DoS Attack Inference Using Traffic Wave Analysis

P. Jayashree, T. Aravinth, S. Ashok Kumar, and S.K.R. Manikandan

Department Of Information Technology,
Anna University Chennai, Chennai-600044
pjshree@annauniv.edu, thiyagu.ily@gmail.com,
ashok_acp@yahoo.com, skrau89@gmail.com

Abstract. DoS attacks are still remaining unsolved mystery in internet. Though various methods such as change point detection, classifier method, packet marking, use of efficient filters and gateways have been proposed to mitigate DoS attacks, all these methods lack in enough accuracy in detection and hence the false alarm. The proposed work performs network traffic monitoring by way of analyzing the generated traffic signal and determines the traffic wavelet coefficients using continuous wavelet transform and based on the wavelet coefficients and energy distribution in successive time intervals, inference of attack occurrence is confirmed. In this paper, DoS attack detection is performed using three types of wavelet functions and the efficiency of different wavelets in the attack detection is compared.

Keywords: continuous wavelet transform, denial of service, mother wavelet, wavelet analysis.

1 Introduction

DoS is a type of attack in which an attacker uses malicious code to attack a single target. This type of network anomaly occupies the resources of victim so that victim may not be allowed for further communication. DDoS attacks involve breaking into hundreds or thousands of machines all over the Internet by installing malicious software on them, allowing them to control all these machines to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims.TCP SYN Flood [12], Smurf, Tear Drop, UDP Flood, ICMP Flood and peer-to-peer are common attacks reported in the present days. There are many defensive mechanisms available for DoS attack such as detection, prevention, IP spoofing, etc. Attack detection involves raising the alarm after the occurrences of attack. Prevention involves protect the network from the attack in future. IP spoofing involves the identification of the attackers involved in the attack launching.

Wavelet analysis is a mathematical technique used to represent data or functions. The wavelets used in the analysis possess some mathematical properties, and break the data down into different scales or resolutions. The wavelet transform is a powerful tool in the analysis of transient phenomena because of its ability to extract time and frequency information from the transient signal. Further choosing a mother wavelet is

N. Meghanathan et al. (Eds.): NeCoM, WiMoN, and WeST 2010, CCIS 90, pp. 171–179, 2010.

application specific. Wavelets were developed independently in the fields of mathematics, quantum physics, electrical engineering, and seismic geology. During the last ten years wavelets have been used in many applications such as image compression [15], turbulence, power analysis in transmission lines [6], [10], human vision, radar, and earthquake prediction.

2 Related Work

[7] used vector subspaces for wavelet analysis and obtain the detail signals by projection. From implementation point of view, this becomes more complex in case of continuous flooding attacks, in terms of computational cost. Here energy distribution based on wavelet analysis is used to detect DoS attacks. The use of sliding window requires more concentration, because when the size of window is small, it may lead to overlap of signals and when the size is small, the anomalies may get absorbed and may not be revealed. While [5] eliminated the risk of using windows. CWT was used to obtain the wavelet coefficients rather than DWT, which is a major advantage. But this system modifies the amplitude and duration of the signal, due to which there are chances for many false detections and missing the duration of real attacks. The time series is constructed by considering the packet rate.

[3] monitors only a link or node in network to detect the anomaly. This is not aptly characterize the network traffic, as the attack launching and detection can not be centralized. The authors reported that if the energy value changes and continues to remain constant then it is the result of attack. But when traffic changes from attack to normal, there will be a sharp decrement in energy value and this remains constant till next attack happens. This constant value cannot be claimed as attack. [1] uses DWT for finding wavelet coefficients. This is not as efficient as CWT because it is not assured that DWT will give wavelet coefficient for each input given. And also not all wavelets can be used in DWT. Such restrictions make DWT inefficient.

3 Need for Wavelets

It is well known from Fourier theory that a signal can be expressed as the sum of a, possibly infinite, series of sines and cosines. This sum is also referred to as a Fourier expansion. The big disadvantage of a Fourier expansion is that it has only frequency resolution and no time resolution. This means that although determining all the frequencies present in a signal is possible, the time of presence of those frequency bands is missing. To overcome this problem in the past decades several solutions have been developed which are more or less able to represent a signal in the time and frequency domain at the same time. The *wavelet transform* or *wavelet analysis* is probably the most recent solution to overcome the shortcomings of the Fourier transform. They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes.

