明显提高.

针对 TCP 拥塞控制机制的 Shrew 攻击是目前受到普遍关注的一种 LDoS 攻击方式.TCP 协议中,无论是慢开始(slow start)还是和增积减(additive increase/multiplicative decrease,简称 AIMD),核心思想均是不断探测网络所能承受的最大传输上限,当发现数据包丢失,立即减小拥塞窗口,降低发送速率.Shrew 攻击利用此机制,在特定时刻发送脉冲式攻击流,造成大量网络数据包丢失,使得 TCP 发送方误认为网络始终存在拥塞.根据 TCP 协议,数据发送速率一直很低,传输效率急剧减小.

根据 RFC 2988,TCP 发送方存在相同的 minRTO(1s),Shrew 攻击的周期 T 一般设置为 minRTO+2RTT~

minRTO+3RTT,此时攻击效果最佳[1].由于网络性能的动态变化,RTT 无法实时精确测量,脉冲持续时间和脉冲强度也很难把握.实验证明,即使不严格遵照 LDoS 攻击模型,只要保证攻击周期 T,脉冲持续时间 τ,脉冲强度 δ 在理想攻击参数附近,周期性脉冲数据流同样具有相当大的危害[9],可大幅度降低受害端的服务质量.此类攻击仍保持有低平均速率的特性,本文称其为 LDoS 的变种攻击 LDoSV(LDoS variants).

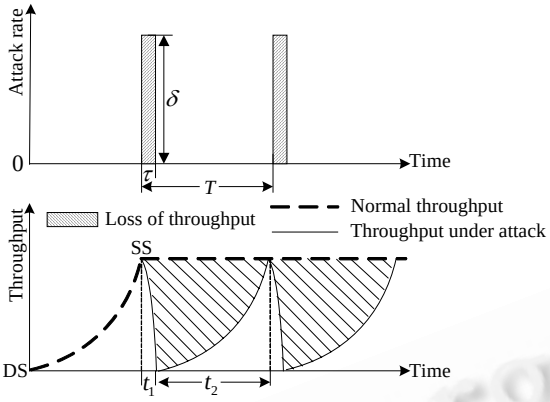


Fig.1 LDoS attack model and its effect on system performance
图1 LDoS攻击模型及其对系统性能的影响

2 基于小波分析的 LDoS 特征提取

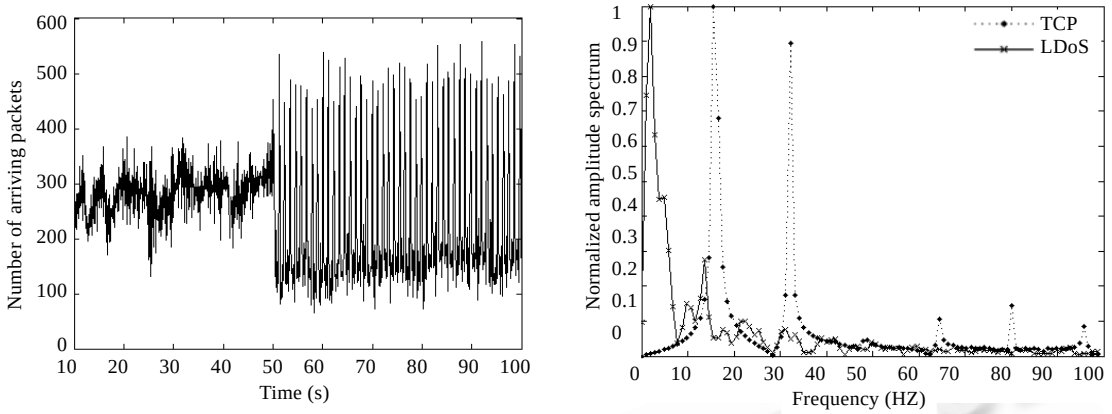
2.1 LDoS流量分析

从网络体系架构的角度,网络流量是一切研究的基础,网络的行为特征往往可以通过其承载流量的动态特性来反映.定义随机过程 $\{X(t), t=n\Delta t, n\in Z^+\}$ 为包过程[10],其中 Δt 为采样时间间隔,$X(t)$ 表示在时间段 $(t-\Delta t, t]$ 到达检测路由器的数据包数量.本文的检测方法从网络流量的包过程出发,通过小波分析提取 LDoS 的攻击特征,探测网络的运行状态.

大量研究表明,在一定时间尺度内,正常网络流量具有自相似性,是长相关的,其包过程是广义平稳过程[11].LDoS 攻击者发起周期性脉冲攻击,严重影响了网络适应性机制(如:TCP 协议中的 AIMD 机制和路由器队列管理机制)对网络性能的调节作用[1,7],极大地抑制了相对平稳的合法数据流量,特别是 LDoS 攻击流本身就是周期性脉冲流,所以攻击情况下,LDoS 攻击流和合法用户流量叠加后的包过程难以保持平稳.图 2(a)显示在 NS-2 上模拟一次典型 LDoS 攻击的网络流量变化情况,其中包过程的采样时间间隔为 100ms,攻击发起时刻为 50s.攻击发起前(10s~50s),流量波动不大,各统计量(均值、方差和自相关函数)基本满足广义平稳要求;LDoS 攻击发起后(50s~100s),包过程波动加剧,合法用户的平均包速率急剧降低,系统性能下降.

