2011 Seventh International Conference on Computational Intelligence and Security

A Wavelet-Based Detection Approach to Traffic Anomalies

Dingde Jiang[1,*] Peng Zhang[1] Zhengzheng Xu[1, 2] Cheng Yao[1] Wenda Qin[1]

1. College of Information Science and Engineering, Northeastern University, Shenyang 110819, China
2. School of Business Administration, Northeastern University, Shenyang 110819, China
*jiangdingde@ise.neu.edu.cn

***Abstract*-Anomaly traffic often breaks out without any omen and brings a breakdown to networks in a short time, and thus the adaptive detection of anomalies in network traffic is an important and challenging task. In this paper, we propose a wavelet-based adaptive approach to detect anomalies in network traffic. We can use wavelet packet transform and continuous wavelet transform to perform the adaptive detect anomaly. First, wavelet packet transform is exploited to extract the anomaly characteristics on the different scales. Then continue wavelet transform is exploited to obtain the further anomaly information about network traffic. Simulation results show that our method is effective and feasible.**

Keywords-traffic anomalies; anomaly detection; wavelet transform; network traffic; backbone network

I. INTRODUCTION

Network traffic anomalies refer to the status that network traffic departs from the normal behaviors. The causes resulting in network traffic anomalies are diverse, such as outages, network operations anomaly, flash crowd, network warms, attacks and so on. Also, efficient operation and management of current large networks heavily depend on the correct analysis of network anomalies. Therefore, detecting traffic anomaly accurately is one of the preconditions of ensuring the efficient network operation. This has received wide attention.

Many schemes and methods are proposed for network traffic anomaly detection, such as the exponential smoothing, adaptive threshold, cumulative sum [1], maximum entropy estimation [2], and principal component analysis [3, 4]. All the methods are based on statistical techniques. Some of these methods analyzed the statistic properties of the network traffic flow, based on measurements of the statistic in consecutive interval with the same duration, and others looked at the time series of specific kinds of packets in aggregate traffic, focusing on a few kinds of attacks. Thatte et al. [5] used only aggregate traffic statistics to detect network anomalies. Wavelet analysis as a new technology has recently been taken to perform anomaly detections of network traffic. Time and scale localization abilities of wavelets make them ideally suited to detect irregular traffic patterns in network traffic trace. In [6] the authors exploited a property of some network misconfigurations that is reflected by the energy function calculated at a specific set of scales. Dainotti et al. [7] presented an anomaly detection system, which combined more traditional approaches with the continuous wavelet transform, to detect volume-based anomalies in network traffic caused by DoS attacks. In [8] the authors utilize a method based on analytical discrete wavelet transform and high-order statistical analysis to detect traffic anomalies. We also employed time-frequency analysis to detect traffic anomalies [9].

In this paper we propose an adaptive method to detect anomalies in network traffic based on the wavelet packet analysis and continuous wavelet analysis. Generally, for a backbone network [10, 11], network traffic holds all kinds of inherent characteristics. Firstly, to analyze anomaly traffic in a network, we use wavelet packet transform to extract anomalies characteristics in network traffic. Because wavelet packet transform can adjust the decomposition process adaptively and has the same detective ability to the anomaly of various frequencies, it is a powerful tool to anomaly detection. By making the initial detection of wavelet packet coefficient on each scale and checking whether there is any anomaly at some moments on this scale, we can obtain some information about traffic anomalies. Second, we carry out continuous wavelet transform for network traffic signals on different scales. Continuous wavelet transform on different scales embodies the individual properties of network traffic, and hence it is helpful to detect and analyze further the duration that traffic anomalies last. To describe the total characteristics of network traffic, we calculate the average coefficients of continuous wavelet transform in some center scales. Thirdly, we employ the continue wavelet transform to confirm the anomaly detected by wavelet packet analysis, and for each detected anomaly we also estimate the start and the end time. Finally, the detected result output is equal to 0 or 1 for each input sample. Simulation results show that our method can detect the network traffic anomalies efficiently.

