ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Anomaly Detection and Prevention in Network Traffic based on Statistical approach and α-Stable Model

[1]Anup Bhange
[1]M.tech Scholar, Dept CSE
[1] Patel Institute of Technology
Bhopal

[2] Sumit Utareja
[2]Asst.Prof, Dept CSE
[2]Patel Institute of Technology
Bhopal

ABSTRACT:--
Network traffic anomalies plunk for a huge division of the Internet traffic and conciliation the performance of the network resources. Detecting and diagnosing these threats is a protracted and time overriding task that network operators face daily. During the past years researchers have rigorous their efforts on this problem and projected several apparatus to automate this task. So, recent progress in anomaly detection has allowable to detect new or unknown anomalies by taking benefit of statistical analysis of the traffic. This analysis study on flood attacks and Flash Crowd and their improvement, classifying such attacks as either high-rate flood or low-rate flood. Finally, the attacks are appraised against principle related to their characteristics, technique and collision.

This paper discusses a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior The Research proposals in anomaly detection typically follow a four-stage approach, in which the first three stages define the detection method, while the last stage is dedicated to validate the approach method to detect anomalies in network traffic, based on a non restricted α -stable first-order model and statistical hypothesis testing. Here we focus on detecting and preventing two anomaly types, namely floods and flash-crowd .Here we use NS2 simulator to calculate result.

Keywords: Statistical Approach, α-Stable Distribution, Network traffic representation

I. INTRODUCTION:

Recognize network anomalies are serious for the timely mitigation of events, like attacks or failures that can affect the security, SLAs, and performance of a network. Anomalies can come from action with malicious intentions (e.g., scanning, DDoS, prefix hijacking), or from misconfigurations and failures of network components (e.g., link failures, routing problems, outages in measurement equipment), or even rightful events such as strangely large file transfers or flash crowds. Traffic analysis and anomaly detection are extensively used to understand and characterize network traffic behavior, as well as to identify abnormal operational conditions such as malicious attacks. However, techniques for traffic analysis and anomaly detection are typically carried out independently in different parts of the network, either in the edge or in the core networks alone. In fact, different traffic characteristics and anomalies can normally be better observed in a specific part of the network, although they affect the network as a whole Most works these days center on flow-level data. At least five minutes(net flow data) delay is predictable even for the online detection methods, so anomaly detection methods depend on flow-level data are usually use for the warning/alerting to the network manager and hard to be used for the next generation intrusion detection system design. Ideal IDS, besides warning, should identify the anomaly packet in real time and block it. Hence, exploring detection methods based on packet-level data is indispensable. Our work mainly focuses on anomaly detection for the packet-level data. A number of techniques have been proposed in order to identify anomalies by analyzing network traffic. They all seek to expose anomalies by detecting deviations from some underlying model of normal traffic. Usually, these kinds of models have to be learned from days or weeks of anomaly-free traffic traces, which is a practical problem since the training data is never guaranteed to be clean and training should be performed periodically.

Research proposals in anomaly detection typically follow a four-stage approach, in which the first three stages define the detection method, while the last stage is dedicated to validate the approach. So, in the first stage, traffic data are collected from the network (data collection). Second, data are analyzed to extract its most relevant features (data analysis). Third, traffic is classified as normal1 or abnormal (inference); and fourth, the whole approach is validated with various types of traffic anomalies.

1) Statistics Collection.
2) Statistics analysis (feature extraction).

3) Conclusion (classifying normal vs. anomalous traffic).

4) Justification.

Statistics Collection is typically carried out by polling one or more routers periodically, so that traffic data are collected and stored for posterior analysis in the second stage. Some authors sample data at the packet level, gathering information from headers, latencies, etc., while others prefer to use aggregated traffic as the source of information, often through the use of the Simple Network Management Protocol (SNMP). Sampling data at the packet level provides more information, but at the cost of a higher computational load and dedicated hardware must be employed. Aggregated traffic, on the other hand, gives less information from which to decide for the presence or absence of anomalies, but is a simpler approach and does not need any special hardware.

In the statistics analysis phase, several techniques can be applied to extract interesting features from current traffic. Some of them include information theory [4], [9] wavelets [6], statistics-based measurements [3], and statistical models. Of these techniques, the use of statistical models as a means to extract significant features for data analysis has been found to be very promising, since they allow for a robust analysis even with small sample sizes (provided that the model is adequate for real data). Moreover, with a traffic model, its set of parameters can be used as extracted traffic features, since any traffic sample is determined by the model parameters.