从频域来分析网络流量,正常网络流量和 LDoS 攻击下的网络流量存在很大的频率差异[10].由于 Internet 大部分业务数据流受 TCP 拥塞机制控制,各 TCP 连接每隔 RTT(round trip time)时间出现一次流量高峰,所以单个 TCP 的流量呈现一定程度的周期性变化趋势,并且其周期性与 RTT 紧密相关,图 2(b)显示了单个合法 TCP 流的规范化幅度谱,其峰值点对应着动态变化的 RTT,分散至各频段.而对于 LDoS 攻击流而言,长周期(秒级)特性决定了频谱更集中于低频段[0,10]Hz(图 2(b)所示).如前所述,包过程是所有流经检测结点流量的叠加,根据信号分析理论,汇聚后包过程的频谱是所有通过检测结点的 TCP,UDP 的频谱叠加.正常情况下,单个 TCP 连接的 RTT 随网络负载情况动态变化,其频谱峰值点分布较分散,叠加后的包过程的频率成分也分布较均衡;而在 LDoS 攻击情况下,各 TCP 连接的流量受到严重抑制,检测结点很少转发合法用户的 TCP 数据包,叠加后的包过程主要包含 LDoS 攻击流,从而其频率成分主要集中于低频段.另外,即使是 LDoSV 攻击流也仍保持有周期性脉冲突发的本质,攻击前后包过程的频谱变化也有类似的效果.所以从频谱分析角度得到如下结论:正常情况下,网络流量包过程的频谱分布较分散、较均衡;而在 LDoS 攻击情况下,包过程的频谱更集中于低频段[0,10]Hz.

尽管 LDoS 攻击设计精巧,在传统的 DDoS 基础上有很大改进,降低了攻击流的平均数据率,但从网络流量的包过程考虑,它仍然在时频两域有着较为显著的特征.检测系统 DSBWA 将通过提取这些特征来检测网络中是否存在 LDoS 攻击.



(a) Packet process of a LDoS attack in NS-2

(a) NS-2模拟LDoS攻击的包过程

(b) Difference of spectrum between malicious and TCP flow

(b) LDoS攻击流与TCP数据流的频谱差异

Fig.2 Time-Frequency analysis of network traffic

图 2 网络流量的时频分析

2.2 二进离散小波变换

小波变换是一种时-频窗面积固定、形状可自适应调整的信号分析工具,在时、频局部化方面具有独特优势,非常适合于信号的异常检测[12].本文将二进离散小波变换应用于包过程的处理.首先通过小波函数 $\psi_{j,k}(t)$ 和尺度函数 $\varphi_{j,k}(t)$ 将包过程 $\{X(t)\}$ 作 J 层分解[13]:

$$X(t)=\sum_{j=1}^{J}\sum_{k}d_{j,k}\psi_{j,k}(t)+\sum_{k}a_{J,k}\varphi_{J,k}(t) \tag{1}$$

$d_{j,k}$ 为小波系数,表示尺度 j 上的细节信息; $a_{J,k}$ 为近似系数,表示尺度 J 上的逼近信息.进而可以得到信号 $\{X(t)\}$ 分布在中心频率为 $2^{-j}\nu_0$ 的子频带的能量[17]:

$$E_j=\frac{1}{n_j}\sum_{k}\left|d_{j,k}\right|^2,$$

其中,ν_0 为母小波的中心频率,n_j 为j尺度下小波系数的个数.

式(1)中的小波分解过程是可逆的,由近似系数和细节系数可以重构原信号{$X(t)$}.在小波分解下,不同的尺度具有不同的时间和频率分辨率,选择特定尺度上的小波系数和近似系数重构信号可以分离出相应的频率成分.采用 Db4 小波对图 2(a)的包过程{$X(n)$}进行 5 层小波分解,通过频率计算,选取 3、4、5 层的小波系数重构反映低频段变化信息的攻击流子带 $X_a(n)$,其余分解系数重构反映网络流量整体趋势的背景流子带 $X_b(n)$,如图 3 所示.这样,各流量子带

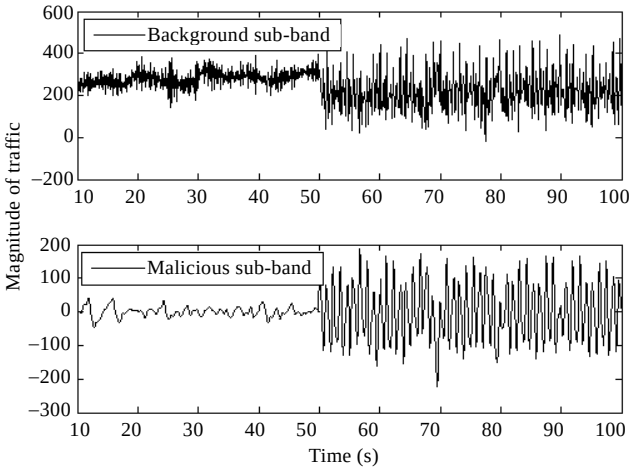


Fig.3 Sub-Bands derived from wavelet reconstruction

图 3 波重构的流量子带

的频率成分更加单纯,便于针对 LDoS 攻击提取特征指标.

2.3 LDoS攻击特征提取

LDoS 攻击十分隐蔽,仅仅从某一方面(如攻击流的周期性,脉冲强度或背景流量强度)刻画其攻击行为都是片面的,否则很多恰好具备某些特征的合法数据流可能会被误判为攻击流[3].为此,我们在包过程 $X(n)$及其子带 $X_a(n)$ 和 $X_b(n)$ 上提取 5 个计算量小且区分度高的特征指标,力争从多角度全面描述 LDoS 攻击流的行为,以提高系统的检测性能.

特征指标 1:攻击流子带中 $|X_a(n)|$ 的平均值为 $Avg_a=\dfrac{\sum_{n=1}^{N}|X_a(n)|}{N}$,其中 N 为包过程的长度.

