International Journal of Security and Its Applications
Vol. 11, No. 8 (2017), pp.27-44
http://dx.doi.org/10.14257/ijsia.2017.11.8.03

Study of Self-Similarity for Detection of Rate-based Network Anomalies

Gagandeep Kaur, Vikas Saxena and Jay Prakash Gupta

Deptt. Of CSE&IT
JIIT, Noida, India
gagandeep.kaur@jiit.ac.in, vikas.saxena@jiit.ac.in, jaip.gupta@gmail.com

Abstract

In this paper, we have reviewed state of the art works done in the field of anomaly detection in general and network based anomaly detection in particular. The current anomaly detection techniques with respect to rate based network anomalies have been examined and their strengths and weaknesses have been highlighted. The applicability of scale-invariant property of self-similarity as a parameter for detection of anomalies from normal network traffic behaviors has been studied in depth. From the studies of scale-invariance and it's usage in detecting anomalies like flash crowds, DDoS attacks, outages, portscans, etc. it was realized that wavelets are a good tool that can be used for n-level decomposition of aggregated network traffic.

1. Introduction

It's a known fact that internet is now an integral part of everyday life. Since its birth in the eighties it has become more and more famous amongst its users in the public domain, defense and in the field of research. But this system was not designed for such wide-spread use. Due to its infrastructure weaknesses and architecture vulnerabilities on one hand and its humongous success on the other hand it has become a heaven for malicious users. *Network intrusions* or *cyber intrusions* have become one of the top most problems for system administrators, network engineers as well as researchers [1]. The need for better solutions combined with interestingness of this area has led to development and deployment of intrusion detection algorithms in general and Network Intrusion Detection Systems (NIDSs) in particular.

Intrusion detection research is based on two broad concepts: anomaly detection and signature based detection [2], [3]. Anomaly detection is based on tagging of all network traffic behavior patterns that are abnormal for an entity [1], whereas signature based detection is based on tagging an event anomalous that has resemblance to previously profiled signature of a known intrusion. The weakness of signature based detection systems is that they always require a profile to be matched for detecting an intrusion or attack whereas anomaly based detection systems declare anything going beyond a threshold as a possible candidate for an attack or anomaly. It is because of this *strength of anomaly detection mechanisms that we chose to do state of the art study in field of network anomaly detection*.

In **anomaly detection** the network traffic is captured and is watched for abnormalities in the traffic. Alarm is raised in case something abnormal raises the suspicion [3]. Network based anomaly detection therefore requires the user to first know about what is normal traffic behavior and then the detector can be set to threshold to decide at what level an alarm for abnormal traffic has to be raised. Examples of anomalous traffic in today's internet include legitimate events like flash crowds, and illegitimate events like DDoS, port-scans, outages, worms, viruses, etc.

There has been remarkable work done in the area of network based intrusion detection systems. To name a few, some of the pioneer works have been done using techniques

ISSN: 1738-9976 IJSIA

such as, statistical methods, neural networks, Markov models, fuzzy logic, decision trees [7-10], PCA based, sketch based, clustering based, signal or spectral processing based [11-16], etc. But there are always changes happening in the areas of network modeling and structuring, causing the behavioral changes in the network traffic [33]. The detection techniques for intrusions that were earlier based on signatures, have now given way to threshold based anomaly detection. *The anomaly based detection schemes therefore require opportunities to be explored to advance the art of detecting and thwarting network based traffic anomalies*.

In this paper, we have tried to present a comprehensive survey of recent literature in the area of network anomaly detection. In doing so, the attempt has been made to assess the state-of-the-art work done in this area as well as consolidate the existing works. We have given brief overview on the network intrusion detection systems in section 2, its two broad categories-misuse based detection system in section 2.1 and anomaly based detection system in section 2.2. The brief differentiation between host-based and network-based network anomaly detection systems has been done in section 2.2. The field of anomaly detection, in general and network anomaly detection in particular, is very vast and after studying some of the highly cited survey papers in this area, we zeroed in on anomaly detection based on transformation of the network traffic as a chosen characteristic. The paper therefore, is an attempt to provide detailed study based on transformation of the captured traffic from one space to another as a characteristic. Signal based network anomaly detection being one such stream, has been covered in section 3. The section highlights signal processing techniques, namely, statistical based approaches in, spectral based approaches in 3.1 and *wavelets based approaches* in 3.3.
A brief overview on network intrusion detection systems is discussed next.

2. Network Intrusion Detection Systems

A Network Intrusion Detection System (NIDS) can be defined as software that is designed to specifically detect attacks and malicious attempts made to gain unauthorized access against computer network. An NIDS gathers information from various network sources and does automatic analysis of signs of any intrusions or misuses and triggers alarms for the network administrators. Figure [1] shows the taxonomy of an NIDS. For any IDS *sensors* detect intrusions, *analysis* of the intrusion is done and appropriate *response* is generated. In network intrusion detection there are two broad categories, namely, *misuse detection* and *anomaly detection*. Since the focus of this paper is anomaly detection, therefore we give a brief overview on misuse detection and detailed view on anomaly detection.

2.1 Misuse Based Detection System

Misuse detection systems maintain record of intrusion patterns or rules called *signatures* [17]. The detection system captures the incoming and outgoing traffic and maps it with these signatures. When the system detects a pattern that matches with any of these pre-recorded signatures, it triggers an alarm. There are quite a few highly successful pattern matching systems like Bro [18] and Snort [19]. A detailed review of misuse based detection techniques is given in a 2008 survey by Sabahi *et al*. [20] and a 2009 survey by Garcia-Teodoroa *et al*. [21]. Misuse detection systems have high true positive rate for intrusions that can be matched with known attack patterns but *they fail adversely in the presence of new anomalies*. Moreover, maintainenace and upgradation of the signature databases to the new attacks is very time and memory consuming process.

The main drawbacks or weaknesses of signature based systems are:

- Signature based intrusion detection systems are automatic security models that rely on simple, straight forward rules for detection of intrusions. But for complicated analysis and decision making these models have been failing increasingly [1].
- One should remember that within the last decade the network traffic complexity and rate has increased many a folds, but signature based IDSs with their rule based approaches have not been able to match the needs of the users. They have failed to scale to the present day intrusions like zero-day attacks [22].
- The signatures rely on profile matching and record keeping for detecting attacks. But they fail to detect new, unrecorded anomalies in the traffic. In today's world newer and newer attacks are being experienced by the users and these old rule based models are failing in such scenarios.

There is however, a second category, namely, **anomaly based detection systems**, of intrusion detection that helps to solve this problem is discussed next.

2.2 Anomaly Based Detection System

Anomaly detection was introduced by Denning [3] and refers to the problem of finding patterns in data that do not conform to expected behavior. These nonconforming patterns are often referred to as anomalies, outliers, discordant observations, exceptions, aberrations, surprises, peculiarities, or contaminants in different application domains [4].

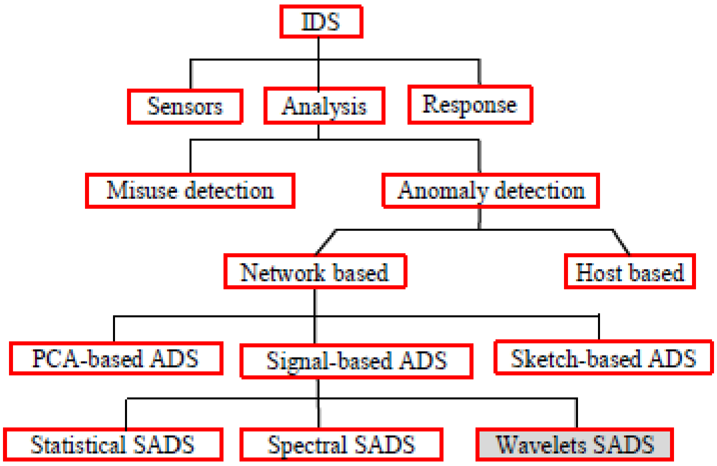

Figure 1. Taxonomy of Intrusion Detection Systems wrt Anomaly Detection

An Anomaly Detection System (ADS), uses mathematical as well as signal processing techniques to find out outliers from the normal traffic behaviors. These systems do normal traffic profiling and whenever deviations from these profiles are detected, they are cross checked with threshold values. Anomalous activity alarm is triggered for the outliers lying above threshold values. Since these systems rely on dynamic threshold values therefore they do not depend on *a priori* information of anomalies. *Anomaly detection therefore is a better candidate for fighting against unknown attacks and vulnerabilities*. Another benefit of anomaly detection techniques is that depending upon the underlying network the threshold profiles can be customized thus making it difficult for the intruders to attack the public networks. We therefore did an in-depth study of network based anomaly detection techniques.

