LoSS Detection Approach Based on ESOSS and ASOSS Models

Mohd Fo'ad Rohani
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
81300 Skudai, Johor, Malaysia
Tel:+607-5532377
foad@utm.my

Mohd Aizaini Maarof
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
81300 Skudai, Johor, Malaysia
Tel:+607-5532002
aizaini@utm.my

Ali Selamat
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia
81300 Skudai, Johor, Malaysia
Tel:+607-5532099
aselamat@utm.my

Houssain Kettani
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico
P. O. Box 192017
San Juan, Puerto Rico 00919, USA
Tel:+787-6228000 ext. 340, 472
hkettani@pupr.edu

ABSTRACT

This paper investigates Loss of Self-similarity (LoSS) detection analysis using Exactly Second Order Self-Similarity (ESOSS) and Asymptotically Second Order Self-Similarity (ASOSS) models. Recently, anomaly detection based on LoSS has shown results with high false alarm rate detection which needs further improvement. Previous works on LoSS detection have used ESOSS model and fixed sampling that we believe insufficient to reveal LoSS occurrences efficiently, especially at small sampling level packets such as 10ms or 100ms. In this work, we consider ESOSS and ASOSS models concurrently in order to improve LoSS detection performance. We analyze two variables, known as sampling level and correlation lag, to study their effect on LoSS detection accuracy for normal and abnormal traffic. We use Optimization Method (OM) to estimate the self-similarity parameter since it was proven faster and more accurate compared to known methods in the literature. We have tested the proposed analyses approach with synthetic and real Internet traffic simulation traces. Our results show that normal traffic behavior does not influenced by sampling parameter. For malicious traffic, however, the results show that LoSS detection accuracy is very much affected by the value of sampling level and correlation lag used in the estimation.

Keywords

Loss of Self-similarity (LoSS), Anomaly Detection, Parameter Adjustment, Second Order Self-Similarity (SOSS) Model

1. INTRODUCTION

Monitoring Internet traffic especially to detect anomaly traffic is very important to provide 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. When dealing with huge amount of traffic packets that the behavior keep changing unpredictably, anomaly detection using time series model is suggested since the model can produce better results than others statistical models [17]. Recent studies have shown that self-similarity model is widely used for Internet traffic modeling [3], [7], [10], [11], [16]. According to self-similarity model, the autocorrelation of inter arrival traffic packets is assuming to exhibit hyperbolic decay and Long Range Dependent (LRD). These assumptions are true for normal traffic but in the presence of malicious traffic such as Denial of Service (DoS) packets, the self-similarity distribution error [20], [21] is introduced and perturbs the self-similarity model. Consequently, Loss of Self-similarity (LoSS) is detected [1], [6], [20], [21], to alert security analysts due to uncontrolled self-similarity structure in network queue buffer [4], [13]. Thus, packets queue buffer time delay and packets drop rates will drastically increased [4], [13] 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], [18]. Previous works [6],

however, have used fixed sampling time series packets which is insufficient to reveal self-similarity distribution error correctly [18]. In this work, we investigate LoSS detection accuracy and its dependency on two variables known as sampling (or aggregation) level and correlation lag. We use Second Order Self-similarity (SOSS) statistical model and the Optimization Method (OM) that was developed in [7], [8] 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. This paper analyzes LoSS detection performance using different values of sampling level and correlation lag. The effect of these parameters to minimizing the CFE accuracy and estimation time speed is investigated. The sequel of this paper is organized as follows: Section 2 discuses related works. Section 3 discuses in brief the self-similarity model and LoSS detection method. The experimental and empirical analyses are presented in Section 4. Finally, our conclusions are summarized in Section 5.

