Journal of Marine Science and Technology
DOI: 10.6119/JMST-013-0516-1

NETWORK BURST MONITORING AND DETECTION BASED ON FRACTAL DIMENSION WITH ADAPTIVE TIME SLOT MONITORING MECHANISM

Hsiao-Wen Tin [1], Shao-Wei Leu [1], Shun-Hsyung Chang [2], and Gene Eu Jan [3]

Key words: underwater acoustic communication, direct-sequence spread spectrum, delay-locked loop, synchronization.

ABSTRACT

This study proposed an approach to measure the burstiness of network traffic based on fractal dimensions (FDs). By definition, burstiness is the degree of variation in network traffic. This study defined two types of FDs: 1) the FD of network traffic that describes the flow variation of network traffic, and 2) the FD of the range that describes the degree of flow dispersal. The proposed method uses an adaptive time-slot monitoring mechanism to monitor the network. The relevant FDs are derived from measurements obtained during each time slot in a monitoring window.

This study conducted experiments using NS2 simulation data. The experimental results indicated that the proposed method can effectively measure the burstiness of network traffic, provides a meaningful method to describe the variation of network traffic, and reduces monitoring overhead by using the adaptive time-slot monitoring mechanism.

I. INTRODUCTION

Network traffic measurement has attracted considerable interest in recent decades [1, 2, 20]. One of the main objectives of network traffic measurement is detecting bursty traffic that degrades network performance and reliability [5]. In general, a network burst causes undesirable buffer overflow and increases queuing delays [3, 17, 21].

Burstiness is usually defined as the tendency of network packets to arrive in bursts. The definition for burstiness has not been standardized because the objectives of each study have differed. For example, Lan et al. [5] defined train burstiness as the product of the mean packet arrival rate in a unit of time and the mean interval between bursts. Sarvotham et al. [13] stated that a bursty flow was a flow in which the peak rate exceeded the mean rate of traffic plus three standard deviations of aggregated traffic. Regardless of the varying definitions of burstiness, an appropriately measuring burstiness is critical for traffic monitoring and administration.

Since the discovery of fractal properties inherent in the traffic of various computer communication networks, such as the Ethernet local area network (LAN) [6], wide area network (WAN) [11], and wireless network [16], fractal techniques have been widely used in network management studies. For example, researchers have been using the fractal dimension (FD) to describe network traffic for more than a decade [10, 12, 19] . Recent studies have also indicated that the FD is extremely useful in describing traffic burstiness [15]. Network traffic is often characterized by its chaotic and irregular variability. By focusing on the irregularity of the variation of network traffic, the FD is well suited to quantify those morphological characteristics that several studies have used in a qualitative sense to analyze the characterization of network traffic.

Based on these research trends, this study proposed two FDs to analyze the complexity of network traffic, namely, the FD of traffic (*TFD*) and the FD of range (*RFD*). The proposed method derives the FDs for burstiness from measurements obtained in two consecutive monitoring windows. Each window is subdivided into a fixed number of time slots. One traffic measurement is taken per slot. Using these measurements to plot a network traffic graph. An FD method is then applied to the network traffic graph to derive the FDs.

This study proposed an adaptive time-slot monitoring mechanism to reduce the execution overhead of traffic monitoring. If burstiness is not detected in the current window, then the duration of the time slots in the next window is increased. Longer slots indicate that the number of traffic measurements is fewer, hence the overhead is lowered. If bursty traffic does occur, then the duration of the time slots in next window is reset to the initial value.

The remainder of this study is arranged as follows: Section 2 presents a review of several previous studies including some definitions of bursty flow, the Box-Counting Method

Paper submitted 09/17/12; revised 04/26/13; accepted 05/16/13. Author for correspondence: Shao-Wei Leu (e-mail: B0119@mail.ntou.edu.tw).
[1]Department of Electrical Engineering, National Taiwan Ocean University, Keelung, Taiwan. R.O.C.
[2]Department of Microelectronics Engineering, National Kaohsiung Marine University, Kaohsiung, Taiwan, R.O.C.
[3]Department of Electrical Engineering, National Taipei University, Taipei County ,Taiwan , R.O.C.

(BCM)-based FD calculation, and time-slot based network traffic monitoring. Section 3 introduces burstiness measurement using two proposed FDs with the adaptive time-slot monitoring mechanism. Section 4 shows the application of the proposed method to two network models established with NS2, illustrating its ability to detect bursty traffic. The frequency of traffic readings with or without the adaptive time-slot monitoring mechanism is also compared. Section 5 offers a conclusion.

II. RELATED WORKS

1. Current Approaches to Defining Bursty Flow

Most current burstiness measurements focus on counting network flows. The most widely used definition of a flow was suggested by Lan et al. [5] , in which the flow is a series of unidirectional packets that have the same source/destination addresses, protocol, and port numbers. The next paragraph introduces two conventional methods that were proposed by Sarvotham et al. [13] and by Lan et al. [5]. Both methods are performed on the basis of counting flows.

Sarvotham et al. suggested that bursty traffic was caused by numerous bytes or packets arriving simultaneously. They classified the flows as either *alpha flows* or *beta flows*. According to Sarvotham et al., an alpha flow is a flow whose peak rate exceeds the threshold defined as the mean of the flow rate plus three standard deviations of the aggregate traffic [13]. If a flow satisfies (1), then it is considered an alpha flow:

$$alpha\ flow := burst_{peak} > Agg_{\mu} + 3 \times Agg_{sd} \quad (1)$$

where $burst_{peak}$, Agg_{μ} , and Agg_{sd} represent the flow peak rate in this duration, the mean rate of traffic, and the standard deviation of the aggregate traffic, respectively.