LDoS 攻击只需占用少量网络带宽,其平均数据率与合法用户相差不远.但考虑到 LDoS 攻击流与正常流的频率差异,若通过小波分析聚焦到较低的攻击频带,那么该频率范围内的平均流量将是衡量 LDoS 攻击是否存在的重要指标.根据小波理论,不论网络流量增大还是减小,$|X_a(n)|$ 均能反映网络流量在攻击频段的局部变化程度,LDoS 攻击流的长周期性决定其频率成分主要集中于低频段,所以 $|X_a(n)|$ 实际代表其攻击强度,于是 Avg_a 也就表征了 LDoS 攻击流的平均强度.正常流量主要包含高频成分, Avg_a 小;而攻击流的 Avg_a 则较大.

特征指标 2:攻击流子带中 $|X_a(n)|$ 的标准差: $S_a=\sqrt{\dfrac{\sum_{n=1}^{N}\left(|X_a(n)|-E(|X_a|)\right)^2}{N-1}}$,其中 $E(|X_a|)=\dfrac{\sum_{n=1}^{N}|X_a(n)|}{N}$.

据前所述,$|X_a(n)|$ 实际上代表 LDoS 攻击流的强度.LDoS 本身是周期性脉冲攻击,数据率并不恒定,具有很大的波动性,其波动程度决定攻击子带中 $|X_a(n)|$ 的标准差 S_a .当攻击方处于活动时间段时,突发脉冲流量足以在瞬间淹没瓶颈链路,攻击目标不堪重负,服务质量下降,网络情况极不稳定,$|X_a(n)|$ 很大;当其进入休眠时间段时,背景数据流以较小数据率传输,网络流量波动不明显,$|X_a(n)|$ 很小. S_a 描述了 LDoS 攻击流本身的波动程度,将其作为攻击特征指标.当网络中发起 LDoS 攻击时,$|X_a(n)|$ 的波动增大, S_a 显著增加.

特征指标 3:攻击频带内的能量: $E_a=\sum_{j\in Attackband}\dfrac{1}{n_j}\sum_{k=1}^{n_j}|d_{j,k}|^2$,攻击频带的能量 E_a 为中心频率落在攻击频带内的各尺度能量之和.

小波系数 $d_{j,k}$ 能够反映信号的能量在时频窗(j,k)(其中频率中心为 $2^{-j}v_0$,时域中心为 $2^j k$)内的分布情况,如第 2.2 节所述,小波变换后 $|d_{j,k}|$ 表征信号在该时频窗内的能量强度.这里考察网络流量在攻击频带的能量,将 E_a 作为攻击特征提取.对于正常网络数据,大部分为TCP流量,集中于高频带,低频能量很小.当发起LDoS周期性攻击后,高频的合法背景数据被抑制,攻击流周期 T 一般为 1s~5s[1,7],集中于低频带,从而使低频能量 E_a 增大.

特征指标 4:背景流子带 $X_b(n)$ 的平均值: $Avg_b=\dfrac{1}{N}\sum_{n=1}^{N}X_b(n)$.

背景流子带反映合法用户背景流量的整体趋势,统计量 Avg_b 表示在观察窗口内系统或网络的平均有效性能,可以为异常检测提供参考.正常情况下,合法用户数据流基本保持平稳,完全充满整个链路,网络带宽的有效利用率很高,网络平均流量达到最大.LDoS 发起周期性脉冲攻击,利用安全漏洞制造网络资源消耗殆尽的假象,迫使系统进入失效状态,无法利用有效资源;另外,系统需要经历缓慢的调整过程才能从失效状态中恢复过来,这段时间又浪费了大量的网络带宽,所以合法用户的平均数据率将显著下降, Avg_b 减小.

特征指标 5:网络流量 $X(n)$ 的脉冲因子: $I=\dfrac{\max\{X(n)\}}{\dfrac{1}{N}\sum_{n=1}^{N}X(n)}$.

脉冲因子用于衡量网络中脉冲流量的强度.正常情况下,网络流量比较平稳,突发数据强度不大,脉冲因子接近于 1.LDoS 混入合法用户流之后,其数据流能够在瞬间淹没整个链路,使攻击目标来不及处理,所以 LDoS 突

发强度很大,即使存在大量背景数据流,其脉冲式攻击特征仍无法被掩饰,攻击后的网络流量脉冲因子 I 将急剧增大.考虑到 Internet 的复杂性,正常数据流中也偶尔夹杂高强度突发数据,由于突发概率很低,其突发次数远小于 LDoS 攻击.为加强脉冲因子在 LDoS 攻击检测中的区分能力,可将其修正为

$$I=\frac{\frac{1}{P}\sum_{i=1}^{P}X^{i}(n)}{\frac{1}{N}\sum_{n=1}^{N}X(n)},$$

其中 $X^{i}(n)$ 表示在观察窗口内前 P 个最大的测量值.

当 P 的取值接近于观察窗口内 LDoS 的脉冲次数时,偶然突发数据对正常网络流量的影响被削弱,而 LDoS 攻击流的脉冲因子基本保持不变,从而加强了攻击前后的对比.

以上 5 个特征指标从 LDoS 的攻击规律出发全面揭示了 LDoS 攻击给网络流量带来的变化,是本文检测技术的基础.设定检测窗口大小为 10s,对图 2(a)的包过程提取各检测窗口的特征指标,见表 1.可以看出,各特征指标区分度较高,在攻击前后有显著变化.