The rest of this paper is organized as follows. In Section II we provide some detailed analysis that justifies the techniques adopted and show the details on the system architecture and algorithms implemented are given. In Section III we illustrate the simulation results of our detection method. Finally, in Section IV we conclude our work.

II. PROBLEM STATEMENT

The wavelet packet analysis can select different time-frequency resolution to decompose adaptively according to the characteristics of traffic signals. Using this method, we can locate time-frequency domains and get the faint signals effectively. It can effectively detect the anomaly traffic with the long-time duration and that with the short-time sudden change, and also it can effectively detect middle-high

978-0-7695-4584-4/11 $26.00 © 2011 IEEE
DOI 10.1109/CIS.2011.222

frequency attack traffic which hardly can be checked out by the previous methods of network traffic anomaly detection.

Generally, wavelet packet analysis mainly includes two aspects, namely decomposition algorithm and reconstruction algorithm. The following will describe them in detail and propose our method.

If $g_j^n(t) \in U_j^n$ then g_j^n is defined as:

$$g_j^n(t) = \sum_l d_l^{j,n} u_n(2^j t - l), \tag{1}$$

where U_j^n is a subspace that represents the scale-space and the wavelet-space.

Then decomposition algorithm of wavelet packet analysis is that given $\{d_l^{j,n}\}$, we compute $\{d_l^{j,2n}\}$ and $\{d_l^{j,2n+1}\}$, which is denoted into:

$$\begin{cases} d_l^{j,2n} = \sum_k a_{k-2l} d_k^{j+1,n} \\ d_l^{j,2n+1} = \sum_k b_{k-2l} d_k^{j+1} \end{cases} \tag{2}$$

Similarly, reconstruction algorithm of wavelet packet analysis is that given $\{d_l^{j,2n}\}$ and $\{d_l^{j,2n+1}\}$, we compute $\{d_l^{j+1,n}\}$, which is described as follows:

$$d_l^{j+1,n} = \sum_k \left[h_{l-2k} d_k^{j,2n} + g_{l-2k} d_k^{j,2n+1} \right] \tag{3}$$

The continuous wavelet transform is defined as:

$$WT_f(a,\tau) = \langle f(t), \psi_{a,\tau}(t) \rangle = \frac{1}{\sqrt{a}} \int_R f(t) \psi^0 \left(\frac{t-\tau}{a} \right) dt, \tag{4}$$

where $f(.)$ is the signal under analysis, $\psi(.)$ is a function of finite energy whose integral over R is 0, called mother wavelet, and a and b are the scaling and translation factors respectively. Each (a,b) pair furnishes a wavelet coefficient, which can also be seen as the cross-correlation at lag b between $f(t)$ and the mother wavelet function dilated to scaling factor a. The scale of the coefficients global maximum is where the input signal is most similar to the mother wavelet. This function is chosen to be oscillating but with a fast decay from the center to its sides, in order to have good scale and time localization properties. If we use the continuous wavelet transform to analyze the approximate nature of signals as a whole, tend to select a larger-scale, while to show changes in details the smaller-scale should be selected.

In figure 1, a block diagram representing the adaptive detection system model is shown. This system consists of four components, namely signal generation, wavelet packet analysis, continue wavelet transform, and anomaly detection. In this model, the generated traffic signal is obtained by superimposing anomaly profiles to real traffic traces in which no anomalies were present. This choice is partly due to the scarce availability of traffic traces containing classified anomalies along with all the necessary details. For example, the lack of information on the exact beginning and end of each anomaly would not allow us to evaluate the temporal precision of the detection system. On the other hand, being able to generate different traces containing anomalies allowed us to dispose of much more test cases than those that were practically possible to obtain by capturing real traffic traces with real anomalies. By the means of the wavelet packet analysis, we can get the location of the anomaly in the network traffic. At the same time, according to the continuous wavelet transform, we can compute a wavelet coefficient line to present the wave situation of the generated traffic. And then we can get the final detected signal.