Lan et al. defined the burst as a train of packets within the interarrival time [5] as defined in (2):

$$burst := packets\ with\ interarrival\ time < tt \quad (2)$$

where tt is a time threshold.

Train burstiness is defined as the product of the mean burst rate and mean inter-burst time, as follows:

$$burstiness := mean\left(burst_{rate}\right) \times mean\left(burst_{iter}\right) \quad (3)$$

where $burst_{rate}$ is the packet arrival rate in a time unit, and $burst_{iter}$ is the interval between bursts.

Bursty flow is a flow with burstiness greater than the mean plus three standard deviations of the sampled flows, as indicated in (4):

$$bursty\ flow := flow_{burstiness} > mean + 3 \times sd \quad (4)$$

where $flow_{burstiness}$, $mean$, and sd represent flows with burstiness, the mean of the sampled flows, and the standard deviations of the sampled data, respectively.

2. Counting Boxes to Estimate the Fractal Dimension

By expressing the degree of complexity, the FD is a useful tool to describe natural objects [9]. One popular approach to obtaining the FDs, as measurements of the space filling property of an object, is the BCM. The main process of the BCM is to fully cover a planar object with N boxes, with each side being of length l , which is also the scale of measurement. The correlation of l and $N\left(l\right)$ is expressed in (5):

$$N\left(l\right) \propto l^{-D} \quad (5)$$

where D represents the FD. From (5), the relationship $\log N\left(l\right) \propto D \log l^{-1}$ follows naturally. According to the definition of FD by [7, 8], D may be obtained as in (6):

$$D = \lim_{l \to 0} \frac{\log(N\left(l\right))}{\log\left(1/l\right)} \quad (6)$$

When scale l approaches infinitesimal, $N\left(l\right)$ approximates infinity. The result of calculating a physical object by using (6) is approximate. To obtain the FD, various scales can be applied to produce differing $N\left(l\right)$ values; by plotting $\log N\left(l\right)$ against $\log\left(1/l\right)$, and fitting a regression function to the plot, the FD is obtained as the slope of the regression line.

3. Time Slot in Network Monitoring

To avoid relative errors in the process of network traffic measurement, a network administrator must continuously monitor the network traffic and log the details. Gilly et al. [4] indicated that continuous monitoring of network traffic causes considerably high overhead in the monitoring process. Therefore, reducing the monitoring frequency and preventing relative errors are critical for network administrators. Currently, the most common practice is to execute the monitoring according to a certain time interval (i.e., a time slot).

Most Time Period Studies have focused on obtaining the best possible accuracy with the smallest possible number of periods for reducing the overhead of the monitoring process. Two primary period scheduling mechanisms of monitoring process based on the number of time slots are the static time-slot mechanism and the dynamic time-slot mechanism. The static time-slot method uses a fixed number of slots, which is a disadvantage because the monitoring overhead is constant. In contrast, the dynamic time-slot method is flexible in time scheduling, and its monitoring overhead relies on the process of determining the number of slots.

III. TECHNIQUES METHOD OF BURSTINESS MEASUREMENT

1. Fractal Dimension of Traffic

This study collected a sequence of network traffic data as a summation of flows within a period and then plotted the data on the Y-axis against the start time of each period on the X-axis. This study obtained the FD of the measured network traffic by applying the BCM to the plot. The FD of the curve represents the variation of traffic over a certain period and is referred to in this study as TFD . The TFD could reflect the complexity of

the curve that represents the degree of the variation of the network traffic.

In theory, a curve can be completely covered with $N(l)$ contiguous square boxes with each box measured $l \times l$. As the size of the box approaches zero, the total area covered by the boxes converges to the measurement of the curve. In practice, the FD of the curve is estimated by first counting the number of boxes that is required to fully cover the curve for several box sizes, and then by fitting a regression line to the log-log plot of $\log N(l)$ versus $\log l$. The slope of the regression line $\log N(l)$ versus $\log l$ is the FD of the curve that represents the TFD.

2. Fractal Dimension of Range

Network traffic consists of several flows. The traffic can be bursty when a relatively large flow occurs. The measurement of the degree of the dispersal of flows in each interval is useful for detecting burstiness.

The proposed method regards the difference between the maximal flow and minimal flow sizes within a time slot as the range. This study plotted the maximal flow and the minimal flow within a period on the Y-axis against the start time of each period on the X-axis; two curves were then obtained. The area between two curves represents the flow range. By applying (6) to the area, this study was able to estimate the FD of the area, which represents the RFD and reflects the degree of the flow dispersal and the variation of range trend (i.e., a smaller RFD indicates that the flow sizes are closer). The difference in the flow sizes increases in conjunction with the increase of the RFD.

The *RFD* can be estimated by using the BCM. The estimation procedure is described as the follows: 1) choose a flow range of network traffic within period *P* and place the curves on a space. 2) Choose a set of boxes of various sizes, such that box length l tends to be zero. 3) Cover the area with the boxes. For each l, the corresponding number of boxes necessary to cover the entire range, $N(l)$, is counted. 4) Plot $\log N(l)$ against $\log 1/l$, for various l. By applying a process similar to the one in Section III.1 that solves (6), the FD of the range is readily available as the slope of the regression line. If the flow range of the network traffic is a fractal, then the logarithm plot is a straight line.

