Analysis of Malicious Traffic and Its Impact to QoS Metric LRD and Energy Invariant

Mohd Fo'ad Rohani [1] , Mohd Aizaini Maarof [2], Ali Selamat [3]
Faculty of Computer Science and Information Systems,
University Teknologi Malaysia,
81300 Skudai, Johor.
Email: foad@fsksm.utm.my [1], maarofma@fsksm.utm.my [2], aselamat@fsksm.utm.my [3]

ASTRACT

The Internet is evolving from a single best effort service to a multi-services network. The success of the Internet has increased its vulnerability to misuse and performance problems. The existence of network anomaly packets inside normal traffic can decrease QoS performance substantially. These anomalous events can provoke some changes in the QoS perceived by all users of the network, and then break the service level agreement (SLA) at the Internet service. It is hard to detect and distinguish malicious packet and legitimate packets in the traffic. The reason is behavior of Internet traffic is very far from being regular, and presents large variations in its throughput at all scales due to self-similarity, multi- fractality and long-range dependence (LRD). The aim of this paper is to analysis the impact of malicious network attacks (host and network attacks) on network second order QoS metric. The dynamic traffic behavior is characterized by LRD and Energy Invariant change. These changes in the LRD function and Energy Invariant therefore can give direction of developing more robust network anomaly detection. We use benchmark DARPA for our data testing. From the experiments we categorize the QoS impact into three categories: increase LRD, imitate LRD and decrease LRD.

KEYWORDS

Anomaly Attacks, QoS, LRD, Energy Invariant, Wavelet Analysis

1.0 Introduction

The Internet has evolved from the era of time-sharing into the era of personal computers, client/server and peer-to-peer computing, and the network computer. Internet services is now changing to provide such new services as real-time transport, supporting, for example, audio and video streams. Thus Internet is migrating from a single best effort service to a multi-services network. However, the success of the Internet has increased its vulnerability to misuse and performance problems [12]. Internet service providers are now faced with the challenging task of continuous monitoring of their network to ensure that security is maintained. The existence of network anomaly packets inside normal traffic can decrease QoS performance substantially. Network anomalies can be categorized as malfunctioning network devices, network overload, malicious denial of service attacks, and network intrusions [7]. These anomalous events can provoke some changes in the QoS perceived by all users of the network, and then break the service level agreement (SLA) at the Internet service.

It is hard to detect and distinguish malicious packet and legitimate packets in the traffic. The reason is behavior of Internet traffic is very far from being regular, and presents large variations in its throughput at all scales. Recent studies have shown that Internet traffic exhibits characteristics such as self-similarity [4], multi- fractality [13], and long-range dependence (LRD) [14], which is to say in all cases that traffic can vary significantly. In addition, given the highly variable nature of Internet traffic, anomaly based IDS are raising alarms for many disruptions that are not attacks. The high rate of false positives is one of the major shortcomings of current IDS and the current evolution of Internet traffic with larger and larger variations among time continues to limit the efficiency of anomaly based IDS.

The work in [1] proposes a new QoS metric parameter to analysis the characteristics of current Internet traffic. The studies comparatively analyze the characteristics of normal traffic, and traffic containing DoS attacks, trying to isolate the parameters responsible of the QoS degradation. The result show that DoS attacks break the "invariant" power laws (we call as Energy Invariant) of the LRD function, and introduce more LRD in the global

traffic, and then more disturbances for QoS. The analysis shown LRD has a very bad impact on network QoS [11] and the use of network resources is far from being optimal. Further result shows LRD can be a good parameter to characterize the variability of Internet traffic and also for quantifying the level of QoS (the higher the LRD, the worse the QoS) [11] [15].

The aim of this paper is to analysis the impact of malicious network attacks (host and network attacks) on network second order QoS metric. The dynamic traffic behavior is characterized by LRD and Energy Invariant change. These changes in the LRD function and Energy Invariant therefore can give direction of developing more robust network anomaly detection. This paper is constructed as follows: section 2 discuss the concept of self similar model and LRD, section 3 discuss wavelet analysis and energy invariant law, section 4 discuss experiment procedure and result, and finally section 5 gives conclusion and future work.

2.0 Self Similar Model and LRD

Before the early 1990s traffic and performance studies had been predominantly based on models such as Poisson processes which have no long-term correlation structure. Such models are attractive because of their mathematical tractability and the large body of queuing theory which relies on the assumption of Poisson processes. In 1993, the seminal paper [4], [5] found evidence of long-range correlation in LAN traffic and brought the concept of self-similarity (and the related concept of long-range dependence (LRD) into the field of network traffic and performance analysis.

