MULTI-LEVEL SAMPLING APPROACH FOR CONTINOUS LOSS DETECTION USING ITERATIVE WINDOW AND STATISTICAL MODEL

MOHD FO'AD ROHANI[1], MOHD AIZAINI MAAROF[1], ALI SELAMAT[1] AND HOUSSAIN KETTANI[2]

[1]Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81300 Skudai, Johor, Malaysia

[2]Department of Electrical and Computer Engineering and Computer Science, Polytechnic University of Puerto Rico, P. O. Box 192017, San Juan, Puerto Rico 00919, USA

E-mail: {foad, aizaini, aselamat}@utm.my, hkettani@pupr.edu

***ABSTRACT*:** This paper proposes a Multi-Level Sampling (MLS) approach for continuous Loss of Self-Similarity (LoSS) detection using iterative window. The method defines LoSS based on Second Order Self-Similarity (SOSS) statistical model. The Optimization Method (OM) is used to estimate self-similarity parameter since it is fast and more accurate in comparison with other estimation methods known in the literature. Probability of LoSS detection is introduced to measure continuous LoSS detection performance. The proposed method has been tested with real Internet traffic simulation dataset. The results demonstrate that normal traces have probability of LoSS detection below the threshold at all sampling levels. Meanwhile, false positive detection can occur where abnormal traces have probability of LoSS that imitates normal behavior at sampling levels below 100 ms. However, the LoSS probability exceeds the threshold at sampling levels larger than 100 ms. Our results show the possibility of detecting anomaly traffic behavior based on obtaining continuous LoSS detection monitoring.

KEYWORDS: *Loss of Self-Similarity (LoSS), Multi-Level Sampling, Anomaly Traffic Detection, Second Order Self-Similarity, Iterative Window*

1. INTRODUCTION

The advanced technology 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 to providing continuous network traffic monitoring system to ensure that security is well maintained. Thus, the need for reliable monitoring of network anomaly traffic detection in Ethernet network is crucial to ensure uninterrupted Quality of Service (QoS) performance. This can be achieved by continuously detecting Loss of Self-Similarity (LoSS) occurrences in network traffic when the packets are treated as a time series [1-4]. Malicious traffic such as Denial of Service (DoS) packets have tendency to contribute to the deviation from the self-similarity model [3, 4]. Consequently, LoSS is detected [1-4] and a high percentage of LoSS detection will alert a signal of poor QoS performance [5, 6] due to the uncontrolled self-similarity structure. Implementation of LoSS detection with Second Order Self-Similarity (SOSS) statistical model has been introduced in order to attain high speed and accuracy detection needs [2]. Previous works in [1, 2] have used fixed sampling and fixed window to detect LoSS. However, fixed sampling is insufficient to reveal the self-similarity distribution error efficiently [7, 8]. On the other hand, dynamic window is needed for iterative LoSS detection in order to detect the present of anomaly traffic behavior continuously. In this work, we propose a continuous LoSS detection using iterative window and Multi-Level Sampling (MLS) approach. The Optimization Method (OM) [9, 10] is used to estimate self-similarity parameter or known as Hurst (*H*) value. We have evaluated the LoSS detection performance using probability of LoSS detection measurement. This paper is organized as follows: Section 2 discusses in brief the self-similarity model and the estimation method of the parameter *H*. The proposed LoSS detection method is discussed in Section 3 while the experimental and empirical analyses are presented in Section 4. Finally, our conclusion and future work are summarized in Section 5.

2. SOSS MODEL AND ESTIMATION METHOD

2.1 Second Order Self-Similarity Statistical Model and Parameter 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 $X^{(m)} = \{X^{(m)}(t), t > 0\}$ denote the aggregate process of *X* at aggregation level $m > 0$. Thus, we have:

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

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) 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 $0 < \beta < 1$. *X* is called Asymptotical Second-Order Self-Similar (ASOSS) if

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

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

There are several methods to estimate *H*. In this paper we use OM that was developed in [9, 10] 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 [9].

