Uncovering Anomaly Traffic Based on Loss of Self-Similarity Behavior Using Second Order Statistical Model

Mohd Fo'ad Rohani[†], Mohd Aizaini Maarof[†], Ali Selamat[†] and Houssain Kettani[††],

[†]Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
81300 Skudai, Johor
[††]Department of Electrical and Computer Engineering and Computer Science
Polytechnic University of Puerto Rico
P. O. Box 192017
San Juan, PR 00919, USA

Summary
Malicious traffic such as denial of service (DoS) attack has potential to introduce distribution error and perturbs the self-similarity property of network traffic. As a result, loss of self-similarity (LoSS) is detected which indicates poor quality of service (QoS) performance. In order to fulfill the demand for high speed and detection accuracy, this paper proposes LoSS detection method with second order self-similarity statistical (SOSS) model and estimates the self-similarity parameter using the optimization method (OM). We investigate the behavior of self-similarity property for normal and abnormal traffic traces with different sampling levels. We test our approach using synthetic and real traffic simulation datasets. The results demonstrate that the proposed method has successfully exposed the abnormality of Internet traffic behavior. However, the experimental results show that fixed sampling level is not sufficient to reveal the self-similarity distribution error accurately. Accordingly, we introduce a new set of multi-level sampling parameters and propose a new LoSS detection method with multi-level sampling approach in order to improve the detection accuracy.

Key words:
Anomaly Detection, Loss of Self-Similarity, Second Order Self-Similarity model, Multi-Level Sampling

1. Introduction

The concept of self-similarity and long-range dependence (LRD) for local area network (LAN) traffic and performance analysis was presented in [8] and [9]. Their finding in [8] and [9] had described the self-similarity as traffic behavior is preserved irrespective of scaling in time or space while the LRD indicates that network traffic behavior across widely separated times is correlated. This finding was in contrast to widely accepted Poisson model of the network traffic, which is memoryless and inter-arrival times are exponentially distributed. The finding also challenged the validity of the Poisson assumption and shifted the community's focus from assuming memoryless and smooth behavior network traffic to assuming LRD and bursty behavior. Several causes of the self-similarity phenomenon were pointed out such as the mixed behavior of TCP services model [15], the mixture of actions from individual users, hardware and software in interconnecting networks [3] and the heavy-tailed distribution of large file sizes transferred [3].

The work done in [4] and [14] have demonstrated that the uncontrolled self-similarity structure would congest network buffer hence degrades the quality of service (QoS) performance by drastically increasing queuing delay and packet loss. Therefore, protocol intensity distribution plays an important role in the interactions that produce self-similarity behavior as discussed in [15]. For example, denial of service (DoS) attacks with very high bit rate injection packets dominate the traffic protocol and produce distribution error. As a result, the property of self-similar behavior is disturbed [17] and loss of self-similarity (LoSS) behavior is detected as shown in [1], [10], [17], [18]. This can be used as a flag to alert security analysts of the possible presence of a malicious action as illustrated in [1] and [11], provided that the normal traffic background is self-similar (which is a common network traffic attribute).

The work introduced in [1] has presented a technique for detecting the possible presence of new DoS attacks without a template of the background traffic. The method used LoSS definition with the self-similarity or Hurst parameter H beyond normal self-similarity interval (0.5, 1) using the periodogram and the Whittle methods. The method has high anomaly detection rate with an average of 60% to 84%. However, new methods of estimating Hurst parameter which is more accurate and faster had been developed such as the optimization method (OM) [5], [6] which used the second order self-similarity statistical (SOSS) model. Therefore, we propose LoSS detection method using SOSS model and estimate H using OM. The

Manuscript received September 5, 2007
Manuscript revised September 20, 2007

remainder of this paper is organized as follows: Section 2 presents mathematical definitions and properties of SOSS and how to estimate its parameter. Section 3 on the other hand, discusses the concept of LoSS detection and related work. Section 4 explains the datasets that were used in the simulations while Section 5 presents our experiment procedure and the results. Finally our conclusions and future work directions are summarized in Section 6.

