LoSS Detection Using Parameter's Adjustment Based on Second Order Self-Similarity Statistical Model

Mohd Fo'ad Rohani
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia,
81300 Skudai, Johor, Malaysia.
foad@utm.my

Mohd Aizaini Maarof
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia,
81300 Skudai, Johor, Malaysia.
aizaini@utm.my

Ali Selamat
Faculty of Computer Science and Information Systems,
Universiti Teknologi Malaysia,
81300 Skudai, Johor, Malaysia.
aselamat@utm.my

Houssain Kettani
Department of Electrical and Computer Engineering and Computer Science,
Polytechnic University of Puerto Rico,
San Juan, Puerto Rico 00919, USA.
hkettani@pupr.edu

Abstract

This paper analyzes Loss of Self-Similarity (LoSS) detection accuracy using parameter's adjustment which includes different values of sampling level and correlation lag. This is important when considering exact and asymptotic self-similar models concurrently in the self-similarity parameter estimation method. Due to the needs of high accuracy and fast estimation, the Optimization Method (OM) based on Second Order Self-similarity (SOSS) statistical model was proposed in the previous works to estimate self-similarity parameter. Consequently, Curve Fitting Error (CFE) value estimated from OM is used to detect LoSS efficiently. This work investigates the effect of the parameter's adjustment for improving the CFE accuracy and estimation time speed. We have tested the method with real Internet traffics simulation that consists of normal and malicious packets traffic. Our simulation results show that LoSS detection accuracy and estimation time can be affected by the chosen of sampling level and correlation lag values.

1. Introduction

The advance of attack tools and their availability on Internet have increased network vulnerability to misuse and performance traffic problems. Internet service providers are now faced with the challenging task of continuous monitoring of their network to ensure that security is maintained. Thus, monitoring Internet traffic especially to detect anomaly traffic is very important to assist security experts in analyzing and detecting malicious traffic behavior. The effort is needed by network administrator in order to offer uninterrupted Internet services to the users. There are several models that have been applied to detect anomaly traffic including statistical moments (or mean and standard deviation model), multivariate model or time series model [11]. When dealing with huge amount of traffic packets where behavior traffic keep changing unpredictably, anomaly detection using time series model is suggested since the model can produce better results than others statistical models [11].

Recent studies have shown that self-similarity model is widely used for Internet traffic modeling and analysis [3], [4], [5], [7], [8]. According to self-similarity model, the autocorrelation of inter arrival traffic packets is assuming to exhibit hyperbolic decay and Long Range Dependent (LRD). This assumption is true for normal traffic but in the presence of malicious traffic such as Denial of Service (DoS) packets, the self-similarity distribution error [14] is introduced and perturbs the self-similarity model. Consequently, Loss of Self-similarity (LoSS) is detected [1], [6], [14] to

978-1-4244-2328-6/08/$25.00 © 2008 IEEE

Proceedings of the 3rd International Symposium on Information Technology (ITSim2008), pp. 26-29, Kuala Lumpur, Malaysia, August 2008.

alert security analysts with the existence of uncontrolled self-similarity structure in network queue buffer [4], [10]. Thus, packets queue buffer time delay and packets drop rates are drastically increased [4], [10] hence degrading Quality of Service (QoS) performance. Implementation of LoSS detection with Second Order Self-Similarity (SOSS) statistical model has been introduced due to high speed and accuracy needs [6]. Previous works [1], [6], however, have used fixed sampling time series packets which is insufficient to reveal self-similarity distribution error correctly [12], [13]. In this work, we investigate LoSS detection accuracy and its dependency on two variables known as sampling level and correlation lag. This is crucial when combining the idea of exact and asymptotic self-similarity models concurrently in the estimation method [9].