The fact that these models do not account for high variability may have a negative impact on capturing traffic properties and, as a consequence, on detecting anomalies. High variability manifests itself in the marginal (first-order) traffic distribution and states that traffic is inherently burst. This results in traffic distributions exhibiting heavy tails which cannot be properly modeled with, e.g., Gaussian functions. Long-range dependence, on the other hand, states that traffic is highly dependent over a wide range of time scales, i.e., its autocorrelation function exhibits a slowly decaying tail Several statistical distributions are capable of modeling the high variability property. One of such distributions is the α-stable family [15], which has been previously used to model network traffic [16] (where the detection problem is not addressed). To the best of our knowledge, these distributions have never been applied to anomaly detection. Moreover, in addition to properly modeling highly variable data, α-stable distribution are the limiting distribution of the generalized central limit theorem [17], a fact that sets them as good candidates for aggregated network traffic. Regarding the time evolution model and long-range dependence, the first-order α-stable model is appropriate to detect flood and flash-crowd anomalies.

Several approaches have been used in the conclusion stage as well. Classification methods based on neural networks [10], [11], [18], statistical tests [2], information theory [4], and simple thresholding [19], to cite a few, can be found in anomaly detection literature. There seems to be a common point in all of them, though. The conclusion stage bases its decisions on the existence of a reference traffic window, which allows the classification method to assess whether the current traffic window is normal (i.e., it is sufficiently similar to the reference window) or abnormal (i.e., significantly different from the reference window). How the reference window is chosen not only has an impact on the final normal versus abnormal classification rate, but it also determines the exact definition of a traffic anomaly. An abrupt change in some of the features extracted from traffic, so the reference window is simply the previous-to-current traffic window.

II. RELATED WORK:

2.1 Volume Depends anomaly detectors

Volume depends loom are monitoring the number of bytes, packets or flows broadcast more time and aims at detecting irregular variances that represent abusive usages of network resources or resource failures. Several technique have been proposed to effectively recognize local and global traffic volume variances that place for respectively short and long lasting anomalies. For example, bar ford et al. [15] proposed a technique based on wavelet [16] that inspects the traffic volume at different frequencies. Their loom makes use of the wavelet examination to dissect the traffic into three distinct signals instead of local, normal and global variances of the traffic. The rotten signals are analyzed by a detection procedure that finds the irregularities and information the period of time they occur. Since the three signals represent the traffic at dissimilar time scales this approach is able to report short and long lasting anomalies. Nevertheless, as the whole traffic is collective into a single signal analyze the detected anomalies is challenging and anomalous flows or IP addresses are left unknown.

Lakhina et al. [17] proposed a recognition method that perceive and diagnoses anomalies in large scale networks. First, their approach checks the traffic using a matrix in which each cell symbolizes the traffic volume of a link of the network at a certain time interval. Second, the main behavior of the traffic is removing from the matrix with the principal component analysis (PCA) and anomalies are detected in residual traffic. Finally, the origin and destination nodes of the network that are exaggerated by the anomalous traffic are recognized and reported. Soule et al. proposed another finding method that also observes the

traffic volume in matrices. The main idea fundamental their approach is to represent in a matrix the traffic between nodes of a large network and remove the normal traffic using a Kalman filter. The remaining traffic is analyzed with a statistical method that detects anomalous traffic and reports the pair of nodes exaggerated by the anomalous traffic.

These volume-based anomaly detectors successfully report volume anomalies while their false positive rate is low. Their plan, however, restrict them to report only a few classes of anomaly, thus, network operative need additional detectors to identify threats that are invisible in the interchange volume (e.g., network scan or port scan).

2.2 Abnormality Exposure

Detecting abnormal traffic is a research topic that had recently established a lot of attention. We classify this topic into two domains; network intrusion detection and Internet traffic anomaly detection. The goal of intrusion detection is to protect a network from remote threats, thus, the detection method is monitoring the traffic at the edge of the protected network where complete flows and packet payload are usually accessible. In contrast, Internet traffic anomaly detection aims at identifying anomalous traffic that is transiting in the core of the Internet where the monitored traffic is asymmetric due to routing policies, thus, flows are incomplete. For the last decade researchers have taken a strong interest in anomaly detection and proposed different detection methods that are basically monitoring traffic characteristics and discriminating outliers. We differentiate different categories of anomaly detection method; the methods monitoring the traffic volume and those monitoring the distribution of traffic features.

2.3 Traffic features Depend Abnormality Detectors:

In order to conquer the drawbacks of volume-based anomaly detectors re- searchers proposed to purify the traffic features that are inspect by the anomaly detectors. For example, as many anomalies cause abnormal operation of ports or addresses, inspecting the sharing of the traffic into the port and address spaces permits to identify anomalous traffic that is not reported by volume-based detectors (e.g., port scan). Nevertheless, due to the size of analyzed traffic examine detailed traffic features are costly and impose researchers to complicated effective traffic aggregation schemes. The main challenge in collective network traffic is the tradeoff between maintaining a concise representation of the traffic and preserving its interesting characteristics. We distinguish four groups of detection method in regard to their traffic aggregation scheme; namely, (1) Recognition methods aggregating the traffic in a single signal, (2) those collective the traffic in traffic matrices, (3) methods collective traffic in histograms, and (4) the other methods.