Anomaly detection has been further classified into *host-based* and *network-based* anomaly detection techniques, discussed next.

2.2.1 Host Based Anomaly Detection: Host-based anomaly detection systems deal with single systems and collect information from the operating system call traces [23]. The host-based agents or sensors are installed on individual machines and collect data related to activities taking place on these machines. The collected data is called *audit trails* [23-25]. These audit trails which are simple text files are normally not provided by the operating systems. Modifications in the kernel are done to suit the needs of the user which increases its cost and maintenance and hence are not appreciated by the users. But these systems can work in encrypted environments and therefore are quite valuable. Because they are installed on individual machines so they can work quite well in distributed environments. A comparative evaluation of host based anomaly detection systems has been done by Forrest *et al*. [26] and Dasgupta & Nino [27].

Yet they have their own disadvantages. The biggest *disadvantage* is that they cannot watch the network traffic. They are heavily dependent on the host machines operating system and therefore are not easily scalable or portable. The primary requirement of being installed on all individual machines increases the overall installation cost for large networks as well. Therefore, in today's internet environment host based network anomaly detection techniques suffer from high cost of installation and scalability. We, therefore need to study other techniques of detecting anomalies in the network traffic, namely, *network based anomaly detection*.

2.2.2 Network Based Anomaly Detection: Network based anomaly detection systems aim at protecting the entire network against intrusions by monitoring the network traffic either on designed hosts or specific sensors. The principal challenge in automatically detecting and classifying network based anomalies is that anomalies can span a vast range of events: from network abuse (e.g., DoS attacks, scans, worms) to equipment failures (e.g., outages) to unusual customer behavior (e.g., sudden changes in demand, flash crowds, high volume flows), and even to new, previously unknown events. 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 ones [28-30].

However, fast detection and classification of anomalies is a cumbersome task. **Like profiles or rule based signatures in signature based IDSs, there are no standard thresholds that could always be applied to locate the old anomalies. Moreover, there are no fixed set of anomalies, new ones like new types of DDoS attacks always keep cropping up and one cannot detect them based on old threshold values. As a result researchers and engineers are always looking out for new solutions to handle them**. Some of the areas which have been tried for detection techniques are statistical methods, neural networks, Markov models, fuzzy logic, decision trees, PCA based, sketch based, clustering based, signal or spectral processing based, etc. We have chosen transformation of the signal from one domain to another as a possible characteristic for studying network anomaly detection.

Based on *transformation* of the network traffic the network based anomaly detection schemes are further divided into three categories. We have enlisted few of the important works here:

1) *PCA based Network Anomaly Detection*: Principle Component Analysis (PCA) is a coordinate transformation that forms *n* new axes called principal axes by mapping set of *n-dimensional* network traffic data points. Dimension reduction is therefore done by using PCA. For a given *n* dimensional traffic data if the variance can be represented by $d<n$ principal components, then the dimension of the data can be reduced to *d*. Various researchers have used PCA based techniques for anomaly detection. In [11], Yoshiki Kanda *et al*. combined sketches and PCA to detect and distinguish traffic anomalies in the backbone traces measured at a single link. Mohssen M Z E and Mohammed H *et al*. in [31], have used PCA based detection

technique to determine the most significant strings for detection of polymorphic worms. Lakhina *et al*. [33], applied PCA to group data into a time series and then project it onto an anomalous sub space. In [34], the authors' used time bin features used by Lakhina and used them to distinguish between small scale and large scale anomalies. Ringberg *et al*. [12] proved the dependence on *d* for different types of network sizes and aggregations. Similar works were also done by Brauckhoff *et al*. [32] who proved that PCA lacked temporal considerations. Although PCA based network anomaly detection has been successful in detection of malicious network traffic but they *suffer from some of the inherent problems of PCA*.

- PCA delivers high false positive rates due to the detector sensitivity. The detector if highly sensitive to small variances in the number of chosen principal components PCs in the normal subspace leads to large false detections. The effectiveness of PCA is therefore, heavily dependent on the levels of aggregation, that are directly responsible for the sensitivity of the detector.
- Sometimes heavy anomalies spanning large time spans tend to contaminate the large subspace area of PCA, leading to false alarms. If PCA could be tuned and be made robust to heavy anomalies then it is a good technique.

The next technique that we studied was sketch based network anomaly detection. Some of the works in this field are discussed here. It was found that *sketch based techniques require large number of input parameters for domain reductions*.

2) *Sketch based Network Anomaly Detection:* The standard change detection techniques like sliding window averaging, exponential smoothing, ARIMA etc. suffer from scalability issues when applied to large network traffic traces [1], [35]. *Sketch based techniques could be used to resolve the problem of scalability issues*. The network traffic data is divided into streams and passed to sketch based technique which process them exactly once. In sketch based method, firstly the sketch of normal traffic is generated. Then various models for forecasting are generated. The observed sketch is compared with the forecasted model and result is declared accordingly. Some of the pioneer works in this area have been done by S. Pukkawanna & K. Fukuda in [13]. They have used sketches to identify source IP addresses of anomalous traffic efficiently. The techniques in [8], [38], [46], also rely on sketch-based network traffic analysis of dimensionality reduction. The dimension reduction used is five-tuple of IP source, destination addresses, source and destination ports and protocol type. *The only advantage of sketch based schemes is that they are highly scalable and could be implemented online*. Just like PCA based network anomaly detection, sketch based network anomaly detection techniques also suffer from their inherent weaknesses like:
    - Sketch based techniques suffer majorly at deployment issues. The technique is based on selection of minimal number of parameters for sketching the subspace. For today's highly dynamic traffic parameter reduction is time consuming and complex.
    - Monitoring and then selection of the parameters for wide variety and ever changing anomalies is cumbersome task. The systems therefore result in slow and inaccurate detections.

There is however, a new promising detection technique, namely, signal processing based network anomaly detection, which is being explored these days. *Since the focus of work in this paper is area of using wavelets for computing self similarity falls under signal processing based network anomaly detection therefore, we cover this separately in section* 3.

3. Signal Based Network Anomaly Detection

Considering that the computer networks especially internet as a system whose traffic is comprised of signals, the techniques of *signal processing* can be applied for network anomaly detection. However, signal processing for network anomaly detection involves the challenge of dealing with first order stationarity, self-similarity, long-range dependence or heavy-tailed distributions and implementation problems due to complex and highly dynamic nature of the *internet* and its applications [40]. Nevertheless, sufficient amount of work has been carried out to prove the usefulness of the above mentioned properties in distinguishing an anomalous traffic from normal traffic behavior. Signal processing techniques have been applied to identify network anomalies as well as study network characteristics such as routing and congestion. The biggest advantage of signal processing is that the techniques can be applied to aggregated flows and lesser number of parameters is needed for the job. We next discuss various ways in which signal processing has been used by researchers for anomaly detection. We have categorized signal processing techniques into three types, namely, *Statistical Based Approaches* (SBA), *Spectral Analysis* (SPA) and *Wavelet Based Approaches* (WBA). We discuss them in detail in sections 3.1, 3.2, and 3.3.

