Anomaly Detection in Network Traffic and Role of Wavelets

Gagandeep Kaur
Jaypee Institute of Information Technology
Noida, India
gagandeep.kaur@jiit.ac.in

Dr. Vikas Saxena
Jaypee Institute of Information Technology
Noida, India
vikas.saxena@jiit.ac.in

Prof. J. P. Gupta
Jaypee Institute of Information Technology
Noida,India
jp.gupta@jiit.ac.in

***Abstract*—Network Anomaly Detection covers wide area of research. Current best practices for identifying and diagnosing traffic anomalies consist of visualizing traffic from different perspectives and identifying anomalies from prior experience. Different tools have been developed to automatically generate alerts to failures, but to automate the anomaly identification process remains a challenge. Recently, Signal Processing techniques have found applications in Network Intrusion Detection System because of their ability in detecting novel intrusions and attacks, which cannot be achieved by signature-based detection systems. Visualization techniques are ways of creating and handling graphical representations of data. This survey explains the main techniques known in the field of Statistical based and Wavelet based anomaly detection approaches and focuses on the role of data traffic visualization tools in network traffic anomaly detection.**

Keywords-anomaly detection; wavelet based approaches; visualization tools

I. INTRODUCTION

The Internet is growing at an unprecedented rate. With its wide spread use amongst network users it has become the favorite platform for network criminals and hackers. The number of intrusions into computer systems is growing and raising concerns about computer security. The ever increasing list of Computer Emergency Research Team (CERT) [1] is proof enough of the urgency to look out for robust security mechanisms. Despite the effort devoted to carefully designing a system to protect from attacks like Denial of Service (DoS), Spyware, Worms, Port scans etc., network security is very difficult to guarantee, since attacks exploit unknown weaknesses or bugs, which are usually contained in system and application software. Since its introduction in 1999 a lot has been researched in the area. Intrusion Detection techniques are broadly classified into two categories: misuse detection and anomaly detection. Misuse detection approaches are strictly limited to the latest known attacks. New attack variants go undetected by them, as a result of which a new concept of anomaly detection was introduced by Denning [2]. Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior. Most anomaly detection techniques attempt to establish normal activity profiles by computing various metrics and an intrusion is detected when the actual system behavior deviates from the normal profiles. Anomaly detection is further classified into host-based and network-based. Network based anomaly detection aims at protecting the entire network against intrusions by monitoring the network traffic either on designed hosts or specific sensors. Detecting anomalies quickly and accurately in network traffic is a hot topic in the current field of research ([11, 12, 13 and 22]). A general anomaly diagnosis system should therefore be able to detect a range of anomalies with diverse structure, distinguish between different types of anomalies and group similar anomalies [11].

The growing interest in the research and development of anomaly-based online detection systems raised a need for an up-to-date survey of the research in the field of network anomaly detection. This paper introduces the reader to Wavelet techniques for anomaly detection and provides for Visualization tools using wavelets for network traffic modeling and anomaly detection.

The rest of the paper is organized as follows. Section II presents an idea of anomaly detection approaches and focuses on wavelet based approaches. Section III provides analysis of popular visualization tools based on wavelets being used for network anomaly detections and conclusion in section IV.

II. ANOMALY DETECTION APPROACHES

It is essential to characterize network anomalies to be able to identify them. Over the years they have been classified and categorized depending upon their methodologies and approaches. However, because anomalies in Internet traffic are widely diversified, it is difficult to generally characterize them all, and high volume makes them harder to identify. The anomalous behavior is often dynamic in nature, like some new anomalies, for which there is no labeled training data. Based on labeling, anomaly detection techniques can be categorized as supervised, semi supervised and unsupervised. Supervised-learning methods have mainly been represented by intrusion detection systems (IDSs) based on anomaly signatures. Semi supervised models label data of normal class leaving anomalous data unlabeled. Due to the constant appearance of new anomalies, unsupervised-learning approaches are gaining widespread interest these days. Initially unsupervised anomalies used to be based on volume variance, identifying both short and long-lasting anomalies through local or global variances in the number of bytes whereas recent work has also considered traffic features for a closer analysis of traffic [8]; thus, providing more diversified image of the anomalies.