2.4 Packet Filtering for Flow-Based information:

In packet filtering, packet flows are sampled by capturing the IP headers of a select set of packets at different points in the network Information gathered from these IP headers is then used to provide detailed network performance information. For flow-based monitoring, a flow is identified by source destination addresses and source-destination port numbers. The packet filtering approach requires sophisticated network sampling techniques as well as specialized hardware at the network devices to do IP packet lookup. Data obtained from this method could be used to detect anomalous network flows. However, the hardware requirements required for this measurement method makes it difficult to use in practice.

2.5. Data from Routing Protocols:

Information about network proceedings can be gain through the use of routing peers. For example by using an open shortest path first (OSPF) peer, it is possible to get together all routing table updates that are sent by the routers. The data collected can be use to build the network topology and provides link status updates. If the routers run OSPF with traffic engineering (TE) extensions, it is possible to get link operation levels. Since routing updates occur at recurrent gap, any change in link utilization will be updated in near real time. However, since Routing updates must be kept small; only limited information pertaining to link statistics can be propagated through routing updates [17]

III. Anomaly gratitude Methods:

Statistical approach designed for Network Anomaly recognition:

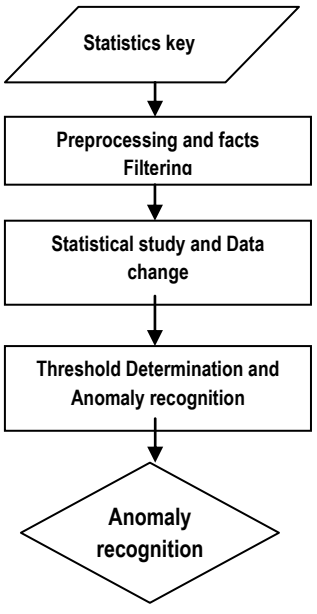

Fig. 1 Statistical Approach for Network Anomaly recognition

Fig. 1 Demonstrates the general steps implicated in statistical anomaly recognition. The first step is to preprocess or filter the given data inputs. This is an important step as the types of data available and the time scales in which these data are measured can significantly affect the recognition performance [5]. In the second step, statistical analysis and/or data transforms are performed to separate normal network behaviors from anomalous behaviors and noise. A variety of method can be applied here, e.g., Wavelet Analysis, Covariance Matrix analysis, and Principal Component Analysis. The main challenge here is to discover computationally efficient techniques for anomaly recognition with low false alarm rate. In the final step, decision theories such as Generalized Likelihood Ratio (GLR) test can be used to conclude whether there is a network anomaly depends on the variation observed. Statistical anomaly recognition can also be viewed from the machine learning perspective, where the goal is to find appropriate discriminate functions that can be used to classify any new input data vector into the normal or anomalous region with good accuracy for anomaly recognition. One subtle difference between statistical anomaly recognition and machine learning based methods is that statistical approaches generally focus on statistical analysis of the composed data, whereas machine learning methods focuses on the "learning" part.

3.1 Change-Point Recognition:

Statistical sequential change-point recognition has been useful successfully to network anomaly recognition. In [5], Thottan et al. characterize network anomalies with Management Information Base (MIB) variables undergoing abrupt changes in a correlated fashion. Given a set of MIB variables sampled at a fixed time-interval, the compute a network health function by combining the abnormality pointer of each individual MIB variable. This network health function can be used to conclude whether there is an anomaly in the network. In, Wang et al. detect SYN flooding attacks based on the dynamics of the differences between the number of SYN and FIN packets, which is modeled as a stationary erotic random process. The non-parametric Cumulative Sum (CUSUM) method is then used to detect the abrupt changes in the observed time series and thus detect the SYN flooding attacks.

3.2. Kalman Filter:

In [5], Soule et al. develop a traffic anomaly recognition scheme support on Kalman Filter. Unlike the work in Soule et al. process the link data using a Kalman filter rather than PCA analysis to forecast the traffic matrix one step into the future. After the forecast is made, the real traffic matrix is expected based on new link data. Then the difference between the forecast and the actual traffic matrix is used to identify traffic volume anomaly based on different threshold methods. Kalman filter has been applied successfully to a wide variety of problems involving the estimation of dynamics of linear systems from incomplete data. Thus, it is a talented tool for network anomaly recognition together with other more difficult models of non-linear dynamics.