LRD means that the behavior of a time-dependent process shows statistically significant correlations across large time scales. Self-similarity describes the phenomenon in which the behavior of a process is preserved irrespective of scaling in space or time. Unlike Poisson processes packet arrival process is memory-less and inter arrival times follow the exponential distribution. The knowledge of LRD states that network traffic always exhibit long- term memory (its behavior across widely separated times is correlated). This statement challenged the validity of the Poisson assumption and shifted the community's focus from assuming memory less and smoothes behavior to assuming long memory and bursty behavior.

2.1 Statistical Sampling and Second Order Model

Let Xi be a second-order stationary process with mean, variance, and covariance μ, σ^2, and $\gamma(k)$, respectively. The sample mean and the sample covariance are given by the following formulas:

$$\mu_n = \frac{1}{n}\sum_{i=1}^{n} X_i$$

and

$$\gamma_n(k) = \frac{1}{n}\sum_{i=1}^{n-k} (X_i - \mu_n)\ (X_{i+k} - \mu_n)$$

where n is the number of samples to be used. The sample variance is given by

$$\sigma_n^2 = \gamma_n(0)$$

Likewise, the sample autocorrelation is given by

$$r(k) = \frac{\gamma_n(k)}{\sigma_n^2}$$

Second-order self-similarity describes the property that a time series correlation structure (ACF) is preserved irrespective of time aggregation. Simply put, a second-order self-similar time series ACF is the same for either coarse or fine time scales. A stationary process X_t is second-order self- similar if $0.5<H<1$

$$r(k) = \frac{1}{2}[(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}] \quad ,$$

and asymptotically exactly self-similar if

$$\lim_{k\to\infty} r(k) = \frac{1}{2}[(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}]$$

2.2 Long-range dependence (LRD)

In second-order stationary for $0<H<1$, $H\neq 0.5$, autocorrelation function $r(k)$ holds

$$r(k):\ H(2H-1)k^{2H-2} \quad ,k \to \infty$$

In particular, if $0.5<H<1$, $r(k)$ asymptotically behaves as $ck^{-\beta}$

$$r(k):\ c_r k^{-\beta}$$

for $0<\beta<1$ where $c_r > 0$ is a constant, $\beta=2-2H$, and we have

$$\sum_{k=-\infty}^{\infty} r(k) = \infty$$

That is, the autocorrelation function decays slowly (hyperbolically) which is the essential property that causes it to be not summable. When $r(k)$ decays hyperbolically such that condition

$\sum_{k=-\infty}^{\infty} r(k) = \infty$ holds, we call the corresponding stationary process X(t) LRD. X(t) is *short-range dependent (SRD)* if the autocorrelation function is summable.

3.0 Wavelet analysis and Energy Invariant

Wavelet techniques are one of the most up-to-date modeling tools to exploit both non-stationary and long-range dependence [3], [8]. Wavelet analysis can reveal scaling properties of the temporal and frequency dynamics simultaneously unlike Fourier Transform which can only reveals frequency properties. The wavelet transform can thus be thought of as a method of simultaneously observing a time series at a full range of different scales, whilst retaining the time dimension of the original data.

A time series $x(t)$ can be represented by wavelet transformation with coarser approximation and details at different resolutions [3]:

$$x(t) = approx_J(t) + \sum_{i=1}^{j=J} detail_j(t)\sigma_X^2$$

$$= \sum_k a_x(J,k)\phi_{J,k}(t) + \sum_{j=1}^{J}\sum_k d_x(j,k)\varphi_{j,k}(t)$$

The $approx_j$ essentially being coarser approximations of x means that ϕ_0 (scaling function) needs to be a low-pass function. The $detail_j$, being an information "differential," indicates φ_0 (mother wavelet) is a bandpass function. The chosen of mother wavelet must satisfy $\int \phi_0(t)dt = 0$ and that its Fourier transform obeys $|\psi_0(v)| \sim v^N, v \to 0$ where N is a positive integer called the number of vanishing moments of the wavelet.

