基于负载预测的分布式拒绝服务攻击检测方法研究

Detecting Distributed Denial of Service Attacks Based on Load Prediction

姚淑萍/YAO Shu-ping, 胡昌振/HU Chang-zhen

北京理工大学信息安全与对抗技术研究中心,北京 100081

Information Security and Antagonism Research Center, Beijing Institute of Technology, Beijing 100081, China

[摘要] 通过分析分布式拒绝服务攻击(Distributed Denial Of Service, DDOS)的特点,提出一种基于主机负载-并发连接时间序列预测的 DDOS 攻击检测方法。该方法改进了传统的异常检测方法,对并发连接序列进行预测,以预测值作为对未来时段内主机负载正常状态的估计,增强了正常行为描述的时效性,提高了攻击检测率,并具有低延时特性。该方法涉及两项关键技术:一是预测技术,二是异常判断方法。为提高预测精度,首次将小波分析引入主机负载预测,建立了小波-神经网络预测模型;为提高异常判断准确性,采用了"滑动窗口"方式。实验表明,基于负载预测的 DDOS 攻击检测优于传统的异常检测方法。

[关键词] 主机负载预测,分布式拒绝服务攻击,小波分析 **[中图分类号]** TP393.08

[文献标识码] A **[文章编号]** 1000-7857(2005)09-0011-03

Abstract: By analyzing of the features of distributed denial of service (DDOS) attacks, a novel approach of detection of DDOS attacks based on host load-concurrent connection time series prediction is proposed. This method has improved the traditional anomaly detection. It predicts concurrent connection time series and adopts prediction results as normal host load estimate of next time range. So the timeliness of normal behavior description is improved; high detection accuracy and low detection latency are acquired. Two key technologies are studied: one is load prediction technology; the other is load anomaly judgment. In order to improve prediction accuracy, a novel wavelet-BP neural network model is established and in order to increase anomaly judgment accuracy, "sliding window" method is used. Experiment results show that our new method is better than traditional anomaly detection technologies.

Key Words: host load prediction, distributed denial of service attack, wavelet analysis

CLC Number: TP393.08 **Document Code:** A **Article ID:** 1000-7857(2005)09-0011-03

1 引言

分布式拒绝服务(Distributed Denial of Service, DDOS)攻击危害巨大、难以防御,是黑客经常采用的主要攻击手段之一。该攻击具有突发性,会导致被攻击主机负载的急剧增加,基于异常的检测是该类攻击最为有效的检测手段[1,2]。

异常检测的核心问题是如何实现负载正常状态的描述。目前普遍的做法是采集大量样本数据, 基于统计或人工智能方法对样本数据进行分析,从中抽取正常模式。这种方式获得的正常行为描述完全依赖于历史数据,时效性差,以此为依据的异常判断准确性也必然受到影响。

本文提出一种基于负载预测的 DDOS 检测方法,首先预测待检测时刻的服务请求数, 将其作为待测时段内正常服务请求的估计值,并以此为参照判断异常,不仅可以提高准确性,而且可以缩减历史记录存储量。

该方法需要解决两个关键技术:一是预测精度,二是异常判断技术。为提高预测精度,本文首次将小波分析引入服务请求的预测,建立了小波-神经网络预测模型;为增加异常判断的准确性,本文采用"滑动窗口"检测方式。这两项关键技术的结合,为 DDOS 攻击的检测提供了一种新思路。

2 检测原理

DDOS 的攻击目标是网络内的重点服务器,对其负载本文采用并发连接数作为衡量指标。对基于 TCP 的服务,并发连接数直接取 Socket 数,对 DNS 等采用 UDP 非连接协议的服务,可以采用虚拟连接的方式,把五元组(协议,源地址,源端口,目的地址,目的端口)相同的访问视为一个连接,效果是一样的。

设采样的时间间隔是 Δt。令 $x(i)$表示第 i 个观测点的并发数,X 表示服务器并发连接时间序列,则

$$X=\{x(1), x(2), x(3), \cdots, x(k), \cdots\} \quad (1)$$

根据 X 构造与预测相关的历史序列。

收稿日期: 2005-06-23

作者简介: 姚淑萍,女,北京市中关村南大街 5 号北京理工大学信息安全与对抗技术研究中心,博士生,研究方向为智能信息处理、信息安全;E-mail: yaosping@163.com

胡昌振(通讯作者),男,北京市中关村南大街 5 号北京理工大学机电学院教授,信息安全与对抗技术研究中心主任,研究方向为网络安全技术与应用;E-mail: chzhoo@public.bta.net.cn

