第42卷 第8期 西 安 交 通 大 学 学 报 Vol.42 №8
2008年8月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Aug. 2008

带可信度评估的连续小波分布式拒绝服务攻击检测算法

杨新宇，侯光霞，杨树森
（西安交通大学计算机科学与技术系，710049，西安）

摘要：针对传统方法难以实时、有效检测分布式拒绝服务(DDoS)攻击的问题，提出了一种带可信度评估的连续小波DDoS攻击检测算法.首先用不间断的连续小波变换对流量信号进行同步分析，通过发现平台突发信号来实时检测DDoS攻击，然后用报警可信度评估算法对经连续小波变换的检测结果进行二次处理，以消除单点突发信号和网络流量噪声带来的影响.经离散小波变换法、N点平均法以及梯度法的实验对比表明，所提算法对流量数据中的平台突发信号的检测效果比较好.

关键词：分布式拒绝服务；平台突发信号；连续小波变换；可信度评估
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2008)08-0936-04

DDoS Attacks Detecting Algorithm Based on Continuous Wavelet Transforms with Reliability Evaluation

YANG Xinyu, HOU Guangxia, YANG Shusen
(Department of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: As traditional methods cannot effectively detect DDoS attacks in time, a DDoS attack detecting algorithm based on continuous wavelet transforms with reliability evaluation is proposed to detect the DDoS attacks in real-time. In the algorithm, continuous wavelet transforms are used to analyze the traffic data uninterruptedly and to detect the short-flat-burst or the long-flat-burst, which always represent DDoS attacks, and then an algorithm evaluates the reliability of alert, and to reduce the inaccurate alerts caused by single-point-burst and flow noise. Experiments show that the detection algorithm is more effective in detecting DDoS attacks than the discrete wavelet transform method, N-point-average method and gradient method.

Keywords: distributed denial of service; flat-burst signal; continuous wavelet transform; reliability evaluating

分布式拒绝服务(DDoS)攻击是目前严重威胁网络安全和影响网站服务质量的一种攻击手段.DDoS攻击就是利用多个分布式攻击源向攻击对象发送超出攻击目标处理能力的海量数据包，来消耗可用系统和带宽资源，从而导致网络服务瘫痪的一种攻击[1].2002年10月21日，DNS(Domain Name System)根服务器受到了DDoS攻击，全球13台DNS根服务器中有8台不能正常工作[2].

从研究状况来看，针对DDoS攻击的防御技术主要集中于DDoS的攻击检测技术、攻击源追踪技术以及攻击包过滤技术，其中DDoS攻击检测技术是技术基础，因为只有快速、准确地检测到DDoS攻击，才能及时实施DDoS攻击源追踪，进行DDoS攻击包过滤[3].目前，检测DDoS攻击的方法主要有DDoS特征分析法、数据包路径分析法和数据包过滤法等.这些方法大多需要对流量的历史记录进行

收稿日期：2007-11-08. 作者简介：杨新宇(1973－)，男，博士，副教授. 基金项目：国家自然科学基金资助项目(60403028).

分析，计算量很大. 如果要对 DDoS 攻击进行快速和简便的实时检测，就需要采用效率较高的自适应方法. 1986 年 Grossmann 首先提出使用小波变换探测信号奇异性的思想[4]，后经 Mallat 等人的发展与完善[5]，小波奇异性检测理论开始应用于非平稳信号的监测和特征分析等领域. 在检测 DDoS 攻击方面，Garcia 等人提出了利用离散小波变换法对流量信号进行分析，从而确定攻击发生的时刻[6]，而 David 等人提出利用多分辨小波和流量的自相似特性来检测某个时间段内发生的攻击[7]，这 2 种方法虽然有效，但前者不能准确定位攻击，后者不能进行实时检测. 鉴于此，本文提出利用连续小波变换法对网络中的突发流量进行检测，并且加入了报警可信度评估算法，以实现对 DDoS 攻击的实时检测和定位.

1　连续小波变换

小波变换是一种强有力的时频分析工具，它是在克服傅里叶变换缺点的基础上发展起来的. 小波变换在时、频 2 个领域都具有表征信号局部特征的能力，并且能很好地刻画非平稳信号，适合检测正常信号中突变的成分. 小波变换包括连续小波变换和离散小波变换，连续小波变换具有线性、平移不变性、伸缩共变性和自相似性等特征[8]. 因此，用连续小波变换检测 DDoS 攻击的突发信号不会丢失信息，而且能够比较容易地对异常信号进行快速定位，实现突发信号的准确定位和实时检测.