Given a scaling function ϕ_0 and mother wavelet φ_0, the discrete (or non-redundant) wavelet transform (DWT) is a mapping process from $L^2(R) \to l^2(Z)$, given by

$$x(t) \to \{\{a_X(J,k), k \in Z\}, \{d_X(j,k), j = 1,2,...,J, k \in Z\}\}$$

These coefficients are defined through inner products of with two sets of functions:

$$a_X(j,k) = \langle x, \phi_{j,k} \rangle \quad and \quad d_X(j,k) = \langle x, \varphi_{j,k} \rangle,$$

where $\phi_{j,k}$ and $\varphi_{j,k}$ are defined as wavelet scaling function and wavelet basis function respectively. The basis is constructed from the dilation (change of scale) operator:

$\{\varphi_{j,0}(t) = 2^{-j/2}\varphi_0(2^{-j}t)\}$. This means that the analyzing family exhibits a scale invariance feature.

The LRD phenomenon can be understood as the absence of any characteristic frequency (and, therefore, scale) in the range of frequencies close to the origin. The LRD property can thus be interpreted as a scale invariance characteristic which is efficiently analyzed by wavelets. For a process with a power-law spectrum such as a LRD process, these features create the following key properties of the wavelet coefficients $d_X(j,k)$ over a range of scales 2^j, $j = j_1 ... j_2$, where the power-law scaling holds [3][8].

The scale invariance (the power-law behavior) is captured exactly as

$$\mathrm{E}\, d_X(j,\cdot)^2 = 2^{j\alpha} c_f C \quad \text{where}$$

$$\mathrm{C} = \int |v|^{-\alpha} |\psi_0(v)|^2 \, dv.$$

Define $\log_2$(scale)=octave j, we can derive

$$\log_2(\mathrm{E}\, d_X(j,\cdot)^2) = j\alpha + \log_2(c_f C)$$

The details $d_X(j,k)$ are a collection of random variables; we use "time average" to define $\mu_j = \frac{1}{n}\sum_{k=1}^{n_j} d_X^2(j,k)$ where n_j is the number of coefficients at octave j available to be analyzed.

This quantity is an unbiased and efficient estimator of $\mathrm{E}\, d_X(j,\cdot)^2$. Nonlinearity is introduced by the $\log_2$ which biases the estimation. From the plot of $y_j = \log_2(\mu_j)$ against j, the *Logscale Diagram*, the scaling range $\{j_1, j_2\}$ where scaling occurs (i.e., where the y_j fall on a straight line) can be determined. The nalysis using the Logscale Diagram between scaling range $\{j_1, j_2\}$ (octave $\{j_1, j_2\}$) will determine Energy Invariant properties in the scaling range $\{j_1, j_2\}$.

3.1 QoS metrics LRD and Energy Invariant

A drawback of current QoS performance results is that they concentrate on first-order performance measures that relate to packet loss rate but less so on second-order measures e.g., variance of packet loss or delay (generically referred to as jitter which are of import in multimedia communication). The confusion of first order metric is described as follow. Two loss processes may have the same first-order statistic but if one has higher variance than the other in the form of concentrated periods of packet loss (as is the case in self-similar traffic) then this can adversely impact the efficacy of packet-level forward error correction

used in the QoS-sensitive transport of real-time traffic [10][17]. Even less is known about transient performance measures which are more relevant in practice when convergence rate is too slow as in the case of LRD and self similar in network traffic.

A pioneering effort [1] has introduced second order QoS metric base on LRD and Energy Invariant. It has been shown that the existence of denial of service attacks (DoS) in the normal traffic packets, the level of LRD is increased significantly. The properties of Energy Invariant also are also changed clearly. We extend of the finding to study how network malicious attack impact the behavior of second order QoS metric LRD and Energy Invariant in details.

4.0 Experiment and Result

4.1 Tools and Data

The experiments are using simulation benchmark data of efense Advanced Research Projects Agency (DARPA99) [16] of first and second week. In the simulation, activities in first week are known as normal activities while in second week contain normal and label attack. The label malicious attacks are categorized into Denial of Service Attacks (DoS), User to Root Attacks (U2R), Remote to Local Attacks (R2L) and Probes attacks (probing). Table 1 shows attacks that incorporate in second week and group as follows:

- Denial of Service Attacks (back, crashiis, land, mailbomb, SYN flood (neptune), ping of death (pod), smurf, udpstorm)
- User to Root Attacks (eject , loadmodule , perl, ps)
- Remote to Local Attacks (guest, httptunnel, imap, phf)
- Probes (ipsweep, NTinfoscan, nmap, satan)

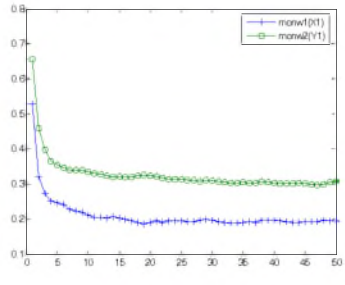
U2R, R2L and probing attacks are classified as host attack and DoS attacks as network attack. The aim of host attack is trying to disrupt host system activities while network attack aims to disrupt bandwidth resource. Both activities degrade the performance of normal operation.