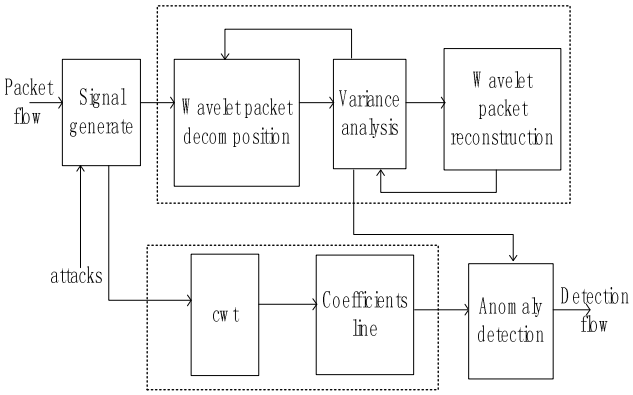

Fig. 1 Adaptive detection system model

In the model of wavelet packet analysis, we will get the initial detection. At first, we make multi-scale 1-level decomposition for the generated traffic signals and make wavelet packet decomposition for the coefficient of node [1, 0] to level 3. Then, we analyze the coefficients under different scales to detect the anomaly by means of variance analysis algorithm. When it is found that anomaly reaches the alert threshold in some certain scale of the former three levels, reconstruction detection starts immediately; if it is still anomalous, it alarms. When it is found that anomaly reaches the decomposition threshold in certain level of the third scale, the process of decomposition continues to detect on level 4 and it will end until the anomaly reaches the alert threshold or the anomaly is below the decomposition threshold.

The step of the wavelet packet analysis is as follows:

Step1: Make the wavelet packet decomposition of the generated traffic signal to level 3, and afterwards they will continue adaptive decomposition with the specific detection situations.

Step2: Make the initial detection on the wavelet packet coefficient of each scale, and check whether there is any anomaly at some moments on this scale by the means of

variance analysis. When it is found that anomaly in some certain scale of the former three levels, reconstruction detection starts immediately. When it is found that anomaly in certain level of the third scale, decomposition continues to detect on level 4.

Step3: We reconstruct the wavelet packet coefficient to traffic signal on the scale analyzed anomaly, and then make the second detection on the reconstructed traffic signal to find the location of the anomaly in the generated traffic. Finally, we get the detection signal which is equal to 0 or 1 for each signal sample generated.

The variance analysis algorithm is a modified version of the deviation scoring algorithm that combines the mean and variance of the historical traffic. According to the results of variance analysis and experience of historical traffic, set an alarm threshold that is defined as:

$$T = e + 3 * \sigma, \tag{5}$$

Where e refers to the mean value of traffic flow, and σ refers to the deviation standard of traffic flow.

The change point can be detected by the coefficient line based on the continuous wavelet transform, and the effect will be different in each scale. The larger scale gets the approximate nature of the signal as a whole, while the smaller scale gets the details of the change-points. Considering the experimental results like anomaly location, anomaly duration, the start and the end time of the anomaly, our approach was to select a center scale. At first, by analyzing the historical network traffic signal, we find that a few scales can obtain the main characteristics of network traffic. Then, find the scales that can clearly indicate traffic characteristics, and compute the averaged wavelet coefficient line by the coefficients on those scales. Finally, to improve the accuracy of the detection, we take a denoising method to smooth the wavelet coefficient line. The line is fed as an input to the Anomaly Detection block, which receives as inputs also the rough detection by wavelet packet analysis.

The anomaly detection block operates as follows:

Step1: In the rough detection of wavelet packet analysis, find the anomaly location information about the generated traffic signal, and group it.

Step2: Looking at all the coefficients on the coefficients line, the coefficients that correspond to the location for each group of information is found.

Step3: Starting from the left and the right of the coefficient, the extreme values (the local maximum and local minimum) are determined. The coefficients between them represent the anomaly traffic; their distance represents the anomaly interval.

Step4: For each group of information, find out the anomaly traffic, then somehow all this anomaly is combined. In the end, output the detection result.