假设复函数 $\psi(x)$ 满足 $\int_{-\infty}^{+\infty}\psi(u)\mathrm{d}u=0$，如果它的傅里叶变换 $\hat{\psi}(x)$ 满足

$$\int_0^{+\infty}\frac{|\hat{\psi}(\omega)|^2}{\omega}\mathrm{d}\omega=\int_{-\infty}^{0}\frac{|\hat{\psi}(\omega)|^2}{|\omega|}\mathrm{d}\omega=C_\psi<+\infty \tag{1}$$

则称 $\psi(x)$ 为小波. 对于任意函数 $f(x)\in L^2(R)$，它的连续小波变换可表示为

$$W_f(a,b)=\langle f,\Psi_{a,b}\rangle=|a|^{-1/2}\int_{-\infty}^{+\infty}f(t)\overline{\Psi}\left(\frac{t-b}{a}\right)\mathrm{d}t \tag{2}$$

其逆变换为

$$f(x)=\frac{1}{C_\Psi}\int_0^{+\infty}\int_{-\infty}^{+\infty}\frac{1}{a^2}W_f(a,b)\Psi\left(\frac{t-b}{a}\right)\mathrm{d}a\mathrm{d}b \tag{3}$$

式中：a 为伸缩因子；b 为平移因子.

2　带可信度评估的连续小波 DDoS 攻击检测算法

2.1　DDoS 攻击特征分析

DDoS 攻击是为了消耗目标主机的资源，它通常会采用下面 2 种方式向目标主机发出请求服务，一是对目标主机的端口发出大量服务请求，二是对目标主机的多个端口请求服务[9]. 因此，在发生 DDoS 攻击时，最主要的特征就是网络流量突然增大，表现出突发状态. 若按突发信号持续时间的长短来看，可将网络流量中的突发信号分为 3 种类型（假设窗口中包含有 N 个数据点，N 的数量级为 10^n）：①单点突发信号，突发值位于某一个时间点；②短时平台突发信号，突发流量中数据点的个数大于 1 且小于等于 $\left(\lceil\frac{N}{10^n}\rceil\times10\right)$；③长时平台突发信号，突发数据点的个数大于 $\left(\lceil\frac{N}{10^n}\rceil\times10\right)$.

2.2　连续小波 DDoS 攻击检测算法描述

在一定时间尺度下测得的单点突发信号，如果确实是 DDoS 攻击流量所引起的，则它在较小时间尺度下会表现出短时或者长时平台突发信号. 相反，如果该信号在较小的时间尺度下仍表现为单点突发信号，则它只是一般的流量突发，与攻击无关. 因此，本文关注的是，如何实时检测网络中的短时或者长时平台突发信号，从而快速检测出 DDoS 攻击. 由于上述 3 种突发信号是相对于测量时间尺度定义的，在大时间尺度下的短时平台突发信号和单点突发信号，而在小时间尺度下可能是长时平台突发信号，所以最好同时使用几种不同的时间尺度进行流量测量，然后对获得的流量信号进行分析.

如前所述，本文关注的是网络流量中的平台突发信号（长时平台突发信号和短时平台突发信号），所以本文算法主要是用于实时检测网络流量中出现的平台突发信号. 在算法中，使用了一个滑动的时间窗口对流量测量系统获得的流量信号进行不间断的同步分析，如果发现时间窗口中出现长时平台突发信号或短时平台突发信号，则做出标记或报警，从而实现实时检测.

在一定的时间尺度下，实时地检测流量中突发信号的算法（算法 1）步骤描述如下.

（1）读入一组信号数据 S，其大小等于窗口的大小.

（2）选择合适的小波变换函数和特征尺度，对原

始信号 S 进行连续小波变换，得到不同尺度下的小波变换系数.

(3)选择合适的检测尺度提取变换后的小波系数集合 C.

(4)选择合适的阈值 t 对所提取的小波系数进行过滤，并采样突发信号变换后的小波系数.

(5)滑动 n 个时间单位的步长，返回步骤(3).

由于突发信号经过小波变换以后的小波系数比较大，从而可以确定突发信号的起始位置，然后做出标记或报警.

2.3 报警可信度评估算法

由于检测尺度及域值的影响，所以利用上述检测算法来报警存在误报现象. 因为该算法不能很好地区分出单点突发信号，这将导致出现单点突发信号报警的现象，从而增大了误报率. 频繁的误报会降低管理效率，影响正常应用，为此如何减少误报意义重大. 为此，本文又提出了一种报警可信度的评估算法，通过对检出的突发信号进行小波系数的关联性分析，可进一步去除大量的单点突发信号. 带有报警可信度评估的连续小波 DDoS 攻击检测算法(算法2)流程如图1所示，具体步骤描述如下.