2. SOSS Statistical Model

Let $X = \{X(t), t = 0,1,2,....,N\}$ be a second-order stationary process with constant mean μ, finite variance σ^2, and autocorrelation function $\rho(k)$ that depends only on the integer *k*. Their definitions are given as follows:

$$\mu = E[X(t)],\ \ \sigma^2 = E[(X(t)-\mu)]^2$$

$$\rho(k) = E[(X(t)-\mu)(X(t+k)-\mu)]/\sigma^2$$

Let $X^{(m)} = \{X^{(m)}(t), t = 0,1,2,....,N\}$ denote the aggregate process of *X* at aggregation level $m,\ m = 1,2,....,N$. That is, for each *m*, $X^{(m)}$ is given by

$$X^{(m)}(t) = \frac{1}{m}\sum_{l=m(t-1)+1}^{mt} X(l)\ ,\ t = 1,2,....,N.$$

Let $\gamma^{(m)}(k)$ and $\rho^{(m)}(k)$ denote the variance and autocorrelation function of $X^{(m)}$ respectively. *X* is called exactly second-order self-similar (ESOSS) with self-similarity parameter $H = 1-\frac{\beta}{2}$, $0<\beta<1$ if

$$\rho(k) = \frac{1}{2}[(k+1)^{2-\beta} - 2k^{2-\beta} + (k-1)^{2-\beta}]\ ,\ k = 1,2,....,N.$$

X is called long-range dependent (LRD) with $H = 1-\frac{\beta}{2}$, $0<\beta<1$, if its autocorrelation function satisfies $\rho(k) = ck^{-\beta}, k \to \infty$, where *c* is a positive constant. *X* is called asymptotical second-order self-similar (ASOSS) with $H = 1-\frac{\beta}{2}$, $0<\beta<1$, if

$$\lim_{m\to\infty}\rho^{(m)}(k) = \rho(k),\ k > 0\ .$$

Exact self-similar process implies $\rho(k) = \rho^{(m)}(k)$ for all m≥1. Thus, second order self-similarity captures the property of correlation structure preserving under time aggregation and is represented by $\rho(k) = \frac{1}{2}[(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}]$ for ESOSS or $\lim_{m\to\infty}\rho^{m}(k) = \frac{1}{2}[(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}]$ for ASOSS. In second-order stationary process for $0<H<1$ and $H\neq 0.5$, the autocorrelation function satisfies

$$\rho(k) = H(2H-1)k^{2H-2},\ k \to \infty\ .$$

More details on the SOSS statistical model can be found in [5], [8], [9] and [12].

There are several methods to estimate H. In this paper we will be using the optimization method (OM) which was developed in [5], [6] and was shown to be comparatively fast and accurate with respect to other methods. The method is based on how close is the sample autocorrelation measure fits to ESOSS model. The estimation method defines error fitting function $E_K(\beta)$ as $E_K(\beta) = \frac{1}{4K}\sum_{k=1}^{K}(\rho(k)-\rho_n(k))^2$ where $\rho(k)$ denotes the autocorrelation function of the model with parameter β that OM will fit the data to, $\rho_n(k)$ is the sample autocorrelation function of the data, *k* is autocorrelation lag and *K* is the largest value of *k* for which $\rho_n(k)$ is to be computed to reduce edge effects. The estimation of parameter β is based on optimizing $E_K(\beta)$ with threshold value $\leq 10^{-3}$ is chosen from experiment as introduced in [5].

3. LoSS Detection with SOSS Model

Normal Internet traffic always exhibits the ESOSS model. However in the presence of malicious packets such as DoS attacks, the self-similarity property is disturbed hence LoSS is detected as shown in [1], [10], [17] and [18]. The LoSS detection in [17] used the abrupt change property of distribution ratio of higher scale to lower scale. However, the work did not suggest an optimum level of scale to be used for revealing the abrupt change significantly. Meanwhile, the work in [1] defined LoSS as Hurst value beyond normal range of LRD which is 0.5<H<1 using periodogram or Whittle estimation methods. The results show that the LoSS detection method can expose new DoS attack pattern without specific normal template. The results also demonstrate that the method has high detection rate with an average of 60% to 84% which depends on the intensity of the attack packets.