3. FD Based Detection of Bursty Traffic

To estimate the burstiness of the traffic, this study designated two adjacent time windows: the reference window and target window. The designated window consists of a given number of time slots. The window size changes as the slot periods change. Within each of the alternating windows, traffic measurements are obtained and the two FDs discussed earlier are derived. By definition, bursty traffic has occurred when the FDs in the reference window are both less than their counterparts in the target window, each by a certain threshold.

As the monitoring continues, the duration of the time slot for the next target window is determined by the result of the comparison between the FDs in the current reference and target windows. The mechanism for changing the duration of a time slot is described below:

(a) Initially, both windows consist of n time slots of duration t. Hence, the size of each window is $n \times t$. Let the start point of the reference window be W_S. Therefore, the start point of the target window is $W_S + nt$, as shown in Fig. 1(a).

(b) Let ΔTFD be the difference between the *TFD* in the reference window and its counterpart in the target window. Similarly, let ΔRFD be the difference between the *RFD* in the reference window and its counterpart in the target window. The following conditions are suggested for the detection of bursty traffic:

$$\{\Delta TFD \geq threshold_t\} \text{ and } \{\Delta RFD \geq threshold_r\} \quad (7)$$

where $threshold_t$ is the threshold of the FD of traffic and $threshold_r$ is the threshold of the FD of range. Bursty traffic is detected when the traffic satisfies both conditions in (7).

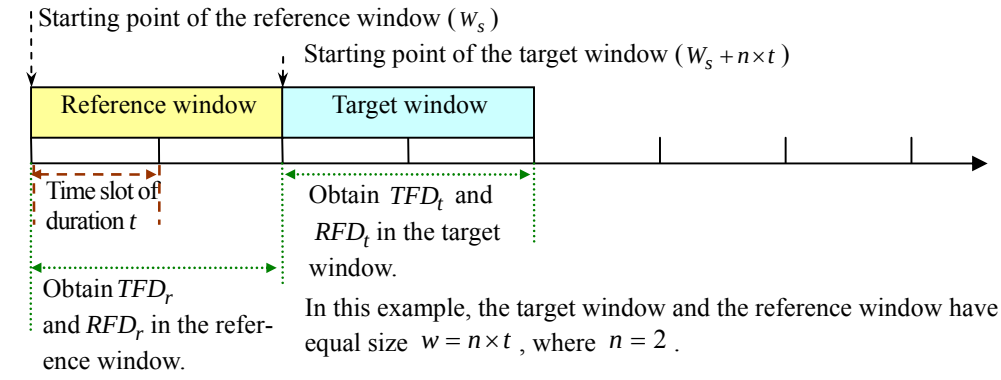
(c) If any condition in (7) is not satisfied, then bursty traffic has not occurred in the target window. In such a case, it is reasonable to decrease the monitoring frequency by increasing the duration of the time slots for the next target window. This study chose to double the duration of the time slots in the upcoming window. For the subsequent comparisons to be meaningful, the last original reference and target windows were combined into a new reference window. The new target window is the same size. The TFD and RFD of the new reference window are the means of the two respective counterparts from each of the two original windows.

(d) If both of the conditions in (7) are satisfied, then bursty traffic is detected and the target window is a bursty window. Consequently, the duration of the time slots for the next target window reverts to the initial value and the size of the next target window is also restored to the initial value. The duration of the time slots reverts to the initial values, indicating that the size of the next target window also reverts to the initial length as presented in Fig. 1(c).

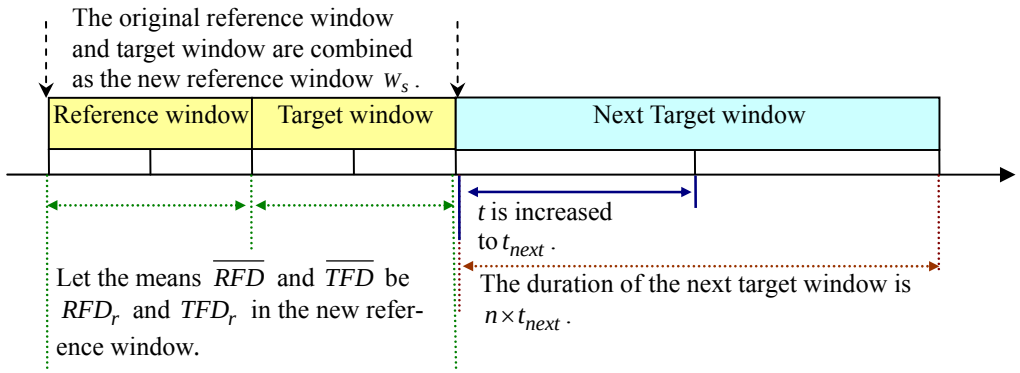
The adaptive time-slot monitoring mechanism shown in Figs. 1(b) and 1(c) is summarized by (8):

$$t_{next} = \begin{cases} t_{initial}, & \text{If both of the conditions in (7) hold} \\ t_{current} + t_{initial}, & \text{otherwise} \end{cases} \quad (8)$$