2.2 Loss of Self-Similarity Detection Model

Let *X(t)* be a stochastic time series data with second order stationary property. The autocovariance decay of *X(t)* and aggregated $X^{(m)}(t)$ that follow ESOSS model can be written as 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. Equation (7) shows sampling level *m* does not play an important role in the autocorrelation process for exactly self-similarity model. Nevertheless, the self-similarity processes can also be treated as processes *x(j)* in the class *X* of those stationary processes that feature an asymptotic decay in autocovariance [11]. Thus, we should take into account ESOSS and ASOSS models concurrently in order to estimate the self-similarity parameter for normal and abnormal traffic correctly. To develop LoSS detection using both models; let denotes autocovariance, variance and autocorrelation for aggregated process $X^{(m)}(t)$ as shown in equation (8), (9) and (10):

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

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

$$\lim_{m,k\to\infty} \rho^m(k) = \lim_{m,k\to\infty}\left(\frac{\gamma^m(k)}{\gamma^m(0)}\right) \sim \frac{C_1 m^{-\beta} k^{-\beta}}{C_2 m^{-\beta}} \sim C_3 k^{-\beta} \qquad (10)$$

where C_1, C_2 and C_3 are constants. Previous works in [9, 12, 13] have assumed normal Internet traffic always follow ESOSS model where its characteristics can be described by equations (8) to (10). It is clearly shown in equation (10) that autocorrelation decay is not influenced by aggregation (*m*) parameter for normal traffic. In ESOSS model, the correlation lag (*k*) plays an important role to obtain high accuracy self-similarity parameter (β) estimation.

A high density of DoS packet, such as in the presence of malicious traffic DoS traffic, can produce self-similarity distribution error and disturbs Internet traffic behavior. The normal characteristics of equations (8), (9) and (10) are disrupted. Consequently, LoSS is detected. Equation (11) shows that for abnormal traffic, the autocovariance and variance decay of $C_1 m^{-\beta} k^{-\beta}$ and $(C_2 m^{-\beta})'$ are not identically distributed. As a result, the characteristic of equation (11) deviates from normal self-similarity pattern as shown in equation (10).

$$\lim_{m,k\to\infty} \rho^m(k) = \lim_{m,k\to\infty} \left(\frac{\gamma^m(k)}{\gamma^m(0)} \right) \sim \left(\frac{C_1 m^{-\beta}}{(C_2 m^{-\beta})'} \right) k^{-\beta} \not\simeq C_3 k^{-\beta} \qquad (11)$$

Equations (10) and (11) demonstrate that aggregation (*m*) and correlation lag (*k*) are two parameters that need to be considered for estimating the CFE (or $E_K(\beta)$) value in equation (6) correctly in order to improve LoSS detection accuracy. Previous work in [2] had used OM to estimate self-similarity parameter to detect anomaly traffic. Their method is based on LoSS detection and their definition of normal traffic behavior as follows:

$$H_L \cap CF_N \qquad (12)$$

where $H_L : H \in [0.5,1]$ and $CF_N : CFE < Threshold$ (at fixed sampling *m*).

On the other hand, abnormal behavior defined as LoSS is detected at normal fixed sampling such as CF_N' where $CFE > Threshold$. Nevertheless their technique has only considered fixed sampling such as 10ms or 100ms which is not sufficient to reveal the hidden self-similarity distribution error accurately. Uncovering LoSS at multi-level sampling (MLS) time scale was suggested in [7, 8] in order to reveal the hidden self-similarity distribution error effectively. We investigate multi-level sampling at micro sampling range that is below one second which known as engineering factor [14] for Internet protocol design. We limit the value of correlation lag below five hundred in order to avoid longer time estimation in order to maintain high speed LoSS detection performance.