A new method of estimating Hurst parameter which is more accurate and faster was developed in [5] and [6]. The method is known as the optimization method (OM) and the estimation is based on the SOSS model. The advantage of OM method is that it can provide a technique to identify whether the data tend toward the self-similarity model or not according to the curve-fitting error. Accordingly, the work in [18] demonstrates the capability of OM to detect

anomaly traffic based on the curve-fitting error. However, their works only considered fixed sampling which we believe is not sufficient to reveal the hidden self-similarity distribution error accurately. The reason is that recent modern Internet applications became more complex and new sampling strategies are required to estimate the self-similarity parameter accurately [2].

The behavior of Internet traffic is considered as normal when the traffic is near to the self-similarity model while otherwise it is considered as abnormal [18]. An example of abnormal traffic behavior is DoS traffic that introduces distribution error and shifts the stationary property toward non-stationary as shown in [1], [10], [17] and [18]. Data insufficient probability and detection loss probability are two important attributes that can influence the correctness of anomaly detection [18]. The data insufficient probability is to identify the minimum required window size to obtain reliable self-similarity measurement, while detection loss probability is probability of detecting non-stationary data.

LoSS is detected if it fulfils two conditions where the data must be longer than minimum window size and it must be non-stationary. Experiments in [8], [9] and [18] demonstrate that windows sizes from 15-30 minutes are practical and sufficient for modern LANs Ethernet Internet traffic to comply with data insufficient probability. The self-similarity tests become more sensitive as the window size gets smaller and consequently generate false alarms if it gets too small. Therefore, in our experiments we use traces of 30 minutes in length which is above the minimum required window to fulfill data insufficient probability [18].

Based on our assumptions, we define normal behavior of self-similarity traffic as the estimated Hurst parameter $\hat{H}$ using OM is in the LRD range with $0.5 < (\hat{H}, OM) < 1$ and fitting error $E_K \leq 10^{-3}$. Otherwise if $E_K > 10^{-3}$, LoSS is detected and consequently the corresponding Internet traffic is considered as abnormal. As ESOSS process has $\rho(k) = \rho^{(m)}(k)$ for all $m \geq 1$, it follows that ESOSS captures the property of correlation structure which is preserved under time aggregation. Therefore, it is required to study the effect of different aggregation level (or multi-level) especially at shortest timescale such as 10ms≤*m*≤1000ms that represent engineering factors [2] in order to reveal any hidden changes of self-similarity property efficiently.

4. Data Preparation

We use three datasets to investigate the pattern of normal and abnormal Internet traffic self-similarity behavior. The first dataset used synthetic Fractional Gaussian Noise (FGN) generator [7] and the second dataset contains data from Internet traffic simulation FSKSMNet [16] on September 29, 2006 at Faculty of Computer Science and Information (FSKSM) LANs. The third dataset are UNC2002 and UNC2003 described in [12] and [13]. We divided our experiments dataset into normal and abnormal behavior. For the normal dataset we used FGN that will generate synthetic traffic which is ESOSS and UNC2003 dataset. On the other hand, the abnormal dataset used malicious traffic simulation of FSKSMNet that was simulated on local Internet LANs FSKSM infrastructure and UNC2002 dataset. Each of the packet traces is sampled with different sampling level within the range of 10ms≤*m*≤1000ms. The details of the experimental datasets are shown in Table 1.

Table 1 Experimental Dataset with FGN [7], FSKSMNet [16], UNC2002 and UNC2003 [12],[13]

Trace	*Normal*				*Trace*	*Abnormal*			
	SI	*Window*	*Hurst*	*Error* (x 10^{-3})		*SI*	*Window*	*Hurst*	*Error* (x10^{-3})
FGN (Synthetic)	10	360000	0.81	0.01	UNC-2002 (suspicious) Apr_09 _Tue_0300	10	732243	0.91	0.98
	50	72000	0.82	0.01		50	146448	0.96	0.22
	100	36000	0.82	0.01		100	73224	0.97	0.11
	200	18000	0.82	0.02		200	36612	0.97	0.64
	500	7200	0.82	0.05		500	14644	0.96	1.83
	700	5142	0.82	0.05		700	10460	0.95	1.52
	1000	3600	0.81	0.09		1000	7322	0.94	2.11
UNC-2003 (normal) Apr_09_ Wed_1100	10	360050	0.84	0.53	FsksmNet-2006 (Malicious) Sep29_ Fri_1146	10	173991	0.99	0.02
	50	72010	0.84	0.36		50	34798	0.98	0.65
	100	36005	0.83	0.23		100	17399	0.98	1.32
	200	18002	0.82	0.14		200	8699	0.95	5.94
	500	7201	0.82	0.09		500	3479	0.88	20.19
	700	5143	0.81	0.14		700	2485	0.85	18.47
	1000	3600	0.81	0.30		1000	1739	0.82	15.28