2. RELATED WORKS

LoSS detection was used in previous works [1], [6], [20], [21] as indicator to detect the presence of anomaly Internet traffic activities. The work in [20], [21] used the abrupt change property of self-similarity distribution ratio of higher scale to lower scale as an indicator to the presence of distribution error. Their results show that the deviation error of distribution scaling ratio due to malicious traffic is clearly exposed when compared to normal traffic. The weakness of scaling distribution ratio method such as in [20] used a fixed distribution time scale as a reference template. Nevertheless the works are not suggesting at what level of aggregation scale to be used for significantly reveals the self-similarity distribution error. Alternatively, the work in [1] defined LoSS as self-similarity parameter or Hurst *(H)* value beyond normal range of LRD using Periodogram and Whittle estimation method. Their method did not depend on specific template to detect new DoS attack pattern. Their 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. Recently, a new method of estimating *H* parameter known as the Optimization Method (OM) which is more accurate and faster was developed in [7]. The estimation method provides a technique to identify whether the data tend to follow the self-similarity model or not according to the CFE estimation. Consequently, the work in [6] used OM to detect anomaly traffic based on LoSS using CFE criterion. Nevertheless the technique only considered fixed sampling and fixed correlation lag (we refer as dependent parameters) which we believe insufficient to reveal the hidden of self-similarity distribution error efficiently. Therefore, this paper gives more efforts to investigate the effect of dependent parameters toward obtaining an accurate CFE estimation in order to reduce high false alarm rate LoSS detection.

3. SELF-SIMILARITY MODEL AND ESTIMATION METHOD

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

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

Let $\rho^{(m)}(k)$ denote 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 $0<\beta<1$. X is called Asymptotical Second-Order Self-Similar (ASOSS) if

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

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 [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].

3.2 LoSS Detection Using Parameter's Adjustment Based On ASOSS Model

Let $X(t)$ as a stochastic time series processes with second order stationary that follow self-similarity features. The autocovariance decay of $X(t)$ and aggregated $X^{(m)}(t)$ should follow ESOSS model as shown in equation (7):

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

where *m* is sampling level, *k* is correlation lag, C_o is constant and β is self-similarity parameter with $0 < \beta < 1$.

In real Internet traffic packets, however, the self-similarity processes is also considered as processes *x(j)* in the class *X* of those stationary processes that feature an asymptotic decay in autocovariance [12]. Thus, we should consider ESOSS and ASOSS models concurrently in order to estimate the self-similarity parameter correctly for normal and abnormal traffic.

Let denotes autocovariance, variance and autocorrelation for aggregated process $X^{(m)}(t)$ as follow [12]:

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

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

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

where C_1, C_2 and C_3 are constants.

The self-similarity parameter estimation from previous works [7], [10], [11], [14] have used assumption that normal Internet traffic follows ESOSS model which its characteristics should follow equations (8) to (10). Equation (10) clearly demonstrates that autocorrelation function 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 theory, *k* equal to one is enough to estimate β provided the self-similarity behavior pattern is known prior to the estimation process. In reality, however, real Internet traffic behaviors have mixed from many sources such as Internet traffic models [16], Internet applications, user's actions and network infrastructure [3]. Thus, modern Internet traffic can go beyond normal self-similarity or LRD behavior such as multi-fractal and chaotic behavior [2], [5]. Therefore, suitable value of *k* is needed in order to accurately estimate CFE without sacrificing negligible long tail correlation value.

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 decaying's pattern of $C_1 m^{-\beta}$ and $(C_2 m^{-\beta})'$ are not identical and not following normal self-similarity pattern as in equation (10).

$$\lim_{m,k\to\infty} \rho^m(k) = \lim_{m,k\to\infty} \left(\frac{\gamma^m(k)}{\gamma^m(0)} \right) \approx \left(\frac{C_1 m^{-\beta}}{(C_2 m^{-\beta})'} \right) k^{-\beta} \neq C_3 k^{-\beta} \tag{11}$$

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's accuracy. Therefore, we investigate parameter's adjustment that considers sampling level at micro sampling range (i.e. below 1 second) [2], [5], [18] which known as engineering factor [2] in designing new protocol. We limit the change value of correlation lag below one thousand in order to avoid longer estimation time hence maintaining high speed LoSS detection performance.