The wavelet transform is also less computationally complex taking O(N) time as compared to $O(N \log N)$ for the fast Fourier Transform(FFT). It is also important to note that this complexity only applies when the filter size has no relation to the signal size. A wavelet without compact support such as the Shannon wavelet would require O(*N*^2).

4 Proposed Method

The network traffic is viewed as a sequence of packets, each of which is represented using a set of 41 parameters as mentioned in KDD 1999 dataset. The times series representation of the traffic is constructed using certain significant parameters in the traffic. The parameters that are considered are protocol type, service, src bytes, count, srv count, dst_host_srv_count. The traffic signal is constructed by calculating the entropy value for the chosen parameters for each of the packets arriving at a particular time and then the average of all entropy values is plotted to obtain the time series. The time series of the traffic signal is constructed using the function as described in equation (1).

$$f_t = {}^1\!/_n\left(-\sum_{i=1}^{n}\sum_{j=1}^{v} S_{ij}\log\left({}^{S_{ij}}\!/_n\right)\right) \tag{1}$$

where the subscript *i* stands for a parameter out of the of n chosen parameters and the subscript *j* stands for the set of values existing in the traffic for the parameter *i.* S_{ij} is the value j of the parameter *i.* Then the time series is smoothened using moving average [3], with α=0.3, in order to avoid false alarms. This smoothened time series is taken as the input for wavelet analysis. The wavelet analysis procedure involves the use of the abstract wavelet function, called mother wavelet. Here the initial analysis is performed on the mother wavelet function, while further analysis is performed with a wavelet obtained with a scaled and translated version of the same wavelet. As the original signal or function can be represented in terms of a wavelet coefficient, any further operations can be performed using wavelet coefficients itself.

Since the network traffic is continuous, it is better to choose the wavelet corresponding to continuous wavelet transform. Some of the continuous wavelets are Morlet, Gaussian, Mexican hat, etc. The energy distribution variance in traffic behaviour under DoS attack changes markedly and this change in distribution is used to detect the attacks. The energy values generated using different wavelets are compared and the properties of wavelets are anlysed to identify the most efficient one for attack detection.

4.1 Continuous Wavelet Transform

A brief description of the wavelet analysis, *continuous wavelet transform* or *CWT is presented.* More formally it is written as in equation (2).

$$\gamma(s,\tau)=\int f(t)\, w^{*}_{s,\tau}(t)dt \tag{2}$$

where * denotes complex conjugation. The variables *s* and τ, represent scale and translation factors. It shows how a function *f(t)* is decomposed into a set of basis functions, $w_{s,\tau}(t)$ called the wavelets. The CWT for network traffic is defined as in equation (3).

$$C(f_t) = f_t \Psi s,\tau\,(t)\;dt \qquad (3)$$

The function *f(t)* in the equation denotes the time series of network traffic f_t as said earlier. Ψ(t) is the wavelet chosen for the study, which is discussed in the following sections.

4.2 Scaling and Translation

The wavelets are generated from a single basic wavelet W(t), the so-called *mother wavelet*, by scaling and translation as shown in equation (4).

$$Ws,\tau\,(t) = (1/\surd s)W((t\text{-}\tau)/s) \qquad (4)$$

The factor s-1/2 is used for for energy normalization across the different scales. The scale refers to the width of the wavelet and as the scale increases and the wavelet gets wider, it includes more of the time series, but the finer details get smeared out. So a smaller scale value of 3 is chosen for the experiment.

The translation and scaling operations applied to the mother wavelet are performed to calculate the wavelet coefficients. The wavelet coefficients are calculated for each wavelet segment. The CWT uses discretely sampled data, however the translation process is a smooth operation across the length of the sampled data, and the scaling can be defined from the minimum to a maximum chosen by the user. The effect of this translation and scaling process is to produce a time-scale representation. This process of translation and dilation of the mother wavelet is depicted in figure 1.