[定义] 设与待预测时刻 t 相关的序列为 $H(t)$,则

$$H(t)=\{x(t-i),\ N\geqslant i\geqslant 1\} \tag{2}$$

其中 $H(t)$表示 t 时刻之前 N 个数据按时间顺序的排列,称为历史序列。

对序列中元素分别重新编号,则 $H(t)$可表示为:

$$H(t)=\{h_k\}_{k=1}^{N} \tag{3}$$

采用并发连接数作为负载衡量指标的优势在于:每个用户的 1 次服务请求只产生 1 个并发连接,这样,虽然 DDOS 攻击和正常用户的请求增加都能导致并发连接数的上升,但一个正常用户在一定时间段内所要求的服务相对单一,而 DDOS 发生时则会在短时间内出现大量、多源的请求,二者引起的并发连接的增加模式有显著不同。所以,基于并发连接时间序列检测 DDOS 攻击应该是有效的。

基于预测的检测原理如图 1。

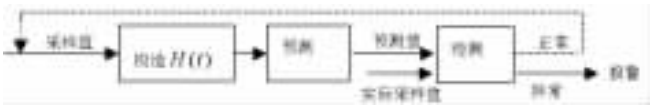

图 1 攻击检测原理

3 系统算法描述

3.1 $H(t)$序列的预测算法

3.1.1 非平稳性分析

时间序列的非平稳性可以通过计算自相关系数[3]判定,公式为:

$$r_k=\frac{\frac{1}{N-k}\sum_{i=1}^{N-k}(h_i-\overline{h})(h_{i+k}-\overline{h})}{\frac{1}{N}\sum_{i=1}^{N}(h_i-\overline{h})^2} \tag{4}$$

其中, $\overline{h}$是样本的平均值,r_k是第 k 个样本的自相关系数,其它符号含义与式(3)同。

通过计算可知,当样本足够大时,若随着 k 的增大,其自相关系数呈下降趋势但并不趋于零,则该序列是非平稳时间序列。

按照该方法可以验证,并发连接时间序列是非平稳的,传统的 AR 等平稳时间序列预测模型显然不是预测的理想选择。考虑到小波分析在处理非平稳信号方面的特有优势,本文将小波引入负载预测,首先对具有非平稳特征的时间序列进行小波分解并单支重构[分解使其低频部分(逼近信号)和高频部分(细节信号)分离,各分支频率成分更加单纯,相关性增强;单支重构则保证了各分支与原始信号长度一致],然后对各分支分别建立 BP 神经网络模型并进行预测,最后将各模型预测结果合成,以实现对服务器负载的预测。

3.1.2 预测原理图

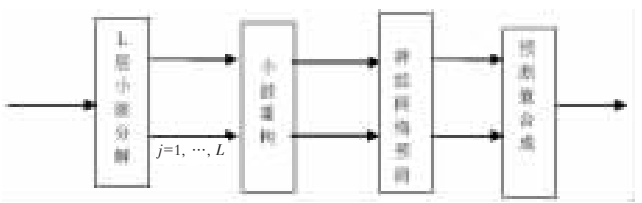

图 2 预测模型

进行一步预测,即求 h_{N+1} 的预测值,记为$\hat{h}_{N+1}$。

对 $H(t)$进行 L 层小波分解。原始序列分离为第 1~L 层共 L 个高频信号和 1 个第 L 层低频信号:

$$W_j=\{w_{j,i}\}\quad j=1,2,\cdots,L;\quad V_L=\{v_{L,i}\} \tag{5}$$

其中,W_j 表示第 j 层高频信号,V_L 表示第 L 层低频信号。每进行一层分解所得的高频信号和低频信号的点数都会比分解前的信号减少 1 倍,这对预测是不利的.为了使各分支的长度保持不变,对各分支进行单支重构,重构后的 L+1 个分支与原始序列的长度一致,即:

$$\widetilde{W}_j=(\widetilde{w}_{j,i},1\leqslant i\leqslant N\}\quad j=1,2,\cdots,L;\quad \widetilde{V}_L=\{\widetilde{v}_{L,i},\ 1\leqslant i\leqslant N\} \tag{6}$$

其中 W_j 为重构后的第 j 层高频信号,$\widetilde{V}_L$为重构后的第 L 层低频信号。分别对$\widetilde{W}_j$和$\widetilde{V}_L$建立神经预测模型进行 1 步预测,获得 L+1 个预测值$\hat{\widetilde{w}}_{j,N+1}$和$\hat{\widetilde{v}}_{L,N+1}$,将其合成得$\hat{h}_{N+1}$。

3.1.3 序列的小波分解与重构

确定尺度函数 $\phi(t)$和小波函数 $\psi(t)$,以及小波分解的低通滤波器 H、高通滤波器 G 及其对偶算子 H^*G^*,选定分解层数 L。分解层数确定标准是使预测误差基本达到最小。