4. EXPERIMENTAL AND EMPIRICAL ANALYSES

4.1 Experimental Simulation Datasets

We evaluate the proposed LoSS analysis approach with different datasets which includes synthetic Fractional gaussion (fGn) [9], University of Carolina (UNC) 2002 and 2003 datasets [14], [15] and our Internet traffic dataset FSKSMNet 2006 [19]. The synthetic traffic fGn trace is artificial traffic packets that exhibit ESOSS model and about 180,000 packets are generated for the testing. On the other hand, UNC2002 is a suspicious trace that was captured in the UNC network infrastructure while UNC2003 represents a normal traffic trace. We simulate FSKSMNet traffic traces as to compare with current Internet traffic packets in the Faculty of Computer Science and Information Systems (FCSIS). Our traffic simulation is about 30 minute's duration which consists of normal traffic that was filtered by network firewall and administration network policy of FCSIS. On the other hand, our malicious simulation traffic contains TCP SYN and UDP flood attacks at controlled rates less than 60 second each. The percentage protocol for normal traffic is presented as 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 malicious traffic contains protocol 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%. For each of the traces, we provide different sets of sampling level at micro sampling which known as engineering factor that is important for designing and analysis protocol purposes [2]. We sample all traces with sampling level 10ms < *m* < 1000ms [18], [19]. On the other hand, we use the correlation lag parameter with the value changes from 50 up to 500. In the process of LoSS detection purposes, we use the criterion of normal behavior as CFE < 10^{-3} [7] while abnormal behavior as CFE > 10^{-3} where LoSS is detected [6].

4.2 LoSS Detection for Synthetic fGn

Figure 1 shows the result of LoSS estimation for fGn trace with different sampling level (*m*) and correlation lag (*k*) values. In the result, it is clearly shown that no LoSS is detected since the CFE estimation is always below the threshold value regardless of *m* and *k* values are used. This shows that the fGn trace follows ESOSS model where the sampling parameter does not affect estimation process of self-similarity parameter. Thus, the traffic behavior estimated using small or high *m* will give similar behavior as shown by equation (4). Based on equation (4), the only parameter that can influence CFE estimation is *k*. In our simulation result, however, the estimated CFE of fGn trace is still below the threshold despite the incremental values of *k*.

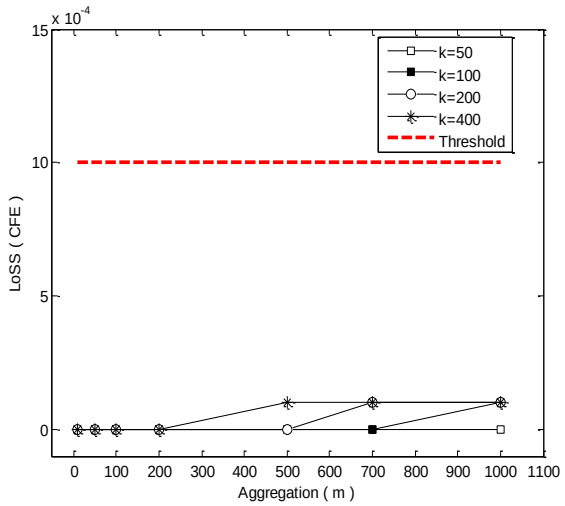


Figure 1. LoSS detection performance for fGn

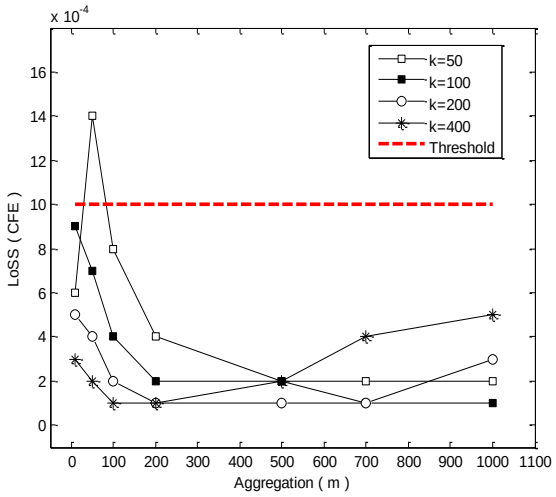
4.3 LoSS Detection for Normal Traffic

The results of LoSS detection for normal Internet traffic simulation traces are shown in Figure 2 (a) for UNC2003 and (b) for FSKSMNet 2006 respectively. The details of CFE estimation for normal UNC2003 trace are presented in Table 1. It is clearly illustrated in Figure 2(a) that normal of UNC2003 trace is almost following ESOSS model as shown in equation (4). The result shows that the UNC2003 trace preserves the self-similarity behavior for all *m* and *k* values, except if the estimation is done at *m* less than 100ms and *k* less than 100 where LoSS can be detected.

