Front. Electr. Electron. Eng. China 2007, 2(1): 73–77
DOI 10.1007/s11460-007-0013-z

RESEARCH ARTICLE

REN Xunyi, WANG Ruchuan, WANG Haiyan

Wavelet analysis method for detection of DDoS attack on the basis of self-similarity

Abstract As the traditional methods were not suitable for the detection of small distribute denial of service (DDoS) attack and identification of busy traffic, on the basis of the influence of DDoS attack, one wavelet analysis method was proposed. Wavelet method of coefficient variance analysis was deduced and a software model for the method was designed. In addition, key issues of the choice of wavelet and calculation of Hurst were resolved. The experimental results show that the proposed method has more advantages in accurately identifying busy traffic and detection of small DDoS attack.

Keywords abnormal detection, distribute denial of service, self-similarity, wavelet transform

1 Introduction

Distribute denial of service (DdoS) attacks have done great damage to internet [1], such as, in the beginning of the year 2000, Yahoo, Amazon, and CNN web sites were forced to close because of DDoS attacks [2]. However, according to the report of United States Computer Emergency Readiness Team (US-CERT), till date, there is no one method that can deal with DDoS attacks for good. Generally, people think the kernel of TCP/IP protocol must be changed; otherwise, DDoS attacks cannot be thoroughly resolved in theory. Nevertheless, some technical methods such as detection of DDoS attacks and filters can be adopted to effectively prevent some DDoS attacks and cut losses.

Conventional methods of detection and guard were founded on character match, which often needed some experimental knowledge. In addition, it could not distinguish between burst normal traffic and DDoS attacks [3]. Many studies show that normal networks have a self-similarity feature [4–7]. DDoS attacks can produce noticeable influence on self-similarity of network traffic. So, according to the change of Hurst, the DDoS attacks can be detected. Now, methods of computing Hurst parameter have variance time plot (VTP), periodogram, R/S analysis, and Whittle's estimator. These methods need more samples and computing process is slow, so they require more large-scale memory and high computing power [8]. They also cannot accurately identify DDoS attacks and busy traffic, and cannot detect small DDoS attacks. Wavelet analysis is a local time-frequency analysis method, which has a fixed window, but the shape, time scale, and frequency windows can shift. The feature causes the special multiple resolution advantage in fractal signal process and parameter estimation [9,10]. So, wavelet analysis has an important application value. This study proposed one wavelet analysis method of detection for DDoS attacks, and experimental results show that the proposed method has more advantages in accurately identifying busy traffic and detection of small DDoS attack.

Translated from *Journal on Communications*, 2006, 27(5): 6–11 [译自: 通信学报]

REN Xunyi, WANG Ruchuan (✉), WANG Haiyan
College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
E-mail: wangrc@njupt.edu.cn

2 The self-similarity of network traffic

Conventional models of network traffic are made on the basis of Poisson or Bernoulli distribution, such as IPP, MMPP, IBP, and MMBP. These models think that if s is large enough, the traffic of current time t is not related to that of past time t-s. It means that only when s is very small, packets have correlation property, which is called short dependent relation (SDR) [11]. But these models do not agree with the practical measurement results. In fact, network traffic presents statistic self-similarity, namely long-range dependence (LRD). So, current traffic should adopt an LRD model, such as self-similarity process.

If the self-similar process is exact, it is called exact second order self-similarity; that is, for every $a>0$, $x(t)=a^{-H}x(at)$, and a is scale, H is constant. If self-similar process is statistical, it is called asymptotical second order self-similarity; that is, for every $a>0$, stochastic process $\{x(t)\}$ satisfies the form: $x(t)_{(d)}=a^{-H}x(at)$, (d) is probability distribution, and

H is partial scale index number. The autocorrelation function of $x(t)$ [9] is

$$R_x(t_1,t_2)=R_x(\tau)=a^{-2H}R_x(a\tau) \tag{1}$$

where $\tau=t_2-t_1$. Making the Fourier transform, power spectrum of $x(t)$ can be obtained

$$P_x(\omega)=a^{-2H-1}P_x\left(\frac{\omega}{a}\right) \tag{2}$$

When a is replaced with a^{-1}, it can be then written as

$$P_x(\omega)\propto\frac{1}{|\omega|^{\gamma}},\ \gamma=2H+1 \tag{3}$$

It means, the power spectrum of self-similar process satisfies Eq. (3), and H is only a parameter of self-similarity, the range of H is (1/2, 1). If H is more, the degree of self-similarity is higher. Many methods of wavelet analysis for estimation of H are made on the basis of Eq. (3).