Table 1 Change of feature values under LDoS attac

表 1 攻击后的特征值变化

Feature metrics	Detection windows before LDoS attack (20s~50s)				Detection windows under LDoS attack (50s~80s)				Variance ratio of average
	1	2	3	Average	4	5	6	Average	
Avg_a	8.82	7.82	9.94	8.86	68.9	73.3	71.6	71.3	7.05
S_a	7.23	4.87	8.41	6.84	42.5	49.1	40.9	44.2	5.46
$E_a(10^3)$	1.861	0.961	1.798	1.54	60.1	82.7	57.2	66.7	42.3
Avg_b	271	299	294	288	204	212	217	211	0.267
I	1.36	1.26	1.29	1.30	2.47	2.55	2.39	2.47	0.9

3 基于小波特征提取的 LDoS 检测系统框架

3.1 系统结构

基于以上特征提取方法,本文设计了一种 LDoS 检测系统 DSBWA,其基本思想是根据已提取的 5 个特征指标,引入 BP 神经网络进行综合诊断,一旦发现 LDoS 攻击,定位攻击脉冲的到达时刻,以获得攻击源的相关信息.LDoS 攻击者为了躲避检测,很可能发起分布式进攻,这样攻击数据流将更难发现[5],考虑到分布式攻击具有相同的目标,攻击数据流将汇聚于受害端,于是将 DSBWA 检测系统部署在靠近受害端的边界路由器上,以达到较好的检测效果.DSBWA 系统结构如图 4 所示.

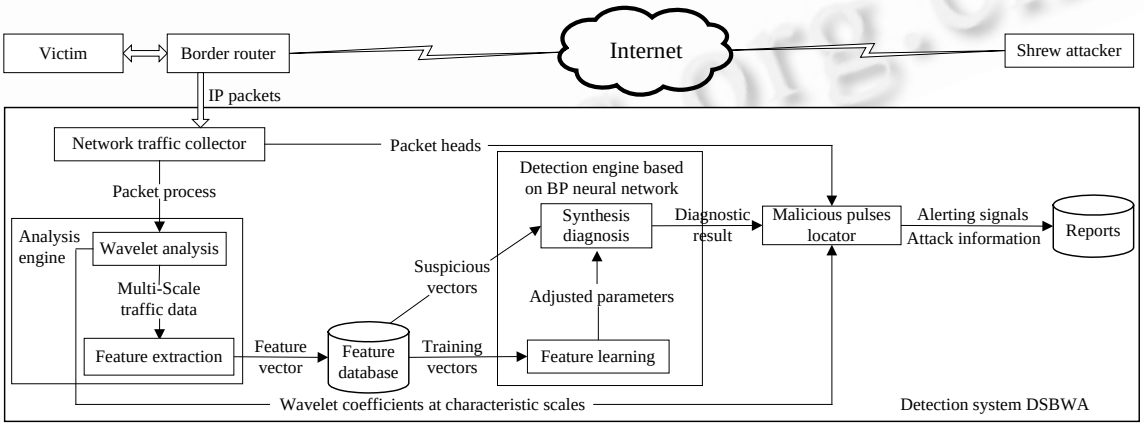


Fig.4 Architecture of DSBWA

图 4 DSBWA 的系统结构

首先检测路由器以一定频率采样网络数据包,获得流量信息,建立包过程,并按照数据包的到达时刻顺序记录包头信息;在观察窗口内,对包过程进行小波分解,计算各尺度的小波系数,根据频率差异,选取特定尺度的分解系数重构攻击流子带和背景流子带;接着采用特征提取算法计算特征指标并存入特征库;将攻击和非攻击情况下的标准特征向量用于训练 BP 神经网络,学习后的 BP 网络对可疑流量的特征向量进行异常诊断;一旦判断网络中存在 LDoS 攻击,那么,攻击脉冲定位器分析特征尺度上的小波系数,在时间轴上定位攻击脉冲的到达时刻,并结合该时刻记录的包头信息,将报警信号与攻击包信息记入报告.

3.2 BP网络检测引擎

Kolmogorov 已证明一个三层前馈神经网络能以任意精度逼近非线性函数[14],具有强大的分类能力.对于 LDoS 攻击的检测,实际上是一个二分类问题,神经网络的训练就是寻找最佳分类面的过程.DSBWA 的检测引擎是具有 3 层结构的 BP 神经网络,输入层由 5 个神经元组成,分别对应 5 个归一化攻击特征;输出层由 2 个神经元组成,网络输出值 m_1,m_2 分别为 0,1 时,表示正常;为 1,0 时,表示有 LDoS 攻击.隐含层神经元个数根据下式选择:

$$h=\sqrt{q+t}+a\text{,其中, }a\in[1,10]\text{,}q,t\text{ 分别为输入层和输出层的神经元个数} \tag{2}$$

选取隐含层神经元的传递函数为双曲正切 S 型函数,输出层神经元的传递函数为 S 型对数函数.当学习样本提供给 BP 网络后,从输出层得到对输入的响应,按照减少目标输出与实际输出误差的方向,从输出层经过隐含层逐层反向修正连接权值等参数,以达到实际输出与期望输出的最大拟合.检测引擎中选用收敛速度快,网络训练误差比较小的 Levenberg-Marquardt 优化学习算法[14].采用包含有 9 个隐含层节点的 BP 网络对图 2(a)的包过程进行综合诊断,各检测窗口内的输出结果如图 5 所示,攻击发起后,在第 1 个检测窗口(50s~60s),系统就开始报警,基本上没有延迟.