3.1 Statistical Signal Based Network Anomaly Detection Approaches

Statistical Anomaly detection techniques assume that normal data occurs in high probability regions of a stochastic model, while anomalies occur in the low probability regions of the stochastic model.

The anomalies in internet traffic are widely diversified and it is difficult to characterize them all, and high volume makes them harder to identify. Over the years they have been classified and categorized depending upon different methodologies and approaches. *Statistical techniques fit a statistical model to the given data and then apply a statistical inference test to determine if an unseen instance belongs to this model or not*. Instances with low probability of been generated from the learned model are declared as anomalies. Statistical anomaly detection techniques have been categorized as *parametric* and *non-parametric* [4]. *Parametric Measures* are used when a distribution of the profiled attributes is assumed to fit a particular pattern whereas *Non-parametric Measures* are used when the distribution of the profiled attribute is gathered from a set of historical values observed over a period of time. We give brief overview of parametric and non-parametric techniques.

3.1.1 Statistical Parametric Techniques: Based on the type of distribution assumed, parametric techniques are categorized as Gaussian Model (GM) based, Regression Model (RM) based and mixtures of Parametric Distribution based.

1) *Gaussian Model Based:* GM assumes Gaussian distribution of the data. The parameters are estimated using *Maximum Likelihood Estimates* (MLE). The distance to the estimated mean gives anomaly score and using threshold value on anomaly scores anomalies are extracted. Distance to the mean is computed in many different ways. GM based techniques have been applied in domains like medicine, process quality control, structural engineering, operating systems, network intrusion detections, etc. to detect *univariate*} and *multivariate anomalies*. Some of the popular Gaussian based models are *Box plot* rule [47], *Grubb's* test [48], student's *t-test* [49], modified version of *t-test* called *Hotelling* t^2*-test* [50] and *Chi-Square Statistic* [51].
2) *Regression Model Based:* For each tested instance, the residual is used to determine anomaly score in a regression model fitted data. Several types of regression model techniques exist in the literature. The popular ones are *Robust Regression* [52], robust regression applied to *Auto-regressive Integrated Moving*

Average (ARIMA) models [53], [54], *Exponentially Weighted Moving Average* (EWMA) [56], and *Autoregressive Moving Average* (ARMA) [57].

3) *Mixture of Parametric Distributions Based:* Mixed parametric distributions are a mixture of parametric statistical distributions that are used to model the data. There are two subcategories in this. The first subcategory considers normal instances as one type of parametric distributions and anomalies as another set of parametric distributions. In the testing phase the test sample is checked to determine to which distribution-normal or anomalous it belongs and the *Grubb's test*} is tested on both the distributions to determine which of them is normal and which one is anomalous. The second subcategory of mixed parametric techniques models only the normal instances of a set as a mixture of parametric distributions. Any test instance that is an outlier to any of the learned models is considered as an anomaly.

3.1.2 Statistical Non Parametric Techniques: The non-parametric statistical model structure is not defined beforehand, but is determined from given data. *Histogram based* and *Kernel function based* models are two popular non parametric techniques.

1) *Histogram Based:* These techniques are popular in network intrusion detection community [36], [58-59]. The technique can be applied to both univariate and multivariate data sets. This technique consists of two steps: First step involves building a histogram and second step involves checking the bins of histogram in which *test instance* will fall. The instances that fail to fall in any of the bins are considered anomalous. Key challenge for histogram based techniques is to determine an optimal size of the bins to construct the histogram that maintains a low false alarm rate and a low false negative rate. For multivariate data, basic technique is to construct attribute wise histogram.
2) *Kernel Function-Based:* A non-parametric technique for probability density estimation is *parzen windows estimation*. This involves using kernel functions to approximate the actual density. Anomaly detection techniques based on kernel functions are similar to the parametric methods described earlier. The only difference is in the way density estimation technique is used. Desforges *et al.* [60], proposed a semi-supervised statistical technique to detect anomalies, which uses kernel functions to estimate the *probability distribution function* (pdf) for the normal instances. A new instance, which lies in the low probability area of this *pdf* is declared to be anomalous. Similar application of parzen windows is proposed for network intrusion detection.

Table 1. Comparison of Statistical Anomaly Detection Techniques wrt No. of Parameters

Reference	*No. of Parameters*	*Detection Technique*
Eleazar E. [71]	2	Probabilistic model
Constantine M. *et al.* [72]	3	Statistical & neural model
Matthew V. M. *et al.* [17]	2	LERAD
Ke W. *et al.* [73]	3	Payload statistical model
Xiuyao S. *et al.* [74]	3	GMM
Parmindar C. *et al.* [75]	2	FDR model
Federico S. W. *et al.* [9]	4	GLRT model
Yu M. [76]	1	Adaptive CUSUM

Table [1] enlists some of the works with respect to statistical detection technique used and number of parameters required for input. While studying the works of different researchers our primary focus was to look out for the required number of input parameters for detection of anomalies. We believe that for heavily fast and dynamically changing network traffic it is important to be able to apply techniques on aggregated flows, rather than capturing and analyzing the packets individually. The need for lesser number of parameters therefore asks for further studying.

Drawbacks of Statistical Techniques: Main drawbacks of spectral techniques are:

- The foremost drawback of statistical techniques is that for network anomaly detection they rely on the assumption that the traffic follows some definitive distribution. For internet traffic this is seldom true and hence statistical techniques cannot be used single to detect anomalies.
- Another big challenge is of finding the right hypothesis test so as to correctly distinguish anomalies from regular traffic with complex characteristics.

We therefore need a technique for anomaly detection which can adjust to dynamically changing behaviors of network traffic and anomalies. Spectral based network anomaly detection approaches, discussed next, are one such possible solution.

3.2 Spectral Signal Based Network Anomaly Detection Approaches

Spectral approaches transform the network traffic data to a lower dimensional subspace in order to find clearly distinguishable points of variability between the normal instances and the traffic anomalies [4], [55]. Generally, subspace reduction in spectral techniques is done by using PCA. Series of *adjacency matrix* graphs is used to trace an anomaly. For each window of captured data, an *activity vector* is calculated. Principal left singular vector (PLSV) is then formed to trace the normal dependencies. When the new data is captured it is compared with the activity vector and it's PLSV to find an anomaly. Another spectral technique of *Compact Matrix Decomposition* has been used by Sun *et al.* [61]. Spectral techniques are a combination of PCA based mechanisms and statistical computations. C. M. Cheng *et al.* in [16] used spectral analysis technique for distinguishing normal TCP traffic from rate-limited DoS attacks. Similarly, M. Thotton and C. Ji in [69] used spectral processing to detect anomalies in IP network traffic. Spectral analysis to TCP flows has also been applied by Y. Chen *et al.* in [70] to protect from reduction of quality attacks. More cases of spectral techniques using wavelets are discussed later. Table [2] shows some of the works, with respect to number of parameters and detection rate, where spectral techniques have been applied for anomaly detection.

Drawbacks of Spectral Techniques: Main drawbacks of spectral techniques are:

- Spectral techniques are PCA dependent, which means that they show good efficiency only if the distinction between anomalous traffic and normal traffic can be done in lower dimensions of the network traffic data.
- For very large and fast internet traffic, spectral techniques with high computational difficulty and non-scalability are not very useful.

This paper is focused on usage of wavelets for detection of anomalous traffic in computer network traffic. Wavelets based network anomaly detection techniques are discussed next.

3.3 Wavelets Signal Based Network Anomaly Detection Approaches

Wavelets first entered the literature in the mid-80’s, with the work of *Grossman* and his colleagues [62]. There has since been a rapid growth of wavelet applications in areas as diverse as quantum mechanics, audio signal analysis and image processing. V. Alarcon-Aquino and J.A. Barria brought in the application of *wavelets* into *Network Anomaly Detection* [63].