5. Empirical Analyses

5.1 Estimated Hurst and Curve Fitting Error

Our experiments have two purposes. Firstly, to investigate how self-similarity or LRD property is preserved at different levels of *m* and secondly, to investigate the efficiency of anomaly detection method based on LoSS by considering multi-level sampling *m*. The experiments used threshold of curve fitting error equal to 10^{-3} and maximum autocorrelation lag K=200 for the OM.

Table 1 shows the estimated Hurst value and curve fitting error for experimental datasets traces. The results illustrate that the synthetic FGN trace preserves self-similarity property at all levels of *m* from lower to higher value, which was shown by curve fitting error $<10^{-3}$. Similarly for trace UNC2003, the self-similarity property is also preserved at all levels of *m*. This is a crucial criterion for determining normal Internet behavior which stated that no LoSS occurrence is detected through multi-levels of *m* from lower *m*=10ms to higher *m*=1000ms. For the malicious traffic that contains DoS flooding packets such as in the FSKSMNet trace, the results demonstrate that self-similarity property is not preserved through multi-levels of *m*. This is shown by curve fitting error$<10^{-3}$ for lower *m*<100ms but exceeds threshold value at higher level of *m*≥100ms where LoSS is detected.

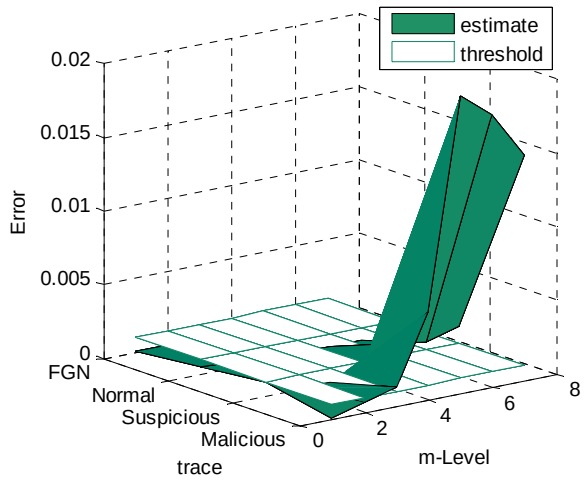

Figure 1 Curve fitting error distribution pattern for multi-level sampling

Figure 1 illustrates the graphical view of curve fitting error distribution for normal, suspicious and malicious traces behavior at different sampling level value of *m*. It is clearly shown that for the normal trace, none of LoSS occurrence is detected at all value of *m*. On the other hand, the LoSS behavior of malicious traffic is clearly revealed at higher value of *m* as shown by a larger value of curve fitting error exceeding the threshold. Similarly for the suspicious behavior, the LoSS occurrence is also detected at higher value of *m*. However, curve fitting error exceeded the threshold for suspicious trace is relatively small if compared to malicious trace.

5.2 Self-Similarity LRD Behavior Observation

We use the ESOSS autocorrelation structure (i.e. $\rho(k)$ structure) to investigate in details how self-similarity or LRD structure is preserved at different levels of sampling *m*.

Observation I: Normal Behavior

We define normal behavior as the $\rho(k)$ structure preserved the LRD property at all values of *m*. This can be shown clearly by Figure 2(a) and (b) that illustrate the $\rho(k)$ structure of the FGN and UNC2003 traces are following the LRD structure. The self-similarity property of normal behavior is preserved in two ways. Firstly, the traces follow the ESOSS model, i.e. fitting error$<10^{-3}$ at all values of *m*. Secondly, the deviation of variance for multi-level sampling for Hurst and curve fitting error are small, i.e. *Var(m-H)*$<1.0\text{x}10^{-4}$ and *Var(m-Err)*$<1.0\text{x}10^{-7}$ as shown in Table 2.