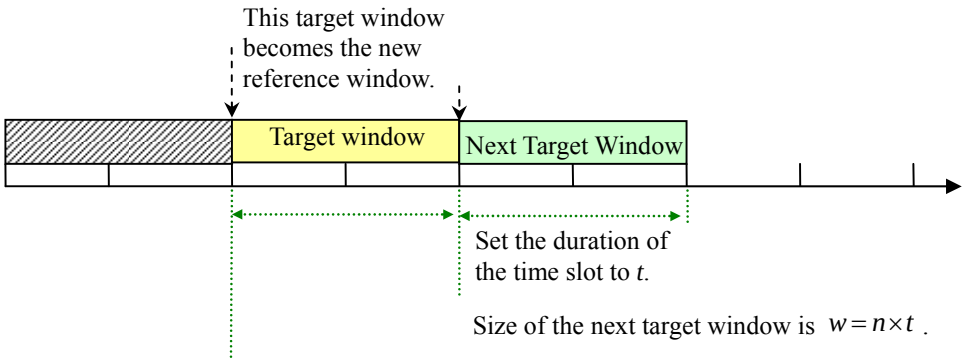
where $t_{initial}$ is the duration of the time slot at the initial step, $t_{current}$ is the duration of the time slot in the current target window, t_{next} is the new duration of the time slot for the next target window.



(a) Initial step: setting the initial values.



(b) If any of the differences of FDs between the target window and reference window is less than the threshold, non-bursty traffic is detected in the target window. Hence, the duration of the time slot is increased.



(c) If both of the FDs in the target window are greater than the FDs in the reference window and the differences of the FDs are greater than or equal to the thresholds, a bursty traffic is detected. That is, the target window is a bursty window. So, set the duration of time slots to the default value for the next target window and let the current target window be the new reference window.

Fig. 1 Adaptive time slot monitoring mechanism.

IV. SIMULATION SCENARIO AND ANALYSIS

1. Network Traffic Model

This study used the Pareto ON/OFF model; the connection-level traffic model [13] for both models have been used in major studies on bursty traffic, such as Willinger et al. [18] and Sarvotham et al. [13]. This study set the simulation of TCP flow at the packet level to simplify the experimental conditions.

Simulation 1. Pareto ON/OFF Model:

The simulator transmits the packets according to parameter $\alpha = 1.2$, which is the same value used by Sarvotham et al. [13]. The OFF state of the Pareto ON/OFF model is the idle time during which packets are not transmitted. The waiting time depends on parameters γ and ω, where $\gamma = 1.1$ and $\omega = 0.36$. The topology is depicted in Fig. 2.

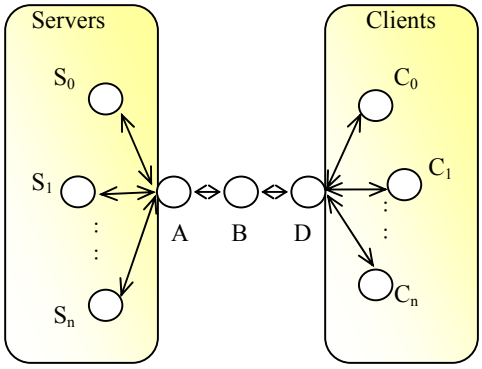


Fig. 2. Topology of the Pareto ON/OFF model

The parameters used in the experiment are presented in Tables 1 and 2. These values were selected according to the NS2

Table 1. Link parameters for Pareto ON/OFF model.

Link	Bandwidth (Kbps)	Latency (ms)
D – clients	5000	10
A – B	20000	20
B – D	20000	20
A – servers	10000	20

Table 2. Topology parameters for Pareto ON/OFF mode.

Parameter	Value
Number of server	40
Number of clients	90
Mean ON time	0.5 sec
Mean OFF time	0.5 sec
Pareto parameter α	1.2
Burst Rate	200k
Packet size	15

parameters used in Savotham et al. [13] as well as the parameters recommended in the user guide of the NS2. Overall, 40 sources, 90 clients, and 3 middle nodes were included in the simulation. A total of 90 flows between the source nodes and client nodes were established as evenly as possible. The observation period was 10 s, and the time slot was set to 0.1 s. Therefore, the number of measurements was 100.

Node A in Fig. 2 is designated as the observation point for this topology. This study collected the packets that were generated by 90 flows passing through node A and plotted the data, as shown in Fig. 3.

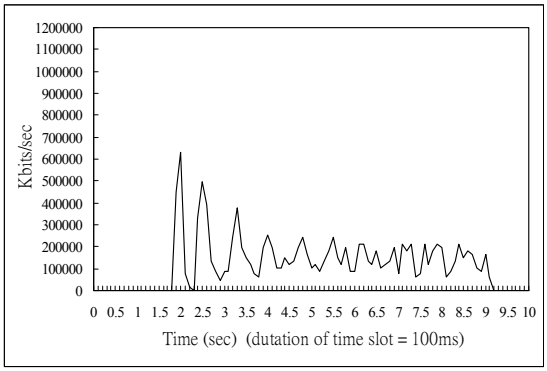


Fig. 3 TCP traffic in Pareto ON/OFF model.

Simulation 2. Connection-level Traffic Model:

The topology of the connection-level traffic model is depicted in Fig. 4 based on the model used in the Sarvotham et al. experiment [13]. The parameters of this model are presented in Tables 3 and 4.

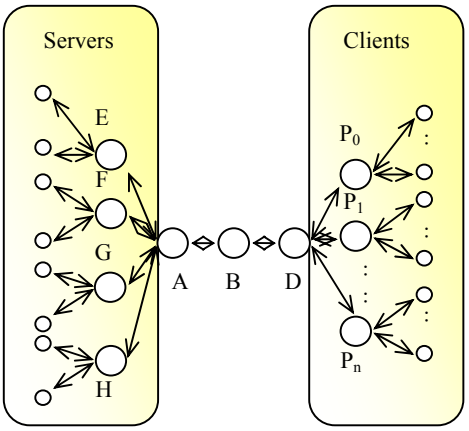


Fig. 4: Topology of the connection-level traffic model.