4.2 Testing Procedure

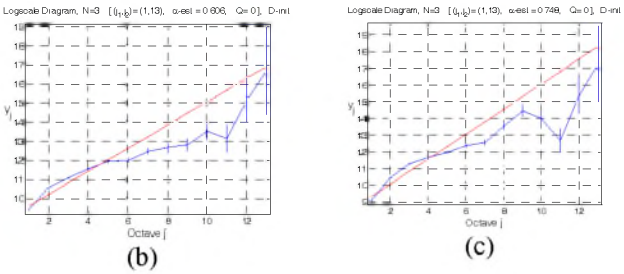
We are more interested to use this packet traces to investigate the impact of known network intrusion attack towards second order QoS metric LRD and Energy Invariant. We test DARPA data and try to understand how the changes occurred in details. We make assumption that the activities of DARPA data are defined as daily routine. Therefore, as our comparison purpose we compare the traces according to daily activities in the following week. We divide our experiments into three cases. We use second order model and autocorrelation r(k) to evaluate LRD and Hurst value [9] and wavelet model [3][8] to evaluate Energy Invariant effect.

Table 1. Packet traces of DARPA99 first and second week

Packet Traces	First Week (Activities)	Second Week (Activities)	Attack traces detected
Mon	Normal	Normal and label attack	NTinfoscan, pod, back, httptunnel, land, secret, ps attack
Tues	Normal	Normal and label attack	Portsweep, eject, back, loadmodule, secret, mailbomb, ipsweep, phf, httptunnel
Wed	Normal	Normal and label attack	Satan, mailbomb, perl (failed), ipsweep, eject (console), crashiis



(a)



(b) (c)

Figure 1. Comparison QoS metric indicator for LRD (r(k)) packet traces MonW1 and MonW2 (a) and Energy Invariant packet traces MonW1 (b) and MonW2 (c)

Case I

Firstly we compare the packet traces on Monday of first and second week and Figure 1 depicts the result. The existence of the injected attack on Monday on second week has increased the value of LRD significantly and clearly shown in Figure 1(a). From figure 1(b) and (c) show Energy Invariant has changed slightly at higher scale at octave j>8.

Case II

Second traces of interest are comparing packet traces on Tuesday of first and second week and Figure 2 depicts the result. From Figure 2(a) the LRD effect of both traces are not significantly shown. The LRD impact of the injected malicious packet upon normal packet traces is slightly small. The slope of Energy Invariant is start to change slightly at higher scale octave j>10.

Case III

Lastly we compare traces on Tuesday of first and second week and the result is shown at Figure 3. From Figure 3(a), we can see a significant impact of LRD change. However, it contrasts with result on case I. Malicious packets that exist in overall packet traces on second week reduce significantly of LRD metric. From LRD impact, the malicious packets seem not dragging queuing delay at the router. However, the changes of Energy Invariant at Figure 3(b) and (c) are quite obvious. The pattern of the slope totally changes at octave scale > 3.

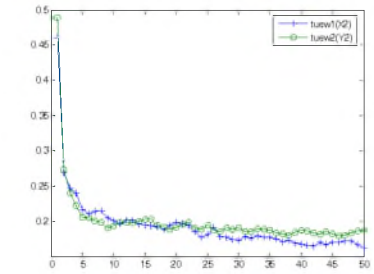
Table 2 shows the estimated Hurst value of the packet traces for first and second week of DARPA99 data. All estimated Hurst values are following second order self similar model since the error is less than 0.001.

Table 2. Estimated Hurst of packet traces.