3. CONTINOUS LOSS DETECTION USING ITERATIVE WINDOW AND MULTI-LEVEL SAMPLING APPROACH

We have considered a multi-level sampling approach with sampling level (*m*) in the range of *10ms ≤ m ≤ 1000ms* in order to investigate the proposed LoSS detection method [7, 8, 14]. We define iterative window as the window size is continuously incremented in a defined fixed size window denoted by *ΔW*. Each of packet traces that accumulated at the current iterative window buffer is then being evaluated for LoSS detection occurrence. The proposed LoSS detection method has considered ESOSS and ASOSS models with their properties are described in equations (7), (10) and (11). Meanwhile, the normal and abnormal traffic behavior has implemented definition based on equation (12) for each of fixed sampling traces in the MLS structure. The procedure of continuous LoSS detection method consists of two processes that includes initializing window and LoSS detection process. The initialization window is done to fulfill the minimum window size requirement before correct estimation of *H* [2] can be obtained. This involves window size that meets the *CFE* criterion below the threshold value. In addition, the definition of initialization window also considers normal LRD behavior such as shown in equation (12). The process of LoSS and SOSS detection can only be continued if the initialization window has been established. However, if initialization window fails (IF) even though enough capturing time is given such as 30 minutes as used in [12, 13], we declare malicious traffic behavior is captured. The algorithm for initialization window process is shown in Fig. 1.

```
set stepSize, $\Delta W$
set window, $W = W + \Delta W$
while ($W < Wmax$)
    estimate H and CFE
    if ($CFE < Threshold$) && ($0.5 < H < 1$)
            Inialization Window success
            SOSS is detected
            proceed with LoSS detection
            else
            increment $\Delta W$++
            set $W = W + \Delta W$
    end
end
if ($W \geq Wmax$) && ($errCheck = 0$)
    Initialization Window failed
    suspect suspicious behavior
end
```

Fig. 1: Initialization window process.

On the other hand, continuous LoSS and SOSS detection with iterative window is based on whether $CFE > 10^{-3}$ for LoSS and $CFE \leq 10^{-3}$ for SOSS. Similar to the process of initialization window procedure, the normal self-similarity behavior that follow SOSS model is also taken into account the normal LRD behavior as defined in equation (12). The LoSS detection algorithm is shown in Fig. 2.

```
while ($W < Wmax$)
    increment $\Delta W$++
    update $W=W+ \Delta W$
    estimate H and CFE
    if ($CFE < Threshold$) && ($0.5 < H <1$)
        SOSS is detected
        else
        LoSS is detected
    end
end
```

Fig. 2: LoSS and SOSS detection process.

We introduce measurement probability of LoSS detection to assess the effectiveness of the proposed detection algorithm. Thus, we define iterative window update in a continuous hunting mode as $W_i = \{W_1, W_2, W_3, ..., W_N\}$ for $i = 1, 2, 3, ..., N$. For each of the updated window *W_i*, if LoSS is detected then we update LoSS window equal to W_i or else update SOSS window with W_i. Suppose we have the updated LoSS and SOSS window as follows: $LoSS(i) = \{L_1, L_2, L_3, ..., L_K\}$ for $i = 1, 2, 3, ..., K$ and $SOSS(j) = \{S_1, S_2, S_3, ..., S_M\}$ for $j = 1, 2, 3, ..., M$. Then, we define the probability of LoSS (P_L) and the probability of SOSS (P_S) detection using equations (12) and (13):

$$P_L = P(LoSS) = \sum_{i=1}^{K} \frac{L_i}{\sum_{j=1}^{K} L_j + \sum_{k=1}^{M} S_k}, \qquad (12)$$

$$P_S = P(SOSS) = \sum_{i=1}^{M} \frac{S_i}{\sum_{j=1}^{K} L_j + \sum_{k=1}^{M} S_k} \qquad (13)$$