3.3. Holt-Winters Predict Technique:

Holt-Winters Forecasting is a complicated algorithm that builds upon exponential level. Holt-Winters Forecasting rests on the basis that the pragmatic time series can be rotting into three components: a baseline, a linear trend, and a seasonal effect. The algorithm supposes each of these components evolves over time and this is skilled by applying exponential smoothing to incrementally update the components. The prediction is the sum of the three components: [2]

$XT+1 = nt + DT + Mt+1-m.$ (1)

The update formulas for the three components, or coefficients a, b, c is:

Baseline ("intercept"):

$at = \alpha (yt + ct-m) + (1 – \alpha)(at-1 + bt-1)$. (2)

Linear Trend ("slope"):

$bt = \beta (at – at-1) + (1 – \beta) bt-1.$ (3)

Trend:

$ct = \gamma (yt – at) + (1 – \gamma) ct-m.$ (4)

As in exponential smoothing, the updated coefficient is an average of the calculation and an estimate obtained solely from the observed value yt, with fractions resolute by a model parameter (α, β, γ). Recall m is the period of the seasonal cycle; so the seasonal coefficient at time t references the last calculate coefficient for the same time point in the seasonal cycle.

The new approximation of the baseline is the observed value attuned by the best available estimate of the seasonal coefficient (ct-m). As the updated baseline needs to account for change due to the linear trend, the forecast slope is added to the baseline coefficient. The new estimate of the slope is simply the difference between the old and the new baseline (as the time interval between comments is fixed, it is not relevant). The new estimate of the seasonal component is the difference between the observed value and the corresponding baseline.

α, β and γ are the adaptation parameters of the algorithm and $0 < \alpha, \beta, \gamma < 1$. Larger values mean the algorithm adapts faster and predictions reflect recent observations in the time series; smaller values means the algorithm adapts slower, placing more weight on the past history of the time series. These values should be optimized when the algorithm is implemented.

3.4 Rule-Based Process:

Problematic work in this area of error or anomaly gratitude was depending on expert systems. In expert systems, a complete database grasp the rules of behavior of the injured system are used to finish

if a fault arise, [17]. Rule-based systems are too slow for real-time purpose and are reliant on prior knowledge about the fault conditions on the network. The recognition of faults in this approach depends on indication that is specific to a particular manifestation of a fault. Examples of these symptoms are excessive utilization of bandwidth, number of open TCP connections, total throughput exceeded, etc. These rule-based systems rely heavily on the expertise of the network manager and do not adapt well to the developing network environment. Thus, it is possible that entirely new faults may escape detection. In, the authors describe an expert system model using fuzzy cognitive maps (FCMs) to overcome this limitation. FCM can be used to get an intelligent modeling of the spread and interaction of network faults. FCMs are constructed with the nodes of the FCM specify managed objects such as network nodes and the arcs signify the fault propagation model.

3.5 Pattern Matching:

A new approach projected and execute by Maxion and others [17] explain anomalies as variation from normal behavior. This approach effort to deal with the inconsistency in the network surroundings. In this approach, online learning is used to build a traffic profile for a given network. Traffic profiles are built using symptom-specific feature vectors such as link utilization, packet loss, and number of collisions. These profiles are then categorized by time of day, day of week, and special days, such as weekends and holidays. When newly acquired data fails to fit within some confidence interval of the developed profiles then an anomaly is declared.

3.6 Generalized Likelihood Ratio test:

The usual approach for identify a change in a random process is the CUSUM (Cumulative Summation) method and its variation [3]. The main perception behind the CUSUM technique is that when a adjust happen the log-likelihood ratio of an observation yi, defined as si = log L1(y) L0(y), shifts from a harmful value to a positive one (as after the change hypothesis H1 becomes more likely). This means that the log-likelihood of observing a sequence of N observations {yN−1 0}, defined as

SN−1 =PN−1

i=0 si, that was declining with N, begins to increase after the change. The minimum value of Sj gives an estimate of the change point. Therefore a simple statistical test for change detection consists of testing whether:

Sk − min

0≥j≥k

Sj > T,

Where Sk is the log-likelihood ratio distinct previously and T is a threshold. After a change has been detected, the time of change can be projected as: ˆtc = arg min 0≥j≥k {Sj}. The previously explain CUSUM algorithm has been extensively used for anomaly recognition. However it suffers from a key drawback. It is stated in the context of a simple hypothesis, where the alternative hypothesis H1 should be completely defined, i.e. the level of the change or in other terms the intensity of the anomaly should be known a priori. However in practical settings, this is accurately unknown as by definition anomalies are not predictable.

A solution for this issue is afforded by the General Likelihood Ratio Test. In this advance the level of change in the CUSUM algorithm is substitute by its maximum likelihood estimate. To describe the approach let's fix a scenario.

IV. EXPERIMENTAL SETUP:

This Research work design and implemented in NS2. NS (version 2) is an object-oriented, discrete event driven network simulator developed at UC Berkelywritten in C++ and OTcl. NS is primarily useful for simulating local and wide area networks. Tcl is a general purpose scripting language. While it can do anything other languages could possibly do, its integration with other languages has proven even more powerful.