Table 3. Link parameters for connection-level traffic model.

Link	Bandwidth (Kbps)	Latency (ms)
D – P_0	12000	20
D – P_1 to D – P_n	Unif (50,120)	20
P_i – clients	5000	10
A – B	20000	20
B – D	20000	20
A – E to A – H	10000	20
E – servers to H – servers	10000	Unif (10,100)

Table 4. Topology parameters for connection-level traffic model.

Parameter	Value
Number of servers per E – H	10
Number of nodes P_i	15
Number of clients per P_i	6
Mean ON time	0.5.
Mean OFF time	0.5
Pareto parameter α	1.2
Burst Rate	200k
Packet size	15

As shown in Fig. 4, four transmission nodes, from E to H, were established on the Server side. Each transmission node connects to 10 source nodes. On the client side, six receiver nodes each connect to 15 destination nodes. Two sides are connected by three middle nodes. The source nodes and destination nodes were connected as evenly as possible. The observation period was 10 s, and the time slot was 0.1 s. Overall, 100 measurements were performed.

For this topology, node A is the observation point, and the packets from 90 flows were collected. Fig. 5 shows the results of the observation over the entire period.

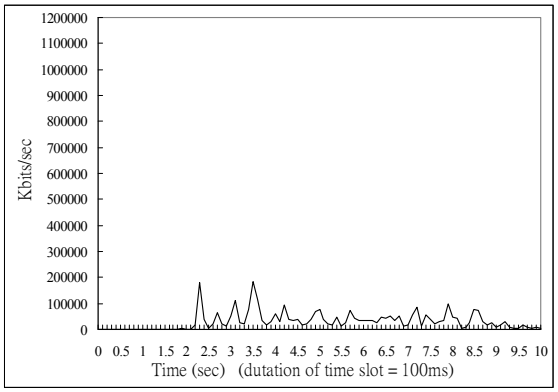


Fig. 5 TCP traffic in the connection-level traffic model.

2. Measuring Burstiness by Using Adaptive Time Slot Monitoring Mechanism

By applying the adaptive time-slot monitoring mechanism, the size of the reference window and the size of the target window were initialized to the same value $n \times t$. Let $n = 20$, $t = 0.1$, and the starting point of reference window $W_s = 0$. This study applied Fractalyse version 3.4.7 [14] to obtain the FDs. The plots of the traffic data and their corresponding *TFD* are depicted in Figs. 6 and 7. The plots of the range data and the corresponding *RFD* are shown in Figs. 8 and 9.

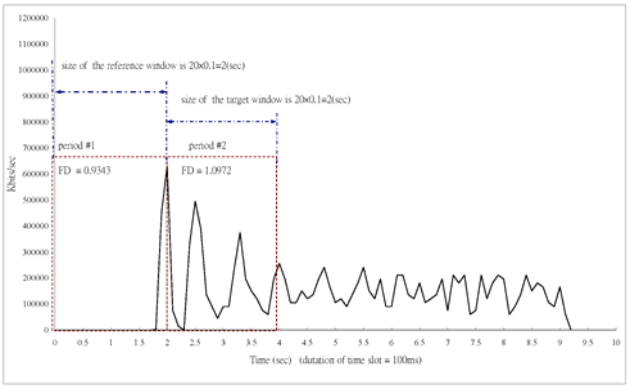


Fig. 6 Analysis of the *TFD* in the Pareto ON/OFF model with the duration of the time slots = 0.1 sec.

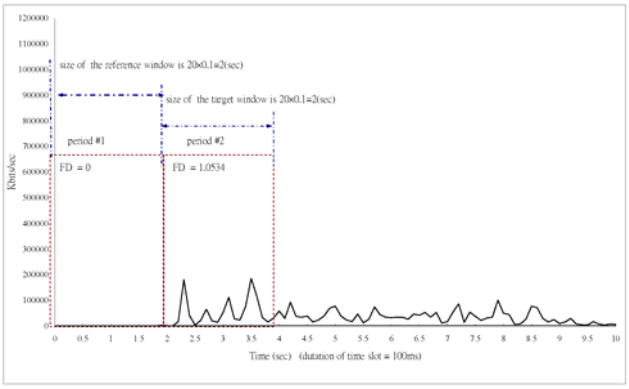


Fig. 7 Analysis of the *TFD* in the connection-level traffic model with the duration of the time slots = 0.1 sec.

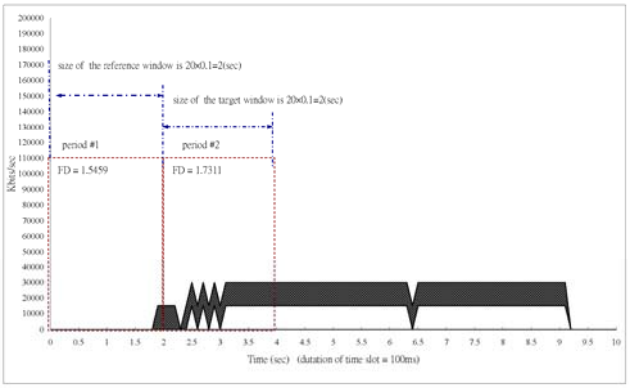


Fig. 8 Analysis of the *RFD* in the Pareto ON/OFF model with the duration of the time slots = 0.1 sec.