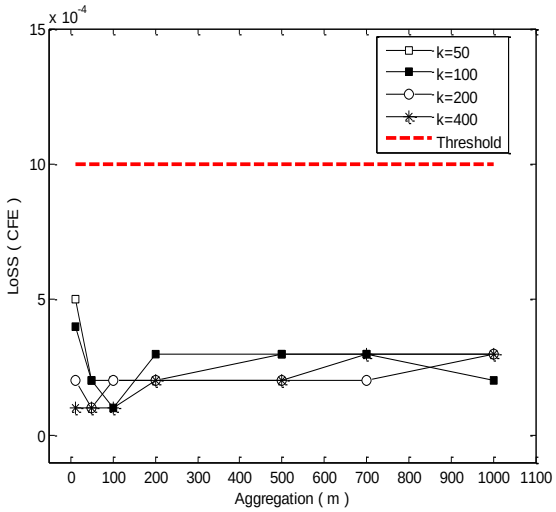
Table 1. Details CFE estimation for normal: UNC2003

Sampling (m)	Auto-correlation lag (k)					
	50	100	200	300	400	500
10	0.0006	0.0009	0.0005	0.0004	0.0003	0.0002
50	0.0014	0.0007	0.0004	0.0002	0.0002	0.0002
100	0.0008	0.0004	0.0002	0.0002	0.0001	0.0001
200	0.0004	0.0002	0.0001	0.0001	0.0001	0.0001
500	0.0002	0.0002	0.0001	0.0001	0.0002	0.0002
700	0.0002	0.0001	0.0001	0.0002	0.0004	0.0004
1000	0.0002	0.0001	0.0003	0.0005	0.0005	0.0004

As shown in Table 1, the self-similarity parameter of normal trace is incorrectly estimated if small sampling level such as *m* equal 50ms and insufficient correlation of long tailed autocorrelation process when using small *k* such as *k* equal 50. On the other hand, FSKSMNet 2006 normal traffic exhibits ESOSS model since at all *m* and *k* values the self-similarity behavior is preserved where zero LoSS is detected. Our result shows that for normal Internet traffic that follows ESOSS model, *m* does not affecting the self-similarity parameter estimation accuracy. The results also agree with previous works in [7], [10], [11] that fixed sampling can be used to correctly estimate the self-similarity parameter provided the traffic trace follows ESOSS model. Furthermore, sufficient correlation lag value has to be used in order to obtain adequate long tailed autocorrelation process for the traffic time series packets.



(a) UNC2003



(b) FSKSMNet 2006

Figure 2. LoSS detection performance for normal traffic traces: (a) UNC2003 (b) FSKSMNet 2006

4.4 LoSS Detection for Abnormal Traffic

Unlike normal traffic behavior, our results show that ESOSS model is not valid for abnormal traffic. As shown by equations (10) and (11), representing real traffic with both ESOSS and ASOSS models can improve LoSS detection accuracy. Thus, it is important to analyze LoSS at different sampling level and correlation lag in order to reduce false alarm LoSS detection performance. Table 2 presents details of LoSS detection's results for suspicious trace UNC2002 while Figure 3 illustrates its LoSS detection pattern. As shown in Table 2, at small *m* such as 10ms and *k* uses less than 100, LoSS is detected. However, the traffic follows SOSS model at *k* more than 100 is used. Meanwile, the suspicious trace has zero LoSS detection at sampling levels equal 50ms and 100ms when *k* less than 500 is used. Consequently, the

LoSS occurrence can be revealed efficiently if we increase sampling value to higher level such as larger than 200ms. This can be shown in the results such as at sampling level *m* equal 200ms and *k* bigger than 200, LoSS is fully detected. Similarly, the LoSS occurrence is also entirely revealed and detected at *m* larger than 500ms and *k* bigger than 50 are used.