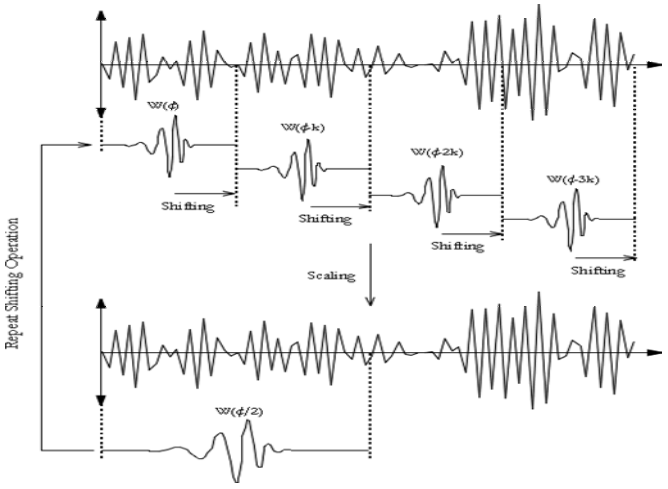

Fig. 1. Scaling and shifting of a mother wavelet

4.3 Morlet Wavelet

The wavelet basis function of Morlet [5] is given by the equation (5).

$$W = (1/(\sigma\,.k.\surd k))e^{-(\sigma\,t/k)\wedge 2}\;cos(2\pi ft/k) \qquad (5)$$

where σ =0.05 is the morlet wavelet bandwidth and f=0.9 is the centre frequency of morlet wavelet chosen in order to satisfy the admissibility condition. The wavelet is subjected to CWT and the corresponding wavelet coefficients are obtained. Only the real part of the transform evaluation is considered.

4.4 Spline Wavelet

The B-spline wavelets satisfy all the desirable properties namely biorthogonality, compact support, smoothness, symmetry, good localization, and efficient implementation. Nowadays B-spline scaling functions find place in many applications.

B-spline wavelet is defined by the equation (6) using the three parameters of integer order parameter (m≥1), bandwidth parameter (f_b) and wavelet center frequency (f_c).

$$w(x) = \sqrt{f_b}\, (sinc(f_b x/m))^x\, e^{2i\,n\,f_c\,x} \tag{6}$$

One property that is exclusively possessed by these splines is that they have the best approximation among all known wavelet families. Here the values of above said parameters are chosen as 3, 0.05 and 0.9 respectively. In order to satisfy the properties of wavelets and to have best approximation, the periodic boundary conditions are used and the length of signal must be a power of two.

4.5 Daubechies Wavelet

Daubechies D4 wavelets are commonly used as it easy to put into practice. Daubechies wavelet is widely used in solving a broad range of problems, like self-likely properties of a signal or fractal problem, signal discontinuities, etc. The wavelet scaling and translation function is given by the following set of equations (7).

$$\begin{gathered}
h_0 = (1+\sqrt{3})\,/\,(4\sqrt{2}) \\
h_1 = (3+\sqrt{3})\,/\,(4\sqrt{2}) \\
h_2 = (3-\sqrt{3})\,/\,(4\sqrt{2}) \\
h_3 = (1-\sqrt{3})\,/\,(4\sqrt{2}) \\
g_0 = h_3 \\
g_1 = -h_2 \\
g_2 = h_1 \\
g_3 = -h_0
\end{gathered} \tag{7}$$

$$\begin{gathered}
a_t = h_0\, s_{2t} + h_1\, s_{2t+1} + h_2\, s_{2t+2} + h_3\, s_{2t+3} \\
a[i] = h_0 s[2i] + h_1 s[2i+1] + h_2 s[2i+2] + h_3 s[2i+3] \\
c_t = g_0\, s_{2t} + g_1\, s_{2t+1} + g_2\, s_{2t+2} + g_3\, s_{2t+3} \\
c[i] = g_0 s[2i] + g_1 s[2i+1] + g_2 s[2i+2] + g_3 s[2i+3]
\end{gathered}$$

5 Implementation and Results

In this paper, the attack detection process is implemented on the network traffic data set provided by KDD. Morlet, Spline and Daubechies wavelets are used for the network traffic transformation and the accuracy of these wavelets in detecting the attack is compared.The continuous wavelets may be real or complex valued. For implementation purpose, only real values are considered. The selection of parameters is based on their entropy values and attack detection rate. Then the time series is constructed by taking average value of those parameters, which represent the traffic and are considered to be significant in detecting the attack.

5.1 Energy Distribution

The energy values of wavelets [7], at two different time instants t and t+ τ are given by equation (8).

$$E_i^t = (1/n_i) \sum_i |d^t (s, \tau)|^2 \text{ and}$$
$$E_i^{t+\tau} = (1/n_i) \sum_i |d^{t+\tau} (s, \tau)|^2 \tag{8}$$

where d^t (s, τ) and $d^{t+\tau}$ (s, τ) are the wavelet coefficients obtained from CWT with a scaling factor of 3 and translation factor of 6 and n_i is the total number of samples taken in the experiment. In this paper, 5000 samples of packets from the KDD CUP 1999 data set have taken used over various runs of detection. Then the energy difference between successive wavelets are found using the equation (9).

$$\Delta E_i = \log E_i^t - \log E_i^{t+\tau} \tag{9}$$

The wavelet coefficients obtained using Morlet wavelet is shown in Figure 2 and the energy values obtained from above wavelet coefficients is provided in table 1.