978-1-4244-6349-7/10/$26.00 ©2010 IEEE

A. *Wavelets Based Approaches*

Daubechies has done a lot of work on the theory of the Wavelet Transform [3] and has also designed some short and computationally cheap wavelet sequences. V.Alarcon-Aquino and J.A.Barria brought in the application of Wavelets into Network Intrusion Detection [4].

Anomaly detection and identification techniques have been studied for many years [5-8].Recent research has applied signal processing techniques to identify network anomalies, and study network characteristics such as routing and congestion. The Signal processing techniques are mainly categorized into four types, namely a) Wavelet based approaches, b) Maximum entropy estimation, c) Principal Component Analysis Techniques and d) Spectral analysis. Many of the approaches rely on known statistical properties of normal traffic when the observed traffic deviates significantly from the normal behavior. Initial line of Intrusion Detection Systems (IDSs) used spectral techniques. Current applications of spectral techniques look for high-frequency occurrences to identify anomalous behavior [9, 10, 14, 33]. The wavelet tool [11] allows a single signal to be decomposed in several signals representing different frequencies. High frequencies indicate spontaneous behavior by traffic while low frequencies exhibit global behavior by traffic. As a first line, methods of detection involve finding global and local variances in wavelet coefficients to detect respective short and long-term anomalies. Hussain *et al.* [15] apply spectral techniques to time series of packet arrival times. Based on spectral characteristics, they are able to distinguish between single and multi-source attacks, and identify repeat attacks. Barford *et al.* use wavelets to analyze SNMP and flow-level information to identify DoS attack and other high frequency anomalies [9]. Magnaghi *et al.* detect anomalies within TCP flows using a wavelet-based approach to identify network misconfigurations [16]. G. Bartlett *et al.* in [17] look at periodicity between flows to identify hosts which maintain regular contact while considering low frequency behavior under long observation windows and use iterated filtering for full decomposition. Carl *et al.* in [26] applied wavelets transform for detecting change-points in the Cumulative SUM (CUSUM) statistic. Hamdi and Boudriga in [27], Xunyi *et al.* in [28] devise wavelet techniques for detecting DoS attacks. Lu *et al.* in [29] study wavelet basis functions that have an important impact on the intrusion detection performance. In [22] the authors propose a new network anomaly detection model based on wavelet approximation and system identification theory.

Second line of Intrusion Detection focuses on signal processing by monitoring statistical changes in signals. Lakhina *et al.* [8], proposed subspace method to analyze relationships between volume of all links and Origin Destination (OD) flows. They proposed to apply PCA on the feature distribution of network-wide traffic. Li *et al.* [18] introduced a method combining traffic sketch and subspace for network-wide detection. Huang *et al.* proposed a network disruption detection method by applying PCA to network-wide routing updates data and developed *Waveman* [20] for real time wavelet-based analysis of network traffic anomalies. Ringberg *et al.* [19] shows that the first few principal components are not adequate to capture the vast majority of the variance in the traffic data. Zong-Lin Li *et al.* [21] use Auto Regressive Integrated Moving Average (ARIMA) models to detect the change of correlation across OD flows which caused by the inherent correlative characteristics between attack flows, is used to reveal small attacks correctly. While Lakhina *et al.* took advantage of PCA Dewaele *et al.'s* [10] approach is based on non-Gaussian procedures. The method of Thottan and Ji in [25] detects abrupt changes in signals.

The work of Kim and Reddy in [36] and Kompella *et al.* in [24] are third type of statistical approaches. Kim proposed Bayesian statistics based Distributed Denial of Service (DDoS) algorithm for detection, which calculated the likelihood of non-legitimate packets for each arrived packet. Dewaele *et al.* in [10], uses sketch techniques and Gaussian marginal distribution modeling as a means of extracting hidden anomalies from a large-scale packet trace database. Xiapu Luo *et al.* in [30] address the problem of detecting a class of low-rate DoS attacks, called pulsing denial of service (PDoS) attacks. Romain Fontugne *et al.* in [31] propose a new approach to detecting anomalies based on pattern recognition .