Table 2 Mean of Curve Fitting Error, Variance of Hurst and Variance of Curve Fitting Error for multi-level *m*

Trace	*Mean (m-H)*	*Var (m-H)*	*Var (m-Err)*
FGN(*N*)	$0.034\text{ x}10^{-03}$	$2.38\text{ x}10^{-05}$	$9.29\text{ x}10^{-10}$
UNC2003(*N*)	$0.256\text{ x}10^{-03}$	$1.62\text{ x}10^{-04}$	$2.38\text{ x}10^{-08}$
UNC2002(*S*)	$1.059\text{ x}10^{-03}$	$4.48\text{ x}10^{-04}$	$6.16\text{ x}10^{-07}$
FSKSMNet(*M*)	$8.839\text{ x}10^{-03}$	$4.91\text{ x}10^{-03}$	$7.88\text{ x}10^{-05}$

Observation II: Abnormal Behavior

We define abnormal behavior as the $\rho(k)$ structure is inconsistent with the LRD structure at different levels of *m*. For example in FSKSMNet trace, at *m*<100ms the $\rho(k)$ structure is following the LRD structure with curve fitting error $<10^{-3}$ but the structure gradually diminishes from hyperbolic decay at *m*>100ms. This phenomenon is known as LoSS where the $\rho(k)$ structure deviates from SOSS autocorrelation model with a larger curve fitting error exceeded the threshold especially at *m*≥500ms. The disturbance of distribution error to the $\rho(k)$ structure is clearly revealed as shown in Figure 2(d). In contrast, the distortion of the LRD structure for the suspicious UNC2002 trace is not obvious if compared to the