3 Detection method for DDoS attacks

Wavelet analysis methods for Hurst have wavelet variance analyses, power spectra, and energy analysis. Similar to the study made in Ref. [12], these methods are consistent in essence. In this section, the wavelet variance analysis is introduced initially, and on this basis, the detection method for DDoS attacks is proposed.

3.1 Wavelet variance analysis

If $\{x(t)\}$ is a asymptotical second order self-similarity, its power spectra is $P_x(\omega)$, making wavelet transform for it, the wavelet coefficient can be obtained

$$d_l^{(j)}=2^{\frac{j}{2}}\int x(t)\psi(2^j t-l)\mathrm{d}t \tag{4}$$

$\psi_{j,l}(t)=2^{j/2}\psi(2^j t-l)\mathrm{d}t$, $\psi_{j,l}(t)$ is orthogonal wavelet, and its regularity degree is R. From Eq. (4)

$$\mathrm{E}\left[d_l^{(j)}\right]=\mathrm{E}[x(t)]2^{\frac{j}{2}}\int\psi\left(2^j t-l\right)\mathrm{d}t=0 \tag{5}$$

According to the definition of correlation coefficient, for every two wavelets coefficient $d_l^{(j)}$, $d_{l'}^{(j')}$

$$\begin{aligned}\mathrm{E}\left[d_l^{(j)},d_{l'}^{(j')}\right]&=\iint\mathrm{E}\left[x(t)\psi_{j,l}(t)x(t')\psi_{j',l'}(t')\right]\mathrm{d}t\mathrm{d}t'\\&=\int\psi_{j,l}(t)\left[R_x(t)*\psi_{j',l'}(t')\right]\mathrm{d}t\end{aligned} \tag{6}$$

Making Fourier transform and using Parseval formula

$$\begin{aligned}&\mathrm{E}\left[d_l^{(j)},d_{l'}^{(j')}\right]=\frac{2^{-\frac{j+j'}{2}}}{2\pi}\cdot\\&\int_{-\infty}^{+\infty}\frac{\sigma_x^2}{|\omega|^{\gamma}}\hat{\psi}\left(2^{-j}\omega\right)\overline{\hat{\psi}\left(2^{-j'}\omega\right)}\mathrm{e}^{-i[l2^{-j}-l'2^{-j'}]\omega}\Big]\mathrm{d}\omega\end{aligned} \tag{7}$$

From Eqs. (6) and (7), the variance of $d_l^{(j)}$ can be derived;

$$\mathrm{var}\left[d_l^{(j)}\right]=\frac{2^{-j\gamma}}{2\pi}\int_{-\infty}^{+\infty}\frac{\sigma_x^2}{|\omega|^{\gamma}}\left|\hat{\psi}(\omega)\right|^2\mathrm{d}\omega \tag{8}$$

Setting

$$\sigma^2=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\frac{\sigma_x^2}{|\omega|^{\gamma}}\left|\hat{\psi}(\omega)\right|^2\mathrm{d}\omega \tag{9}$$

Then from Eqs. (8) and (9)

$$\mathrm{var}[d_l^{(j)}]=\sigma^2 2^{-j\gamma} \tag{10}$$

Taking logarithm of both sides of Eq. (10), when square error of mean is minimum, one straight line is obtained, its slope is γ, $H=(\gamma-1)/2$.