III. Role of Data Traffic Visualization in Network Anomaly Detection

The Internet Service Providers (ISPs) are aware of major events after the fact, but lack tools to detect live intrusions. The network traffic is high dimensional and noisy, which makes it difficult to extract meaningful information about anomalies from any kind of traffic statistics. The current best practices for identifying and diagnosing traffic anomalies consist of visualizing traffic from different perspectives and identifying anomalies from prior experience. Different tools have been developed to automatically generate alerts to failures, but to automate the anomaly identification process remains a challenge. Signal processing techniques have found applications in Network Intrusion Detection System (NIDS), because of their ability of detecting novel intrusions and attacks, which cannot be achieved by signature-based NIDS. Therefore, the primary objective of an NIDS based on signal processing techniques is to profile the normal network traffic pattern or application-level behavior and to classify intrusions or unwanted traffic as anomalies. However, the major challenge of the signal processing-based approaches lies in the adaptive modeling of normal network traffic and the high false alarm rate due to the inaccuracy of the modeled normal traffic pattern. The emergence of a variety of wireless networks and the mobility of nodes in such networks only adds to the complexity of the problems.

A. *Visualization Tools and Techniques*

The first step in anomaly diagnosis is detection — designating the points in time at which an anomaly is present [21]. Visualization techniques are ways of creating and handling graphical representations of data. There are several visualization techniques, such as: line graphs, histogram, bar chart, surface view, image display, scatter plot, isosurfaces, volume rendering and multiple line graphs with parallel coordinates, among others. These representations are used in order to obtain better insight and understanding of the problem in study, because pictures can convey an overall message much better than a list of numbers.

Because of currently used wavelet transformations there is interesting work done in order to graphically represent the network traffic. The section ahead reports few of these tools and their comparison is tabulated in Table 1.

1) Wavelet-based INference Detection (WIND): The objective of WIND is to enable an on-line real time wavelet-based analysis of measured traffic. WIND operates from observation period to observation period and at the end of each period, it generates various statistics. Among these are energy function plots for detecting network problems and various counters to notice and react to changes in server popularity, user behavior, and/or protocol and application usage. The simulations are carried out on NS2 and 80-90% success rate has been reported [38].

2) NetViewer: The NetViewer is based on wavelet analysis techniques [36]. It is based on the idea of observing the traffic and correlating it to the previous normal states of traffic, to make it possible to see whether the current traffic is behaving in an anomalous manner. Kim *et al.* proposed a technique for traffic anomaly detection through analyzing correlation of destination IP addresses in outgoing traffic at an egress router. They hypothesize that the destination IP addresses will have a high correlation degree for a number of reasons and the changes in the correlation of outgoing addresses can be used to identify network traffic anomalies. Based on this, they apply discrete wavelet transform on the address and port number correlation data over several time scales. Any deviation from historical regular norms will alert the network administrator of the potential anomalies. A&M University network environment data set is used for analysis. Wavelet analysis is used to detect DoS or DDoS attacks.

3) Waveman: Traffic is captured and sampled using counters. Time series signal is implemented in the form of a linked list data structure and sent to Lastwave. LastWave plost only first three components. Percentage deviations are calculated and recorded which are then normalized for comparison. Gnuplot is used to plot the graphs in JPEG files. The evaluation results for Waveman[20] with part of the 1999 DARPA intrusion detection dataset and real network traffic data show that the Coiflet and Paul wavelets perform better than other wavelets in detecting most anomalies under same benchmark environment.

4) RGCom:A network traffic visualization tool developed at INPE[32]. This application performs data reading from a database, data normalization, and data plotting in parallel coordinates on the computer screen. Graphical and database communication resources from Java programming environment are used in its implementation. The graph produced by RGCom contains nine parallel coordinates with values of a determined attribute each one. Nine attribute points of a same session are plotted in that axis and they are interconnected, shaping a session line. All lines of one happened session in a selected by the user date and time interval is drawn and the resultant graph represents the network traffic behavior in that time.