III. Simulation Result and Analysis

To verify our method, we exploit the traffic data from the

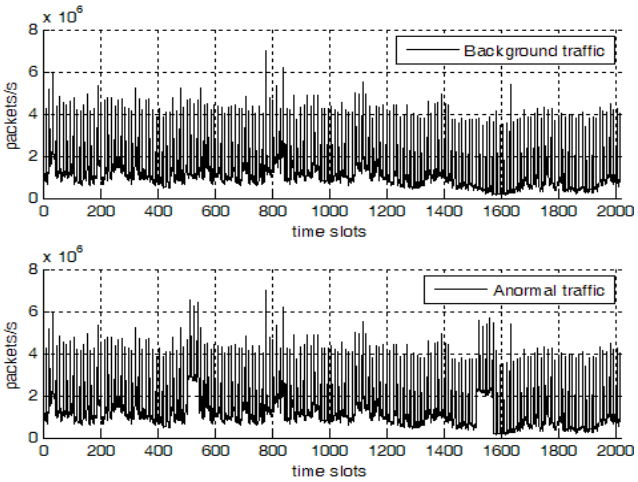

Fig. 2 Background traffic and mixed traffic.

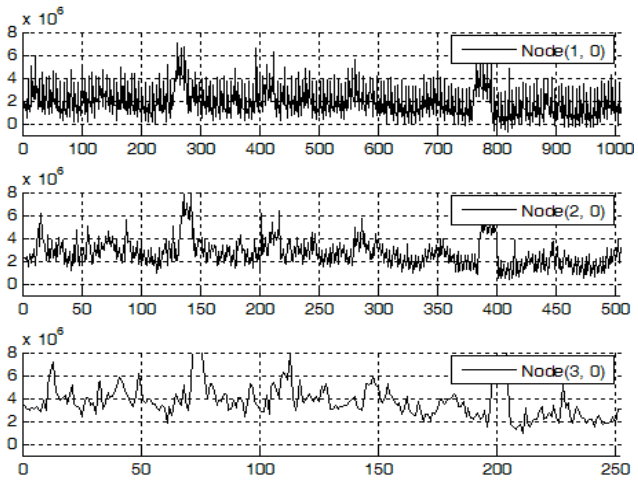

Fig. 3 Wavelet packet decomposed coefficients of level 1, 2, and 3

Abilene network as background traffic, while DDoS attack traffic is emulated in real local network using eight personal computers to attack a server by DDoS attack tool Autocrat. And then attack traffic captured is superimposed to the background traffic to construct data set of anomalous traffic for performance simulation. And we compare our method with the known PCA (Principal Component Analysis) detection approach [12] to analyze their detection performance. For a specific trace, the amplitude of an anomaly was scaled in order to make its maximum peak proportional to the root mean square of the original traffic trace. The choice of the proportionality factor was 1.

Figure 2 shows background traffic and mixed traffic. Attack traffic is superimposed in the samples in [501, 540] and the samples in [1501, 1560], respectively. From Figure 2, we can not easily find the difference between them in these time zones. Hence, it is very difficult to detect anomalous components in network traffic only in time domain.

Figure 3 shows the wavelet packet decomposition of

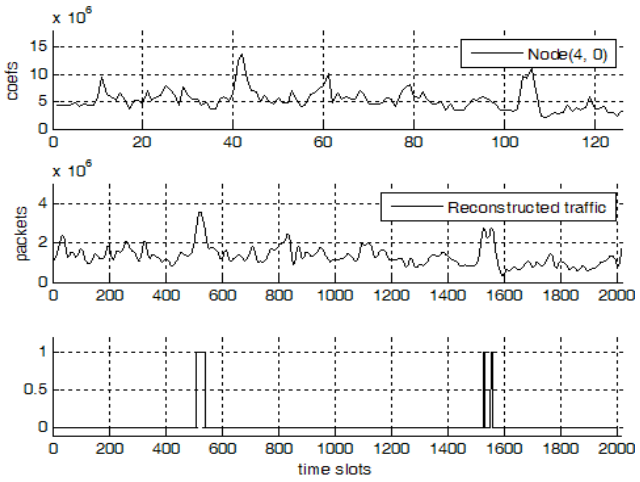

Fig. 4 Reconstructed traffic signal and rough detection signal.