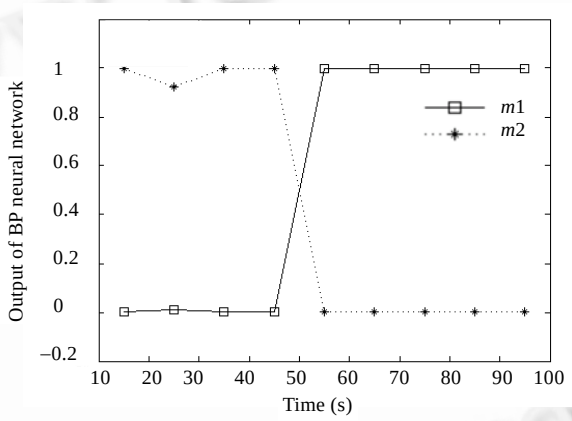


Fig.5 Output of BP neural network

图 5 BP 网络的输出

定义 BP 网络的综合诊断结果,即检测系统 DSBWA 的最终决策指标为

$$m=\sqrt{\frac{m_1^2+(1-m_2)^2}{2}} \tag{3}$$

m 趋近于 0 表明正常,趋近于 1 表明存在攻击.设置阈值 $M_{\min}(M_{\min}\in(0,1))$,当决策指标 m 大于 $M_{\min}$ 时,判定网络中存在 LDoS 攻击,否则认为网络正常.

3.3 攻击脉冲定位器

从检测系统角度,发现攻击后应该尽可能提供攻击者的相关线索,以便于采取有效的防范措施.根据前面的分析,LDoS 是周期性脉冲攻击,攻击者只在脉冲突发点发送数据包,其他时间保持沉默.并且攻击发起后,合法 TCP 用户的数据传输受到严重抑制,链路上传输的合法数据包很少,在最坏攻击下,设置攻击周期 T 为 minRTO+2RTT~minRTO+3RTT,合法数据传输的吞吐量将下降至 0[1].也就是说,即使 LDoS 攻击者在攻击间隙一直沉默,

各合法 TCP 发送方由于受拥塞机制的控制,始终等待丢失数据包的 ACK,不再发送新数据包,直至超时.另外,根据 MCI 的统计,互联网上总字节数的 95%及总数据包数的 90%均使用 TCP 协议传输[15].所以在 LDoS 脉冲突发时刻,目标链路上基本只传输攻击数据包,即使还有少量合法数据包,将其忽略也是在允许误差范围之内的.根据 LDoS 攻击方式的特殊性,攻击脉冲定位器首先确定攻击脉冲的到达时刻,再查找该时刻记录的包头内容就可以获得攻击者的相关线索.

利用小波分析时域局部化特性设计攻击脉冲定位器,以确定检测窗口内攻击数据包的到达时刻.当 LDoS 攻击发起后,攻击者在活动期间发送的脉冲数据足以占据瓶颈链路带宽,合法流量受到严重抑制,整个包过程基本上可以看成是周期脉冲信号和低幅度的平稳背景信号的叠加,如图 2(a)所示.在检测窗口中确定攻击数据包到达时刻以获取攻击者信息, 关键就是从混合信号中确定周期脉冲信号的突变点. 根据小波系数模极大原理,若选择小波为光滑函数的一阶导数,则小波系数的模极大点对应原信号的突变点[13],因此确定攻击脉冲的突变点进一步转化为确定由攻击脉冲产生的小波系数模极大点.

小波系数模极大值具有沿尺度传递的性质,冲击脉冲信号的 Lipschitz 指数小于 0,其模极大值随尺度增大而减小;而平稳背景信号的 Lipschitz 指数非负,其模极大值不会随尺度增大而衰减[13].因此,设计如下算法搜索在观察窗口内由脉冲信号产生的局部模极大点,以排除背景信号模极大的干扰.算法分为 4 个步骤:

Step 1. 在第 2.2 节小波分解基础上,选取小特征尺度集 $J^{low}=\left\{j_1^{low},j_2^{low},...,j_m^{low}\right\}$ ($j_1^{low}<j_2^{low}<...<j_m^{low},m\ge 1$) 和大特征尺度集 $J^{high}=\left\{j_1^{high},j_2^{high},...,j_n^{high}\right\}$ ($j_1^{high}<j_2^{high}<...<j_n^{high},n\ge 1$),并且满足 $j_m^{low}<j_1^{high}$.

Step 2. 在每个尺度 $j_p^{low}\left(1\le p\le m\right)$ 上搜索小波系数的局部模极大点集合 S_p^{low}.计算小特征尺度集 J^{low} 的所有局部模极大点集合 $S^{low}=\bigcup_{p=1}^{m}S_p^{low}$.

Step 3. 在每个尺度 $j_q^{high}\left(1\le q\le n\right)$ 上搜索小波系数的局部模极大点集合 S_q^{high},设置阈值 $Th_q=\max\left\{\left|d_{j_q^{high},k}\right|\right\}\Big/j_q^{high}$,将 S_q^{high} 中小于 Th_q 的模极大点剔除.计算大特征尺度集 J^{high} 的所有局部模极大点集合 $S^{high}=\bigcup_{q=1}^{n}S_q^{high}$.

Step 4. 计算 $S=S^{low}-S^{high}$, S 就是本算法确定的由攻击脉冲信号产生的模极大点集合.

注:在实际计算中,我们将时间轴划分成连续不相交的离散区间,集合中的元素为以某一时刻为中心的邻域.

本算法首先选择特征尺度,这是搜索局部模极大点的基础;小特征尺度上脉冲信号和背景信号的模极大都很显著,所以,集合 S^{low} 基本上包括混合流量的所有突变点;在大特征尺度上攻击信号的模极大已经衰减得很小,而背景流量的模极大依然明显,设置阈值 Th_q 以剔除衰减的攻击信号模极大,这样,集合 S^{high} 中只包含背景流量的模极大;于是 $S=S^{low}-S^{high}$ 为由攻击脉冲产生的小波模极大点,也就是攻击脉冲的突变点.据此,在时间轴上定位出攻击脉冲的到达时刻,再结合建立包过程时按到达顺序记录的包头信息,可获得攻击者的相关线索,记入报告.算法中选择多个大特征尺度和多个小特征尺度是为了保证时间定位的精度.