5) Vanguard: To address some limitations of wavelet analysis-based anomaly detection, such as, scale sensitive during anomaly detection, high computation complexity of wavelet transformation Chang et al. [23][30] proposed a new network anomaly detection method based on wavelet packet transform, which can adjust the decomposition process adaptively, and thus improving the detection capability on the middle and high frequency anomalies that cannot otherwise be detected by multi-resolution analysis [39]. The data set used comprises of Lawrence Berkeley National Laboratory (LBNL) enterprise data traces & WIDE backbone data traces. The evaluation results with simulated attacks show that the proposed method detects the network traffic anomaly efficiently and quickly.

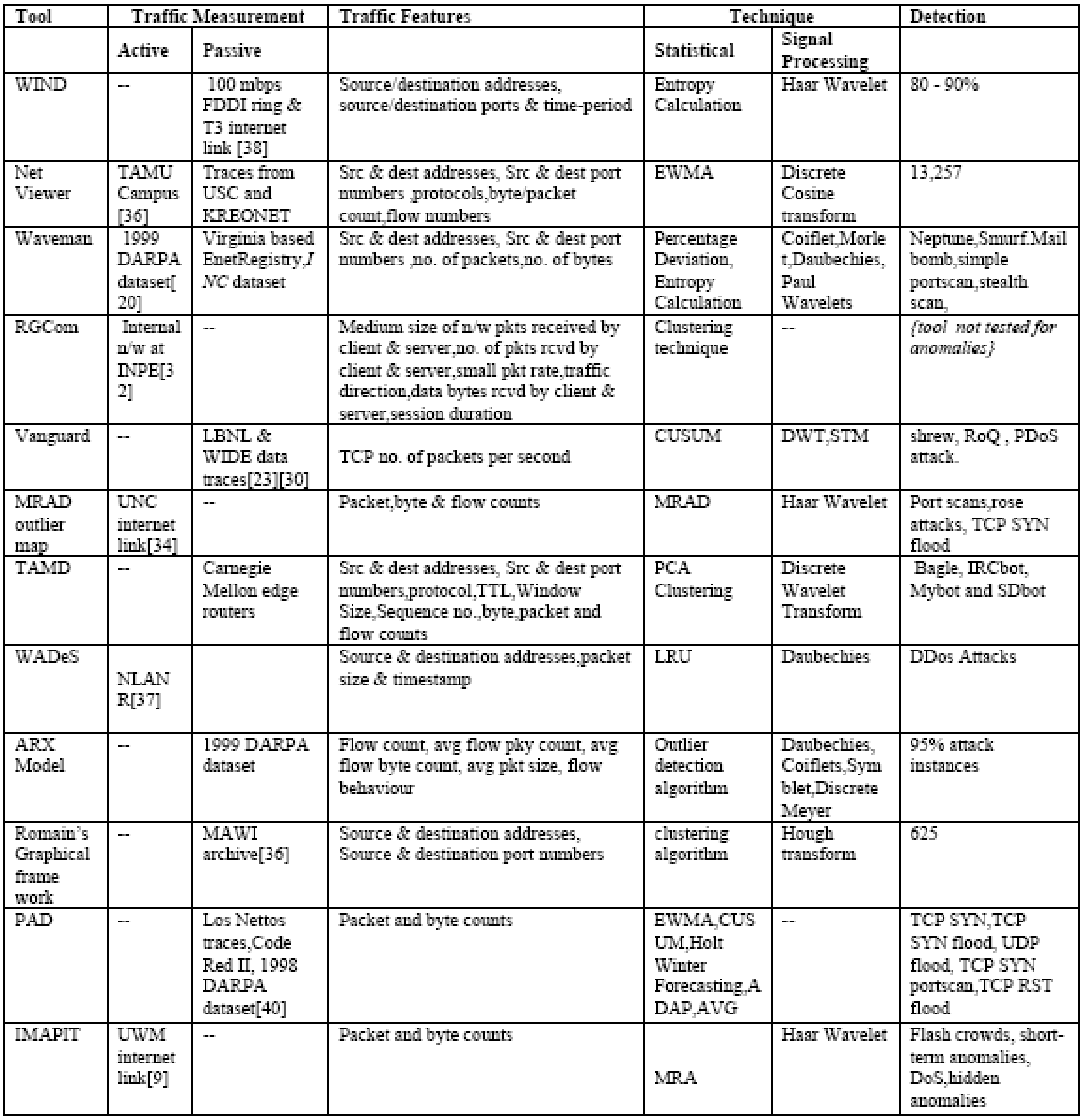
6) MRAD outlier map: Multi Resolution Anomaly Detection analyzes Long Range Dependency (LRD) time series. The MRAD map visualizes the significance probability simultaneously over scale and time. Under suitable assumptions the marginal distribution of each pixel in the map (i.e. each observation at a particular time and scale) is the same when there are no outliers at all. It uses hotter colors (red) to show small p values, i.e., higher chance to be outliers. And cooler colors (blue) are used to display large p values, i.e., they are less likely to be outliers [34].

