{tag}

{/tag}
International Journal of Computer Applications

Volume 37 - Number 3

Year of Publication: 2012

Authors:
Seyed Mahmoud Anisheh

Hamid Hassanpour

10.5120/4592-6039

{bibtex}pxc3976039.bib{/bibtex}

Abstract

The aim of this research is to analyze aggregate network traffic for anomaly detection. The accurate and rapid detection of network traffic anomaly is crucial to enhance the effective operation of a network. It is often difficult to detect the time when the faults occur in a network. In this paper, a new algorithm is presented to monitor the aggregate network traffic to rapidly detect the time anomaly occurs in a network. This is accomplished by monitoring the statistical characteristics of the time series representing the network behavior. The technique analyzes the network behavior using fractal dimension and discrete stationary wavelet transform. In the proposed method, after applying discrete stationary wavelet transform on the signal representing the network traffic, the fractal dimension of the decomposed signal is calculated in a sliding window. Then, variations of signal fractal dimension are considered for anomaly detection. Performance of the proposed method is compared with that of three other existing methods using both synthetic signal and real data. The results indicate superiority of the proposed technique in terms of accuracy compared to existing methods.

References

- Yao, X., Zhang, P., Gao, J. and Hu, G. 2006 .Detection of Network Traffic Anomaly Based on Instantaneous Parameters Analysis, International Conference on Communication Technology, ICCT '06. , 1-4.
- Tran, D., Ma W. and Sharma, D. 2006. Network Anomaly Detection using Fuzzy Gaussian Mixture Models, International Journal of Future Generation Communication and Networking, 37-42.
- Marina, T., and Ji, C. 1998. Adaptive Thresholding for Proactive Network Problem Detection, IEEE International Workshop on Systems Management, 5, 108-116.
- Sotiris, V.A., Tse, P.W. and Pecht, M.G. 2010. Anomaly Detection Through a Bayesian Support Vector Machine, IEEE Transactions on Reliability, 59, 277 – 286.
- Lu, W. and Ghorbani, A. 2008. Network Anomaly Detection Based on Wavelet Analysis, EURASIP Journal on Advances in Signal Processing, 2009, 1-16.
- Anisheh, S. M. and Hassanpour, H. 2009. Adaptive Segmentation with Optimal Window Length Scheme Using Fractal Dimension and Wavelet Transform, International Journal of Engineering, 22, 257-268.
- Luv, J., Li, X. and Li, T. 2007. Research on Network Traffic Anomaly Detection Algorithm, 12th IEEE Symposium on Computers and Communications, 95-100.
- Paxson, V. 1997. Fast approximate synthesis of fractional gaussian noise for generating self- similar network traffic [J]. Computer communication review. 10, 5-18.
- Salagean, M. and Firoiu, I. 2010. Anomaly detection of network traffic based on Analytical Discrete Wavelet Transform, 8th IEEE International Conference on Communications (COMM), 49 – 52.
- Kim, S. S. and Reddy, A. 2004. Detecting traffic anomalies at the source through aggregate analysis of packet header data, Proceedings of Networking.
- Lan, L. and Gyungho, L. 2005. Ddos attack detection and wavelets, Telecommunication Systems, 435-451.
- Thangavel, M., Thangaraj, P. and Saravanan, K. 2010. Defend against Anomaly Intrusion Detection using SWT Mechanism, International Journal of Innovation, Management and Technology, Vol. 1, No. 2, 209-213.
- Bachmann, G., Narici, L. and Beckenstein, E. 2002. Fourier and Wavelet Analysis, Springer.
- Nason, G.P. and Silverman, B.W. 1995. The stationary wavelet transform and some statistical application, Lecture Notes in Statistics, vol.103, pp. 281-299.
- Falconer, J. 2003. Fractal Geometry-Mathematical Foundations and Applications, John Wiley and Sons.
- Tykierko, M. 2008. Using invariants to change detection in dynamical system with chaos, Physica D: Nonlinear Phenomena, 237, 6-13.
- Paramanathan, P. and Uthayakumar, R. 2007. Application of fractal theory in analysis of human electroencephalographic signals, Computers in Biology and Medicine, 38. 372 – 378.
- Li, Y., Le Fan, Y. and Ye Tong, Q. 2007. Endpoint detection in noisy environment using complexity measure, Proc. IEEE International Conference, 3, 1004-1007.
- Liu, M., He, Y., Meng, Q. and Wang, Z. 2010. Research on Anomaly Detection of Network Traffic Based on Fractal Technology and Vector Quantization, IEEE International Workshop on Education Technology and Computer Science (ETCS), 2, 428 – 431.
- Higuchi, T. 1988. Aproach to an irregular time series on the basis of the fractal theory. Physica D, 31, 277-283.

- Petrosian, A. 1995. Kolmogorov Complexity of Finite Sequences and Recognition of Different Preictal EEG Patterns, Proc. IEEE Symposium on Computer-Based Medical Systems, 5, 212-217.
- Katz, M. J. 1988. Fractals and the Analysis of Waveforms, Comput. Biol. Med., 18, 145-156.
- Esteller, R., Vachtsevanos, G., Echauz, J. and litt, B. 2001. A comparison of fractal dimension algorithms using synthetic and experimental data, IEEE Trans. Circuits Syst., 48, 177-183.
- Malarvili, M., Hassanpour, H., Mesbah, M. and Boashash, B. 2005. A histogram-based electroencephalogram spike detection, Proc. IEEE Int Symposium on Signal Processing and its App,1, 207-210.

Index Terms

Computer Science Network Security

Keywords

anomaly detection effective operation of the network fractal dimension wavelet transform