(1)将通过算法1检测的起始突发信号记为 C_n，其后的2个信号依次记为 C_{n+1}、C_{n+2}.

(2)用阈值 t 来衡量 C_{n+1}、C_{n+2}.

(3)如果 $C_{n+1}<t$，或 $C_{n+1}\geqslant t$ 且 $C_{n+2}<t$，则突发信号为正常信号，反之为攻击信号并做报警处理.

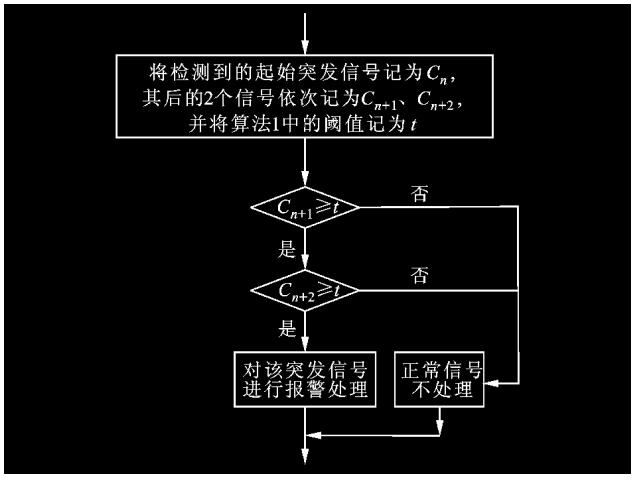


图1 带有报警可信度评估的连续小波 DDos 攻击检测算法流程

算法2是在大量的实验数据的基础上，通过分析经小波变换了的突发信号特征值总结得出的. 如果从检测到的突发起始点起，只有连续2个点的小波变换系数值大于阈值，这样的信号均为单点突发信号或者噪声信号，属于正常突发信号，不予报警；反之，则为短时或者长时平台突发信号，需要作报警处理.

3 实 验

3.1 数据获取

实验数据来自本文作者实验室获得的网络流量测量记录，取自一台对公众开放的 FTP 服务器. 数据的测量长度为 4 000 s，采样间隔为 1 s，其中某些时段用制造 Syn-Flooding 攻击的程序对服务器进行 DDoS 攻击.

攻击的原始信号 S 如图2所示，S 中突发信号的位置、持续时间以及平均强度如表1所示.

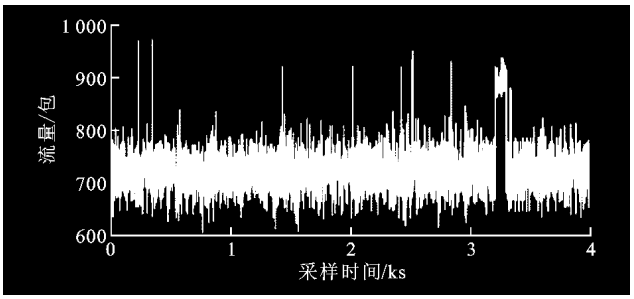


图2 攻击的原始信号 S

表1 原始信号中各种突发信号的位置、持续时间、平均强度

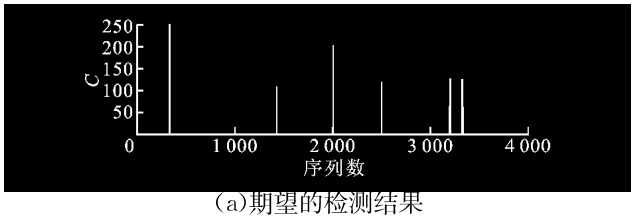
突发信号类型	起始点地址	持续时间/s	平均强度/包·s^{-1}
单点突发 A	229	1	971.00
单点突发 B	2418	1	923.00
单点突发 C	2829	1	931.00
短时平台 A	341	3	947.67
短时平台 B	1428	3	910.67
短时平台 C	3328	3	872.67
短时平台 D	2009	5	904.00
短时平台 E	2508	5	918.60
长时平台 A	3202	90	902.67

3.2 攻击检测与实验结果分析

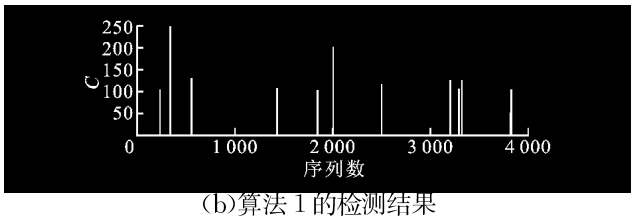
实验中，用 coif3 对原始信号 S 进行了16层变换，并选择第7层的变换系数作为检测数据，同时取阈值 $t=100$，步长为 10 s，滑动的时间窗口大小分别为 4 000 s、1 000 s、500 s、200 s、100 s，待测的原始信号如图2所示.