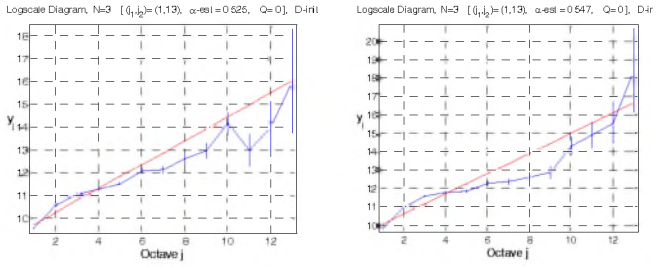
Packet traces	Day	Hurst H	Error
Week 1	Mon	0.83	0.0004365500
	Tues	0.82	0.0004489600
	Wed	0.84	0.0004653800
Week 2	Mon	0.88	0.0004998800
	Tues	0.82	0.0006010200
	Wed	0.79	0.0006627200

4.3 Discussion

We raise several points to discuss. We agreed that the existence of malicious packet especially DoS packet will change the behavior of QoS metric LRD and Energy Invariant. However, the patterns of the impact changes are unpredictable. Pioneering result of second order QoS metric [1] shows that in the existence of DoS attack traces, it will raise the level of LRD and add additional Energy Invariant slope.

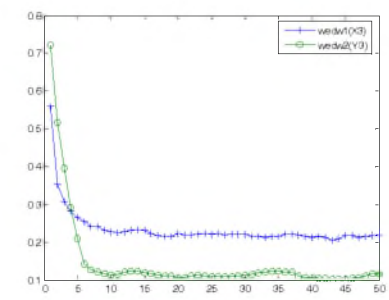


(a)

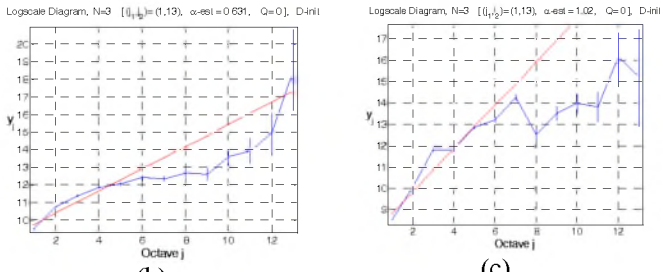


(b) (c)

Figure 2. Comparison QoS metric indicator for LRD (r(k)) packet traces TuesW1 and TuesW2 (a) and Energy Invariant packet traces TuesW1 (b) and TuesW2 (c)



(a)



(b) (c)

Figure 3. Comparison QoS metric indicator for LRD(r(k)) packet traces WedW1 and WedW2 (a) and Energy Invariant packet traces WedW1 (b) and WedW2 (c)

The effects align with our observation as shown on Figure 1(a),(b) and (c). The Hurst value has increased from H=0.83 to H=0.88. However, this assumption is not always true. The portion of mixed packets DoS and other malicious packets throughout overall normal traffic will shape the pattern of QoS metrics behavior. Figure 2(a),(b) and (c) show the impact of malicious packets which are not strong enough to change the overall normal traffic behavior. Even though on that normal traffic is injected by DoS and other malicious packet, the portion on the injected is not enough to change the overall behavior of LRD and Energy Invariant. The estimated of Hurst value is unchanged which is H=0.82. The effect of buffer queue delay at switching point is not affected much as compare to the increasing of LRD effect.

The last observation through this experiment is the portion of injected malicious are reducing the LRD and Energy Invariant effect tremendously. It is contrast with the purpose of malicious packet injected to the normal traffic specifically to reduce the bandwidth resources and degrade the performance. Figure 3(a),(b) and (c) support the argument. In Figure 3(a) the impact of LRD is reduced from higher level to lower level drastically (like exponential decay). This phenomenon is quite strange especially if the packet traces contain malicious. However, without the appearance of DoS attack the impact of LRD shifting is not cleared. Figure 3(b) and (c) show that the normal behavior of Energy Invariant slope has totally changed. The track changes occur either at lower or higher octave scale. The estimated Hurst value for the traces reduce from normal activities H=0.84 to packet traces containing label attacks H=0.79. This significant reduction will reduce queue delay interval at router buffer despite the existence of label attacks in the traffic. The reason for this explanation could be the overall normal activities have been reduced relatively and the label attacks packets are containing a small portion of DoS attacks.