In our work, we use Second Order Self-similarity (SOSS) statistical model and the Optimization Method (OM) [7] to estimate the self-similarity parameter. LoSS is detected if the Curve Fitting Error (CFE) estimated using OM exceeds the threshold value [6]. Anomaly traffic detection based on LoSS will suffer high false alarm detection rate if improper sampling level and insufficient correlation lag process are used in the estimation method [12], [13]. Thus, LoSS detection accuracy using different values of sampling levels and correlation lag are analyzed and the estimation time processing speed is also investigated. This paper is organized as follows: Section 2 discuses in brief the self-similarity model LoSS detection method. The experimental and empirical analyses are presented in Section 3. Finally, our conclusions and future works are summarized in Section 4.

2. Self-Similarity Model and LoSS Detection Method

2.1 SOSS Model and Estimation Method

Let define a second-order stationary process $X = \{X(t), t > 0\}$ with constant mean μ, finite variance σ^2 and autocorrelation $\rho(k)$ as follow:

$$\mu = E[X(t)], \quad \sigma^2 = E[(X(t) - \mu)]^2 \qquad (1)$$

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

Let $X^{(m)} = \{X^{(m)}(t), t > 0\}$ denotes the aggregate process of X at aggregation level $m > 0$.
Thus, we have:

$$X^{(m)}(t) = \frac{1}{m} \sum_{w=m(t-1)+1}^{mt} X(w) \, , t > 0 \qquad (3)$$

Let $\rho^{(m)}(k)$ denotes the autocorrelation function of $X^{(m)}$. X is called Exactly Second-Order Self-Similar (ESOSS) if $\rho(k) = \rho^{(m)}(k)$ for all $m \geq 1$. In ESOSS, the autocorrelation structure is preserved for all m such that:

$$\rho(k) = \frac{1}{2}[(k+1)^{2-\beta} - 2k^{2-\beta} + (k-1)^{2-\beta}] \qquad (4)$$

where k>0 and 0<β<1. X is called Asymptotical Second-Order Self-Similar (ASOSS) if

$$\lim_{m,k\to\infty} \rho^m(k) \sim \frac{1}{2}[(k+1)^{2-\beta} - 2k^{2-\beta} + (k-1)^{2-\beta}] \quad (5)$$

where k>0, m>0 and 0<β<1. X is called Long-Range Dependent (LRD) if its autocorrelation function satisfies: $\rho(k) \sim ck^{-\beta}$ where $k \to \infty$, c>0 and 0<β<1.

There are several methods to estimate H. In this paper we use OM that was developed in [7] which was proven relatively fast and accurate compared to other methods such as the wavelet method. The OM defines Curve-Fitting Error (*CFE*) function as $E_K(\beta)$ such as:

$$E_K(\beta) = \frac{1}{4K} \sum_{k=1}^{K} (\rho(k) - \rho_n(k))^2 \qquad (6)$$

where $\rho(k)$ denotes the autocorrelation function of the model with parameter β that we would like to fit the data to, $\rho_n(k)$ is the sample autocorrelation function of the data, and K is the largest value of k such that it minimize the edge effect for the calculation of $\rho_n(k)$. If the minimum of $E_K(\beta)$ is less than 10^{-3} , then the data fits the model and the minimizer $\hat{\beta}$ is picked to be the estimate of the parameter β [7].

2.2 LoSS Detection Using Parametric Adjustment

Let $X(t)$ as a stochastic time series data with second order stationary property. The autocovariance decay of $X(t)$ and aggregated $X^{(m)}(t)$ should follow ESOSS model which can be written in equation (7):

$$\lim_{m,k\to\infty} \gamma^m(k) = \gamma(k) \sim C_0 k^{-\beta} \qquad (7)$$

where m is sampling level, k is correlation lag, C_o is constant and β is self-similarity parameter.
In real Internet traffic, however, the self-similarity processes are also considered as processes $x(j)$ in the class X of those stationary processes that feature an asymptotic decay in autocovariance [9]. Thus, we

978-1-4244-2328-6/08/$25.00 © 2008 IEEE

should consider ESOSS and ASOSS models concurrently in order to estimate the self-similarity parameter for normal and abnormal traffic correctly.