In this section we present the experimental setup of our research work with complete result. As mentioned we use the NS2 to calculate the result. Basically we focus on to detecting and preventing flood and flash crowd anomaly in network. Here we consider the 10 nodes in network and sending the packet at regular interval of time and providing the proper threshold to calculate the anomaly in network. The generalized ratio test can be used to divide the anomalous network. And draw the result through graph.

Flash Crowd Anomaly:

A flash crowd occurs when there is a surge in demand for a service and is typically manifested by a large number of clients trying to access network resources.

Flash-crowd anomalies encompass traffic patterns which are caused by a net growth of (usually human) users trying to access a network resource. Typical flash-crowd anomalies are related to overwhelming web server usage patterns.

Flood anomaly:

Flood anomalies include attacks, or any other circumstances, which result in a net growth of instantaneous traffic. One can think of flood anomalies as having one or more relatively constant traffic sources added to otherwise normal traffic. DDoS attacks typically give rise to anomalies of this kind.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are one of the most common malefic actions over the Internet. This type of attacks consumes the resources of a remote host or network that would otherwise be used to serve legitimate users. Nowadays a diversity of tools is available to accomplish DoS and DDoS

attacks, and packet flooding is one of the most common approaches to accomplish it.

```
Agent/My Agent set my Val 0
Agent/My Agent set bottle_neck 10; #set a bottle neck for the transmissions
Agent/My Agent set RTSEQ 4200; #set some value for RTSEQ
Agent/My Agent set NUM_NODES $opt(num Of Nodes)
Agent/My Agent set PACKET_THRESHOLD 10

#SET THE SOURCES AND DESTINATIONS
Agent/My Agent set source00 $sources (0)
Agent/My Agent set dest00 $dest(0)
Agent/My Agent set source01 $sources (1)
Agent/My Agent set dest01 $dest(1)
Agent/My Agent set source02 $sources (2)
Agent/My Agent set dest02 $dest(2)
Agent/My Agent set source03 $sources (3)
Agent/My Agent set dest03 $dest(3)
Agent/My Agent set source04 $sources (4)
Agent/My Agent set dest04 $dest(4)
Agent/My Agent set source05 $sources (5)
Agent/My Agent set dest05 $dest(5)
Agent/My Agent set source06 $sources (6)
Agent/My Agent set dest06 $dest(6)
Agent/My Agent set source07 $sources(7)
Agent/My Agent set dest07 $dest(7)
Agent/My Agent set source08 $sources (8)
Agent/My Agent set dest08 $dest(8)
Agent/My Agent set source09 $sources (9)
Agent/My Agent set dest09 $dest(9)
Agent/My Agent set source10 9
Agent/My Agent set dest10 2
Agent/My Agent set source11 9
Agent/My Agent set dest11 7
#Agent/My old Agent set my Val_ 10
```

Using Statistical Approach we statistically indicate source & destination. Here we declare source node 1,2,3---& destination source 2,3,4,5 ---.Source 1 will send packet to destination 2 only & so on. If any abnormal activity occurs just like source 1 sends packet to destination 7, then anomaly is detected, called Flash Anomaly. If any node receives large no packet and cross the threshold limit called flood anomaly. If any unwanted movement occurs the packet would not be send.

Experimental Result:

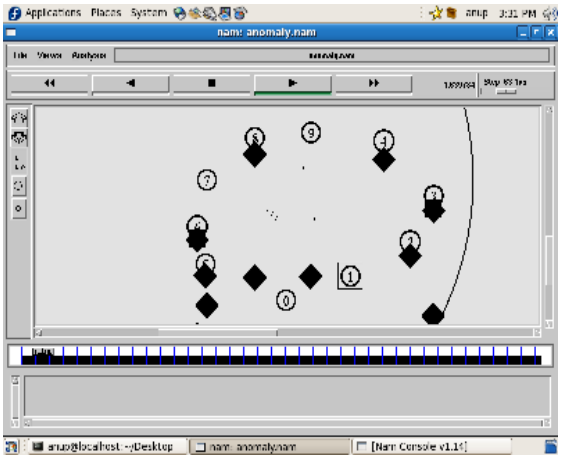

Fig.2 Design of transmission of packet to each node and packet dropping

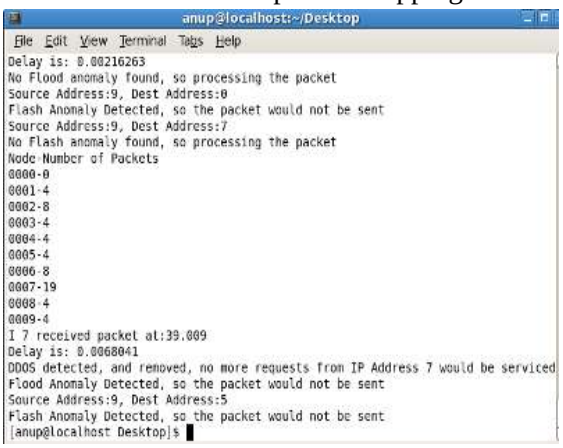

Fig 3 Packet Received by each node and flood anomaly occurs at node I7.