对原始序列进行小波分解[4]的过程为:

$$V_{i+1}=HV_i;\quad W_{i+1}=GV_i\quad i=0,1,2,\cdots,L \tag{7}$$

其中,V_i 和 W_i 分别是分辨率为 2^{-j} 的原始信号的逼近信号(低频信号)和细节信号(高频信号),V_0 即原始信号 $H(t)$。

当分解进行到第 L 层时, 原始信号被分解为 L 个高频信号和 1 个低频信号。对这 L+1 个信号利用 Mallat 重构算法[4]:

$$V_{i-1}=H^*V_i+G^*W_i\qquad i=L,L-1,\cdots,1 \tag{8}$$

重构到原尺度后可得 L+1 个与原始信号长度完全相同的信号$\widetilde{W}_1,\widetilde{W}_2,\cdots,\widetilde{W}_L$和$\widetilde{V}_L$,且有:

$$H(t)=\widetilde{W}_1+\widetilde{W}_2+\cdots+\widetilde{W}_L+\widetilde{V}_L \tag{9}$$

依据第 2 节对各序列的定义,进一步可得:

$$h_i=\widetilde{w}_{1,i}+\widetilde{w}_{2,i}+\cdots+\widetilde{w}_{L,i}+\widetilde{v}_{L,i} \tag{10}$$

令$\hat{v}_{N+1}$表示 v_{N+1} 的预测值, 则对 h_{N+1} 的预测转化为求各分支的预测值$\hat{\widetilde{w}}_{j,N+1}$和$\hat{\widetilde{v}}_{L,N+1}$,即:

$$\hat{h}_{N+1}=\hat{\widetilde{w}}_{1,N+1}+\hat{\widetilde{w}}_{2,N+1}+\cdots+\hat{\widetilde{w}}_{L,N+1}+\hat{\widetilde{v}}_{L,N+1} \tag{11}$$

3.1.4 各分支信号的神经网络预测模型

对 L+1 个信号分量分别建立 BP 神经网络预测模型,每个模型均为输入层、隐层和输出层 3 层。各 BP 模型的输出层单元只有 1 个,输入层单元数则随各分量频段的增高递增。隐层数大约取输入单元数一半左右,然后通过训练调整。以高频信号$\widetilde{W}_L$的训练为例。

将$\widetilde{W}_L$按一定比例分为两组, 第一组为神经网络训练数据,第二组为检验数据,训练精度公式为[5]:

$$\sigma^2=\frac{1}{N-N_1}\sum_{n=N_1+1}^{N}(\widetilde{w}_{L,n}-\hat{\widetilde{w}}_{L,n})^2/\frac{1}{N}\sum_{n=1}^{N}(\widetilde{w}_{L,n}-\overline{\widetilde{W}}_L)^2 \tag{12}$$

其中,N 是总样本数,N_1 是训练样本数,$\overline{\widetilde{W}}_L$ 表示$\widetilde{W}_L$平均值。

若 $\sigma^2=0$,表示预测结果与期望值完全吻合;若 $\sigma^2\geqslant 1$,表示预测的效果不比直接选取序列的均值好。

用训练好的模型对 $L+1$ 个信号分量的第 $N+1$ 点进行预测,共得到 $L+1$ 个预测值$\hat{w}_{j,N+1}$和$\hat{v}_{L,N+1}$。

3.2 异常判断算法

异常检测采用基于滑动窗口的方式实现。系统需要维护两个窗口,一个是描述主机正常行为的历史窗口,记为 W_h; 另一个是描述当前实际行为的当前窗口,记为 W_c,窗口宽度为 T。

计算预测均方根误差 RMSE:

$$\mathrm{RMSE}=\sqrt{\sum_{i=1}^{M}(h_i-\hat{h}_i)^2/M} \qquad (13)$$

其中,M 为测试样本数,h_i 和$\hat{h}_i$分别是样本的实际值和预测值。

攻击检测流程为:

① 检测时刻 t 前 T 个采样值作为 W_h 和 W_c 的初始值;

② [定义]构造 $H(t)$,进行一步预测,得到 $t+1$ 时刻预测值,记为$\hat{f}$;

③ 将 W_h 向右滑动 1 步,使$\hat{f}$进入窗口;

④ 将 W_c 向右滑动 1 步,使 $t+1$ 时刻的采样值 f 进入窗口;