Let denotes autocovariance, variance and autocorrelation for aggregated process $X^{(m)}(t)$ as shown in equation (8), (9) and (10) [9].

$$\lim_{m,k\to\infty} \gamma^{m}(k) \sim C_1 m^{-\beta} k^{-\beta} \qquad (8)$$

$$\lim_{m\to\infty} \gamma^{m}(0) \sim C_2 m^{-\beta} \qquad (9)$$

$$\lim_{m,k\to\infty} \rho^{m}(k) = \lim_{m,k\to\infty} \left(\frac{\gamma^{m}(k)}{\gamma^{m}(0)} \right)$$

$$\sim \frac{C_1 m^{-\beta} k^{-\beta}}{C_2 m^{-\beta}} \sim C_3 k^{-\beta} \qquad (10)$$

where C$_1$, C$_2$ and C$_3$ are constants. The works in [7], [8] have assumed that normal Internet traffic follows ESOSS model and its characteristics are shown in equations (8) to (10). Equation (10) clearly demonstrates that autocorrelation decay does not affected by aggregation (*m*) parameter. On the other hand, correlation lag (*k*) plays an important role to obtain high accuracy of self-similarity parameter (β) estimation.

In the presence of malicious traffic such as DoS packets, the high intensity of DoS packets can disturb Internet traffic behavior and produce self-similarity distribution error. Consequently, normal characteristics of equations (8) to (10) are not valid where LoSS is detected. Equation (11) shows that for abnormal traffic, the autocovariance and variance decay of $C_1 m^{-\beta}$ and $(C_2 m^{-\beta})'$ are not identical and not following normal self-similarity pattern as in equation (10).

$$\lim_{m,k\to\infty} \rho^{m}(k) = \lim_{m,k\to\infty} \left(\frac{\gamma^{m}(k)}{\gamma^{m}(0)} \right) \sim \left(\frac{C_1 m^{-\beta}}{(C_2 m^{-\beta})'} \right) k^{-\beta}$$

$$\nsim C_3 k^{-\beta} \qquad (11)$$

This shows that for detecting malicious traffic, aggregation and correlation lag are two parameters that need to be considered for estimating the CFE value correctly in order to improve LoSS detection accuracy.

3. Experimental and Empirical Analyses

3.1 Simulation Dataset

We have simulated the FSKSMNet Internet traffic traces collected on September 29, 2006 at Faculty of Computer Science and Information Systems (FCSIS) in order to evaluate the proposed LoSS detection approach [13]. The network infrastructure consists of ten VLANs with 100BaseFX Fast Ethernet backbone which is connected to university Gigabit backbone. The simulation is divided into normal and abnormal traffic. Normal traffic is defined as Internet activities that strictly follow FCSIS network policy. On the other hand, abnormal traffic contains simulated injection of DoS flooding packets at controlled rate that includes TCP SYN and UDP flooding packets. Each of simulation traces is about 30 minutes. Table 1 shows the details of our simulated traffic protocols.

The percentage protocol for normal traffic shows that almost 97% is dominated by TCP protocol while UDP is less than 2.5%. The ICMP, IGMP and others protocol are less than 0.5%. On the other hand, the simulated malicious traffic consists of 28% TCP SYN and 27% UDP flooding while normal protocols of TCP and UDP are 41% and 3%. The remainder is ICMP, IGMP and others which less than 0.5%. We use sampling level at micro sampling (i.e. below 1 second) [12], [13] that represents crucial engineering factor [2] design for Internet modeling purpose. Different sampling levels for the traces used in our experiments and their window size (or data length) are shown in Table 2.