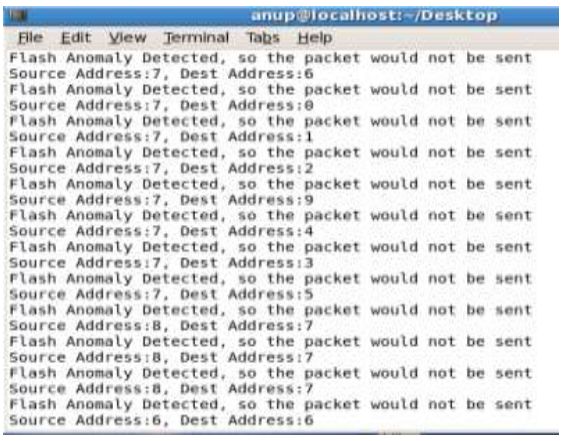

Fig.4 flash anomaly detected result

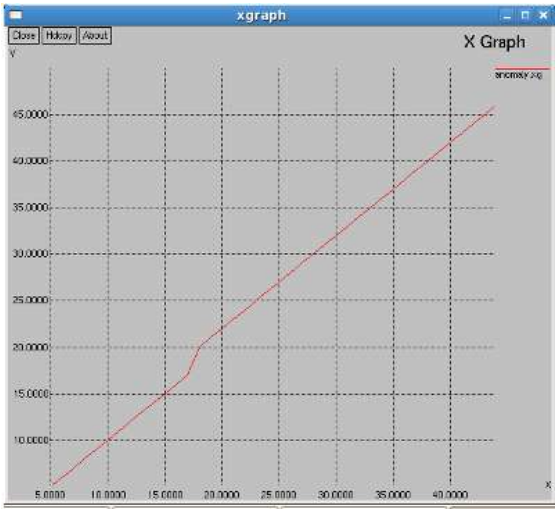

Fig.5 Graph of Anomaly in network. on X-axis= Time and Y-axis= No of anomaly graph

Fig 6. Graph of Flood anomaly. on X- axis= Time and Y-axis= No of anomaly graph

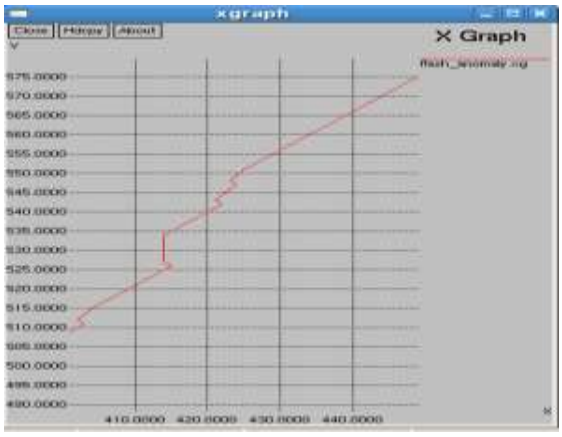

Fig7. Graph of Flash anomaly. On X- axis= Time and Y-axis= No of anomaly

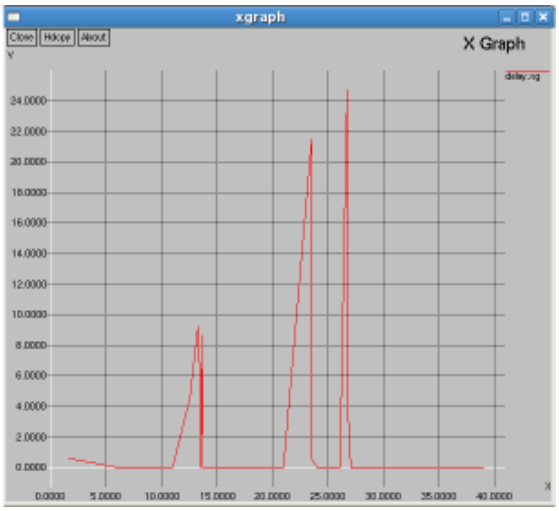

Fig 8. Delay at each node

4.1. α-Stable Distribution as a Model for Network Traffic:

In this sect ion, we will review some statistical distributions which have been previously used to model network traffic, and see how the α-stable model can contribute to enhance traffic modeling. We will do this by looking at Poisson and Gaussian models in detail and stating some traffic properties we found in our data, which should be inherent to traffic coming from any data network. Then, we will see why neither Poisson nor Gaussian models can accommodate to these properties and try to answer the question of whether the α-stable model does.