Reason for choosing wavelets: The wavelet tool 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. Detection techniques therefore could be used to locate local and global variances, monitoring statistical changes in signals and measuring self-similar behavioral changes in the signal. It is for these reasons that *wavelets* were of high interest to us.

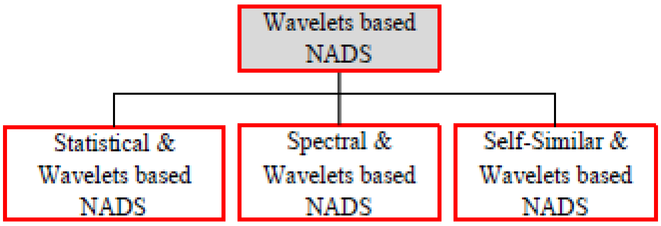
Wavelets based NADS
Statistical & Wavelets based NADS
Spectral & Wavelets based NADS
Self-Similar & Wavelets based NADS

Figure 2. Taxonomy of Wavelets based Network Anomaly Detection Schemes

As shown in Figure [2], the paper covers use of wavelets in anomaly detection by dividing them into three categories, namely, *statistical & wavelets based* detection techniques, *spectral & wavelets based* detection techniques and *self-similarity* based wavelet detection techniques. The detailed study on the three techniques is presented next.

3.3.1 Statistical & Wavelets Based Detection Techniques: First line of detection methods focuses on signal processing by monitoring statistical changes in signals. Huang *et al*. [78] proposed a network disruption detection method by applying PCA to network-wide routing updates data and developed a tool called *Waveman* for real time wavelet-based analysis of network traffic anomalies. They tested with different wavelets and concluded that *Coiflet* and *Paul* wavelets perform better in computing percentage deviation and entropy of the signal. The anomalies considered were DoS and portscans.

The pioneer work of Kim and Reddy in [79] and Kompella *et al*. in [80] also used wavelets based statistical approaches. They have used DWT to transform the data of destination IP addresses for correlation. The anomalies like DDoS attacks, portscans, worms etc. were detected with the help of statistical tool. Xiapu Luo *et al*. in [81] addressed the problem of detecting PDoS attacks by implementing *Vanguard*, which used a CUSUM algorithm to detect three traffic anomalies induced by PDoS attacks. Wavelets have been used to extract the desired frequency components of the computer network data traffic and TCP ACKs traffic. Change point detection algorithm is then applied to localize point of change.

K. Limthong *et al*.'s method performed wavelet-based analysis and a statistical distance calculation of University centre three month long traces on outbound traffic [82]. The detection algorithm generated a baseline region for each level of wavelet component and compared it with the outgoing network traffic baselines. The derived baselines from the statistical parameters were stored in the normal behavior database and their lower and upper bounds are used for comparisons. The technique could discover short duration malicious behavior as well as long duration anomalous behavior in a small volume of packets.

P. Shinde *et al*., in [64] firstly smoothened the traffic using EWMA and afterwards used wavelet analysis tool to analyze the smoothened signal using energy distribution. The authors considered that when there was a DoS attack the traffic pattern changed considerably and that change which could be detected using energy distribution analysis of wavelet.

For example, K.G. Kyriakopoulos and D.J. Parish [65] used wavelets to look out for anomalies in the real network traffic traces. They did MRA using *Haar* wavelet and thresholds were decided based on popular statistical Donoho-Johnstone universal threshold technique. In order to determine the accurate location of the anomaly the coefficients are scanned in progressive way from the largest scale to the smallest scale.

Jun Gao *et al.* [66] implemented scale-adaptive method based on *db6* wavelet packet. The detection algorithm used the same deviation score computational method proposed by P. Barford for reconstruction of the signal. Wavelet packet detection model selectively located the scales where presence of anomalous traffic could be measured beyond threshold value. The regenerated signal used only the coefficients from the scales where anomaly was detected. Our concern is that when the flow of incoming traffic is very high this approach tends to slow down the detection process.

To explore more into wavelets C. Callegari *et al.* [67] tried to use Wavelet Packet Transforms (WPT). They have used *Haar* and *Db2* wavelets to experiment on DARPA datasets. Three different algorithms were tested with high failure rate for two. The third algorithm has good success rate with a limitation of small window sizes. We think that using WPT for signal analysis in networks is not a good choice for two basic reasons, firstly the cost of using both the approximation and detail coefficients is very high and secondly the small window sizes are not the best choice in real time anomaly detection systems.

From the study of statistical wavelets based anomaly detection techniques we realized that though they are successful in detecting network anomalies but like any other statistical technique they *suffer from overly relying on definitive distribution of traffic* which is difficult to maintain in real traffic scenarios. They also *suffer from correctly distinguishing the normal and abnormal traffic* based on correct hypothesis.

Spectral analysis frees us from the burden of analyzing the traffic at packet level. The techniques can be applied to aggregated flows. We study spectral wavelets based detection techniques next.

Table 2. Comparison of Spectral Anomaly Detection Techniques

Reference	*P**	*Detection Technique*	*Attacks Detected*
He X. [77]	3	Fingerprint pattern matching, ML Classifier	18 DDoS
Barford P. *et al.* [84]	4	Local variance shift using wavelets	>100 DoS
Magnaghi A. *et al.* [89]	4	Locality principle measure	TCP-DoS
Bartlett G. *et al.* [85]	2	Iterated filtering	Low-rate
Carl G. *et al.* [86]	3	Change points in the CUSUM	DoS
Hamdi M. *et al.* [87]	5	Lipschitz singularities	DoS
Lu W. *et al.* [88]	15	ARX model	DoS
Dainotti A. *et al.* [91]		CUSUM & Adaptive Threshold	DoS
Li L. *et al.* [92]	5	Energy distribution variation	DDoS flood
Chen Y. *et al.* [70]	5	Gaussian distribution, DFT	RoQ

P*: Number of Parameters

3.3.2 Spectral & Wavelets Based Detection Techniques: Spectral methods of detection involve finding global and local variances in wavelet coefficients to detect respective short and long-term anomalies. Hussain *et al*. [83] applied spectral techniques to time series of packet arrivals to distinguish between single and multi source attacks, and identified repeat attacks. They argued characteristics of attack ramp-up and spectral behavior cannot be forged. Based on their novel algorithm they detected DoS attacks & 80 live attacks. Barford *et al*. [84] have used wavelets to analyze SNMP and flow-level information to identify DoS attack and other high frequency anomalies. They did pioneer work by using wavelets and demonstrated that based on shift in local variance wavelets can be quite effective in detecting abnormal traffic from normal traffic. Similarly, Magnaghi *et al*. [89] detected anomalies within TCP flows using a wavelet-based approach to identify network misconfigurations. They measured the variations in the Round Trip Times of the TCP protocol at different scales and computed the energy at each level. Using the *locality principle* they detected the anomalies.

G. Bartlett *et al.* in [85] used Haar wavelet to look at periodicity between flows to identify hosts which maintain regular contact while considering low frequency behavior under long observation windows and used iterated filtering for full decomposition. There work focused only on low-rate DoS flow periodicities. Carl *et al.* in [86] on the other hand applied *Haar* wavelets transform for detecting change-points in the CUSUM statistic. The detection was two step process, in first step increase in the rate of traffic was found out and later single vanishing moment of *Haar* wavelets was used to capture the abrupt and linear increase in the CUSUM. Hamdi and Boudriga in [87] have also used wavelets to decompose a set of metrics in order to find out an anomaly. Anomalies were traced as *Lipschitz singularities* occurring at specific points in time. Lu and A.A. Ghorbani in [88] did an extensive study of wavelet *basis functions*. They used GMM and experimented with different wavelets but found no particular wavelet to be fit for detection and classification of DDoS attacks.

A. Dainotti *et al.* in [90] designed a system with a two-stage architecture that combined change point detection approaches with CWT. This work was important because in time series analysis only DWTs are performed with advantage of being able to decompose the signal into finite set of coefficients and being able to reconstruct the signal using decomposed coefficients. CWT lacks this property. Using Morlet wavelet they detected anomalies in approximately 12000 time signals.