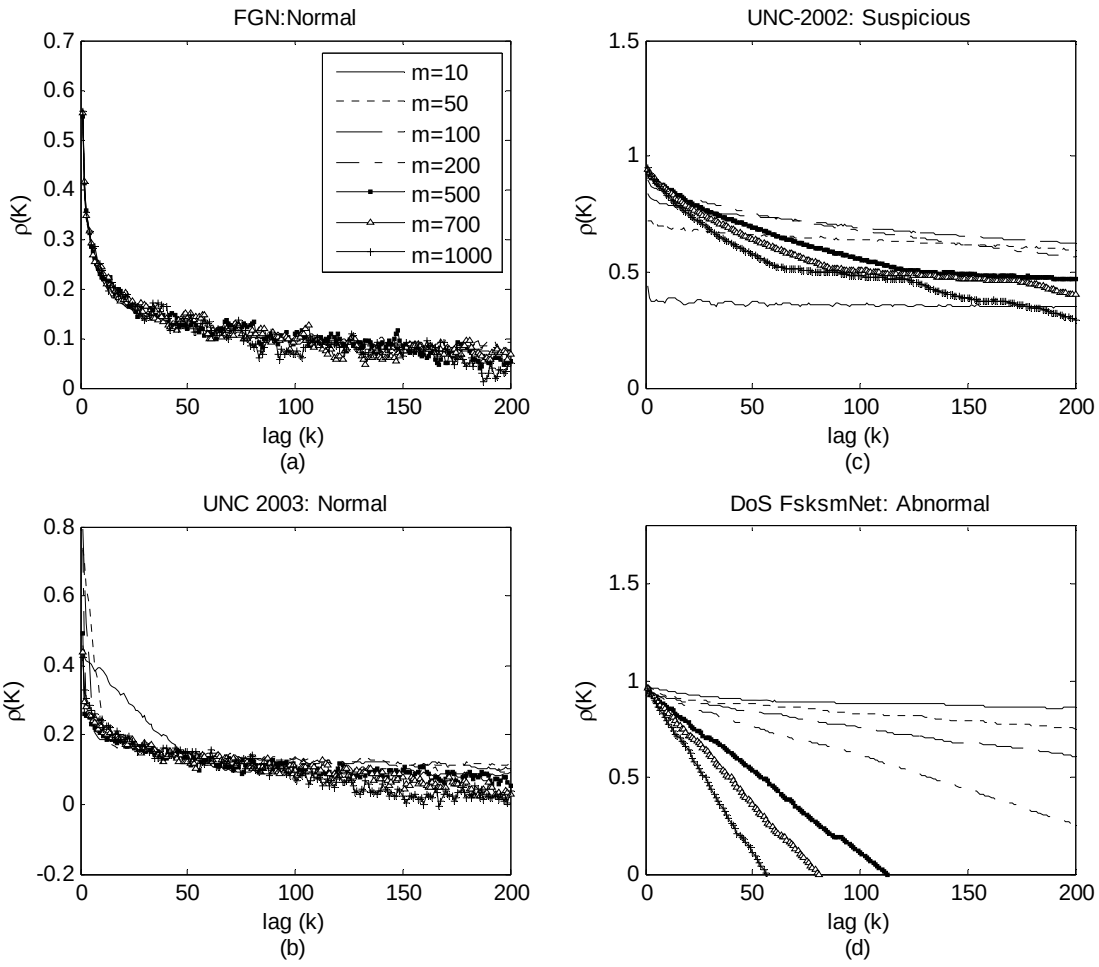

Figure 2 Autocorrelation structure (a) Synthetic FGN (b) UNC 2003 dataset (c) UNC2002 dataset (d) FSKSMNet dataset

malicious traffic. This can be shown by curve fitting error exceeded the threshold for suspicious trace is lower than malicious trace as shown in Figure 2(c). In addition from Table 2, the variance of multi-level Hurst estimation for malicious trace is bigger than suspicious trace. This is shown by *Var(m-H)* >$4.0x10^{-4}$ for suspicious and $4.0x10^{-3}$ for malicious. Moreover, the variance of multi-level curve fitting error also indicates that malicious trace has the highest value if compared to others with *Var(m-Err)*>$1.0x10^{-5}$. However, the differences between these attributes are relatively small for the suspicious and normal hence make it difficult to distinguish.

5.3 Anomaly Detection with Multi-Level sampling *m*

How self-similarity (or LRD property) is preserved over multi-level sampling plays an important role in detecting the behavior of LoSS occurrences accurately. The experimental results have demonstrated that normal traffic behavior always follows the ESOSS model. Therefore at fixed sampling rate such as 10 or 100ms, it is sufficient to estimate Hurst parameter accurately as shown in [5], [8] and [9]. However in the presence of suspicious or malicious packets traffic, the detection of LoSS is difficult if we rely only on fixed sampling level of *m*. The results in Table 1 demonstrate that it is very difficult to choose an optimum value of *m* that is most suitable to reveal the distribution of self-similarity error accurately. Accordingly, we propose multi-level sampling parameters such as multi-level average curve fitting error (*mean(m-Err)*), variance of multi-level Hurst (*var(m-H)*) and variance of multi-level curve fitting error (*var(m-Err*)) for an accurate LoSS detection method.

Figure 3 clearly illustrates that the malicious traffic contributes a significant change of *mean(m-Err)*, *var(m-H)* and *var(m-Err)* when compared to others. Among the

three, *mean(m-Err)* parameter dominates the changes of LoSS behavior significantly. Therefore, it easy to determine between normal and abnormal behavior by using *mean(m-Err)* that exceeds much higher than threshold as shown in Figure 4. However, it is difficult to differentiate between suspicious and normal behavior. The reason is the suspicious trace has minimal curve fitting error exceeded the threshold as illustrates in Figure 4.

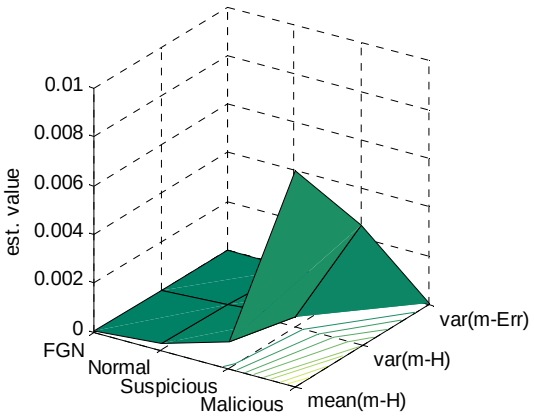

Figure 3 Multi-level parameters –mean (*m*-H), variance (*m*-H) and variance (*m*-Err)