V. Network traffic representation

Conventionally, network traffic has been model as a Poisson process for past reasons. Indeed, the Poisson model has been successfully utilize in telephone networks for many years, and so it was native when telecommunication networks became digital and started to send in order as data Packets [1]. Also, this model has a simple mathematical expression [1], and has only one parameter, λ, which is in turn very natural (the mean traffic in packets per time unit). In the last decade, however, several authors have considered network traffic behavior and proposed other models that conquer the limitations which are inherent to Poisson processes, the most notable one probably being that the Poisson model has a fixed relationship between mean and variance values (both are equal to λ).

More recently proposed models are usually found on the hypothesis that network traffic is self–similar in nature, a statement that was made in [26] for the first time. Naturally, network traffic can be contemplation of as a self–similar process because it is usually "busty" in nature, and this burstiness tends to emerge separately of the used time scale. Thus, in [26] FBM [26] is shown to fit accumulated network traffic data.

A proper model for instantaneous network traffic must be flexible enough to adapt to some properties seen in sampled traffic, namely: The amount of traffic accumulated at time t1 is less than, or equal to the amount of traffic accumulated at time t2, for every t1 < t2; that is, traffic increments are greater than, or equal to zero.

The fact that at time t there is a certain amount of traffic C does not imply in any way that at time t+1 the amount of traffic lies anywhere near C, due to the inherent nature of network traffic, which is often burst and tends to show peaks from time to time. The latter property says that the variation in traffic from one time tick to the next one can be very large, On the other hand, the first aforementioned property makes symmetric distributions (Gaussian and Poisson distribution are symmetric) inappropriate, because if traffic data concentrates near the vertical axis, the model would allow negative traffic increments, and this can never be the case. Accordingly, if

Traffic data concentrates near the maximum transmission rate; a symmetric model would allow traffic increments to be larger than physically possible.

5.1. The α–stable Representation:

α–stable distributions can be consideration of as a superset of Gaussians and originate as the solution to the Central Limit Theorem when 2nd–order moments do not exist [24], that is, when data can abruptly change by huge amounts as time passes by. This fits nicely to the second of the talk about properties seen in network traffic. Moreover, α–stable distributions have an asymmetry parameter which allows their PDF to vary between totally left–asymmetric to totally right–asymmetric. While Poisson and Gaussian distributions are always symmetric. This parameter makes α–stable distributions fit logically to the first traffic property, even when average traffic is practically 0 or very near the maximum theoretical network throughput. In addition, α–stable distributions give an explanation to the restriction imposed in [26] about the need to aggregate so many traffic traces for them to converge to a Gaussian distribution. According to the Generalized Central Limit Theorem [30], which contains the infinite variance case, the sum of n α–stable distributions is another α–stable distribution, although not necessarily a Gaussian one. Since traffic data often has a huge variance (though obviously not infinite), and Under the hypothesis that it is α–stable, then the sum of a few traces will be α–stable but not Gaussian. However, after summing so many traces enough to overcome the enormous variance, the final histogram will converge to a Gaussian curve, as the traditional Central Limit Theorem states.

VI. Conclusion:

This paper has presented idea about the statistical anomaly detection of network traffic. Here paper studied a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior This paper also discussed a method to recognize anomalies in network traffic, based on a non-restricted α-stable model and statistical hypothesis testing.

VII. References:

[1]. Federico Simmross, Juan Ignacio, Pablo Casaseca-de-la-Higuera, Ioannis A. Dimitriadis" Anomaly Detection in Network Traffic Based on Statistical Inference and α-Stable Modeling" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 4, JULY/AUGUST 2011

[2] M. Thottan and C. Ji, "Anomaly Detection in IP Networks," IEEE Trans. Signal Processing, vol. 51, no. 8, pp. 2191-2204, Aug. 2003.

[3] C. Manikopoulos and S. Papavassiliou, "Network Intrusion and Fault Detection: A Statistical Anomaly Approach," IEEE Comm. Magazine, vol. 40, no. 10, pp. 76-82, Oct. 2002.

[4] Y. Gu, A. McCallum, and D. Towsley, "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation," Proc. Internet Measurement Conf., Oct. 2005.

[5] BARFORD, P., KLINE, J., PLONKA, D., AND RON, A. A signal analysis of network traffic anomalies. ACM Sigcomm IMW (2002).

[6] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies," Proc. Second ACM SIGCOMM Workshop Internet Measurement, pp. 71-82, Nov. 2002

[7] Huy Anh Nguyen, Tam Van Nguyen, Dong Il Kim, Deokjai Choi " Network Traffic Anomalies Detection and Identification with Flow Monitoring"

[8] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.