7) Traffic Aggregation for Malware Detection (TAMD):It identifies candidate groups of infected computers within its network by finding new communication aggregates involving multiple internal hosts that share common characteristics. It detects stealthy malware within a network. The key to maximizing the data-reducing precision of TAMD is the characteristics on which it aggregates traffic. A binary vector is formed for each internal host, with each dimension representing one of the selected external destinations. The vectors are processed by PCA for dimension reduction, and clustered by K-means clustering [35].

8) Wavelet based Attack Detection Signatures (WADeS): Ramanarran presented an approach named WADeS for detecting DDoS attacks.Wavelet transform is applied on traffic signals and the variance of corresponding wavelet coefficients is used to estimate the attack points [37].

9) Auto Regressive eXogenous Model (ARX): In ARX Model predicting the expected value of frequency components is trained from network traffic data collected on the current deployment network. The output for the normal daily traffic model is the residual that represents the deviation of current input signal from normal/regular behavioral signals. Residuals are finally input to the intrusion decision engine in which an outlier detection algorithm is running and making intrusion decisions[22].

TABLE I. COMPARISON OF VISUALIZATION TOOLS



Tool	Traffic Measurement		Traffic Features	Technique		Detection
	Active	Passive		Statistical	Signal Processing	
WIND	--	100 mbps FDDI ring & T3 internet link [38]	Source/destination addresses, source/destination ports & time-period	Entropy Calculation	Haar Wavelet	80 - 90%
Net Viewer	TAMU Campus [36]	Traces from USC and KREONET	Src & dest addresses, Src & dest port numbers ,protocols,byte/packet count,flow numbers	EWMA	Discrete Cosine transform	13,257
Waveman	1999 DARPA dataset[20]	Virginia based EnetRegistry,*J NC* dataset	Src & dest addresses, Src & dest port numbers ,no. of packets,no. of bytes	Percentage Deviation, Entropy Calculation	Coiflet,Morle t,Daubechies, Paul Wavelets	Neptune,Smurf.Mail bomb,simple portscan,stealth scan,
RGCom	Internal n/w at INPE[3 2]	--	Medium size of n/w pkts received by client & server,no. of pkts rcvd by client & server,small pkt rate,traffic direction,data bytes rcvd by client & server,session duration	Clustering technique	--	*{tool not tested for anomalies}*
Vanguard	--	LBNL & WIDE data traces[23][30]	TCP no. of packets per second	CUSUM	DWT,STM	shrew, RoQ , PDoS attack.
MRAD outlier map	UNC internet link[34]	--	Packet,byte & flow counts	MRAD	Haar Wavelet	Port scans,rose attacks, TCP SYN flood
TAMD	--	Carnegie Mellon edge routers	Src & dest addresses, Src & dest port numbers,protocol,TTL,Window Size,Sequence no.,byte,packet and flow counts	PCA Clustering	Discrete Wavelet Transform	Bagle, IRCbot, Mybot and SDbot
WADeS	NLAN R[37]		Source & destination addresses,packet size & timestamp	LRU	Daubechies	DDos Attacks
ARX Model	--	1999 DARPA dataset	Flow count, avg flow pky count, avg flow byte count, avg pkt size, flow behaviour	Outlier detection algorithm	Daubechies, Coiflets,Sym blet,Discrete Meyer	95% attack instances
Romain's Graphical frame work	--	MAWI archive[36]	Source & destination addresses, Source & destination port numbers	clustering algorithm	Hough transform	625
PAD	--	Los Nettos traces,Code Red II, 1998 DARPA dataset[40]	Packet and byte counts	EWMA,CUS UM,Holt Winter Forecasting,A DAP,AVG	--	TCP SYN,TCP SYN flood, UDP flood, TCP SYN portscan,TCP RST flood
IMAPIT	UWM internet link[9]	--	Packet and byte counts	MRA	Haar Wavelet	Flash crowds, short-term anomalies, DoS,hidden anomalies