And L. Li *et al.* in [92], observed that the aggregated network traffic has strong bursty behavior across wide range of time scales and wavelets could be used to capture temporal correlation across multiple time scales with low computational cost so they utilized energy distribution based on wavelet analysis to detect DDoS attack traffic.

Yu Chen *et al*. [95-96] on the other hand have done elaborate study of Low-rate DDoS attacks or Shrew attacks. In this paper a novel approach has been proposed that filters shrew attacks by analyzing the *amplitude spectrum distribution* in the frequency domain. Packet arrivals in *time domain* are transformed into frequency domain by Discrete Fourier Transform (DFT) and filter is constructed using hypothesis-test theory. More than 10,000 simulated signals are successfully detected. Table [2] shows comparison of spectral anomaly detection techniques with respect to number of parameters, detection scheme and types of DDoS attacks detected.

After studying various works on spectral based anomaly detection techniques we observed that spectral techniques are good at anomaly detection. But spectral \& wavelets based techniques *suffer* mainly at two points:

- First being that spectral techniques alone are not self sufficient in detecting varied types of anomalies, especially DDoS attacks. A spectral technique may be good for one attack but may produce high false rate for another DDoS attack. With increase in number of detected anomalies there is increase in number of input parameters required for detection.
- Secondly, for complicated domains or heavy anomalies they *suffer* heavy losses and their cost for per degree of freedom also increases.

Next section discusses the use of *self-similarity* in network based anomaly detection.

3.3.3 Self-Similarity Based Wavelet Techniques: The studies by [39-40] laid seeds of presence of scale-invariant behavior called *self-similarity* in network traffic. This resulted in lots of interest by engineering community in measuring self-similarity and interpreting the reasons behind the scale-invariant behavior in the network traffic [41-45], [93]. Self-similarity estimators are approximate methods used to measure the burstiness property of a time-series. Taqqu *et al* [68] provide a detailed study of different estimators that are currently available.

Z. Xia *et al.* in [98] detected DDoS flooding attacks in real-time and used *H* to determine its intensity. The proposed process computes DWT and Schwarz information criterion of the network traffic, finds out the Hurst variations and then uses intelligent fuzzy logic technology to analyze the Hurst parameter and its changing rate to find out the intensity of the flooding DDoS attack. R. Xunyi *et al.* in [97] have use coefficient variance analysis using wavelets to accurately detect and identify anomalies in the network. M. Li in [99] used *averaged Hurst* factor *H* for anomalous traffic like DDoS in comparison to general network traffic and by minutely capturing *H* values detected the attacks. The technique has been tested on Lawrence Berkeley Laboratory datasets.

S. Rawat and C. S. Sastry in [100] were inspired by the methods that use the property of self similarity in computer network traffic as normal behavior and any deviation from it leading to be an anomaly. There method is different in the sense that rather than using Hurst estimated values directly to look out for deviation from normal behavior they measured gradient in *H* to trace out an anomaly. They have used a rather unusual wavelet *Symlet* for their study. S. Chatterjee [106] have demonstrated a new wavelet decomposition technique to detect a change in the Hurst parameter. The technique tests the variance structure of the wavelet coefficients at multiple scales and uses changes in variance to signal a change in the value of the Hurst parameter. The authors devised a new method whereby they find out the subsets of overlapping and non overlapping variances and choose the subset with maximum number of non overlapping levels. The results are better as compared to traditional approaches. Db6 wavelet has been used. No tests have been conducted on network traffic anomalies.

Table 3. Comparison of Self-Similarity Based Anomaly Detection Techniques

Reference	*YOP**	*P**	*Detection Technique*	*Remarks*
Xunyi R. *et al.* [97]	2007	3	Wavelet variance analysis	Detected TCP flooding attack
Li M. *et al.* [99]	2006	1	Auto correlation wavelet function Model	DDoS flood detected
Sastry C. S. [100]	2005	NM*	Wavelets energy distribution Model	Detected two DoS attacks
Cheng X. *et al.* [101]	2009	NM*	HHT wavelet coefficients variance method	Measured periodicity impact as anomaly
Sheng Z. *et al.* [101]	2010	6	R/S variance analysis	Detected self-generated LDoS attacks
Zhang H. [103]	2009	NM*	Parallel DIF-FFT to generate SS traffic, R/S & VT plot	Parallel computation of H was done
Luo X. *et al.* [81]	2009	4	DTW model Tested	LBNL & WIDE n/w traces for PDoS
Ribeiro V. J. *et al.* [105]	2006	6	Multifractal wavelet model	Applied multi fractal property of wavelets to capture effect of different protocols
Zhengmin X. *et al.* [98]	2010	3	DWT and SIC	DoS attacks
Lu L. F. *et al.* [104]	2011	5	Modified Wavelet Analysis method & Isomap	Detected two DoS attacks

YOP*-Year of Publication; P*-Number of Parameters; NM*-Not Mentioned

X. Cheng *et al.* [101] state that since the wavelet transform fails to exclude the influence of non-stationary signal's periodicity and trend term and the fact that Hilbert-Huang Transform (HHT) has unique advantage on non-stationary signal treatment therefore they have used modified self-similar parameter estimation algorithm to detect anomalies in the network traffic. Z. Sheng *et al.* [102] highlighted how *Hurst* could be used for detection of low rate DoS attacks using the four fields of IP header. Z. Huachuan *et al.* [103] on the other hand has used distributed environment to generate self-similar network traffic. M. Li *et al.* [91] discovered that the traffic at any given time of the day is similar to the traffic at that time for another day. And therefore using probability function combined with Db4 based DWT analysis the abrupt change in the days traffic can be measured and DDoS attack can be detected. The plus point of this technique is that one does not need to zero in on the starting point for sampling window. The drawback is it's inefficiency in distinguishing between DDoS attacks and flash crowds.

X. Luo and R. K. C. Chang [81] have also contributed in one of the preliminary works done in establishing the characteristic of computer network traffic being long range dependent at small as well as large scales and bringing an exposure to self similar nature of the traffic. In their work they have tested both the Poisson properties and the LRD properties of the network traffic at different time scales using *Haar* wavelets. They concluded that an at large time scale the traffic is self-similar, Gaussian and has Poisson-like variance-mean relation and at small time scales the traffic has more variations with multi-fractal, non-Gaussian, and quadratic variance-mean relation. The team of V. J. Ribeiro *et al.* [105] also performed an extensive wavelet analysis of internet backbone traffic and observed that for a majority of the traces, at small time scales the second-order scaling exponents are fairly close to 0.5H, indicating nearly uncorrelated traffic fluctuations at these time scales. However, there were some instances where the exponents do exhibit moderately large scaling behavior 0.7H *approx* at small time scales.

L. F. Lu *et al.* [104] have proposed Modified Wavelet Analysis method which is based on the existing Isomap algorithm and wavelet analysis which computes Hurst values and detects DDoS attack based on Hurst variations.

Table [3] enlists some of the important works where self-similarity based detection techniques have been explored for detection of attacks. Majority of the works have used self-similarity in collaboration with other statistical technique for detection of attacks. Moreover, number of attacks detected is also confined to certain set of attacks only. No scheme was self-sufficient in detecting high rate as well as low rate DDoS attacks using self-similarity as a single input parameter.

4. Conclusions

The important points observed in the study of self-similarity and wavelets based network anomaly detection techniques were, firstly, Self-similarity or scale-invariance has been observed in the network traffic and are a measurable value. Secondly, Normal traffic exhibits self-similar behavior and any deviation or variance in self-similarity could be used for detecting abnormal traffic. Thirdly, Self-similarity parameter can be used as a single parameter for detection of anomalies in network traffic.