5.0 Conclusion and Future Works

This research is an extension of pioneering work done by [1] to investigate the impact of malicious attack to second order QoS metric LRD and Energy Invariant. We characterize the impact of malicious towards LRD and Energy Invariant into three. The first category is increasing the level of LRD effect with significant value. Hurst value of normal traffic will largely reduce and queue delay of router is increased. The second category is imitating impact on normal traffic behavior. This type of malicious traffic is very difficult to capture because they try to imitate the normal behavior of network traffic. The Hurst value has very minor changes. It is worst if Hurst value does not change and network administrator will face difficulties to react to the situation. The third category is more confusing. The impact is reducing LRD significantly. Network administration will make false assumption of network health condition. The reduction of LRD as well as Hurst value, indicates that network become more healthy and no worries about malicious. However, as our early experiments show the existence of malicious are buried under the normal traces event though LRD (or Hurst value) is reduced. Furthermore, Energy Invariant changes can reveal the details of malicious packets that exist inside normal traffic packets. Our future research work is to study how to quantify in accurate second order QoS metric LRD and Energy Invariant to represent more meaningful information. Our aim is to develop more robust anomaly detection by considering the impact of anomaly traffic to QoS metric measurement.

Acknowledgements

This research is supported by UTM.

References

[1] P. Owezarski, *On the impact of DoS attacks on Internet traffic characteristics and QoS*, 14th IEEE International Conference and Computer Communications and Networks (ICCCN'2005), San Diego, CA, USA, 17-19 October 2005

[2]. A.Habib, S.Fahmy, S.R.Avasarala, V.Prabhakar and B.Bhargava, *On detecting service violations and bandwidth theft in QoS network domains*, Computer Communications, Volume 26, Issue 8, 20 May 2003, Pages 861-871

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

[4] W. Leland, M. Taqqu, W.Willinger and D.Wilson, *On the self-similar nature of Ethernet traffic*, Proc. of ACM SIGCOMM 23(4) (1993) 183–193

[5] W. Leland, M. Taqqu, W. Willinger and D. Wilson, *On the self-similar nature of Ethernet traffic (extended version)*, IEEE/ACMTransactions on Networking 2(1) (1994) 1–15

[6] R. H. Riedi, M. S. Crouse, V. J. Ribeiro, and R. G.Baraniuk. *A multifractal wavelet model with application to network traffic*, IEEE Special Issue On Information Theory, 45(April):992-1018, 1999

[7] Thottan, M.; Chuanyi Ji, *Anomaly detection in IP networks*, Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on Volume 51, Issue 8, Aug. 2003 Page(s):2191 – 2204

[8] Veitch, D.; Abry, P, *A wavelet-based joint estimator of the parameters of long-range dependence*, IEEE Transactions on Information Theory Volume 45, Issue 3, April 1999 Page(s):878 - 897

[9] M .Kettani (2002); *A Novel Approach to the Estimation of the Long-Range Dependence Parameter*, University of Wisconsin – Madison : PhD. Thesis (2002)

[10] K. Park and W. Willinger. *Self-similar network traffic: An overview*, Self-Similar Network Traffic and Performance Evaluation, Wiley-Interscience, 2000

[11] P. Owezarski, N. Larrieu, *Internet traffic characterization – An analysis of traffic oscillations*, International Conference on High Speed Networks and Multimedia Communications (HSNMC), Toulouse, France, June 30 - July 2, 2004

[12] A.Habib, S.Fahmy, B.Bhargava, *Monitoring and controlling QoS network domains*, International Journal of Network Management, Volume 15 Issue 1, pp 11-29, January 2005

[13] Abry, P.; Baraniuk, R.; Flandrin, P.; Riedi, R.; Veitch, D.,*Multiscale nature of network traffic*, Signal Processing Magazine, IEEE Volume 19, Issue 3, May 2002 Page(s):28 - 46

[14] A. Veres, Kenesi S. Molnár, G. Vattay, *On the propagation of long-range dependence in the Internet*, ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication SIGCOMM '00, Volume 30 Issue 4 , August 2000

[15] K. Park, G. Kim and M. Crovella, *On the Effect of Traffic Selfsimilarity on Network Performance*, SPIE International Conference on Performance and Control of Network Systems, November, 1997.

[16] MIT Lincoln Laboratory. DARPA Intrusion Detection Evaluation. Available on line http://www.ll.mit.edu/IST/ideval/, 1999.

[17] T. Tuan and K. Park. *Multiple time scale redundancy control for QoS-sensitive transport of real-time traffic*, In Proc. IEEE INFOCOM '00, pp. 1683-1692, 2000.