There are three possible conditions for P_L and P_S value when we change the sampling level value from lower *m* to higher *m* as follows:

i) $P_L < P_S$
ii) $P_L = P_S$
iii) $P_L > P_S$

The first condition represents the normal behavior of Internet traffic that dominated by self-similarity model and we refer this as near to normal. The smaller value of P_L indicates the higher probability of Internet traffic follows the normal SOSS model. The critical point occurs when both probability values are the same. At this point, LoSS and SOSS occurrences are equally detected and we refer this as critical point where P_L and P_S equal 0.5. On the other hand, the traffic behavior is treated as near to abnormal when the value of P_L is larger than P_S which shows self-similarity leakage is dominant. This condition is usually occurring at higher sampling level such as *m* is larger than 500 ms. At this condition, we can predict that the traffic is deviated from normal SOSS model and can be treated as contains suspicious or malicious packets traffic such as DoS activities.

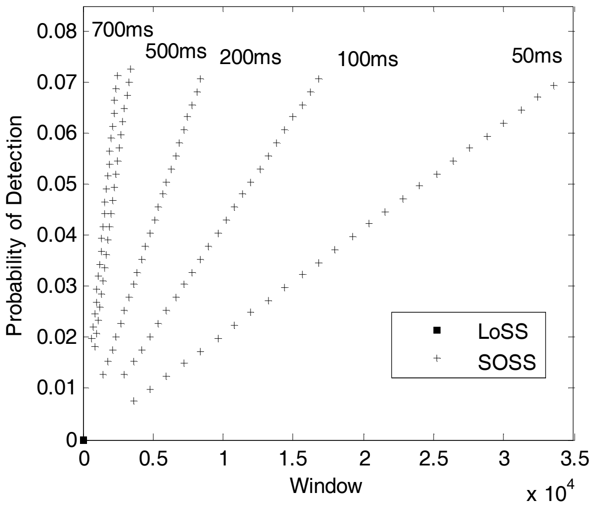
4. EXPERIMENTS AND EMPIRICAL ANALYSES

We have simulated the FSKSMNet Internet traffic traces collected on September 29, 2006 at Faculty of Computer Science and Information Systems (FCSIS) [7] in order to evaluate the proposed LoSS detection method. 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. Each of simulation traces is about 30 minutes and the details are shown in Table 1. FNet-1 and FNet-2 are normal traces while FNet-3 contains UDP, TCP SYN and TCP RST, while FNet-4 has TCP SYN and UDP flooding packets. In the experiments, we set correlation lag *k* equal 100 in order to ensure the elapse time for correlation process in the OM remains fast and optimize. If we set higher value of *k*, we need more sample size packets at the higher sampling level *m* in order to fulfill minimum window requirement as required in the proposed LoSS detection method. In the parameter estimation using OM, the threshold value for estimated *CFE* is set to 10^{-3} to obtain correct estimation *H* as used in [2, 9, 10]. We choose sampling level randomly equal 10ms, 50ms, 100ms, 200ms, 500ms, 700ms and 1000ms [7, 8, 14] to represent multi-level sampling structure in the experiments.

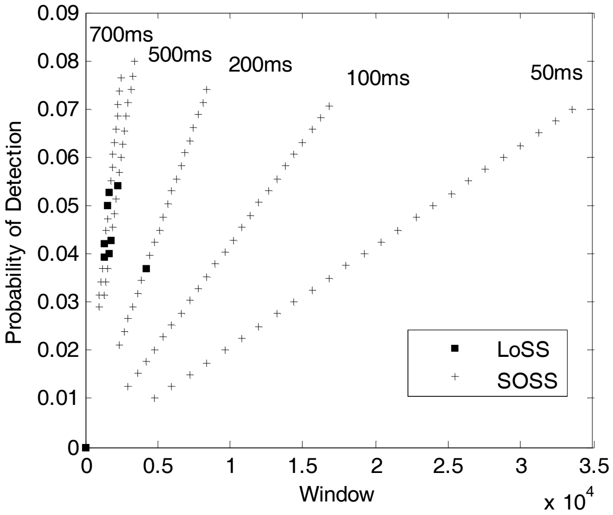
Table 1: FSKSMNet Dataset 2006 [7]