In this paper, we reviewed previous works done in the field of anomaly detection in general and network based anomaly detection in particular. The current anomaly detection techniques with respect to rate based network anomalies were examined and their strengths and weaknesses were studied. The applicability of scale-invariant property of self-similarity as a parameter for detection of anomalies from normal network traffic behaviors as deeply studied. From the studies of scale-invariance and it's usage in detecting anomalies like flash crowds, DDoS attacks, outages, portscans, etc. it was realized that wavelets are a good tool that can be used for n-level decomposition of aggregated network traffic.

References

[1] C. Sample, and K. Schaffer, ‘An Overview of Anomaly Detection ’, IT Professional, vol. 15, no. 1, pp. 8-11, 2013.

[2] S. Axelsson, ‘Intrusion Detection Systems: A Survey and Taxonomy’, in Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2000.

[3] D. E. Denning, ‘An Intrusion-Detection Model’, in Journal IEEE Transactions on Software Engineering - Special issue on computer security and privacy, vol. 13, no. 2, pp. 222-232, 1987.

[4] V. Chandola, A. Banerjee, and V. Kumar, ‘Anomaly Detection : A Survey’, in ACM Computing Surveys, vol. 41, no. 3, pp. 1-58, 2009.

[5] C. Aggarwal, and P. Yu, ‘Outlier Detection for High Dimensional Data’, in Proceedings of the ACM SIGMOD International Conference on Management of Data, pp. 37-46, 2001.

[6] C. C. Aggarwal, and P. S. Yu, ‘ Outlier Detection With Uncertain Data’, in Proceedings of the International Conference on Data Mining, pp. 483-493, 2008

[7] H. Heffes, and D. M. Lucantoni, ‘A Markov Modulated Characterization of Packetized Voice and Data Traffic and Related Statistical Multiplexer Performance’, in IEEE Journal of Selected Areas of Communication, vol. SAC-4, pp. 856-868, 1986.

[8] G. Dewaele, K. Fukuda, P. Borgnat, P. Abry, and K. Cho, ‘Extracting Hidden Anomalies using Sketch and Non Gaussian Multiresolution Statistical Detection Procedure’, in ACM SIGCOMM LSAD ’07, pp. 145-152, 2007.

[9] F. S. Wattenberg, J. I. A. Perez, P. C. Higuera, M. M. Fernandez, and I. A. Dimitriadis, ‘Anomaly Detection in Network Traffic Based on Statistical Inference and alpha-Stable Modeling’, in IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 4, pp. 494-509, 2011.

[10] L. Liu, X. Jin, G. Min, and L. Xu, ‘Real-Time Diagnosis of Network Anomaly based on Statistical Traffic Analysis’, in IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 264-270, 2012.

[11] Y. Kanda, R. Fontugne, K. Fukuda, and T. Sugawara, ‘ADMIRE: Anomaly Detection Method Using Entropy-based PCA with Three-step Sketches’, in Computer Communications, vol. 36, no. 5, pp. 575-588, 2013.

[12] H. Ringberg, A. Soule, J. Rexford, and C. Diot, ‘Sensitivity of PCA for Traffic Anomaly Detection’, in ACM SIGMETRICS, vol. 35, no. 1, pp. 109-120, 2007.

[13] S. Pukkawanna, and K. Fukuda, ‘Combining Sketch and Wavelet Models for Anomaly Detection’, in IEEE International Conference on Intelligent Computer Communication and Processing, pp. 313-319, 2010.

[14] X. He, C. Papadopoulos, J. Heidemann, U. Mitra, and U. Riaz, ‘Remote Detection of Bottleneck Links Using Spectral and Statistical Methods’, in ACM International Journal of Computer and Telecommunications Networking, pp. 279-298, 2009.

[15] S. Novakov, C H Lung, I. Lambadaris, and N. Seddigh, ‘Studies in Applying PCA and Wavel*et al*gorithms for Network Traffic Anomaly Detection’, in IEEE 14th International Conference on High Performance Switching and Routing, pp. 185-190, 2013.

[16] C.M. Cheng, H. Kung, and K.S. Tan, ‘Use of Spectral Analysis In Defense Against Dos Attacks’, in IEEE Global Telecommunications Conference, vol. 3, pp. 2143-2148, 2002.

[17] M. V. Mahoney, and P. K. Chan, ‘Learning Rules For Anomaly Detection of Hostile Network Traffic’, in Proceedings of the 3rd IEEE International Conference on Data Mining, pp. 601-604, 2003.

[18] V. Paxson, ‘Bro: A System for Detecting Network Intruders in Real-time’, in Computer Networks, vol. 31, no. 23-24, pp. 2435-2463, 1999.

[19] M. Roesch, ‘Snort-Lightweight Intrusion Detection for Networks’, in USENIX LISA, pp. 229-238, 1999.

[20] F. Sabahi and A. Movaghar, ‘Intrusion Detection: A Survey’, in International Conference on Systems and Networks Communication, pp. 23-26, 2008.

[21] P. G. Teodoroa, J. D. Verdejoa, G. M. Fernandeza, and E. Vazquez, ‘Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges’, in Journal of Computer and Security, vol. 28, no. 1-2, pp. 18-28, 2009.

[22] B. Bencsath *et al*., ‘Duqu: Analysis, Detection, and Lessons Learned’, in ACM Proceedings of European Workshop on System Security, 2012.

[23] T. Lane, and C. E. Brodley, ‘Temporal Sequence Learning and Data Reduction for Anomaly Detection’, in ACM Transactions of Information Systems Security, vol. 2, no. 3, pp. 295-331, 1999.

[24] S. A. Hofmeyr, S. Forrest, and A. Somayaji, ‘Intrusion Detection Using Sequences of System Calls’, in Journal of Computer Security, vol. 6, no. 3, pp. 151-180, 1998.

[25] L. Mounji, and B. Charlier, ‘Continuous Assessment of a Unix Configuration: Integrating Intrusion Detection and Configuration Analysis’, in Proceedings of Network and Distributed System Security, pp. 27-35A, 1997.

[26] S. Forrest, P. Dhaeseleer, and P. Helman, ‘An Immunological Approach to Change Detection: Algorithms, Analysis and Implications’, in Proceedings of the IEEE Symposium on Security and Privacy, pp. 110-119, 1996.

[27] D. Dasgupta, and F. Andnino, ‘A Comparison of Negative and Positive Selection Algorithms in Novel Pattern Detection’, in Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, vol. 1. pp. 125-130, 2000.

[28] C. Kruegel, T. Toth, and E. Kirda, ‘Service Specific Anomaly Detection For Network Intrusion Detection’, in Proceedings of the ACM symposium on Applied Computing, pp. 201-208, 2002

[29] C. Kruegel, and G. Vigna, ‘Anomaly Detection of Web-based Attacks’, in Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 251-261, 2003

[30] C. Chow, and D.Y. Yeung,‘ Parzen-window Network Intrusion Detectors’, in Proceedings of the 16th International Conference on Pattern Recognition, vol. 4, pp. 385-388, 2002.

[31] M. M. Z. E. Mohammed, H. A. Chan, N. Ventura, M. Hashim, and E. Bashier,‘ An Automated Signature Generation Approach for Polymorphic Worms Using Principal Component Analysis’, in International Journal of Information Security, vol. 1, pp. 45-52, 2011.

[32] D. Brauckhoff, K. Salamatian, and M. May, ‘A Signal Processing View on Packet Sampling and Anomaly Detection’, in IEEE Proceedings of INFOCOM, pp. 1-9, 2010.

[33] I. A. Saroit Ismail, ‘Bandwidth problems in high-speed networks’, in IBM Journal of Research and Development, pp. 919-938, 2000

[34] A. Lakhina, M. Crovella, and C. Diot, ‘Mining Anomalies Using Traffic Feature Distributions’, in Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, vol. 35, no. 4, pp. 217-228, 2005.

[35] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J.K Kalita,‘Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions’, in The computer journal, Oxford University Press, vol. 57, no. 4, pp. 537-556, 2014

[36] M. V. Mahoney, and P. K. Chan, ‘Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks’, in Proceedings of the 8th ACMSIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 376-385, 2002.