在图 2(a)所示的 LDoS 攻击中,根据图 5 的诊断输出,攻击脉冲定位器将在攻击后的第 1 个检测窗口(50s~60s)内启动,选择小特征尺度集 $J^{low}=\{1,2\}$,大特征尺度集 $J^{high}=\{4,5\}$,根据搜索算法,攻击脉冲的定位结果如图 6 所示,模极大点基本逼近 LDoS 攻击点.尽管定位结果与实际攻击点在时间轴上并不严格对应,考虑到每个点代表以该时刻为中心的邻域,图中的误差应该是可以接受的.这样,我们定位 LDoS 攻击数据包的到达时刻,结合相应时刻记录的包头内容可以获得攻击者的相关信息,为攻击源追踪技术或攻击流抑制技术提供有效线索.

在 DSBWA 系统执行效率方面,小波分析可以根据 Mallat 塔式算法,利用滤波器实现[16],整个特征提取过程的计算复杂度与检测窗口内包过程的长度呈线性关系.基于 BP 网络的综合分类器规模不大,实现简单,计算量小.攻击脉冲定位器以小波分解的中间结果为基础,只需遍历特征尺度上的小波系数.总之,DSBWA 为及早、准

确、高效地检测 LDoS 攻击提供了良好的解决方案.

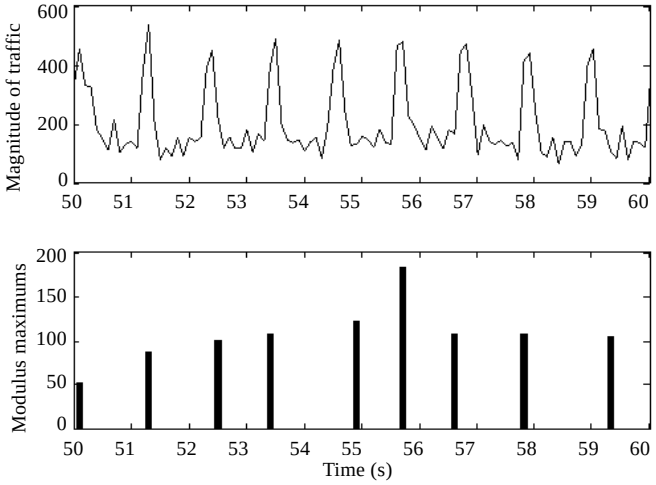


Fig.6 Result of locating the malicious pulses

图 6 攻击脉冲的定位结果

4 实验结果与性能分析

为评测本文方法的有效性, 我们通过 NS-2 上的网络模拟实验对检测系统进行检验.采用 GT-ITM 工具包生成网络拓扑结构以提高模拟实验的仿真度,根据 Transit-Stub 模型建立 3 层网络结构[17],即主域(transit domain)、从域(stub domain)和节点(node).其中主域相当于主干网,主域节点相当于主干网中的路由器,连接在主域节点上的从域相当于端网.实验网络中共有 85 个节点,包含 1 个主域,其中有 5 个主域节点,每个节点平均连接 4 个从域,每个从域平均包含 4 个从域节点.主域各节点间的链路带宽为 40Mpbs,从域各节点间的链路带宽为 10Mbps,连接主域节点和从域的链路带宽为 20Mbps,该链路为网络瓶颈.在此网络拓扑上,共产生 322 条数据流,平均每个节点有接近 4 条数据流,包括 289 条 TCP 连接,33 条 UDP 流.各 TCP 连接的往返时延 RTT 在 90ms~200ms 之间.采用 UDP 发送 LDoS 攻击脉冲,使其与背景数据流混合.LDoS 攻击周期 T 的变化范围为 0.5s~5s,脉冲持续时间 τ的变化范围为 100ms~270ms,脉冲强度 δ的变化范围为 15Mbps~40Mbps,如第 1 节所述,这其中包含有 LDoS 的变种攻击.

本文的检测系统 DSBWA 通过小波分析提取 LDoS 攻击流的特征指标 Avg_a, S_a, E_a 和 Avg_b (脉冲因子 I 可以从包过程直接提取),小波基的选择将影响到特征指标的区分能力.由于 Internet 网络流量的复杂性,从理论上难以求证最佳小波.为此,以 10s 为检测窗口,选用 Db(n),Sym(n)和 Coif(n)系列小波对图 2(a)中的包过程提取特征指标,计算 LDoS 攻击前后各指标平均值的变化率,结果见表 2.

Table 2 Variance ratio of feature metrics using different wavelets

表 2 不同小波提取的特征指标在 LDoS 攻击前后的变化率

Feature metrics	Daubechies wavelet				Symlet wavelet				Coiflet wavelet		
	Db2	Db3	Db4	Db5	Sym2	Sym3	Sym4	Sym5	Coif3	Coif4	Coif5
Avg_a	6.31	6.06	7.05	7.36	6.31	6.06	6.45	6.65	7.04	7.27	7.33
S_a	4.71	5.73	5.46	4.76	4.71	5.73	4.66	4.85	4.79	4.64	4.49
E_a	41.3	37.7	42.3	39.1	41.3	37.7	35.1	42.9	30.2	25.6	18.7
Avg_b	0.25	0.24	0.27	0.27	0.25	0.24	0.26	0.27	0.28	0.28	0.28

对于攻击检测而言,攻击特征指标在攻击前后的变化率越大越好,这样就能增强正常情况和异常情况的对比,为高精度地检测异常行为奠定基础.从表 2 可以看出,在选用 Db4 小波时,各特征指标的变化更为显著,所以本文确定 Db4 小波用于特征提取.