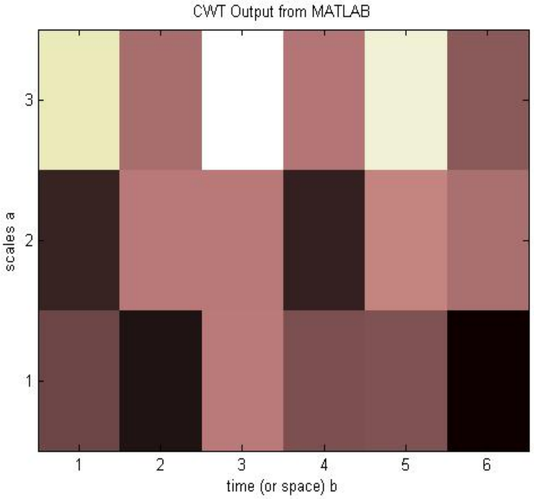

Fig. 2. CWT output for Morlet wavelet

Table 1. Energy values obtained from wavelets

Mother wavelet	Average energy value during attack (x10^{-3})	Average energy value during normal (x10^{-3})
Morlet	340.82	120.45
Daubechies	290.65	101.67
Spline	300.87	113.96

Figure 3 shows the energy values calculated using morlet wavelet over a period of 15 mins.

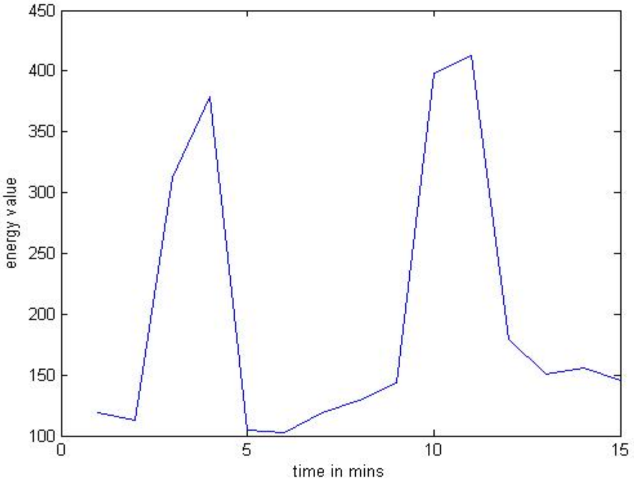

Fig. 3. Graph showing the energy values of traffic

6 Performance Comparison

With respect to wavelet properties, the analysis on the transformed traffic wave is performed. Symmetric wavelets show no preferred direction in time while asymmetric wavelets do for two different directions. A narrow wavelet functions is fast to compute but the narrowness in time implies a very large width in frequency. Conversely wavelets with large compact support are smoother, have finer frequency resolution and are usually more efficient. Regularity gives the approximate measure of the number of continuous derivative that the wavelet functions possess. The regularity therefore gives the smoothness of wavelet function with higher regularity implying a smoother wavelet. A higher vanishing moment implies that more moments will be removed from the signal.

Table 2. Performance Comparison of Wavelet properties

Property	Morlet wavelet	Daubechies D4 wavelet	Spline wavelet
Symmetry	Symmetric	Asymmetric	Symmetric
Compact support	Infinity	15	24
Vanishing moments	1	4	2
Regularity	Infinity	0.85	0.63

From tables 1 and 2, it is clear that the order of efficiency of wavelets in DoS attack detection is as follows

i. Morlet wavelet
ii. Spline wavelet
iii. Daubechies D4 wavelet.

Daubechies wavelet has a major disadvantage that although it can be used in both CWT and DWT, it is not best suited to CWT. Hence a low result is obtained. If the wavelet has highest number of vanishing moments, it may not be able to detect the attack in the traffic wave, as the attack scenario may get vanished. The traffic wave may contain some flash events and in order to avoid false detections, the wavelet should have smoother function. The table 3 gives the attack detection and false alarm raised by the proposed method, ARX model [1], FD (CUSUM) [5] and vector subspace based detection [7].