[37] B. Krishnamurty, S. Sen, Y. Zhang, and Y. Chen, ‘Sketch-based Change Detection: Methods, Evaluation, and Applications’, in Proceedings of the 3rd ACM SIGCOMM Conference on Internet Measurement, pp. 234-247, 2003.

[38] X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G. Iannaccone, and A. Lakhina, ‘Detection and Identification of Network Anomalies Using Sketch Subspaces’, in Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement , pp. 147-152, 2006.

[39] W. E. Leland, M. S. Taqqu, W. Willinger and D. V. Wilson, ‘On the Self-Similar Nature of Ethernet Traffic (extended version)’, in IEEE/ACM Transactions on Networking, vol. 2, pp. 1-15, 1994.

[40] V. Paxson and S. Floyd, ‘Wide Area Traffic: The Failure of Poisson Modeling’, in IEEE/ACM Transactions on Networking, vol. 3, pp. 226-244, 1995.

[41] M. E. Crovella and A. Bestavros, ‘Self-similarity in World Wide Web Traffic: Evidence and Possible Causes’, in IEEE/ACM Transactions on Networking, vol. 5, 1997.

[42] M.S. Borella, S. Uludag, G.B. Brewster, and I. Sidhu, ‘Self-similarity of Internet Packet Delay’, in IEEE International Conference on Communications, vol.1, pp. 513-517, 1997.

[43] A. Erramilli, M. Roughan, D. Veitch, and W. Willinger, ‘Self-similar Traffic and Network Dynamics’, in Proceedings of IEEE , vol. 90, pp. 800-819, 2002.

[44] T. Kushida and Y. Shibata, ‘Empirical Study of Inter-arrival Packet Times and Packet Losses’, in Proceedings of 22nd International Conference on Distributed Computing Systems Workshops, pp. 233-238, 2002.

[45] A. Feldmann, A. C. Gilbert and W. Willinger, ‘Data Networks as Cascades: Investigating the Multifractal Nature of Internet WAN Traffic’, in Proceedings of the ACM/SIGCOMM, pp. 42-55, 1998.

[46] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, ‘Sketch-based Change Detection: Methods, Evaluation, and Applications’, in Proceedings of the 3rd ACM SIGCOMM Internet Measurement Conference, pp. 234-247, 2003.

[47] J. Laurikkala, M. Juhola, and E. Kentala, ‘Informal Identification of Outliers in Medical Data’, Proceedings of the 5th International Workshop on Intelligent Data Analysis in Medicine and Pharmacology, pp. 20-24, 2000.

[48] F. Grubbs, ‘Procedures for Detecting Outlying Observations in Samples’, in Technometrics, vol. 11, no. 1, pp. 1-2, 1969.

[49] C. Surface, and K. Worden, ‘A Novelty Detection Method to Diagnose Damage in Structures: An Application to an Offshore Platform’, in Proceedings of the 8th International Conference of O_-Shore and Polar Engineering, vol. 4. pp. 64-70, 1998

[50] J. P. Liu, and C. S. Weng, ‘Detection of Outlying Data in Bioavailability/Bioequivalence Studies’, in Statistics in Medicine, vol. 10, no. 9, pp. 1375-1389, 1991.

[51] N. Ye, and Q. Chen, ‘An Anomaly Detection Technique Based on a Chi-square Statistic for Detecting Intrusions Into Information Systems’, in International Journal of Quality Reliability Engineering, vol. 17, pp. 105-112, 2001.

[52] P. J. Rousseeuw, and A. M. Leroy, ‘Robust Regression and Outlier Detection’, in John Wiley & Sons, 1987

[53] A. M. Bianco, M. G. Ben, E. J. Martinez, and V. J. Yohai, 'Outlier Detection In Regression Models with Arima Errors Using Robust Estimates', in Journal of Forecasting, vol. 20, no. 8, pp. 565-579, 2001

[54] D. Chen, X. Shao, B. Hu, and Q. Su, 'Simultaneous Wavelength Selection and Outlier Detection in Multivariate Regression of Near-infrared Spectra', in Journal of Analytical Sciences, vol. 21, no. 2, pp. 161-167, 2005.

[55] A. Agovic, A. Banerjee, A. R. Ganguly, and V. Ptotopopescu, 'Anomaly Detection In Transportation Corridors Using Manifold Embedding', in Proceedings of the 1st International Workshop on Knowledge Discovery from Sensor Data, 2007.

[56] M. Roughan, T. Gri_n, Z. M. Mao, A. Greenberg, and B. Freeman, 'IP Forwarding Anomalies and Improving their Detection Using Multiple Data Sources', in Proceedings of ACM SIGCOMM 2004 Workshop on Network Troubleshooting: Research, Theory and Operations Practice Meet Malfunctioning Reality, pp. 307-312 , 2004.

[57] P. Galeano, D. Pea, and R. S. Tsay, 'Outlier Detection in Multivariate Time Series via Projection Pursuit', in Statistics and econometrics working articles, pp. 654-669, 2006.

[58] D. Anderson, T. F. Lunt, H. Javitz, A. Tamaru, and A. Valdes, 'Detecting Unusual Program Behavior Using the Statistical Components of NIDES', in Technical Report SRICSL9506, Computer Science Laboratory, SRI International, 1995

[59] D. Anderson, T. Frivol.d, A. Tamaru, and A. Valdes, 'Next-generation Intrusion Detection Expert System (NIDES), Software User's Manual, Beta-update Release', in Technical Report SRICSL9507, Computer Science Laboratory, SRI International, 1995

[60] M. Desforges, P. Jacob, and J. Cooper, 'Applications of Probability Density Estimation to the Detection of Abnormal Conditions in Engineering', in Proceedings of the Institute of the Mechanical Engineers, vol. 212, pp. 687-703, 1998.

[61] J. Sun, Y. Xie, H. Zhang, and C. Faloutsos, 'Less is More: Compact Matrix Decomposition for Large Sparse Graphs', in Proceedings of SDM, 2007.

[62] A. Grossmann and J. Morlet, 'Decomposition of Hardy Functions Into Square Integrable Wavelets of Constant Shape', in Siam Journal of Mathematical Analytics, vol. 15, no. 4, pp. 723-736, 1984.

[63] V. Alarcon-Aquino, and J.A. Barria, 'Anomaly Detection in Communication Networks Using Wavelets', in IEE Proceedings - Communications, vol. 48, no. 6, pp. 355-362, 2001.

[64] P. Shinde, and S. Guntupalli, 'Early DoS Attack Detection using Smoothened Time-Series and Wavelet Analysis', in IEEE Third International Symposium on Information Assurance and Security, pp. 215-220, 2007.

[65] G. Konstantinos, G. Kyriakopoulos, and D. J. Parish, 'Applying Wavelets for the Controlled Compression of Communication Network Measurements', in IET Communications, vol. 4, no. 5, pp. 507-520, 2010.

[66] G. Jun, H. Guangmin, Y. Xingmiao, and R. K. C. Chang, 'Anomaly Detection of Network Traffic Based on Wavelet Packet', in Asia-Pacific Conference on Communications, pp. 1-5, 2006.

[67] C. Callegari, S. Giordano, and M. Pagano, 'Application of Wavelet Packet Transform to Network Anomaly Detection', in Next Generation Tele Traffic and Wired/Wireless Advanced Networking, pp. 246-257, 2008.

[68] M. S. Taqqu, V. Teverovsky, and W. Willinger, 'Estimators for Long-Range Dependence: An Empirical Study', in Fractals, vol. 3, pp. 785-798, 1995.

[69] M. Thottan, and C. Ji, 'Anomaly Detection In IP Networks', in IEEE Transactions on Signal Processing, vol. 51, no. 8, pp. 2191-2204, 2003.