3.2 Detection method on the basis of wavelet variance analysis

Self-similarity of network traffic is because of heavy-tailed distributions of file. When DDoS attack happens, normal TCP traffic packets are jammed followed by a decrease in self-similarity. When normal traffic was overwhelmed by DDoS attack packets, the traffic model tends to poison distribution, namely H is close to 0.5. That is to say, DDoS attack can cause the noticeable change of H value; so from the change in H value, DDoS attacks can be detected. We can detect DDoS attacks, but do not match packet character, and simultaneously, the method is different from common statistics method, so it can make distinction between DDoS attacks and buy network traffic.

For detecting DDoS attacks, the change of Hurst value should be analyzed. Firstly, according to the wavelet variance analysis, the Hurst value was obtained. Secondly, when DDoS attacks happen, the current Hurst value should also be obtained. Lastly, the change of two Hurst value must be analyzed. Let normal Hurst value be H_n, the abnormal H_a, the subtracted value: $\Delta h=H_n-H_a$. Setting threshold θ, if $\Delta h>\theta$, it is thought that DDoS attacks then happen; otherwise, network traffic is normal. Because the typical value of Hurst is 0.75, if the Hurst value is below 0.5, this network traffic has no self-similarity feature, so θ should be less than 0.25. To quickly detect DDoS attacks, the θ should accord to practical network state. In this experiment, θ was set at 0.15. When the change of Hurst value is more than 0.15, DDoS attacks happened.

4 Method of realization model

Wavelet variance analysis for Hurst includes the design of realization model, the choice of wavelet, extracting wavelet coefficient, and using Eq. (10) for computing H. According to the above analysis, the realization model is designed as shown in Fig. 1.

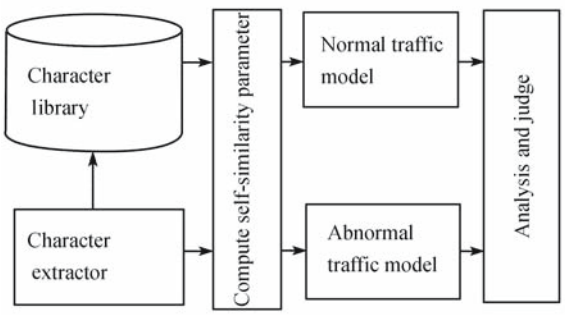

Fig. 1 Realization model made on the basis of self-similarity

In character extractor, one data structure is defined as:

```
struct packetcharacter{
        int time;
        int size;
        }
```

Time is the packet arrive time, size is the length of arrive packet. Character library has no need of one real database; so one circular chain list was adopted. The element of chain list is defined as:

```
struct list{
struct packetcharacter p;
struct list next;
}
```

Character Extractor extracts the packet character, and inserts it to the chain list. According to the chain list that normal traffic produce, Hurst parameter can be sought by wavelet variance analysis. When DDoS attacks happen, abnormal traffic mode is acquired. On the basis of comparing the analysis of the two Hurst parameters and the mode acquired, the occurrence of DDoS attacks can be judged. Next, wavelet must be chosen for computing Hurst, which includes two aspects. One is wavelet type, and the other is wavelet vanishing moments. Wavelet has important influence on the Hurst value, but in theory, the fittest wavelet cannot be proved. So, Db(n), Sym(n), and Coif(n) were selected, and through changing the value of n, the experiment was carried out for getting the best wavelet. Using MATLAB as tools, its functions produced the signal with $H = 0.75$, and its length was 8 215. The computing Hurst results are shown in Table 1.

From Table 1, it can be seen that the average error of Db(n) is 0.055 6 (compared with 0.75), the average error of Sym(n) is 0.072 1, and of Coif(n) is 0.068 0; so, Daubechies wavelet was chosen. Vanishing moment is an important factor that has influence on the self-similarity. For Db(n), n is its vanishing moment. For measuring the regularity degree, the number must be more than the regularity degree calculated in Eq. (9), namely $n > \gamma$, because $\gamma = 2H + 1$, where $0.5 < H < 1$; so $2 < \gamma < 3$, then $n \leqslant 3$. From Table 1, the Hurst of Db(3) is 0.748 5, which has the minimum error compared with 0.75. So, Db(3) is the best wavelet for computing Hurst parameter.