Table 1. FSKSMNet traffic simulation

Trace	Time Injection (SYN/UDP)	Protocol	Packet's Count	
			Normal	DoS
Normal (12.45pm -1.15pm)	None	TCP	3407952	None
		UDP	87375	
		ICMP	5436	
		IGMP	293	
		Others	1055	
Malicious (11.46am-12.16pm)	11.55am (TCP SYN : 60s)	TCP	3979859	2734508
	12.05pm (UDP flood : 60s)	UDP	107680	2878970
	None	ICMP	3599	None
		IGMP	476	
		Others	1919	

Table 2. Details sampling of simulation dataset

Sampling Level *m* (ms)	Normal (N)	Window Size	Malicious (M)	Window Size
10	N_{10}	173999	M_{10}	173991
50	N_{50}	34799	M_{50}	34798
100	N_{100}	17399	M_{100}	17399
200	N_{200}	8699	M_{200}	8699
500	N_{500}	3479	M_{500}	3479
700	N_{700}	2485	M_{700}	2485
1000	N_{1000}	1739	M_{1000}	1739

3.2 LoSS Detection with Parametric Adjustment

The simulation result of CFE estimation using different values of sampling level and correlation lag for normal trace is illustrated in Figure 1. Figure 1 clearly shows that the estimated CFE value for normal trace at all sampling levels and correlation lags are below the threshold. The result shows that sampling level and correlation lag do not influence much on estimating the CFE value correctly for normal traffic that follows ESOSS model. Different sampling level will produce different window packets size while different correlation lag will give different estimation time process. In certain fixed capturing time duration, higher sampling level will produce smaller window packets size compared to lower sampling level. When window size packet is too small, it is possible to estimate the self-similarity parameter incorrectly due to insufficient data that do not fulfill the minimum window requirement [6]. On the other hand, the increasing of correlation lag value can increase the correlation time speed processing. Thus, previous works [8] on estimating self-similarity parameter for normal traffic use small sampling level such as 10ms or 100ms and use small correlation lag such as 50 [7].

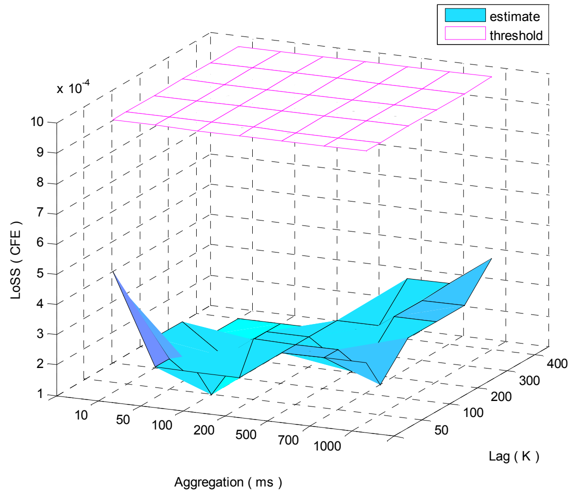


Figure 1. LoSS detection for normal trace

For malicious traffic, however, proper values of sampling level and correlation lag are needed in order to estimate LoSS correctly. Figure 2 illustrates LoSS estimation based on CFE for malicious traffic trace. As shown in Figure 2, the accuracy of CFE estimation for malicious traffic is influenced by the sampling level and correlation lag values. At very small sampling such as 10ms, the sampling level is insufficient to reveal LoSS occurrences despite using large value of correlation lag. Consequently, LoSS detection accuracy can be improved further by increasing higher sampling level such as larger than 100ms and suitable correlation lag such as larger than 200 is used. The details of CFE estimation are presented in Table 3.

As shown in Table 3, at sampling level 10ms none of LoSS is detected even though large correlation lag are used. This can be a possible reason for high false alarm detection if LoSS is detected at 10ms. On the other hand, by increasing sampling level to the higher value, LoSS detection accuracy can be improved. For instance, at sampling level 100ms if small correlation lag is chosen lower than 100, LoSS is not detected but 100% detected if correlation lag larger than 100 is used. At higher sampling such as larger than 500ms, however, the accuracy of LoSS is 100% detected regardless the value of correlation lag used. This observation demonstrates that choosing a proper value of sampling and correlation lag is important in order to detect LoSS correctly.