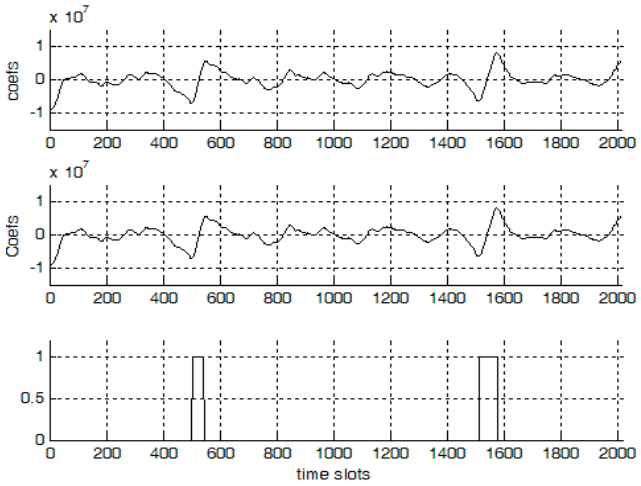

Fig. 6 Coefficient line and detection result.

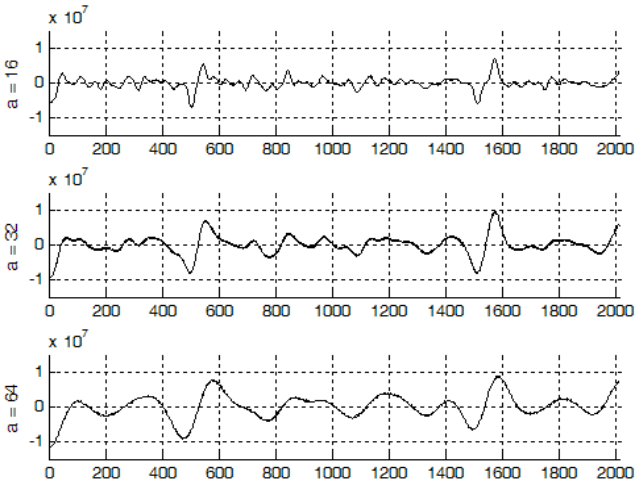

Fig. 5 Continuous wavelet transform for mixed traffic at scale 16, 32, 64.

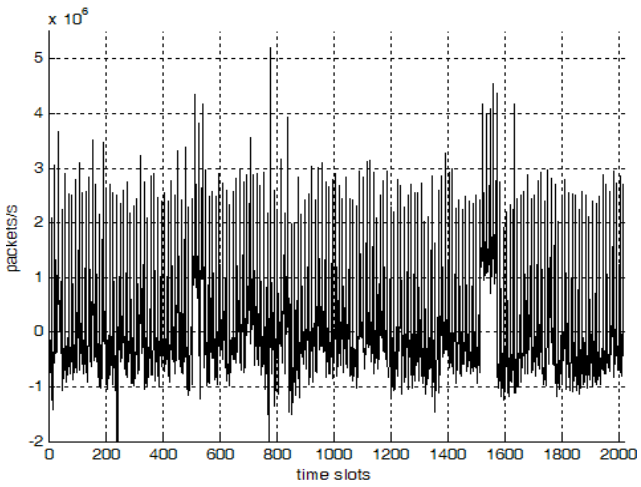

Fig. 7 Detection result with PCA.

different levels. For each level, the first node coefficient was presented. To make the initial detection, the wavelet packet coefficients of each scale are analyzed, and then we check whether there is any anomaly at some moments on this scale by the means of variance analysis. As shown in Figure 3, anomalies are detected at node (3, 0). But it is required to be further decomposed and detected.

In figure 4, we show the wavelet packet coefficients at node (4, 0). At this node we also find the anomaly surpass the threshold by the variance analysis, thus we reconstruct the coefficients. To confirm the anomaly of network traffic, we detect the reconstructed signal. As it is show in the figure 4, we can detect the center location of the anomaly, without the exact anomaly duration.