算法1与算法2的检测结果对比如图3所示. 从中看出，算法1虽然能够实时识别所有的 DDoS

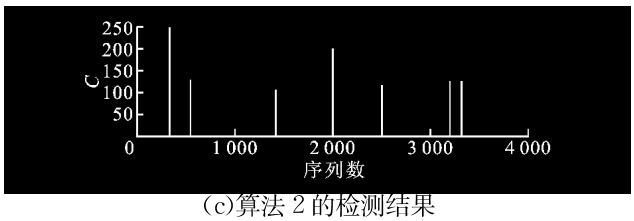
攻击,但结果与理论值误差比较大,而算法 2 不仅能实时检测出所有的 DDoS 攻击,还能有效降低检测误差,使检准率从原来的 54.6%提高到了 85.7%.



(a)期望的检测结果



(b)算法 1 的检测结果



(c)算法 2 的检测结果

图 3　算法 1、算法 2 的检测结果对比

算法 1、算法 2 与离散小波变换法、N 点平均法以及梯度法的检测结果比较如表 2 所示. 从表中可以看出,在相同的检测条件下,只有算法 1 与算法 2 能够实时检测到所有的平台突发信号,并且具有比较高的检准率. 综合来看,引入可信度评估的连续小波变换算法,不仅使检测率达 100%,而且检准率也不低于其他的检测算法.

表 2　4 种检测法检测效果对比

	算法 1	算法 2	离散小波法	N 点平均法	梯度法
突发信号总数	6	6	6	6	6
检到的突发信号数	11	7	4	14	9
检到的正确突发信号数	6	6	4	5	2
检测率/%	100	100	66.7	83.3	33.3
检准率/%	54.6	85.7	100	35.7	22.2

4　结束语

由于网络中的入侵行为,特别是 DDoS 攻击,会引起网络流量突发,所以对其进行准确、实时检测可以及时发现网络异常情况. 为此,本文将网络流量中的突发信号分为长时平台突发信号、短时平台突发信号和单点突发信号,然后依据连续小波变换的特性提出了带可信度评估的连续小波 DDoS 攻击检测算法. 使用 Syn-Flooding 攻击软件对实验室中的 FTP 服务器进行了攻击,并采集了相应的实验数据. 经实验、分析表明,带可信度评估的连续小波变换检测算法对 DDoS 攻击所引起的流量突发信号具有较好的检测效果.

参考文献:

[1] KIM Y, JO J Y, CHAO H J, et al. High-speed router filter for blocking TCP flooding under DDoS attack [C]// Proceedings of the IEEE International Performance, Computing and Communication Conference. Piscataway, NJ, USA: IEEE, 2003:183-190.

[2] YAAR A, PERRIG A, SONG D, et al. Pi: a path identification mechanism to defend against DDoS attacks security and privacy [C]// Proceedings of 2003 Symposium on Security and Privacy. Piscataway, NJ, USA: IEEE, 2003:93-107.

[3] 李金明,王汝传. 基于 VIP 方法的 DDoS 攻击实时检测技术研究 [J]. 电子学报,2007,35(4):791-796.
LI Jinming, WANG Ruchuan. Real-time detection of DDoS attack based on VTP [J]. Acta Electronica Sinica, 2007, 35(4):791-796.

[4] GROSSMANN A. Wavelet transform and edge detection [C]// Stochastics Processes in Physics and Engineering. Dorecht, Netherlands: Reidel, 1986:89-96

[5] MALLAT S. Zero-crossing of wavelet transform [J]. IEEE Trans on Information Theory, 1997, 37(4):1019-1033.

[6] GARCIA R C, SADIKU M N O, CANNADY J D. WAID: wavelet analysis intrusion detection [C]// The 2002 45th Midwest Symposium on Circuits and Systems. Piscataway, NJ, USA: IEEE, 2002:688 -691.

[7] NASH D A, RAGSDALE D J. Simulation of self-similarity in network utilization patterns as a precursor to automated testing of intrusion detection systems [J]. IEEE Trans on Systems, Man and Cybernetics, 2001, 31(4):327-331.

[8] 杨福生. 小波变换的工程分析与应用 [M]. 北京:科学出版社,2006.

[9] 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):768-773.
SUN Qindong, ZHANG Deyun, GAO Peng. Detecting distributed denial of service attacks based on time series analysis [J]. Chinese Journal of Computer, 2005, 28(5):768-773.

(编辑　苗凌)