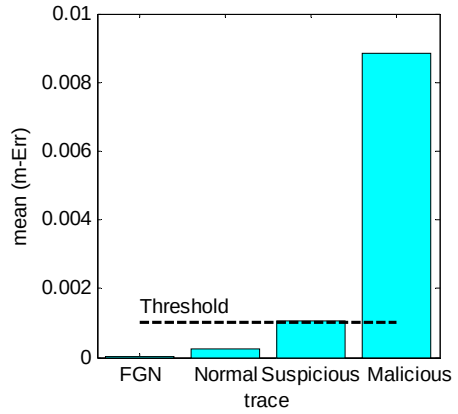

Figure 4 Average multi-level fitting error -mean (*m*-H)

To this end, we propose new definition of normal and abnormal Internet traffic behavior. Normal behavior refers to zero LoSS detection at normal and multi-level sampling in the range of LRD, and is defined as follow:

($H \in 0.5<H<1$) $\cap$ (*curve fitting error <threshold (at normal m))* $\cap$ (*mean (multi-level curve fitting error) < threshold (at multi-level m))*

On the other hand, abnormal behavior refers to at least one LoSS occurrence is detected either at normal or mean multi-level sampling, and is defined as follow:

(*curve fitting error>threshold (at normal m))* $\cup$ (*mean (multi-level curve fitting error) >threshold (at multi-level m))*

For the abnormal behavior, if the difference between attribute *mean(multi-level curve fitting error)* and *threshold* is very small then the traffic can be considered as suspicious. However, more efforts are needed to redefine the accuracy and reliability of the proposed definition. In our work, normal sampling level *m* is referred as *m*=10ms or 100ms as used in [8], [9] and [18], while multi-level sampling considers 10ms≤*m*≤1000ms.

6. Conclusion and Future Work

This paper presents the implementation of anomaly detection method based on LoSS behavior using SOSS model. The results demonstrate that normal Internet traffic preserves the exact self-similarity property while abnormal traffic perturbs the structure of self-similarity property. The results also illustrate that fixed sampling is not sufficient to detect distribution of self-similarity error accurately. Moreover revealing the self-similarity distribution error accurately is a challenging task due to the inconsistent behavior of distribution error at different levels sampling. We believe this can be a possible reason why anomaly detection based on LoSS criterion has high false alarm rate detection. Accordingly, we suggest a new LoSS detection method by considering multi-level sampling parameters. Our future work will concentrate on developing a multi-level sampling approach of LoSS detection method in order to reduce false alarm rate efficiency for Internet traffic monitoring system.

Acknowledgments

This work was funded by Universiti Teknologi Malaysia (UTM). The authors thank to Dr. Sulaiman of CICT, UTM and Mr. Firoz of Unit IT, FSKSM for their helps in simulating the real traffic of FSKSMNet dataset.

References

[1] Allen, W.H. and Marin, G.A., "The LoSS technique for detecting new Denial of Service attacks," SoutheastCon, 2004. Proceedings. IEEE, pp. 302-309, 26-29 March 2004.

[2] Cairano-Gilfedder, C. and Clegg, R.G., "A decade of Internet research -- advances in models and practices," BT Technology Journal 23, vol.4, pp. 115-128, Oct. 2005.

[3] Crovella, M.E. and Bestavros, A., "Self-similarity in World Wide Web traffic: Evidence and possible causes networking," IEEE/ACM Trans. on vol.5(6), pp. 835 – 846, Dec. 1997.

[4] Erramilli, A., Narayan, O. and Willinger, W., "Experimental queuing analysis with long-range dependent