Table 2. Details CFE estimation for suspicious: UNC2002

Sampling (m)	Auto-correlation lag (k)					
	50	100	200	300	400	500
10	0.0014	0.0012	0.001	0.0008	0.0007	0.0007
50	0.0004	0.0003	0.0002	0.0002	0.0001	0.0001
100	0.0001	0.0001	0.0001	0.0004	0.0008	0.0007
200	0.0002	0.0003	0.0006	0.0012	0.0014	0.0016
500	0.0004	0.0012	0.0018	0.0016	0.0024	0.0035
700	0.0005	0.0015	0.0015	0.0024	0.0047	0.0063
1000	0.001	0.0016	0.0021	0.0055	0.0067	0.0071

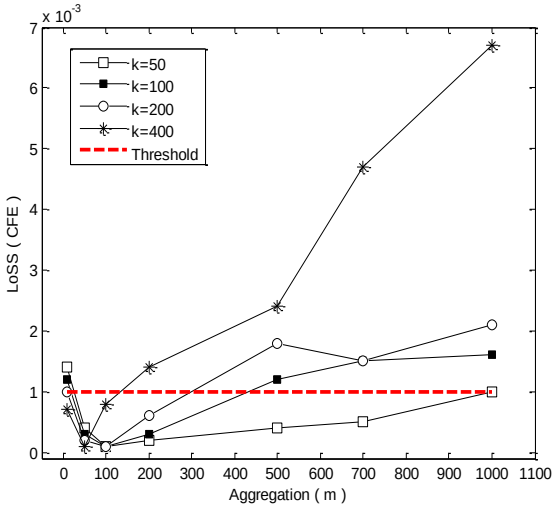


Figure 3. LoSS detection for suspicious traffic UNC2002

In general, different values of *m* and *k* may produce difference CFE estimation for malicious FSKSMNet 2006 traffic which can affect LoSS detection performance. The details result of LoSS detection for FSKSMNet 2006 trace is presented in Table 3 and Figure 4 illustrates its LoSS detection pattern. As shown in Table 3, at small sampling level such ad *m* equal 10ms, the malicious traces follows normal SOSS model where LoSS is hidden and not detected. The increment of sampling level, however, can improve the accuracy of LoSS detection as in the previous UNC2002 trace. This can be shown from Table 3 such as at *m* equal 50ms, 100ms and 200ms; LoSS is revealed when using *k* bigger than 300, 100 and 50 respectively. Furthermore, at *m* larger than 500ms LoSS is fully detected regardless any values of *k* between $50 < k < 500$ are used. Consequently, LoSS detection accuracy performance can be improved by incrementing the value of *m* and *k*. The drawback when using higher level of *m* is the window size packets used must be large enough in order to fulfill minimum window requirement [6] before correct estimation can be done. This means more capturing time duration is needed for time series packets traffic when using larger sampling level *m* such as more than one second compared to micro sampling scale. A bigger size of correlation lag *k* can increase CFE estimation accuracy, however, longer time is needed to execute larger correlation sliding process hence decrease overall estimation time process.