[9] A. Wagner and B. Plattner, "Entropy Based Worm and Anomaly Detection in Fast IP Networks," Proc. 14th IEEE Int'l Workshops Enabling Technologies: Infrastructures for Collaborative Enterprises, pp. 172-177, June 2005

[10] M. Ramadas, S. Ostermann, and B. Tjaden, "Detecting Anomalous Network Traffic with Self-Organizing Maps," Proc. Sixth Int'l Symp. Recent Advances in Intrusion Detection, pp. 36-54, 2003.

[11] S.T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchical Kohonen Net for Anomaly Detection in Network Security," IEEE Trans. Systems, Man and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.

[12] A. Soule, K. Salamatian, and N. Taft, "Combining filtering and statistical methods for anomaly detection," in Proceedings of ACM SIGCOMM conference on Internet Measurement (IMC), 2005

[13] D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K. Salamatian, "Anomaly extraction in backbone networks using association rules," in Proceedings of ACM SIGCOMM conference on Internet Measurement (IMC), 2009.

[14] F. Silveira and C. Diot, "URCA: Pulling out anomalies by their root causes," in Proceedings of IEEE INFOCOM, 2010

[15] G. Samorodnitsky and M.S. Taqqu, Stable Non-Gaussian Random Processes: Stochastic Models with Infinite Variance. Chapman & Hall, 1994.

[16] F. Simmross-Wattenberg, A. Trista´n-Vega, P. Casaseca-de-la Higuera, J.I. Asensio-Pe´rez, M. Martı´n-Ferna´ndez, Y.A. Dimitriadis, and C. Alberola-Lo´pez, "Modelling Network Traffic asα-Stable Stochastic Processes: An Approach Towards Anomaly Detection," Proc. VII Jornadas de Ingenierı´a Telema´tica (JITEL), pp. 25-32, Sept. 2008

[17] G.R. Arce, Nonlinear Signal Processing: A Statistical Approach. John Wiley and Sons, 2005.

[18] J. Jiang and S. Papavassiliou, "Detecting Network Attacks in the Internet via Statistical Network Traffic Normality Prediction," J. Network and Systems Management, vol. 12, no. 1, pp. 51-72, Mar. 2004.

[19] W. Yan, E. Hou, and N. Ansari, "Anomaly Detection and Traffic Shaping under Self-Similar Aggregated Traffic in Optical Switched Networks," Proc. Int'l Conf. Comm. Technology (ICCT '03), vol. 1, pp. 378-381, Apr. 2003.

[20] A. Soule, H. Ringberg, F. Silveira, and C. Diot. Challenging the supremacy of traffic matrices in anomaly detection. *IMC '07*, pages 105{110, 2007. (Cited on pages 13 and 40.)

[21] A. Lakhina, M. Crovella, and C. Diot. Mining anomalies using traffic feature distributions. *SIGCOMM '05*, pages 217{228, 2005. (Cited on pages 12, 13, 25, 32, 40, 48, 57, 91 and 96.)

[22] [48] X. Li, F. Bian, M. Crovella, C. Diot, R. Govindan, G. Iannaccone, and A. Lakhina. Detection and identi_cation of network anomalies using sketch subspaces. *IMC '06*, pages 147{152, 2006. (Cited on pages 3, 5, 12, 13, 22 and 57.)

[23] S. S. Kim and A. L. N. Reddy. A study of analyzing network traffic as images in real-time. *INFOCOM '05*, pages 2056{2067, 2005. (Cited on pages 14 and 32.)

[24] L. I. Kuncheva. *Combining Pattern Classi_ers: Methods and Algorithms*. Wiley-Interscience, 2004. (Cited on pages 15 and 61.)

[25] S. Shanbhag and T. Wolf. Accurate anomaly detection through parallelism. *Netwrk. Mag. of Global Internetwkg.*, 23(1):22{28, 2009. (Cited on page 16.)

[26] [V. Alarcon-Aquino and J.A. Barria, "Anomaly Detection in Communication Networks Using Wavelets," IEE Proc.—Comm.,vol. 148, no. 6, pp. 355-362, Dec. 2001

[27] "Metrology for Security and Quality of Service," http://www.laas.fr/METROSEC/, 2011

[28] " Anup Bhange, Amber Syed , Satyendra Singh Thakur" "ANOMALY DETECTION BASED ON DIVERSE APPROACHES IN NETWORK TRAFFIC" IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905

[29]" Anup Bhange, Amber Syed, Satyendra Singh Thakur" DDoS Attacks Impact on Network Traffic and its Detection Approach" International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.

[30] DDoSVax, http://www.tik.ee.ethz.ch/ddosvax/, 2010

[31]] "Anup Bhange, Amber Syed" To Detect and Prevent the anomaly in Network Traffic Based on Statistical approach and α-stable Model "International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 3, May2012 ISSN: 2278 – 1323"