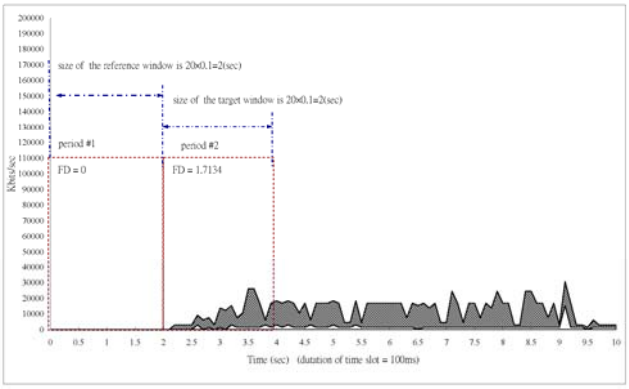


Fig. 9 Analysis of the *RFD* in the connection-level traffic model with the duration of the time slots = 0.1 sec.

The following two experiments are presented as examples to explain the function of the proposed mechanism based on the FDs. The first experiment demonstrated a situation in which bursty traffic was undetected; therefore, the system increased the duration of the time slot in the next target window as depicted in Fig. 1(b). The second experiment shows cases in which bursty traffic exists. Upon detection of bursty traffic, the system reset the duration of the time slot in the next target window as shown in Fig. 1(c).

Experiment 1. Non-bursty TCP Traffic

In a situation where bursty traffic is undetected, assume $threshold_{traffic} = 2$ and $threshold_{range} = 2$.

With the Pareto ON/OFF model, the difference of the *TFD* between the first reference window (Period #1 in Fig. 6) and the first target window (Period #2 in Fig. 6) is $\Delta TFD = 0.1629$. The difference of the FD_{range} between the first reference window (Period #1 in Fig. 8) and the first target window (Period #2 in Fig. 8) is $\Delta RFD = 0.1852$. Because either *TFD* or *RFD* does not satisfy the conditions expressed in (7), the new duration of the time slot for the next target window is $t_{new} = t_{current} + t = 0.2$. The adjustment is depicted in Fig. 10.

In the connection-level traffic model, the difference of the *TFD* between the first reference window (Period #1 in Fig. 7) and the first target window (Period #2 in Fig. 7) is $\Delta TFD = 1.0534$. The difference of the *RFD* between the first reference window (Period #1 in Fig. 9) and the first target window (Period #2 in Fig. 9) is $\Delta RFD = 1.7134$. Again, neither *TFD* nor *RFD* satisfy the conditions expressed in (7). The new duration of the time slot for the next target window should be $t_{new} = t_{current} + t = 0.2$. The adjustment is shown in Fig. 11.

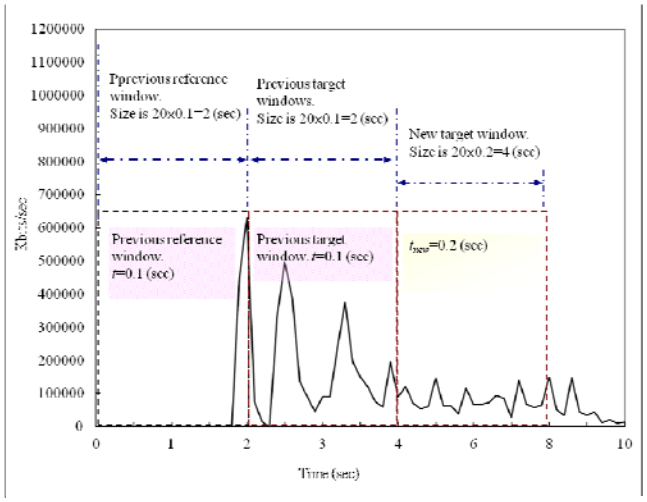


Fig. 10 In the Pareto ON/OFF model, the duration of the time slot in the next target window is increased if no bursty TCP traffic is detected.

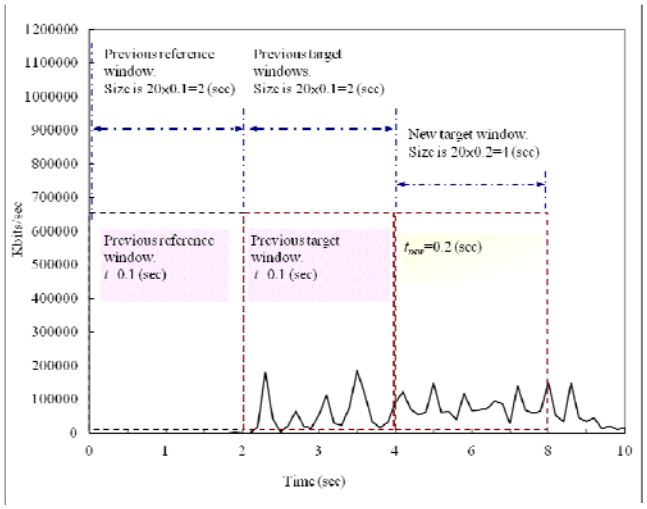


Fig. 11 In the connection-level traffic model, the duration of the time slot in the next target window is increased if no bursty TCP traffic is detected.

Experiment 2. Bursty TCP Traffic

In a situation where bursty traffic exists, let $threshold_{traffic} = 0.1$ and $threshold_{range} = 0.1$.