In figure 5, we show the continuous wavelet transform coefficient line at different scales 16, 32 and 64. In the scale 64, it cannot clearly indicate traffic characteristics by its coefficient line, those at the scale 16 and 32 can significantly demonstrate traffic difference in different time. So we select the scales 16 and 32 to compute the average coefficient line, which is shown in figure 6. It also presents the smoothed wavelet coefficient line, which in order to reduce the small fluctuation. As shown, by the means of the anomaly detection block, we get the final detection. We find two attacks: attack 1 (from sample 500 to sample 540) and attack 2 (from sample 1499 to sample 1563). Hence, these anomalies can be accurately detected, and the estimation errors of the start and the end time of the anomaly are less 3 samples.

To validate further the detection performance of our method, we compare our method with the known PCA. Figure 7 plot the detection result with PCA. From Figure 7， we find that although PCA can extract some changes in those points where anomaly traffic is injected, it is significantly difficult to detect them. Moreover, Figures 6 and 7 show that our method can

find out the traffic anomalies more accurately than PCA approach. Hence, our method is practical and effective.

IV. CONCLUSIONS

This paper proposes a wavelet-based adaptive system to detect anomalies in network traffic. We use a scale-adaptive method based on wavelet packet detect anomaly, and use continuous wavelet transform to analyze the detected result to confirm the anomaly and enhance the reliability of detection. Thanks to the proposed system, we can obtain good results of anomaly detection, and we can also estimate the start and the end time of anomaly traffic. Simulation results show that our approach is more effective than previous method.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (No. 61071124), the Specialized Research Fund for the Doctoral Program of Higher Education (No. 20100042120035), the Fundamental Research Funds for the Central Universities (No. N090404014), and the Open Project of State key Laboratory of Networking and Switching Technology (No. SKLNST-2009-1-04). The authors wish to thank the reviewers for their helpful comments.

REFERENCES

[1] V. A. Siris and F. Papagalou, “Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks,” Proceeding of IEEE GLOBECOM'04, Nov. 2004, pp. 2050-2054.

[2] Y. Gu, A. McCallum, D. Towsley, “Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation,” Proceedings of IMC'05, 2005, pp. 1-6.

[3] A. Wiesel, and A. O. Hero, “Principal component analysis in decomposable Gaussian graphical models,” Proceedings of ICASSP'09, 2009, pp. 1537-1540.

[4] D. Jiang, H. Xu, Z. Xu, et al. "Statistical analysis for origin-destination traffic anomalies," Proceedings of ICCP’10, 2010, pp. 66-70.

[5] G. Thatte, U. Mitra, and J. Heidemann. "Parametric methods for anomaly detection in aggregate traffic," IEEE/ACM Transactions on Networking, vol. 19, no. 2, pp. 512-525, 2011.

[6] A. Magnaghi, T. Hamada, and T. Katsuyama, “A Wavelet-Based Framework for Proactive Detection of Network Misconfigurations,” Proceedings of ACM SIGCOMM’04 Workshops, 2004.

[7] Alberto Dainotti, Antonio Pescape, and Giorgio Ventre, “Wavelet-based Detection of DoS Attacks”, Proceedings of GLOBECOM'06, 2006, pp. 1-6.

[8] Marius Salagean, “Real Network Traffic Anomaly Detection Based on Analytical Discrete Wavelet Transform,” Proceeding of OPTIM'10, 2010, pp. 1-4.

[9] D. Jiang, Y. Han, Z. Xu, et al. "A time-frequency detecting method for network traffic anomalies," Proceedings of ICCP’10, 2010, pp. 94-97.

[10] L. Guo, “LSSP: A novel local segment shared protection for multi-domain optical mesh networks,” Computer Commun., 2007, 30: 1794-1801.

[11] L. Guo, J. Cao, H. Yu, and L. Li, “Path-based routing provisioning with mixed shared protection in WDM mesh networks,” J. Lightwave Technol., 2006, 24: 1129-1141.

[12] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," Computer Communication Review, vol. 34, pp. 219-230, Oct 2004.