[70] Y. Chen, and K. Hwang, 'Spectral Analysis of TCP Flows For Defense Against Reduction-of-quality Attacks', in IEEE International Conference on Communications, pp. 1203-1210, 2007.

[71] E. Eskin, 'Anomaly Detection Over Noisy Data Using Learned Probability Distributions', in Proceedings of the 7th International Conference on Machine Learning, pp. 255-262, 2000.

[72] C. Manikopoulos, and S. Papavassiliou, 'Network Intrusion and Fault Detection: A Statistical Anomaly Approach', in IEEE Communications Magazine, vol. 40, no. 10, pp. 76-82, 2002.

[73] K. Wang, and S. J. Stolfo, 'Anomalous Payload-Based Network Intrusion Detection', in Proceedings of the Recent Advances in Intrusion Detection, pp. 203-222, 2004.

[74] X. Song, M. Wu, C. Jermaine, and S. Ranka, 'Conditional Anomaly Detection', in IEEE Transactions on Knowledge and Data Engineering, vol. 19, pp. 631-645, 2007.

[75] P. Chhabra, C. Scott, E. D. Kolaczyk, and M. Crovella, 'Distributed Spatial Anomaly Detection', in Proceedings of the 27th IEEE International Conference on Computer Communications, pp. 1705-1713, 2008.

[76] M. Yu, 'A Nonparametric Adaptive Cusum Method And Its Application In Network Anomaly Detection', in International Journal of Advancements in Computing Technology, vol. 4, no. 1, pp. 280-288, 2012.

[77] X. He, C. Papadopoulos, J. Heidemann, and A. Hussain, 'Spectral Characteristics of Saturated Links',in Technical Report USC-CSD-TR-827, University of Southern California Computer Science Department, 2004.

[78] C. T. Huang, S. Thareja, and Y. J. Shin, 'Wavelet-based Real Time Detection of Network Traffic Anomalies', in Securecomm and Workshops, pp.1-6, 2006.

[79] S. S. Kim, and A. L. N. Reddy, 'Statistical techniques for detecting Traffic anomalies through packet header data', in IEEE/ACM Transaction on Networking, vol. 16, no. 3, pp. 562-575, 2008.

[80] R. R. Kompella, S. Singh, and G. Varghese, 'On scalable attack detection in the network', in IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 14-25, 2007.

[81] X. Luo, E. W. W. Chan, and R. K. C. Chang, 'Vanguard: A New Detection Scheme for a Class of TCP-targeted Denial-of-Service Attacks', in EURASIP Journal on Advances in Signal Processing, vol. 2009, 2009.

[82] K. Limthong, P. Watanapongse, F. Kensuke, 'A Wavelet-based Anomaly Detection For Outbound Network Traffic', in 8th Asia-Pacific Symposium on Information and Telecommunication Technologies, pp. 1-6, 2010.

[83] A. Hussain, J. Heidemann, and C. Papadopoulos, 'Identification of Repeated Denial of Service Attacks', in Proceedings of the IEEE Infocom, pp. 1-15, 2006.

[84] P. Barford, J. Kline, D. Plonka, and A. Ron, 'A Signal Analysis Of Network Traffic Anomalies', in ACM SIGCOMM Proceedings Internet Measurement Workshop, pp. 71-82, 2002.

[85] G. Bartlett, M. D. Rey, J. Heidemann, and C. Papadopoulos, 'Using Low-Rate Flow Periodicities for Anomaly Detection', in Extended Technical Report ISI-TR-661, 2009.

[86] G. Carl, R. R. Brooks, and S. Rai, 'Wavelet Based Denial-of-Service Detection', in ELSEVIER Journal on Computers & Security, vol. 25, pp. 600-615, 2006.

[87] M. Hamdi, and N. Boudriga, 'Detecting Denial-of Service Attacks Using the Wavelet Transform', in ELSEVIER Computer Communications, vol. 30, pp. 3203-3213, 2007.

[88] W. Lu, M. Tavallaee, A. A. Ghorbani, 'Detecting Network Anomalies Using Different Wavelet Basis Functions', in Proceedings of the Communication Networks and Services Research Conference, pp. 149-156, 2008.

[89] A. Magnaghi, T. Hamada, and T. Katsuyama, 'A Wavelet-Based Framework for Proactive Detection of Network Misconfigurations', in Proceedings of ACM Workshop on Network Troubleshooting, pp. 253-258, 2004.

[90] A. Dainotti, A. Pescape, and G. Ventre, 'NIS04-1: Wavelet-based Detection of DoS Attacks', in IEEE Global Telecommunications Conference, pp. 1-6, 2006.

[91] M. Li, and M. Li, 'A New Approach for Detecting DDoS Attacks Based on Wavelet Analysis', in 2nd international conference on Image and Signal Processing, pp. 1-9, 2009.

[92] L. Li, G. Lee, 'DDoS Attack Detection and Wavelets', in 12th International Conference on Computer Communications and Networks, pp. 421-427, 2003.

[93] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson, 'Self-similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level', in IEEE/ACM Transactions on Networking, vol. 5, no. 1, pp. 71-86, 1997.

[94] X. Zhengmin, L. Songnian, and T. Junhua, 'Note on Studying Change Point of LRD Traffic Based on Li's Detection of DDoS Flood Attacking', in Mathematical Problems in Engineering, vol. 2010, 2010.

[95] Y. Chen, and K. Hwang, 'Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks', in IEEE International Conference on Communications, pp. 1203-1210, 2007.

[96] Y. Chen, Y. K. Kwok, and K. Hwang, 'Filtering Shrew DDoS Attacks Using A New Frequency-Domain Approach', in IEEE Conference on Local Computer Networks, pp. 793-801, 2005.

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

[98] X. Zhengmin, L. Songnian, and T. Junhua, 'Note on Studying Change Point of LRD Traffic Based on Li's Detection of DDoS Flood Attacking', in Mathematical Problems in Engineering, vol. 2010, 2010.

[99] M. Li, 'Change trend of averaged Hurst parameter of Traffic under DDOS flood attacks', in Computers and Security, vol. 25, no. 3, pp.213-220, 2006.

[100] S. Rawat and C. S. Sastry, 'Network intrusion detection using wavelet analysis', in Proceedings of the 7th International Conference on Information Technology, vol. 3356 of Lecture Notes in Computer Science, pp. 224-232, 2004.

[101] X. Cheng, K. Xie, and D. Wang, ' Estimation of Network Traffic Hurst Parameter Using HHT and Wavelet Transform', in 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2009.

[102] Z. Sheng, Z. Qifei, P. Xuezeng and Z. Xuhui, 'Detection of Low-rate DDoS Attack Based on Self-Similarity', in 2010 Second International Workshop on Education Technology and Computer Science, vol. 1 , pp. 333-336, 2010.

[103] H. Zhang, J. Xu, and J. Tian, 'Research on the parallel algorithm for self-similar network Traffic simulation', in International Conference on Computer Science and Information Technology, pp. 355-359, 2009.

[104] L. F. Lu, M. L. Huang, M. A. Orgun, and J. W. Zhang, 'An Improved Wavelet Analysis Method for Detecting DDoS Attacks', in 4th International Conference on Network and System Security, pp. 318-322, 2011.

[105] V. J. Ribeiro, Z. L. Zhang, S. Moon, and C. Diot, 'Small-time Scaling Behavior of Internet Backbone Traffic', in Journal of Computer Networks: The International Journal of Computer and

Telecommunications Networking - Special issue: Long range dependent traffic, vol. 48, no. 3, pp. 315-334, 2005.

[106] S. Chatterjee, M. H. MacGregor, and S. Bates, 'Detecting changes in the Hurst parameter', in 33rd IEEE Conference on Local Computer Networks, pp. 876-883, 2008.

[107] M. Li, and M. Li, 'A New Approach for Detecting DDoS Attacks Based on Wavelet Analysis', in 2nd international conference on Image and Signal Processing, pp. 1-9, 2009.