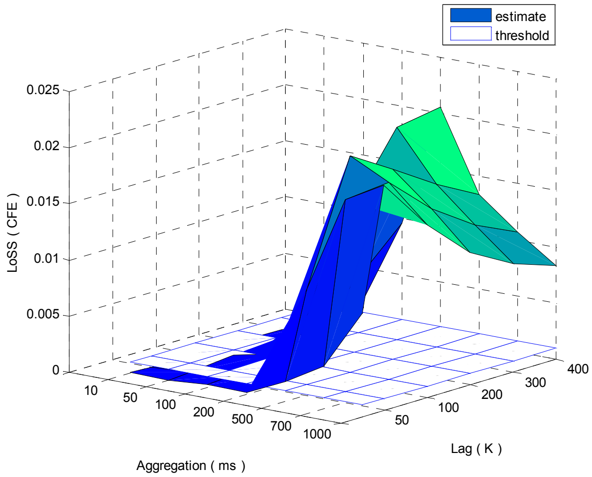


Figure 2. LoSS detection for malicious trace

Table 3. Details CFE estimation for malicious trace

Trace (M)	Auto-correlation lag (k)					
	50	100	200	300	400	500
M_{10}	0.0001	0.0000	0.0000	0.0000	0.0000	0.0001
M_{50}	0.0000	0.0002	0.0006	0.0006	0.0011	0.0022
M_{100}	0.0003	0.0004	0.0013	0.0028	0.0058	0.0096
M_{200}	0.0002	0.0011	0.0059	0.0143	0.0199	0.0205
M_{500}	0.0018	0.0094	0.0202	0.0179	0.0154	0.0134
M_{700}	0.0038	0.0181	0.0185	0.0150	0.0125	0.0107
M_{1000}	0.0092	0.0200	0.0153	0.0118	0.0097	0.0084

978-1-4244-2328-6/08/$25.00 © 2008 IEEE

3.3 LoSS Detection Performance

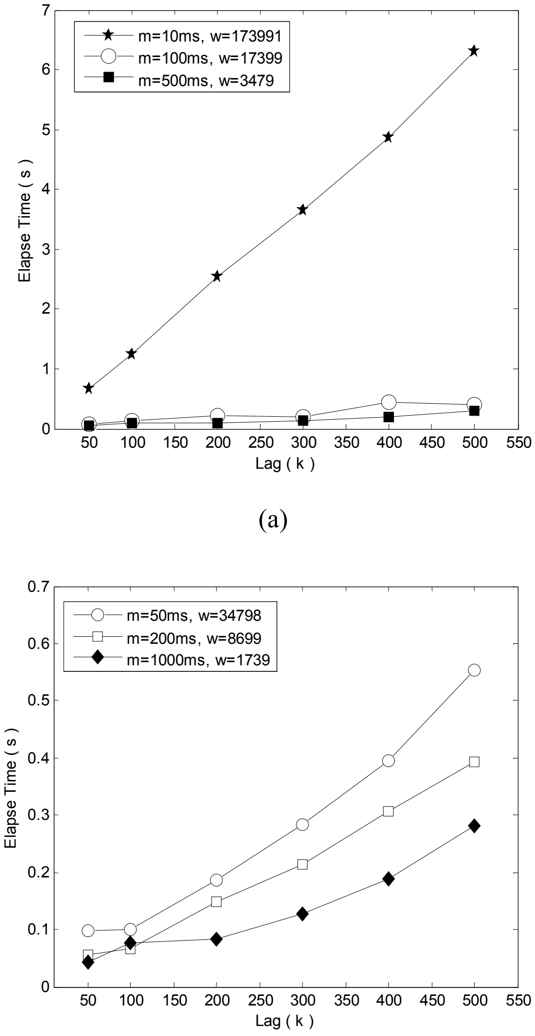
Our simulation results show that for normal traffic that follows ESOSS model, zero LoSS is detected despite a different set of sampling level (from 10ms to 1000ms) and correlation lag (from 50 to 500) are used in the estimation. This demonstrates that parameter's adjustment has less effect on the LoSS detection for normal traffic. This means that small sampling such as 10ms or 100ms as used in [8] and small correlation lag such as 50 as used in [7] are sufficient to estimate self-similarity parameter correctly. On the other hand, LoSS detection for malicious traffic trace has different accuracy when applying different value of sampling level and correlation. The details of LoSS detection performance for malicious trace are shown in Table 4. The results demonstrate that a proper selection of parameter adjustment is needed in order to reduce false alarm LoSS detection. As shown in Table 4, zero LoSS is detected at sampling level 10ms but significantly improved to 100% detected at sampling level higher than 500ms regardless any values of correlation lags are used. The results also show that LoSS detection accuracy for sampling level between 10ms and 500ms is very much depending on the chosen of correlation lag value. For instance, sampling level 100ms requires correlation lag above 200 to detect LoSS successfully compared to small correlation lag. Similarly, sampling level 200ms needs correlation lag above 100 for LoSS is fully detected.