根据 BP 网络理论,隐含层神经元个数对网络的分类性能影响很大.本文根据式(2)确定隐含层神经元个数.在 BP 网络训练阶段,从特征库随机选取 200 组标准正常流特征向量和 200 组含有 LDoS 攻击的混合流特征向量作为学习样本,根据 Levenberg-Marquardt 算法进行有导师学习.图 7 显示了隐含层神经元个数为 6,9,12 时的网络均方误差性能和训练次数,当隐含层神经元个数为 9 时,训练时间最短,其误差也最小,因此,选取该 BP 网络的隐含层神经元个数为 9.

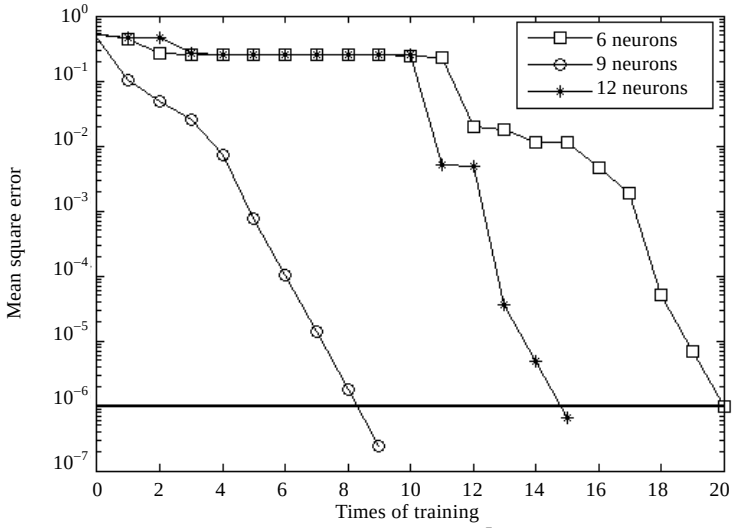


Fig.7 Mean square error curves respectively with 6, 9, 12 neurons in hidden layer

图 7 隐含层神经元个数分别为 6,9,12 时的均方误差性能曲线

BP 网络的输出最终将根据式(3)转化为决策指标 m.本文设定最终决策指标 m 的阈值为 $M_{\min}$,当 m 大于 $M_{\min}$ 时判定存在 LDoS 攻击,否则认为网络流量正常.图 8 给出了 DSBWA 在不同阈值 $M_{\min}$ 下的检测率和误警率.由结果可知,我们的方法具有高检测率和低误警率.当阈值 $M_{\min}$ 在 0.2~0.85 时,检测率达到 95%,误警率在 5%以下,可见系统的检测结果对阈值参数的设置并不敏感.这克服了目前许多入侵检测系统的性能严重依赖于阈值选择的缺点,提高了系统的健壮性和可移植性,也使系统的部署更为方便,无须在参数设定上花费太多时间.

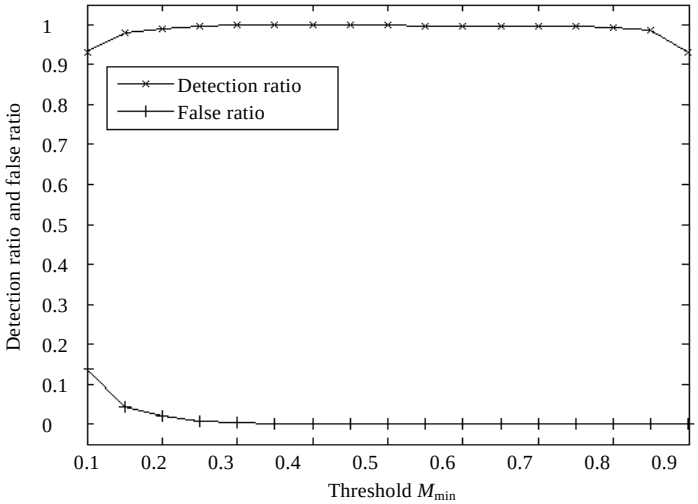


Fig.8 Detection ratio and false ratio under different thresholds $M_{\min}$

图 8 DSBWA 系统在不同阈值 $M_{\min}$ 下的检测率和误警率

选择决策指标的阈值 M_{min}=0.5,从特征库中提取 1 000 组正常流特征向量和 1 000 组混合有 LDoS 攻击的异常流特征向量作为 DBSWA 的测试数据集,实验结果的混淆矩阵见表 3.

Table 3 Confusion matrix

表 3 混淆矩阵

	Flows verified as legitimate	Flows verified as LDoS	Total
Legitimate flows	995	5	1 000
LDoS flows	9	991	1 000

由实验结果的混淆矩阵可以得出,本文基于小波分析的 LDoS 入侵检测系统的正确检测率为 99.3%,漏警率为 0.9%,虚警率为 0.5%,检测系统性能良好.

5 总结与展望

通过分析 LDoS 攻击的规律和现有检测机制的局限性,设计了一种 LDoS 入侵检测系统 DSBWA.该系统有如下几个特点:

(1) 包过程是网络流量分析的有效手段,DSBWA 通过分析包过程检测 LDoS,能够抵御源 IP spoof、协议信息伪造等网络欺骗行为[18],具有良好的健壮性.

(2) 尽管 LDoS 攻击极具隐蔽性和欺骗性,DSBWA 的特征提取算法充分考虑了其攻击流在时频两域的特性,计算量小且区分度高,有利于提高系统的检测率和实时能力.检测引擎基于人工神经网络技术,对 LDoS 变种攻击也有很好的检测效果.

(3) DSBWA 具有定位攻击脉冲的能力,其与 Chen 的基于频谱分析的检测技术相比,后者只能报告在检测窗口内有无 LDoS 攻击,整个窗口均为可疑数据包[10],而 DSBWA 能够提供较准确的线索,缩小追踪范围.