FSKSMNet-Normal	
Trace	*Total Packet*
FNet-1	IP=4197509: TCP(97.87%), UDP(1.69%), ICMP(0.12%), IGMP(0.01%), Others(0.31%)
FNet-2	IP=7371721: TCP(92.17%), UDP(0.93%), ICMP(0.07%), IGMP(0.004%), Others(6.83%)
FSKSMNet-Abnormal	
Trace	*Total Packet*
FNet-3	IP=7468026: TCP(85.60%), UDP(14.35%), ICMP(0.04%), IGMP(0.01%), Others(0.005%)
FNet-4	IP=9707011: TCP(69.17%), UDP(30.77%), ICMP(0.04%), IGMP((0.005%), Others(0.02%)

The results of continuous LoSS detection for FSKSMNet traces are shown in Fig. 3 and Fig. 4 respectively. Fig. 3 illustrates LoSS detection for normal traces while Fig. 4 for malicious traces. Our simulation result shows zero probability of LoSS is detected at all sampling levels of *m* for normal trace FNet-1. The result demonstrates that the normal FNet-1 trace strictly follows ESOSS model as clearly shown in Fig. 3(a). However, there is a tendency for normal Internet activities that produce traffic behavior with a small portion of LoSS detection occurs at higher value of *m* such as above 500ms. This can be illustrated by normal trace FNet-2 in Fig. 3(b). Meanwhile, our result also demonstrates that LoSS is hardly detected for malicious traces FNet-3 at small value of *m* such as lower than 100ms as shown in Fig. 4(a). However, the LoSS occurrence is revealed clearly at higher value of *m* such as larger than 100 ms. The results show that multi-level sampling approach can improve LoSS detection performance as illustrates in Fig. 3 and Fig. 4. The finding is agreed with previous results in [7, 8] where LoSS detection model is implemented by using the property of ESOSS and ASOSS models such as shown in equations (7), (10) and (11).



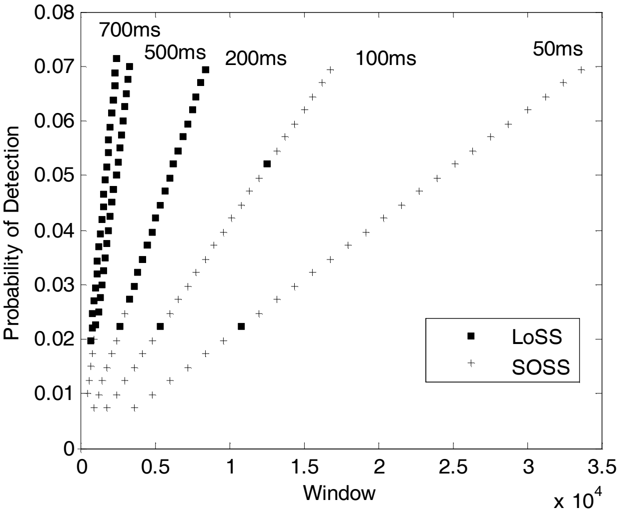
(a)



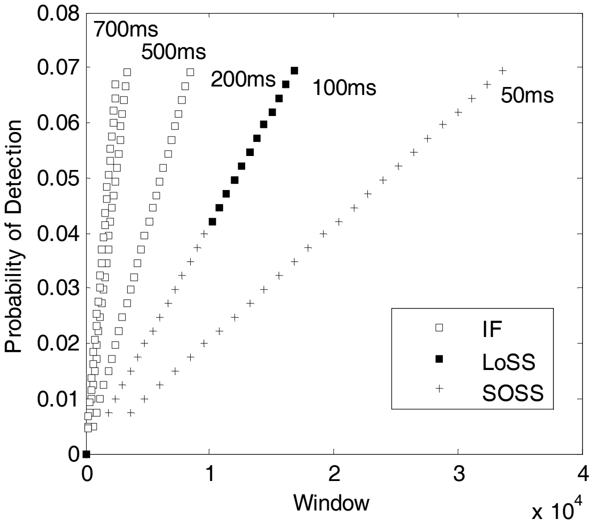
(b)

Fig. 3: LoSS detection for normal traces: FNet-1 (a) and FNet-2 (b).