Finally, as wavelet coefficient must be taken, this study adopted the Mallat decomposition algorithm, namely

$$\begin{cases} c_k^{j+1} = \sum_{l \in z} c_l^{j+1} \overline{h_{l-2k}} \\ d_k^j = \sum_{l \in z} c_l^{j+1} \overline{g_{l-2k}} \end{cases} \tag{11}$$

where c_k^{j+1} is the proximate signal, and d_k^j is the detail signal. d_k^j is the required high frequency wavelet coefficient. Using Matlab, high frequency wavelet coefficient can be quickly extracted, and Hurst can also be easily computed. The main processes are as follows.

Step 1 Extract the single character from character library.

Step 2 Choose the Db(3) as analysis wavelet and compute its maximum scale.

Step 3 On the basis of Eq. (11), use wavedec function to decompose the signal, and obtain the wavelet coefficient matrix [C, L].

Step 4 When ($i \leqslant$ scale): use detcoef function to extract high frequency wavelet coefficient $L[i]$ from [C, L], and compute $\log_2^{\mathrm{var}[d_l^{(j)}]}$, according to matrix[$i$ $\log_2^{\mathrm{var}[d_l^{(j)}]}$], draft the approach straight, and obtain its slope, then Hurst = (slope − 1)/2.

Step 5 According to $\Delta h = H_n - H_a$, compute the change of Hurst. If $\Delta h > \theta$ then DDoS attacks happen.

5 Experiment and analysis

For testing the proposed method, a software was developed with Libpcap tool on the basis of realization model and algorithm. The normal traffic packets were captured at room 903 on main building of Nanjing University of Posts and Telecommunications. Averaging these data, and putting them

Table 1 Computing Hurst results with different wavelets

Number	3	4	5	6	7	8	9	10	11	12	13	14	15
Db(n)	0.748 5	0.728 7	0.700 9	0.709 3	0.712 5	0.706 7	0.689 2	0.689 2	0.670 5	0.663 7	0.680 5	0.682 4	0.673 7
Sym(n)	0.747 5	0.737 3	0.707 9	0.698 8	0.697 8	0.685 3	0.657 2	0.668 9	0.651 4	0.662 0	0.650 1	0.650 8	0.647 0
Coif(n)	-	0.715 7	-	0.661 0	-	0.648 3	-	0.641 3	-	-	-	-	-
Number	16	17	18	19	20	21	22	23	24	25	26	27	28
Db(n)	0.664 7	0.685 3	0.690 2	0.710 7	0.706 6	0.686 2	0.685 3	0.702 1	0.703 7	0.689 5	0.680 1	0.694 2	0.700 7
Sym(n)	0.647 0	0.665 1	0.691 8	0.667 6	0.694 1	0.659 4	0.688 0	0.658 8	0.685 3	0.653 0	0.669 4	0.673 4	0.675 7
Coif(n)	-	-	-	-	-	-	-	-	-	-	-	-	-

in the character library as total network traffic, 8 192 packets were randomly got every 0.01 second. For testing the ability to distinguish busy traffic, using the same method, data was collected 10 times at 8:00–10:00 PM, and Db(3) wavelet was used to decompose the data with 10 scales.

The former represents the normal network traffic, and the latter represents the busy traffic. This experiment mainly detects the TCP flooding attacks. DDoS attacks are added by background traffic by replaying method. DDoS attacks were produced using TFN tool, which can send the specified protocol and length packets to destination with changing attack strong thread. Moreover, it can adopt a random IP source address. Experimental data are shown in Table 2.

Table 2 DDoS attack data

Experiment	Normal tarffic	Busy traffic	Attack traffic
Time	2005.4.1–2005 4.10 8:00–10:00 AM	2005.4.1–2005 4.10 8:00–10:00 PM	2005.4.11
Speed	2–6 Mb/s	8–12 Mb/s	2 Mb/s
Sampling	8 192	8 192	410
Strong	Normal	Busy	Small attack

The main advantages of the proposed method are as follows.