10) Romain's Graphical framework: Romain *et al.* focused on four traffic features for detecting anomalies;thus, four graphical representations were used to compute the snapshots. To reduce noise in network traffic surrounding the anomalies and to facilitate their identification in the analyzed images, they split the entire network traffic into smaller sub-traffics. They propose two general ways of dividing the entire traffic. On the one hand, the whole traffic is classified in N sub-traffics corresponding to data sent from N disjointed blocks of source addresses. On the other hand, the traffic is arranged in N sub-traffics standing for data received by N separated blocks of destination addresses. The basic tool employed to find lines in snapshots was the Hough transform. It is able to detect solid lines as well as lines with missing parts robust against noise, and images generated from traces contain noise due to legitimate traffic [36], [31].

11) PAD: Parallel Anomaly Detection (PAD) system is prototype being developed by S Shanbhag *et al.* [40]. Packet headers captured from the monitored link are classified into different subsets by the packet classifier, and the data pertaining to *those* subsets are then extracted. Packet and byte counts per observation interval are maintained. Each anomaly detection algorithm processes this data for each subset to find volume anomalies characterized by unexpected changes in traffic volume. The continuous anomaly metric output by each algorithm is further normalized. The normalized anomaly metrics for all algorithms for a particular subset are then aggregated to produce an anomaly score that represents the severity of the anomaly. Finally, a binary decision is made based on whether the anomaly score exceeds the threshold.

12) Integrated Measurement Analysis Platform for Internet Traffic (IMAPIT): IMAPIT [9] contains a data management system which supports and integrates IP flow, SNMP and anomaly identification data. It provides robust signal analysis utility which enables the network traffic data to be decomposed into its frequency components using a number of wavelet and framelet systems. The data set spans 6 months and includes a catalog of over 100 anomalies which are organized into two distinct categories i.e. short-lived events and long-lived events for analysis. Analysis is based on two types of network traffic data types: SNMP data and IP flow data. The source of both was a Juniper M10 router which handled all traffic that crossed the University of Wisconsin-Madison campus network's border. It uses redundant wavelet system . The data archive uses Round Robin Database Tool (RRDTOOL) which provides a flexible database and front-end for IP flow and SNMP data. The analysis platform is a framelet signal analysis and visualization system that enables a wide range of wavelet systems to be applied to signals.

IV. Future Work And Conclusion

These tools use bi-directional traffic for analysis and either the datasets of DARPA, NLANR, LBNL are used for testing or the internal campus internet link generated traces are used. Most of them successfully detect the common anomalies like DoS attacks,DDoS attacks, floods,flash crowds etc and few of them achieve success in identifying unknown cases as well. RGCom is still in its development phase and nine attributes for measurement seem to be quite a high number for real time detections. Vanguard is good at detecting pulsating DoS attacks as well as shrew attacks. TAMD acheives success in detecting Bot attacks which can be extended. The concept of parallel anomaly detection in PAD is new and can be extended with signal processing to develop real time detection system.