⑤ 计算并发连接异常度 TMSA:

$$\mathrm{TMSA}=\sqrt{\sum_{i=1}^{T}(f_i-\hat{f}_i)^2/T} \qquad (14)$$

其中,f_i 是实际并发连接数,$\hat{f}_i$是预测值。若

$$\mathrm{TMSA}\geqslant \mathrm{K}\cdot\mathrm{RMSE} \qquad (15)$$

则判定出现异常(K 为预先定义的常数),报警;否则,修改检测时刻 t<-$t+1$ 并将实际采样值剔除"坏值"(明显异常的值)后反馈给系统输入端,转(2)。

4 实验

以 1 台机器作为攻击控制机,10 台机器作为攻击傀儡机,1 台 Web 服务器为攻击目标机, 构建如图 3 所示的 DDOS 攻击模拟环境。

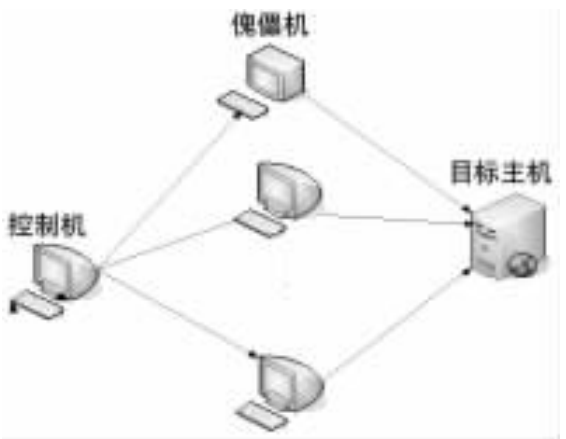

图 3 DDOS 攻击体系结构

在不同时段按不同策略共进行 20 次模拟攻击。图 4 为某次攻击中采集的被攻击服务器并发连接数序列,采样时间间隔为 1 秒,时间跨度 11 分钟,其中,为攻击前 9 分钟,攻击后 2 分钟。

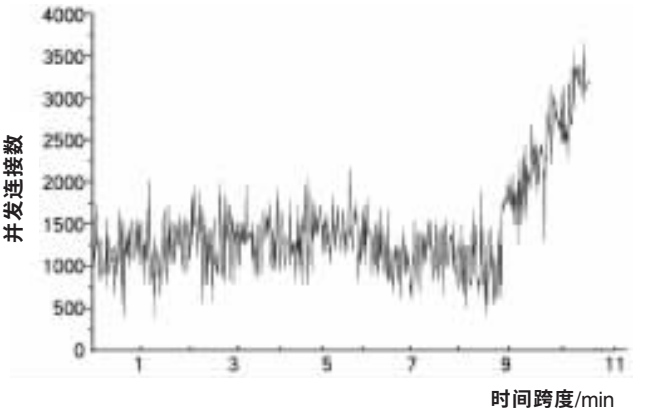

图 4 并发连接序列样本

该次攻击分为两个阶段,攻击手段为传统的 SYN flood 攻击。初始阶段由控制机启动 5 台傀儡机进行攻击;60 秒后,进入第二阶段,控制机启用全部傀儡机;当攻击又持续 60 秒时,我们发现访问被攻击服务器时,网页无法打开,说明攻击已经起到作用。

预测是一步预测,历史序列 $H(t)$取时刻 t 前的 540 个历史数据,即式(2)中 N=540。

对 $H(t)$采用 DB4 进行 3 层小波分解并重构。共获得 4 个信号分量,对其分别建立 BP 模型进行预测。

检测的历史窗口和当前窗口的宽度 T 取为 10, 该次攻击报警延迟为 11 秒。

检测结果统计表明,检测出错率是 5%,产生错误的原因是由于网络噪声的存在使预测值发生偏离以及攻击强度较小而造成。

5 结论

本文提出了一种基于预测的 DDOS 攻击检测方法,该方法以预测值作为未来时段内网络正常行为的描述,改进了正常行为描述的时效性,提高了攻击检测精度,并具有低延时特性。该方法中影响检测率的关键是预测的准确性,本文首次将小波分析引入主机负载预测,建立了小波-神经网络预测模型,与传统预测模型相比较,该模型精度明显提高。

基于负载预测检测攻击是一个新思路,本文已经证明其在检测 DDOS 攻击方面的优势,今后的主要工作是将该方法扩展到蠕虫等其它攻击的异常检测中。

参考文献(References)

[1] Shan Rongsheng, Li Jianhua, Wang Mingzheng. Anomaly detection for network traffic flow[J]. *Journal of Southeast University(English Edition)*, 2004, 20(1): 16~20

[2] 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): 767~773

[3] NIST/SEMATECH Engineering Statistic Handbook. URL:http://www.itl.nist.gov/div898/handbook/

[4] Mallat S G. A theory for multiresolution signal decomposition: the wavelet representation[J]. *IEEE Tran.on Pattern Analysis and Machine Intelligence*, 1989, 11(7): 674~693

[5] Casdagli M. Nonlinear prediction of chaotic time series [J]. *Physica*, 1989, D35: 335~356

(责任编辑 苏 青)