Table 3. Details CFE estimation for malicious: FSKSMNet 2006

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

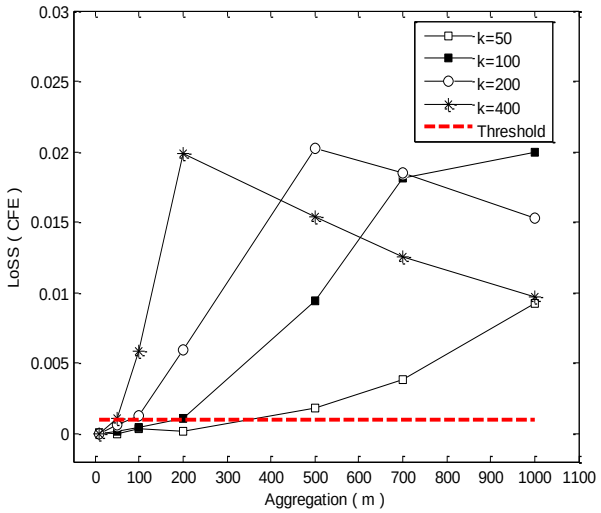


Figure 4. LoSS detection for malicious traffic FSKSMNet 2006

Our experimental results demonstrate that sampling level does not influence the accuracy of the CFE estimation for normal traffic that exhibits ESOSS model. The estimation accuracy, however, is affected by the value of correlation lag. On the other hand, sampling level and correlation lag are two important factors that can affect the CFE estimation accuracy for abnormal traffic that contains suspicious or malicious packets. This is important when real Internet traffic behavior applies both ESOSS and ASOSS models concurrently in order to estimate self-similarity parameter accurately and detect LoSS efficiently.

5. CONCLUSIONS

The simulation results show that LoSS detection accuracy can be improved when we consider ESOSS and ASOSS models

concurrently in self-similarity parameter estimation method. In ESOSS model, autocorrelation decay is only affected by correlation lag. Based on ASOSS model, however, in the existence of self-similarity distribution error where LoSS is detected, sampling and correlation lag parameters are identified as a prime factor that can influence CFE estimation accuracy. The experimental results demonstrate that sampling level does not influences CFE estimation for normal traffic that follows ESOSS model. The accuracy of the estimated CFE, however, is very much depending on correlation lag parameters. The results also show that for normal traffic, the estimated CFE is still not exceeding the threshold value despite various correlation lag values are used. On the other hand, both parameters aggregation and correlation lag have a significant effect on the CFE estimation accuracy for malicious traffic. Meanwhile, LoSS occurrences is possibly hidden when using lower sampling level or smaller correlation lag value which can contribute to false alarm detection.Thus, higher sampling level used in packet sampling time series data can improve LoSS detection accuracy provided the window size is sufficiently provided. Similarly, LoSS detection accuracy is also improved by increasing the correlation lag value. The drawback is, the bigger correlation lag value is used the longer estimation time is needed to execute extra correlation process in the time series data.

5. ACKNOWLEDGMENTS

This work was funded by Universiti Teknologi Malaysia (UTM). The authors are grateful to Dr. Sulaiman Mohd Noor at CICT, UTM and Mr. Firoz at Unit IT, FSKSM for their helps in conducting the simulation of real Internet traffic FSKSMNet dataset.

6. REFERENCES

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

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

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

[4] Erramilli, A., Narayan, O. and Willinger, W. 1996. Experimental queueing analysis with long-range dependent packet traffic. IEEE/ACM Trans. Networking, 4:209–223.

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

[6] Idris, M. Y., Abdullah, A. H. and Maarof, M. A. 2004. 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.

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

[8] Kettani, H. and Gubner, J. A. June 2006. A Novel Approach to the Estimation of the Long-Range Dependence Parameter. IEEE Transactions on Circuits and Systems II, Vol. 53, Issue 6, pp. 463-467.

[9] Ledesma, S. and Liu, D. April 2000. Fractional Gaussian noise power spectrum synthesis using linear approximation for generating self-similar network traffic. ACM Computer Communication Review, Vol. 30, no.2, pp. 4-17.

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

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

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

[13] Park, K., Kim, G. and Crovella, M. November 1997. On the effect of traffic self-similarity on network performance. SPIE International Conference on Performance and Control of Network Systems.

[14] Park, C., Hernández-Campos, F., Marron, J. S., and Smith, F. D. Jun. 2005. Long-range dependence in a changing internet traffic mix. Computer Networks Vol. 48(3), pp. 401-422.

[15] Park, C., Hernández-Campos, F., Marron, J. S., and Smith. 23 May 2003. UNC DIRT Laboratory Internet traces. http://www-dirt.cs.unc.edu/ts/.

[16] Paxson, V. and Floyd, S. June 1995. Wide-area traffic: The failure of Poisson modeling. IEEE-ACM Transactions on Networking, Vol. 3(3).

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

[18] Rohani, M.F., Maarof, M.A., Selamat, A. and Kettani, H. September 2007. 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 No.9, pp 116-122.

[19] Rohani, M.F., Maarof, M.A., Selamat, A. and Kettani, H. 28-30 November 2007. 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, pp. 152-156.

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

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