References

[1] CERT, Overview of attack trends, http://www.cert.org/archive/pdf/attack_trends.pdf (8 April 2002).

[2] D. E. Denning, "An intrusion detection model," IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222–232, 1987.

[3] I. Daubechies, "Ten Lectures on Wavelet"s, SIAM Press, 1992

[4] Alarcon-Aquino, V. Barria, J.A,"Anomaly Detection in Communication networks using wavelets",IEE Proceedings-Communications,pp 355-362, Dec 2001

[5] P. Abry and D. Veitch., " Wavelet analysis of long-range-dependent traffic.", IEEE Transactions on Information Theory, 44(1):2–15, 1998.

[6] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Comput.Netw., vol. 51, no. 12, pp. 3448–3470, 2007.

[7] J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo, "Anomaly detection methods in wired networks: a survey and taxonomy," Computer Communications, vol. 27, no. 16, pp. 1569–1584, Oct. 2004.

[8] P. Barford and D. Plonka, "Characteristics of network traffic flow anomalies," in IMW '01: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. New York, NY, USA: ACM, pp. 69–73, 2001

[9] Paul Barford, Jeffery Kline, David Plonka, and Amos Ron., "A signal analysis of network traffic anomalies." In Proc. of ACM SIGCOMM Internet Measurement Workshop, Marseille, France, Oct 2002. ACM.

[10] G. Dewaele, K. Fukuda, P. Borgnat, P. Abry, andK. Cho., " Extracting hidden anomalies using sketch and non gaussian multiresolution statistical detection procedures.", LSAD '07, pp. 145–152, 2007.

[11] A. Lakhina, M. Crovella, and C. Diot., " Mining anomalies using traffic feature distributions.", SIGCOMM '05, pp. 217–228, 2005.

[12] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson., " Characteristics of internet background radiation.",IMC '04, pp. 27–40, 2004.

[13] Y. Zhang, Z. Ge, A. Greenberg, and M. Roughan., "Network anomography.", IMC '05, pp. 1–14, 2005.

[14] Chen-Mou Cheng, H.T. Kung, and Koan-Sin Tan., " Use of spectral analysis in defense against DoS attacks.", In Proc. of IEEE GLOBECOM, 2002.

[15] Alefiya Hussain, John Heidemann, and Christos Papadopoulos., " Identification of repeated denial of service attacks.",Proceedings of the IEEE Infocom, Barcelona, Spain, Apr 2006.

[16] Antonio Magnaghi, Takeo Hamada, and Tsuneo Katsuyama., " A Wavelet-Based Framework for Proactive Detection of Network Misconfigurations." In Proceedings of ACM workshop on Network Troubleshooting, Aug 2004.

[17] Genevieve Bartlett Marina del Rey John Heidemann Christos Papadopoulos, " Using Low-Rate Flow Periodicities for Anomaly Detection", Extended ISI-TR-661, August 5th, 2009

[18] X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G.Iannaccone, A.Lakhina, "Detection and Identification of Network Anomalies Using Sketch Subspaces", IMC, 2006.

[19] H. Ringberg, A.Soule, J.Rexford and C. Diot, "Sensitivity of PCA for traffic anomaly detection", Sigmetrics, Jun 2007.

[20] Chin-Tser Huang Sachin Thareja Yong-June Shin, "Wavelet-based Real Time Detection of Network Traffic Anomalies", Securecomm and Workshops,pp.1-6, Aug.28-Sept.1,2006

[21] Zong-Lin Li Guang-Min Hu Dan Yang," Global abnormal correlation analysis for DDoS attack detection", Computers and Communications, ISCC 2008 IEEE Symposium on,pp.310-315,6-9 July 2008

[22] Wei Lu and Ali A. Ghorbani, " Network Anomaly Detection Based on Wavelet Analysis", EURASIP Journal on Advances in Signal Processing, Volume 2009

[23] Chin-Tser Huang and Jeff Janies, "An Adaptive Approach to Granular Real-Time Anomaly Detection", EURASIP Journal on Advances in Signal Processing, Volume 2009 , Jan 2009

[24] R. R. Kompella, S. Singh, and G. Varghese, "On scalable attack detection in the network," IEEE/ACM Trans. Netw., vol. 15, no. 1, pp. 14–25, 2007.