(4) DSBWA 无须对每条数据流单独处理,存储开销不大.系统计算复杂度与检测窗口内包过程长度呈线性关系,消耗计算资源少.如果使用 DSP 实现,实时能力可以进一步提高.

检测系统 DSBWA 能够精确检测 LDoS 攻击和定位攻击脉冲的到达时刻,在此基础上研究响应策略,开发一种分布式协同防范机制,在攻击源端实现对攻击流的有效过滤是今后研究的重点.

致谢 本文的审稿专家提出了宝贵的建议,特此谨向所有审稿专家表示感谢.

References:

[1] Kuzmanovic A, Knightly EW. Low-Rate TCP-targeted denial of service attacks—the shrew vs. the mice and elephants. In: Proc. of the ACM SIGCOMM 2003. New York: ACM Press, 2003. 75–86. http://byte.csc.lsu.edu/~durresi/7502/reading/p75-kuzmanovic.pdf

[2] Sarat S, Terzis A. On the effect of router buffer sizes on low-rate denial of service attacks. In: Proc. of the 14th Int'l Conf. on Computer Communications and Networks (ICCCN 2005). New York: IEEE Press, 2005. 281–286. http://www.cs.jhu.edu/~sarat/ICCCN05.pdf

[3] Kwok YK, Tripathi R, Chen Y, Hwang K. HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks. In: Proc. of the 3rd Int'l Conf. on Networking and Mobile Computing (ICCNMC 2005). New York: Springer-Verlag, 2005. 423–432. http://gridsec.usc.edu/files/TR/HAWK-ICCNMC2005-CameraReady.pdf

[4] Sun H, Lui JCS, Yau DKY. Defending against low-rate TCP attacks: Dynamic detection and protection. In: Proc. of the 12th IEEE Int'l Conf. on Network Protocols (ICNP 2004). New York: IEEE Press, 2004. 196–205. http://www.cse.cuhk.edu.hk/~cslui/PUBLICATION/icnp_lowrate.pdf

[5] Sun H, Lui JCS, Yau DKY. Distributed mechanism in detecting and defending against the low-rate TCP attack. Computer Networks, 2006,50(13):2312−2330.

[6] Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. Journal of Parallel and Distributed Computing, 2006,66(9):1137−1151.

[7] Guirguis M, Bestavros A, Matta I. Exploiting the transients of adaptation for RoQ attacks on Internet resources. In: Proc. of the 12th IEEE Int'l Conf. on Network Protocols (ICNP 2004). New York: IEEE Press, 2004. 184−195. http://www.ieee-icnp.org/2004/papers/5-2.pdf

[8] Luo XP, Chang RKC. On a new class of pulsing denial-of-service attacks and the defense. In: Proc. of the Network and Distributed System Security Symp. (NDSS 2005). Reston: Internet Society, 2005. http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/new_pulsing_DOS.pdf

[9] Chertov R, Fahmy S, Shroff NB. Emulation versus simulation: A case study of TCP-targeted denial of service attack. In: Proc. of the 2nd IEEE Conf. on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM 2006). New York: IEEE Press, 2006. http://cobweb.ecn.purdue.edu/~shroff/Shroff/conference/CheFahShr-tridentcom.pdf

[10] Chen Y, Hwang K. Spectral analysis of TCP flows for defense against reduction-of-quality attacks. In: Proc. of the 2007 IEEE Int'l Conf. on Communications (ICC 2007). New York: IEEE Press, 2005. 1203−1210. http://pods.binghamton.edu/~ychen/PID364015.pdf

[11] Abry P, Veitch D. Wavelet analysis of long-range-dependent traffic. IEEE Trans. on Information Theory, 1998,44(1):2−15.

[12] Mallat S, Hwang WL. Singularity detection and processing with wavelets. IEEE Trans. on Information Theory, 1992,38(2):617−643.

[13] Xu C, Zhao RZ, Gan XB. Wavelet Analysis and its Application. Beijing: Science Press, 2004. 81−117 (in Chinese).

[14] Shen SY. Theory and Application of Neural Networks. Beijing: Science Press, 1998. 31−62 (in Chinese).

[15] Thompson K, Miller GJ, Wilder R. Wide-Area Internet traffic patterns and characteristics. IEEE Network, 1997,11(6):10−23.

[16] Daubechies I, Wrote; Li JP, Yang WN, Trans. Ten Lectures on Wavelets. Beijing: National Defense Industry Press, 2004. 127−153 (in Chinese).

[17] GT-ITM: Georgia Tech Internet Topology Models. http://www.cc.gatech.edu/projects/gtitm/

[18] Hastings NE, McLean PA. TCP/IP spoofing fundamentals. In: Proc. of IEEE the 15th Annual Int'l Phoenix Conf. on Computers and Communications. Scottsdale: IEEE Press, 1996. 218−224.

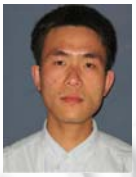
附中文参考文献:

[13] 徐晨,赵瑞珍,甘小冰.小波分析·应用算法.北京:科学出版社,2004.81−117.

[14] 沈世镒.神经网络系统理论及其应用.北京:科学出版社,1998.31−62.

[16] Daubechies I,著;李建平,杨万年,译.小波十讲.北京:国防工业出版社,2004.127−153.

何炎祥(1952－),男,湖北应城人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为分布并行处理,信息安全,数据开采.



韩奕(1985－),男,硕士生,主要研究领域为网络安全,入侵检测.

曹强(1985－),男,硕士生,主要研究领域为网络安全,入侵检测,数据挖掘.

熊琦(1983－),男,博士生,CCF 学生会员,主要研究领域为入侵检测,网络可生存性.

刘陶(1984－),女,博士生,主要研究领域为网络安全,入侵检测,数据挖掘.