Table 5. LoSS detection performance for malicious trace

Trace (M)	Autocorrelation lag (k)					
	50	100	200	300	400	500
M_{10}	No	No	No	No	No	No
M_{50}	No	No	No	No	Yes	Yes
M_{100}	No	No	Yes	Yes	Yes	Yes
M_{200}	No	Yes	Yes	Yes	Yes	Yes
M_{500}	Yes	Yes	Yes	Yes	Yes	Yes
M_{700}	Yes	Yes	Yes	Yes	Yes	Yes
M_{1000}	Yes	Yes	Yes	Yes	Yes	Yes

The different between smaller and higher sampling level is window size produced from certain duration of capturing time. A smaller sampling produces a larger window size compared to a higher sampling level. In our simulation for 30 minutes traffic capturing, sampling level at 10ms, 100ms and 1000ms provide window size of 173991, 17399 and 1739 packets respectively. The advantage of small sampling is less time needed to fulfill minimum window requirement [6] for initialization process before parameter estimation can be done correctly. On the other hand, LoSS can be possibly hidden under small sampling level. Therefore, LoSS detection performance can be improved by combining proper selection of sampling level and correlation lag values.

Another parameter to be considered for developing a reliable LoSS detection method is estimation time factor. Figure 3 illustrates the processing time for estimating LoSS detection using different values of sampling level and correlation lag. The result demonstrates that different window size packet from different sampling level has given different estimation time processing. The longer window size packet is used, the longer time processing is needed.



(a)

(b)

Figure 3. LoSS detection elapse estimation time for malicious trace

978-1-4244-2328-6/08/$25.00 © 2008 IEEE

As shown in Figure 3(a), sampling level 10ms and 1000ms produce almost the longest and shortest estimation time than others at all correlation lag values. Another important observation is that at each sampling level, the increasing of correlation lag will also increases the estimation time processing. This can be seen in smaller sampling level such as 10ms in Figure 3(a) or at larger sampling level in Figure 3(b). The results show that correlation lag equal 50 takes less estimation time compared to 500 at almost all sampling levels.

From the simulation results, a general guideline in order to achieve an accurate LoSS detection using OM as well as to optimize estimation time can be followed. If small sampling level is used then correlation lag must be assigned with bigger value. On the other hand, larger sampling level needs smaller value of correlation lag that can sufficiently reveal the existence of self-similarity distribution error efficiently. Further efforts, however, should be done in order to determine an optimize value of sampling level and correlation lag parameters in order to optimize LoSS detection accuracy performance.