[25] M. Thottan and C. Ji, “Anomaly detection in IP networks,” Signal Processing, IEEE Transactions on, vol. 51, no. 8, pp. 2191–2204, Aug. 2003.

[26] G. Carl, R. R. Brooks, and S. Rai, “Wavelet based denial-of-service detection,” Computers & Security, vol. 25, no. 8, pp. 600–615, Nov. 2006.

[27] M. Hamdi and N. Boudriga, “Detecting denial-of service attacks using the wavelet transform,” Comput. Commun., vol. 30, no. 16, pp. 3203–3213, 2007.

[28] R. Xunyi, W. Ruchuan, and W. Haiyan, “Wavelet analysis method for detection of DDoS attack on the basis of self-similarity,” Frontiers of Electrical and Electronic engineering in China, vol. 2, no. 1, pp. 73–77, March 2007.

[29] W. Lu, M. Tavallaee, and A. A. Ghorbani, “Detecting network anomalies using different wavelet basis functions,” cnsr, vol. 0, pp. 149–156, 2008.

[30] Xiapu Luo, Edmond W. W. Chan, and Rocky K.C.Chang, “ Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals”, EURASIP Journal on Advances in Signal Processing, Volume 2009

[31] Romain Fontugne, Yosuke Himura, Kensuke Fukuda,” Anomaly Detection Method based on Pattern Recognition”, PAM2009, April 13,2009, Seoul, Korea.

[32] L.S. Silva, T.D. Mancilha, J.D.S. Silva, A.C.F. Santos, e A. Montes, “Framework for Analysis of Anomalies in the Network Traffic”, available in: http://mtc-m18.sid.inpe.br/col/sid.inpe.br/ePrint%4080/2006/12.20.23.21/doc/v1.pdf

[33] Kriangkrai Limthong, Fukuda Kensuke, Pirawat Watanapongse, “Wavelet-Based Unwanted Traffic Time Series Analysis”, IEEE International conference on computer and electrical engineering, 20-22 Dec 2008.

[34] Lingsong Zhang, Zhengyuan Zhu Jeffay, K. Marron, J.S. Smith, F.D. Multi-Resolution Anomaly Detection for the Internet, INFOCOM Workshops 2008, IEEE, pp. 1-6, 13-18 April 2008

[35] Michael K. Reiter Ting-Fang Yen, “Traffic Aggregation for Malware Detection”, LNCS 5137, pp. 207–227, 2008, Springer-Verlag Berlin Heidelberg 2008

[36] Seong Soo Kim and A. L. Narasimha Reddy, “ NetViewer: A Network Traffic Visualization and Analysis Tool”, LISA XIX – December 4-9, 2005 – San Diego, CA

[37] A. Ramanarran, “WADES: a tool for distributed denial of service attack detection”, M.S. thesis, Texas A&M University, College Station, Tex, USA, 2002, TAMU-ECE-2002

[38] Polly Huang, Anja Feldmann, Walter Willinger, “A non-intrusive, wavelet-based approach to detecting network performance problems”, IMW'OZ, November l-2,2001, San Francisco, CA, 2001 ACM

[39] J.Gao, G. Hu,X. Yao, and R. K. C. Chang, “Anomaly detection of network traffic based on wavelet packet,” in Proceedings of the Asia-Pacific Conference on Communications (APCC ’06),pp. 1–5, Busan, Korea, August 2006.

[40] Shashank Shanbhag and Tilman Wolf,“Accurate Anomaly Detection through Parallelism”, IEEE Network,Jan/Feb 2009Dong Cheul Lee, Byungjoo Park, Ki Eung Kim, Jae Jin Lee, “ Fast Traffic Anomalies Detection Using SNMP MIB Correlation Analysis”, ICACT 2009, Feb. 15-18, 2009