Another indication for malicious or suspicious behavior presence in the traces is that the failure to obtain the initialized window as illustrated by abnormal trace FNet-4 in Fig. 4(b). As shown in Fig. 4(b), the algorithm is not able to obtain the initialized window or window Initialization Failed (IF) when the value of *m* is larger than 100 ms. This is an additional alert signal that reveals the presence of abnormal traffic packets in the network despite the capability to imitate SOSS model behavior at lower sampling such as value of *m* is less than 100 ms.



(a)



(b)

Fig. 4: LoSS detection for abnormal traces: FNet-3 (a) and FNet-4 (b).

The probability of continuous LoSS detection for normal and abnormal traffic is shown in Fig. 5. The LoSS probability for the normal FNet-1 trace is less than 0.1 for all values of *m,* which is much smaller than the threshold 0.5. Similarly, the normal FNet-2 trace has probability of LoSS value less than 0.1 at sampling level *m* below 500 ms but increase slowly to 0.4 at higher value of *m* larger than 500 ms. However, the probability of LoSS for malicious traces FNet-3 and FNet-4 have similar patterns with FNet-2. They hide the self-similarity distribution error at value of *m* below 100 ms but the error is exposed clearly at value of *m* larger than 100 ms. The result in Fig. 5 also illustrates that both malicious traces FNet-3 and FNet-4 have exceeded the critical probability of LoSS threshold at 0.5. This will give a clear alarm signal to network security analyst that a severe ESOSS leakage is occurred during the continuous LoSS detection process. We define ESOSS leakage as in any level of *m*; there is at least one sampling level where LoSS can be detected. Another word, the self-similarity leakage demonstrates the breach indication of ESOSS model property. Our assumption is that if probability of LoSS value estimated below the threshold i.e. $P_L < 0.5$, then the traffic behavior will be dominated by SOSS model. Otherwise, the majority of updated windows are detected with LoSS which alerts a large amount of ESOSS leakage occurrence. This can be shown in Fig. 5 where FNet-3 and FNet-4 have critical ESOSS leakage warning compared to FNet-1 and FNet-2 at sampling level *m* larger than 100ms. Thus, the probability of LoSS measurement can be used as a technique to reveal the abnormal traffic behavior in a continuous LoSS detection at multi-level sampling approach as illustrates in Fig. 5.

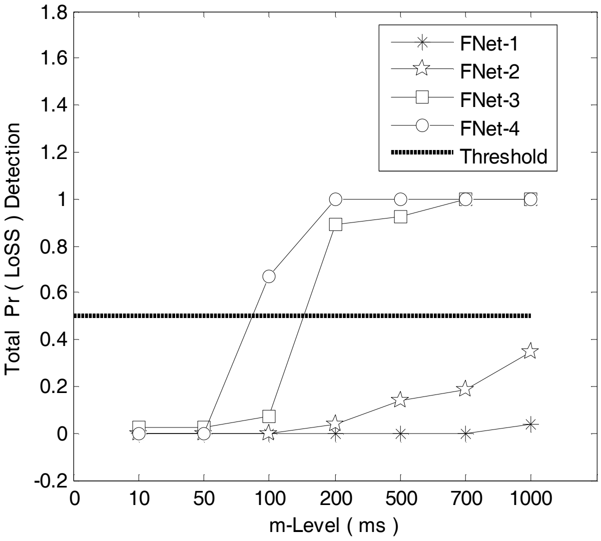


Fig. 5: Probability of continuous LoSS detection.