4. Conclusions and Future Works

Parameter's adjustment which includes sampling level and correlation lag are identified as a prime factor that can influence LoSS detection accuracy. The simulation results show that sampling level does not influence CFE estimation for normal traffic that follows ESOSS model. The accuracy of the estimated CFE, however, is very much depending on correlation lag parameters. On the other hand, both parameters sampling level and correlation lag have a significant effect on the CFE estimation accuracy for malicious traffic. Our results show that LoSS is possibly hidden either at small sampling level or correlation lag which can contribute to false alarm detection. The higher sampling level can increase LoSS detection accuracy provided the window size is sufficient. Similarly, the increment of correlation lag can reduce overall detection performance where the estimation time is increased. Therefore, sampling level and correlation lag can affect the performance of LoSS detection for both accuracy and speed. We plan to test the proposed analysis method to various Internet traffic datasets in future to study the reliability of the method.

6. Acknowledgments

This work was funded by Universiti Teknologi Malaysia and Ministry of Science and Innovation Malaysia. The authors are grateful to Dr. Sulaiman Mohd Noor and Mr. Firoz for their helps in preparing the simulation of FSKSMNet dataset.

7. References

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

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

[3] Crovella, M.E. and Bestavros, "A. Self-similarity in World Wide Web traffic: Evidence and possible causes networking," *IEEE/ACM Transactions on Networking*, Volume 5, Issue 6, December 1997, pp. 835 – 846.

[4] Erramilli, A., Narayan, O. and Willinger, W., "Experimental queueing analysis with long-range dependent packet traffic," *Transactions on Networking*, Vol(4), 1996, pp. 209–223.

[5] Feldmann, A., Gilbert, A.C., Willinger, W. and Kurtz, T.G., "The changing nature of network traffic: scaling phenomena," *ACM Computer Communication,* Vol.28(2), April 1998, pp. 5-29.

[6] Idris, M. Y., Abdullah, A. 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), 2004, pp. 83-91.

[7] Kettani, H., "A Novel Approach to the Estimation of the Long-Range Dependence Parameter," *University of Wisconsin – Madison* : PhD. Thesis, 2002.

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

[9] Mazzini, G., Rovatti, R. and Setti, G., "On the Aggregation of Self-Similar Processes," *IEICE Transactions Fundamentals*, Vol.E88–A (10), October 2005, pp 2656 - 2663.

[10] Park, K., Kim, G. and Crovella, M., "On the effect of traffic self-similarity on network performance," *Proceedings*

978-1-4244-2328-6/08/$25.00 © 2008 IEEE

of SPIE International Conference on Performance and Control of Network Systems, November 1997.

[11] Qayyum, A., Islam, M.H., Jamil, M., "Taxonomy of statistical based anomaly detection techniques for intrusion detection," *Emerging Technologies, 2005. Proceedings of the IEEE Symposium on*, 17-18 Sept. 2005, pp. 270-276.

[12] Rohani, M.F., Maarof, M.A., Selamat, A. and Kettani, H., "Uncovering Anomaly Traffic Based on Loss of Self-Similarity Behavior Using Second Order Statistical Model," *International Journal of Computer Science and Network Security (IJCSNS),* Vol.7(9), pp 116-122, September 2007.

[13] Rohani, M.F., Maarof, M.A., Selamat, A. and Kettani, H., "Loss of Self-Similarity Detection with Second Order Statistical Model and Multi-Level Aggregation Approach," *Proceedings of the International Conference on Robotics, Vision, Information and Signal Processing ROVISP2007,* 28-30 November 2007, pp. 152-156.

[14] Schleifer, W. and Mannle, M., "Online error detection through observation of traffic self-similarity", *IEE Proceedings on Communications*, 148(1), Feb. 2001.

978-1-4244-2328-6/08/$25.00 © 2008 IEEE