1) It can detect the attacks that do not cause the obvious change in total traffic.

Because the large-scale network background traffic is very great, small strong DDoS attacks do not cause the obvious change in the total traffic, but these attacks have a bad influence on the destination and network. Through wavelet decomposing, normal network traffic can be divided into low frequency wavelet coefficiences and high frequency wavelet coefficiences. Small attacks can change the similarity of high frequency wavelet coefficiences, and cause the change of Hurst parameter. In this experiment, two thread attacks were adopted strongly occupying 5% of total traffic.

2) It can identify the busy traffic and strong DDoS attacks.

Busy traffic can cause false DDoS attacks; correctly judging the busy traffic can enable filter selection accurate. When traffic becomes busy, the self-similarity changes less, and through wavelet transformation, Hurst parameter can accurately be obtained, on the basis of whichthe busy traffic and DDoS attacks can be identified.

For the above two cases, wavelet analysis was made using MATLAB software.

The Hurst computing of normal traffic is as in Fig. 2. Its slope is 2.711 2, so H is 0.855 6. Figure 3 shows the Hurst computing of abnormal traffic, its slope is 2.630 6, so $H =$ is 0.815 3. When compared with Fig. 2, $\Delta h = 0.040\ 3 < 0.15$, so DDoS attacks do not happen and the self-similarity of traffic is very good. This means that the proposed method does not regard busy traffic as DDoS attacks, thus enabling it to identify the busy traffic. Figure 4 is the experiment results of small DDoS attacks, its slope is 2.291 6, $H = 0.645\ 8$, and $\Delta h = 0.209\ 8 > 0.15$, So, DDoS attacks happened. Moreover, small DDoS attacks cause the Hurst to decline very evidently, which is obviously different from the influence of busy traffic on network.

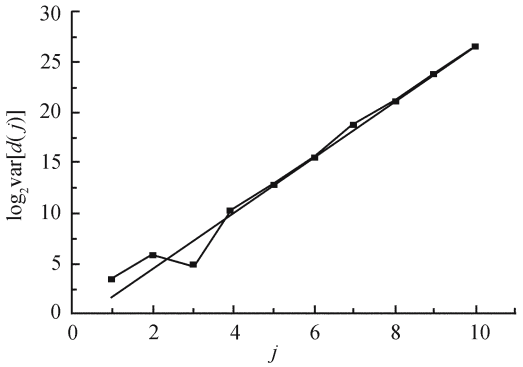

Fig. 2 Hurst computing of normal traffic

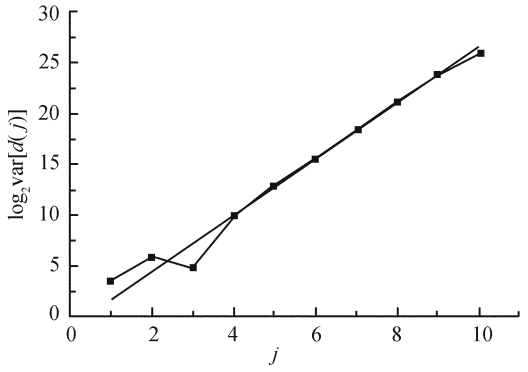

Fig. 3 Hurst computing of busy traffic

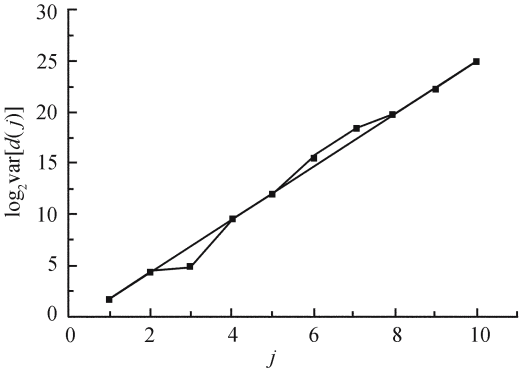

Fig. 4 Hurst computing of abnormal traffic including samll DDoS attacks

Hurst results with traditional methods are shown in Table 3. The Hurst values with these methods are more than 0.7. Many experiments showed the effectiveness of proposed method.