packet traffic," IEEE/ACM Trans. Networking, 4:209–223, 1996.
[5] Kettani, H., "A Novel Approach to the Estimation of the Long-Range Dependence Parameter," University of Wisconsin – Madison : PhD. Thesis (2002).
[6] Kettani, H., and Gubner, J.A., "A Novel Approach to the Estimation of the Long-Range Dependence Parameter," IEEE Transactions on Circuits and Systems II, vol. 53(6), pp. 463-467, June 2006.
[7] Ledesma, S. and Liu, D., "Fractional Gaussian noise power spectrum synthesis using linear approximation for generating self-similar network traffic," ACM Computer Communication Review, vol.30(2), pp. 4-17, April 2000.
[8] Leland, W., Taqqu, M., Willinger, W. and Wilson, D., "On the self-similar nature of Ethernet traffic," Proc. of ACM SIGCOMM 23(4) (1993), pp. 183–193.
[9] Leland, W., Taqqu, M., Willinger, W. and Wilson, D., "On the self-similar nature of Ethernet traffic (extended version)," IEEE/ACM Transactions on Networking 2(1) (1994), pp. 1–15.
[10] Li, M., "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks", Computers & Security, Volume 25, Issue 3, pp. 213-220, May 2006.
[11] Li, M., Jia, W., and Zhao, W., "Decision analysis of network-based intrusion detection systems for denial-of-service attacks," Proceedings of IEEE International Conferences on Info-tech and Info-net (ICII 2001), Vol. 5, Beijing, PRC, pp. 1-6, 29 Oct. - 1 Nov. 2001.
[12] Park, C., Hernández-Campos, F., Marron, J. S., and Smith, F. D., "Long-range dependence in a changing internet traffic mix," Computer Networks vol.48(3), pp. 401-422, Jun. 2005.
[13] Park, C., Hernández-Campos, F., Marron, J. S., and Smith, UNC DIRT Laboratory Internet traces, http://www-dirt.cs.unc.edu/ts/ , 23 May 2003.
[14] Park, K., Kim G., and Crovella, M., "On the effect of traffic self-similarity on network performance," SPIE International Conference on Performance and Control of Network Systems, November 1997.
[15] Paxson, V., and Floyd, S., "Wide-area traffic: The failure of Poisson modeling," IEEE-ACM Transactions on Networking, 3(3), June 1995.
[16] Rohani, M.F., Maarof, M.A., Selamat, A. and Kettani, H., "An Implementation of LoSS Detection with Second Order Statistical Model", Postgraduate Annual Research Seminar 2007, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 3-4 July 2007.
[17] Schleifer, W., and Mannle, M., "Online error detection through observation of traffic self-similarity," IEE Proceedings on Communications, 148(1), Feb. 2001.
[18] Idris, M.Y., Abdullah, H., and Maarof, M.A., "Iterative window size estimation on self-similarity measurement for network traffic anomaly detection," International Journal of Computing and Information Science, (IJCIS), vol. 2(2), pp. 83-91, 2004.

Mohd Fo'ad Rohani received his B.E (Hons.). and M.Sc. degrees in Electrical and Electronic Engineering from University Malaya (UM), Kuala Lumpur and University of Wales, Cardiff UK in 1994 and 1998, respectively. Currently he is a Lecturer in the Department of System and Communication Computer, Faculty of Computer Science Information Systems, Universiti Teknologi Malaysia (UTM) and now is pursuing his PhD degree. His research interests include Digital Signal Processing (DSP), Network Monitoring and Security.

Mohd Aizaini Maarof is an Associate Professor at Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM). He obtained his B.Sc (Computer Science) and M.Sc (Computer Science) from U.S.A and his Ph.D degrees from Aston University, Birmingham, United Kingdom in the area of Information Technology (IT) Security. He is currently leading the Secure Systems & Cryptography Research Group (SSCRG) in the faculty. Currently his research involve in the areas of Network Security, Web Content Filtering, MANET Security and Cryptography.

Ali Selamat received a B.Sc. (Hons.) in IT from Teesside University, U.K. and M.Sc. in Distributed Multimedia Interactive Systems from Lancaster University, U.K. in 1997 and 1998, respectively. He obtained his Ph.D. degree from Osaka Prefecture University, Japan in 2003. He is currently a Senior Lecturer and Head of Postgraduate Studies Department, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia (UTM). His research interests include software engineering, software agents, web engineering, information retrieval, DNA Computing and soft-computing.

Houssain Kettani received his B.S. in Electrical and Electronic Engineering from Eastern Mediterranean University, Famagusta, North Cyprus, in 1998. In 2000 and 2002 respectively, he obtained his M.Sc. and Ph.D. degrees both in Electrical Engineering from the University of Wisconsin, Madison, WI. He is currently a Full Professor and Research Professor of Electrical and Computer Engineering and Computer Science at Polytechnic University of Puerto Rico, San Juan, PR, as of August 2007. Dr. Kettani's research interests include computational science and engineering, computer networks, network traffic characterization, network storage management, number theory, parameter estimation, pattern recognition, and robust control and optimization.