In the Pareto ON/OFF model, $\Delta TFD = 0.1629$, $\Delta RFD = 0.1852$, and both conditions in (8) are satisfied. The new duration of the time slot for the next target window was reset to the initial value (i.e., $t_{new} = t = 0.1$). The adjustment is shown in Fig. 12.

In the connection-level traffic model, $\Delta TFD = 1.0534$, $\Delta RFD = 1.7134$, and both conditions in (8) are satisfied. The new duration of the time slot for the next target window was reset to the initial value, $t_{new} = t = 0.1$. The adjustment is presented in Fig. 13.

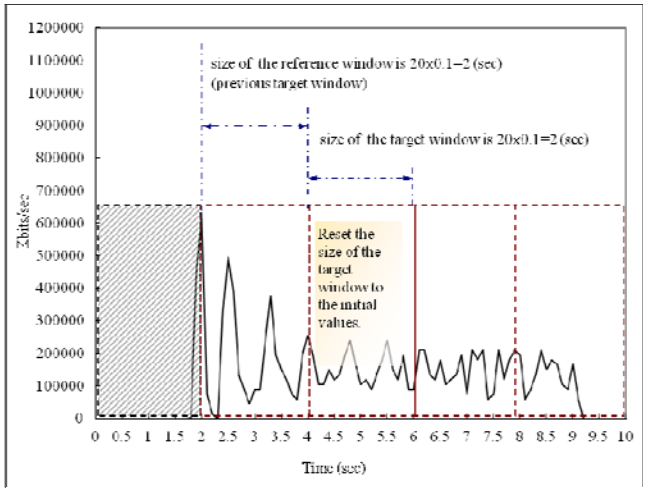


Fig. 12 When a bursty TCP traffic is detected in the Pareto ON/OFF model, reset the duration of the time slot in the next target window.

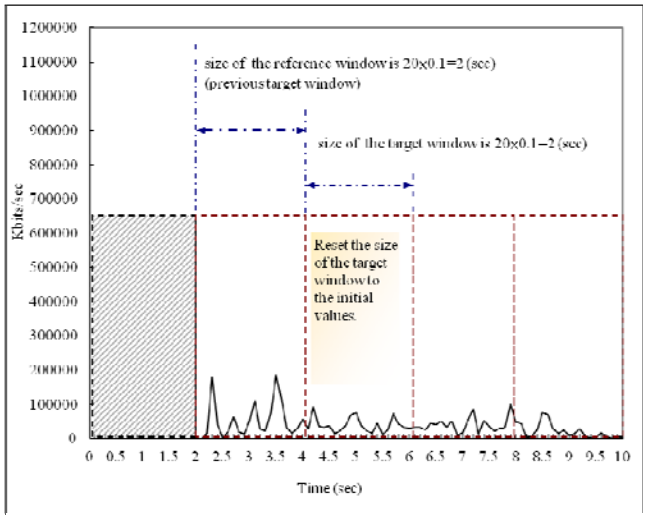


Fig. 13 When a bursty TCP traffic is detected in the connection-level traffic model, reset the duration of the time slot in the next target window.

3. Analysis of the Experimental Results

This experiment considered the number of time slots during the entire observation period to compare the results obtained with and without the adaptive time-slot monitoring mechanism.

Experiment 1 emphasized a situation where non-bursty traffic was detected during an observation period of 8 s as shown in Figs. 10 and 11. When using the adaptive time-slot monitoring mechanism, the duration of time slots increased after the first comparison. The number of time slots required during the period of observation for both models was $4/0.1+4/0.2=60$. In contrast, when the adaptive time-slot monitoring mechanism was not used, the number of time slots required for both models became $8/0.1=80$. The results clearly demonstrate the ability of the adaptive time-slot monitoring mechanism in reducing the number of monitoring operations.

Experiment 2 emphasized situations where bursty traffic could appear. When using the adaptive time-slot monitoring mechanism, upon the detection of bursty traffic, the duration of time slots was set to the default value for the following target window. For an observation period of 6 s, the number of time slots required was $6/0.1=60$ with or without applying the adaptive time-slot monitoring mechanism. This result neither reduced nor increased the overhead of traffic monitoring.

Table 5 presents the numbers of time slots in both experiments. The results indicated that increasing the duration of the time slots requires fewer number of time slots to obtain samples of network data, thereby incurring less computational overhead.

Table 5. The number of slots in the observation time of 8 sec. and 6 sec. for monitoring (i) without the adaptive time slot monitoring mechanism and (ii) with the adaptive time slot monitoring mechanism.

The number of slots in experiment 1		The number of slots in experiment 2	
(i)	(ii)	(i)	(ii)
80	60	60	60

Burstiness is related to network traffic behavior, which is characterized by flow variation and flow dispersion. In this study, to obtain the relationship between the network traffic and the *TFDs*, the standard Pearson method was chosen to compute their correlation. The correlation values represent how the differential of the FDs react when detecting bursty traffic; this only requires considering Experiment 2. In the Pareto ON/OFF model, the Pearson correlation value is 0.858095, and in the connection-level traffic model, the Pearson correlation is value 0.987001. Both correlations show the relationships are strong and positive, which explains how burstiness detection can be conducted by measuring the flow variation of network traffic.

To obtain the relationship between the flows and the *RFDs*, the standard Pearson method was chosen to compute the correlation. In the Pareto ON/OFF model, the Pearson correlation value is 0.366558, and the relationship is medium and positive. In the connection-level traffic model, the Pearson correlation value is 0.551530, and the relationship is strong and positive, which explains how burstiness detection can be conducted by measuring the dispersion of flows.