Table 3 Hurst results with traditional methods

VTP	Periodogram	R/S	Whittle
0.735 4	0.765 8	0.725 3	0.755 6

6 Conclusions

This study was made to detect DDoS on the basis of self-similarity of network traffic, which uses the hot topic wavelet analysis in the process. The method can accurately judge DDoS attacks. When one server is either busy or at leisure, the method has more advantages than traditional methods. Because statistics of leisure web site is very different from the one of busy traffic, the character match methods and common self-similarity method cannot accurately identify the DDoS attacks and busy traffic, also causing some problems such as misreport and failure report. However, wavelet analysis method has the same model for leisure and busy conditions, but when DDoS attacks happen, the model changes very greatly. As a result, the proposed method can more accurately detect DDoS attacks. The future work will focus on real-time detection for DDoS attacks, and on intelligent filter technology.

Acknowledgements The work was sponsored by the National Natural Science Foundation of China (Grant Nos. 60573141, 70271050), the Hi-Tech Research and Development Program of China (Nos. 2005AA775050, 2006AA01Z219, 2006AA01Z201, 2006AA01Z439), the Natural Science Foundation of Jiangsu Province (No. BK2005146), High Technology Research Programme of Jiangsu Province (Nos. BG2005037, BG2006001), High Technology Research Programme of Nanjing (No. 2006RZ105), Foundation of State Key Laboratory for Modern Communications (No. 9140C1101010603), Key Laboratory of Information Technology processing of Jiangsu Province (Nos. kjs05001, kjs0606), Project sponsored by Jiangsu Provincial Research Scheme Of Natural Science for Higher Education Institutions (No. 05KJB520092).

References

1. Chang R K C. Defending against flooding-based distributed denial-of-service attack: A tutorial. IEEE Comm Magazine, 2002, 40(10): 42–51
2. Lau F, Rubin S H, Smith M H. Distributed denial of service attacks. In: Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. Nashville, 2000, 2275–2280
3. Sun Qingdong, Zhang Deyun, Gao Peng. Detecting distributed denial of service attacks based on time series analysis. Chinese Journal of Computers, 2005, 28(5): 768–773 (in Chinese)
4. Leland W, Taqqu M, Willinger W. On the self-similar nature of ethernet traffic (Extended Version). IEEE/ACM Trans on Networking, 1994, 2(1): 1–15
5. Paxson V, Floyd S. Wide area traffic: The failure of poison modeling. IEEE/ACM Trans on Networking, 1995, 3(3): 226–244
6. Dang T D, Molnar S. On the effects of non-stationarity in long range dependent tests. Budapest University Technology and Economics Tech. Rep. Budapest, Hungary, 1999
7. Abry P, Veitch D. Wavelet analysis of long range dependent traffic. IEEE Trans on Infor Theory, 1998, 44(1): 2–15
8. Di Wenjun, Xue Lijun, Jiang Shiqi. Abnormity detection of network traffic applied self-similarity analysis of network traffics. O. I. Automation, 2003, 22(6): 28–31 (in Chinese)
9. Li Bincheng, Luo Jianshu. Analysis and Application of Wavelet. Beijing: Publishing House of Electronics Industry, 2003 (in Chinese)
10. Daubechies I. Ten Lectures on Wavelets. Philadelphia, PA: SIAM, 1992
11. Cai Hong, Chen Huimin, Li Yanda. Self-similar traffic model: A new approach for modeling bursty traffic in telecommunication networks. Journal of China Institute of Communications, 1997, 18(11): 51–58 (in Chinese)
12. Li Yongli, Liu Guizhong, Wang Haijun. Wavelet-based analysis of hurst parameter estimation for self-similar traffic. Journal of Electronics & Information Technology, 2003, 25(1): 100–105 (in Chinese)