5. CONCLUSION AND FUTURE WORK

In this paper, we proposed a multi-level sampling approach for continuous Loss of Self-Similarity (LoSS) detection monitoring using iterative window technique. The LoSS detection method is based on Second Order Self-Similarity Statistical (SOSS) model while the Optimization Method (OM) is used to estimate the self-similarity parameter. The proposed method uses CFE criterion and LRD behavior to detect LoSS. If the estimated CFE is not exceeding threshold value and *H* is in the range of LRD, then it is identified as SOSS detection. Otherwise, LoSS is detected. The probability of LoSS introduced in this work can continuously measure LoSS detection performance. Our simulation results show that at all sampling levels, normal traces is usually exhibit small probability of LoSS detection compared to probability of SOSS detection. On the other hand, there is a possibility for malicious traces to have probability of LoSS detection that imitate normal traffic behavior which normally occur at lower sampling level such as below 100ms. However, the probability of LoSS detection for abnormal traffic is clearly exposed when sampling level is larger than 100 ms. This is a promising approach to develop an improved continuous LoSS detection for anomaly traffic behavior monitoring based on SOSS model and multi-level sampling approach. In future, we plan to implement continuous LoSS detection method using average value of multi-level sampling parameters such as average CFE and *H* in multi-level sampling structure. Moreover, the approach can verify whether Internet traffic traces are preserving or violating the self-similarity property based on ESOSS and ASOSS models in order to develop a reliable network traffic monitoring systems.

ACKNOWLEDGEMENT

This work was funded by Universiti Teknologi Malaysia (UTM) under the Human Resource Development Program. The authors are grateful to Dr. Sulaiman Mohd Noor at CICT, UTM and Mr. Firoz at Unit IT, FSKSM for their help in preparing the simulation of FSKSMNet 2006 datasets.

REFERENCES

[1] W. H. Allen and G. A. Marin, "The LoSS Technique for Detecting New Denial of Service Attacks," in *SoutheastCon, 2004. Proceedings. IEEE,* Alabama, USA, 2004, pp. 302-309.

[2] M. Y. Idris, A. H. Abdullah, and M. A. Maarof, "Iterative Window Size Estimation on Self-Similarity Measurement for Network Traffic Anomaly Detection," *International Journal of Computing & Information Sciences,* vol. 2, pp. 83-91, 2004.

[3] W. Schleifer and M. Mannle, "Online error detection through observation of traffic self-similarity," in *Communications, IEE Proceedings-*, 2001, pp. 38-42.

[4] W. Yan, E. Hou, and N. Ansari, "Anomaly Detection and Traffic Shaping under Self-similar Aggregated Traffic in Optical Switched Networks," in *ICCTZ003,* 2003, pp. 378-381.

[5] A. Erramilli, O. Narayan, and W. Willinger, "Experimental queueing analysis with long-range dependent packet traffic," *Networking, IEEE/ACM Transactions on,* vol. 4, pp. 209-223, 1996.

[6] K. Park, G. Kim, and M. E. Crovella, "Effect of traffic self-similarity on network performance," in *Performance and Control of Network Systems,* Dallas, TX, USA, 1997, pp. 296-310.

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

[8] M. F. Rohani, M. A. Maarof, A. Selamat, and H. Kettani, "Loss of Self-Similarity Detection with Second Order Statistical Model and Multi-Level Aggregation

Approach," in *International Conference on Robotics, Vision, Information and Signal Processing (ROVISP2007)*, 2007, pp. 152-156.

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

[10] H. Kettani and J. A. Gubner, "A novel approach to the estimation of the long-range dependence parameter," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 53, pp. 463-467, June 2006.

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

[12] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the self-similar nature of Ethernet traffic," in *ACM SIGCOMM*, 1993, pp. 183–193.

[13] W. E. Leland, M. S. Taqqu, W. Willinger, D. V. Wilson, and M. Bellcore, "On the self-similar nature of Ethernet traffic (extended version)," *IEEE/ACM Transactions on Networking*, vol. 2, pp. 1-15, 1994.

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