V. CONCLUSION

This study presented a novel approach to measuring bursty network traffic based on FDs. Two FDs, *TFD* and *RFD*, were proposed and detailed. The experimental results based on simulated network traffic demonstrate the effectiveness of the proposed method in measuring bursty traffic. By applying the adaptive time-slot monitoring mechanism, the proposed method was also able to reduce the frequency of traffic probing operations, thereby lowering the overall cost of network monitoring.

ACKNOWLEDGMENTS

The authors thank Dr. H. Sasaki, S. Shibata, and T. Hatanaka of the National Institute of Livestock and Grassland Science for providing us with the Fractal analysis system for Windows software for our experiments. The authors also thank the

anonymous reviewers for their useful comments regarding this paper. This work is supported by the National Science Council of Taiwan, under contract NSC99-2923-E-022-001-MY3.

REFERENCES

1. Callado, A., Kamienski, C., Szabo, G., Gero, B., Kelner, J., Fernandes, S.,Sadok, D., "A Survey on Internet Traffic Identification," *IEEE Communications Surveys & Tutorials*, 2009, pp. 37-52 (2009).
2. G. Aceto, A. Botta, A. Pescape, C. Westphal, "Efficient Storage and Processing of High-Volume Network Monitoring Data," *IEEE Transactions on Network and Service Management*, pp. 1-4 (2013).
3. Garetto M. and Towsley D., "Modeling, simulation and measurements of queuing delay under long-tail internet traffic," *Proceedings of the 2003 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, pp. 47-57 (2003).
4. Gilly K, Alcaraz S., Juiz C. and Puigjaner R., "Analysis of burstiness monitoring and detection in an adaptive Web system," *Computer Networks* , pp. 668-679 (2009).
5. Lan K. C., and Heidemann J., "An measurement study on the correlation of Internet flow characteristics," *ISI-TR-574. Computer Network*, Vol. 1, No. 50, pp.46-62 (2006).
6. Leland, W. E., Taqqu, M. S., Willinger, W. and Wilson, D. V., "On the Self-Similar Nature of Ethernet Traffic (Extended Version)," *IEEE/ACM Trans. on Networking*, Vol.2, No.1, pp.1-15 (1994).
7. Li J., Sun C., and Du Q., "A new box-counting method for estimation of image fractal dimension," *2006 IEEE International Conference on Image Processing*, pp. 3029-3032 (2006).
8. Liu S. T.. "An improved differential box-counting approach to compute fractal dimension of gray-level image," *Information Science and Engieering*, Vol. 1, 2008, pp.303-306 (2008).
9. Mandelbrot B. B., *Fractal Geometry of Nature*, Fkeeman Press, San Fkancisco (1982).
10. Mansfield, G., Roy, T. K., Shiratori, N., Proceedings., "Self-similar and fractal nature of Internet traffic data," *15th International Conference on Information Networking*, pp. 227-231 (2001).
11. Paxson V. and Floyd S., "Wide Area Traffic: A Failure of Poison Modeling, " *IEEE/ACM Transactions on Networking*, pp. 226-244 (1995).
12. Riihijarvi, J., Wellens, M. and Mahonen, P., "Measuring Complexity and Predictability in Networks with Multiscale Entropy Analysis," *INFOCOM 2009*, pp.1107-1115 (2009).
13. Sarvotham S., Riedi R., and Baraniuk R., "Connection-level Analysis and Modeling of Network Traffic," *ACM SIGCOMM Internet Measurement Workshop*, pp. 99-103 (2001).
14. Sasaki H., Shibata S. and Hatanaka T., An Evaluation Method of Ecotypes of Japanese Lawn Grass (Zoysia japonica STEUD.) for Three Different Ecological Functions. *Bull. Natl. Grassl. Res. Inst.* Vol.49, pp. 17-24 (1994)
15. Tin H.W., Leu S.W. and Chang S.H., "Measurement of flow burstiness by fractal technique," *2010 International Computer Symposium*, pp. 722-727 (2010).
16. Wang T., Yu Q., Mao Y., "Fractal characteristics analysis of wireless network traffic based on Hurst parameter," *ICCCAS 2009*, pp. 173-176 (2009).
17. Wei D.X., Cao P., and Low S.H., "Packet Loss Burstiness: Measurements and Implications for Distributed Applications," *IPDPS 2007*, pp. 1-8 (2007).
18. Willinger W., Taqqu M.S., Sherman R., Wilson D.V., AT&T Bell Labs. and NJ. Murray Hill, "Self-Similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level," *IEEE/ACM Trans. on Networking*, Vol.5, No.1, pp. 71-86 (1997).
19. Xu Zongyan, Xing Linfang, Zhou Feifei, Wang Yilin, "Fractal characteristics of transportation network of Tianjin city," *2010 International Conference on Mechatronics and Automation (ICMA)*, pp. 356-359 (2010).
20. Zhang Jun, Xiang Yang, Wang Yu, Zhou Wanlei, Xiang Yong, Guan Yong, "Network Traffic Classification Using Correlation Information," *IEEE Transactions on Parallel and Distributed Systems*, pp. 104-117 (2013).
21. Zhang K., Ge X., Liu C., and Xiang L., "Analysis of Frame Traffic Characteristics in IEEE 802.11 Networks," *ChinaCOM 2009*, pp. 1-5 (2009).