Table 3. Comparison of proposed method with existing methods.

Methodology	Attack detection (%)
Proposed method	93.27
ARX model [1]	80.34
FD (CUSUM) [5]	84.70
Vector subspace [7]	88.65

The proposed method is found to be better than the earlier ones in [1], [5], [7]. [1] used DWT for finding wavelet coefficients, but this does not give coefficients for all given inputs. This difficulty can be overcome by using CWT. [3] claimed that attack can be detected by monitoring the energy difference. But this does not detect the flooding attacks. In this paper, rather than using energy difference, the energy values are directly used to detect the attack. Hence most of the attacks can be detected. Using [5] the attack cannot be detected efficiently, because even when the packet rate is low, there is a possibility of non-flooding DoS attack. [7] used sliding windows, which needs more concentration, because when the size of window is small, it may lead to overlap of signals and when the size is large, the anomalies may get absorbed and may not be revealed.

7 Conclusion and Future Work

This paper presented the work of detecting DoS attacks by means of wavelet analysis. Further by choosing three different types of mother wavelet, analysis is done based on their properties for comparing their performance with respect to DoS attack detection. The continuous wavelet transform gives wavelet coefficients for each input value, while the discrete wavelet transform does not do so and also the number of coefficients decreases as scale increases. The multi resolution analysis of wavelets is being carried out using tree based decomposition of signal associated with selected mother wavelets.

References

[1] Lu, W., Ghorbani, A.A.: Network Anomaly Detection Based on Wavelet Analysis. EURASIP Journal on Advances in Signal Processing, Article ID 837601, 16–32 (2009)

[2] He, W., Hu, G., Yao, X., Kan, G., Xiang, H., Wang, H.: Applying Multiple Time Series Data Mining to Large-Scale Network Traffic Analysis. In: CIS 2008, pp. 394–399 (2008)

[3] Shinde, P., Guntupalli, S.: Early DoS Attack Detection using Smoothened Time-Series and Wavelet Analysis. In: Third International Symposium on Information Assurance and Security, pp. 215–220 (2007)

[4] Benetazzo, L., Narduzzi, C., Pegoraro, P.A.: Internet Traffic Measurement: A Critical Study of Wavelet Analysis. IEEE transactions on instrumentation and measurement 56(3), 800–806 (2007)

[5] Dainotti, A., Pescapé, A., Ventre, G.: Wavelet-based Detection of DoS Attacks. In: IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM, pp. 494–499 (2006)

[6] Soares, L.R., de Oliveira, H.M., Cintra, R.J.S.: Signal Analysis Using Fourier-like Wavelets

[7] Li, L., Lee, G.: DDoS attack detection and wavelets. Springer Science Telecommunication Systems 28(3, 4), 435–451 (2005)

[8] Liu, L., Li, Z., Xu, Y., Mei, C., Tan, X.: A wavelet based distributed ID model. In: Proceedings of the 2005 IEEE International Conference on Services Computing (SCC 2005), pp. 104–110 (2005)

[9] Huang, M.-C.: Wave parameters and functions in wavelet Analysis. In: Ocean Engineering, pp. 111–125. Elsevier, Amsterdam (2004)

[10] Probert, S.A., Song, Y.H.: Detection and Classification of High Frequency Transients using Wavelet Analysis. In: IEEE Power Engineering Society, pp. 801–806 (2002)

[11] Crovella, M., Kolaczyk, E.: Graph Wavelets for Spatial Traffic Analysis. In: Proceedings of ACM SIGCOMM, pp. 185–195 (2002)

[12] Cheng, C.-M., Kung, H.T., Tan, K.-S.: Use of Spectral Analysis in Defense against DoS Attacks. In: Proceedings of IEEE GLOBECOM (2002)

[13] Barford, P., Kline, J., Plonka, D., Amos, R.: A Signal Analysis of Network Traffic Anomalies. In: Proceedings of ACM IMW, pp. 71–82 (2002)

[14] Abry, P., Veitch, D.: Wavelet Analysis of Long-Range-Dependent Traffic. IEEE transactions on Information Theory 44(1), 2–15 (1998)

[15] Ramachandran, K., Vetterli, M., Herley, C.: Wavelets, subband coding, and best bases. Proceedings of IEEE 84(4), 541–560 (1996)

[16] Flandrin, P.: Wavelet analysis and synthesis of Brownian motion. IEEE transaction on Information Thoery 38(2), 910–917 (1992)