Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2008, Article ID 475878, 11 pages
doi:10.1155/2008/475878

Research Article

Detection of Variations of Local Irregularity of Traffic under DDOS Flood Attack

Ming Li[1] and Wei Zhao[2]

[1] *School of Information Science and Technology, East China Normal University, No. 500, Dong-Chuan Road, Shanghai 200241, China*
[2] *Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY 12180-3590, USA*

Correspondence should be addressed to Ming Li, ming_lihk@yahoo.com

Received 24 March 2008; Accepted 1 April 2008

Recommended by Cristian Toma

The aim of distributed denial-of-service (DDOS) flood attacks is to overwhelm the attacked site or to make its service performance deterioration considerably by sending flood packets to the target from the machines distributed all over the world. This is a kind of local behavior of traffic at the protected site because the attacked site can be recovered to its normal service state sooner or later even though it is in reality overwhelmed during attack. From a view of mathematics, it can be taken as a kind of short-range phenomenon in computer networks. In this paper, we use the Hurst parameter (H) to measure the local irregularity or self-similarity of traffic under DDOS flood attack provided that fractional Gaussian noise (fGn) is used as the traffic model. As flood attack packets of DDOS make the H value of arrival traffic vary significantly away from that of traffic normally arriving at the protected site, we discuss a method to statistically detect signs of DDOS flood attacks with predetermined detection probability and false alarm probability.

1. Introduction

IP Networks are subject to electronic attacks [1]. An intrusion detection system (IDS) collects information from a variety of systems and network sources to analyze the information of attack signs. A network-based IDS monitors the traffic on its network as a data source [2]. For distributed denial-of-service (DDOS) flood attack, an intruder bombs attack packets upon a site (victim) with a huge amount of traffic the sources of which are distributed over the world [3]. Hence the pattern of traffic under DDOS flood attack may suddenly differ significantly from the normal pattern of the arrival traffic. From the perspective of dynamical aspects for limited time interval in physics [4], one may regard this sudden change as a specific "pulse." Though DDOS flood attack may not be a sole factor to make traffic pattern vary significantly, we assume that secure officers can distinguish significant variation of monitored traffic pattern caused by other known factors (e.g., normally heavy traffic) from DDOS flood

attack. Without confusions causing, the term abnormal traffic used in this paper specifically implies a traffic series that has significant variation of traffic pattern caused by DDOS flood attack.

In this research, we ponder two fundamental issues in detection. One is feature extraction of monitored traffic time series. The other is detection scheme that can be used to assure predetermined detection probability (P_d) and false alarm probability (P_f). The first issue will be discussed in Section 2 from a view of feature extraction of traffic based on self-similarity of traffic. The second will be dissertated in Section 3 based on statistical detection. Section 4 will explain the performance analysis of the present detection system. A case study is demonstrated in Section 5. Discussions are given in Section 6, which is followed by conclusions.

2. Feature extraction of traffic

2.1. Self-similar traffic

Computer scientists in the last decade discovered that traffic is a type of fractal time series. It has the properties of self-similarity, long memory, and multiscales (see e.g., [5]). A commonly used model in traffic engineering is fractional Gaussian noise (fGn) (see e.g., [6–8]).

Let $B(t)$, $t \in (0,\infty)$ be Wiener Brownian motion. Let $B_H(t)$ be fractional Brownian motion with the Hurst parameter $H \in (0,1)$ [9]. Let $\Gamma(\cdot)$ be Gamma function. Then by using fractional calculus, $B_H(t)$ is expressed by

$$B_H(t) - B_H(0) = \frac{1}{\Gamma(H+1/2)}\left\{\int_{-\infty}^{0}\left[(t-u)^{H-0.5} - (-u)^{H-0.5}\right]\mathrm{dB}(u) + \int_{0}^{t}(t-u)^{H-0.5}\,\mathrm{dB}(u)\right\}. \tag{2.1}$$

Let $G(t)$ be the increment series of $B_H(t)$:

$$G(t) = B_H(t+a) - B_H(t), \tag{2.2}$$

where a is a real number. Then $G(t)$ is fGn [9]. The autocorrelation function (ACF) of fGn in the discrete case is given by

$$\rho(\tau) = \frac{\sigma^2}{2}\left[\left||\tau|+1\right|^{2H} - 2|\tau|^{2H} + \left||\tau|-1\right|^{2H}\right], \tag{2.3a}$$

where $\sigma^2 = \Gamma(2-H)\cos(\pi H)/\pi H(2H-1)$ is the intensity of fGn [10]. The normalized ACF of fGn is given by

$$R(\tau) = \frac{1}{2}\left[\left||\tau|+1\right|^{2H} - 2|\tau|^{2H} + \left||\tau|-1\right|^{2H}\right]. \tag{2.3b}$$

The relationship between the fractal dimension of fGn and H is given by

$$D = 2 - H. \tag{2.4}$$

Approximating the right side of (2.3b) with the second-order differential of $0.5(\tau)^{2H}$, see [9, H15, page 350], for $\tau \geq 0$, yields

$$0.5\left[(\tau+1)^{2H} - 2\tau^{2H} + (\tau-1)^{2H}\right] \approx H(2H-1)\tau^{2H-2}. \tag{2.5}$$

Let y and R be a traffic series and its ACF, respectively. Then according to (2.5),

$$R(\tau) \sim c\tau^{2H-2}, \quad H \in (0.5, 1), \tag{2.6}$$

where $\sim$ implies the asymptotical equivalence under the limit $\tau \to \infty$ and $c > 0$ is a constant [11].

The ACF (2.5) is nonsummable for $H > 0.5$, implying long-range dependence (LRD). Hence H is a measure of LRD of traffic. It is kindly noted that LRD of traffic does not mean that DDOS attacking is a long-range phenomenon. On the contrary, DDOS attacking and its detection are short-range phenomena since both sides, namely, an attacker and its opponent, are engaged with each other during a short period of time. Such a battle makes local irregularity of traffic vary dramatically [12].

Without losing generality, we consider traffic series y in the discrete case. By dividing y into nonoverlapping blocks of size L and averaging over each block, we obtain another series given by

$$y(i)^{(L)} = \frac{1}{L} \sum_{j=iL}^{(i+1)L} y(j). \tag{2.7}$$

According to the analysis in [5, 9, 11], in the fGn sense, one has

$$\mathrm{Var}\left(y^{(L)}\right) = L^{2H-2}\,\mathrm{Var}(y), \tag{2.8}$$

where Var implies the variance operator. Thus the self-similarity is measured by H.

A series encountered in engineering is usually of finite length. Let y be a series of P length. Divide it into N nonoverlapping sections. Each section is divided into M nonoverlapping segments. Divide each segment into K nonoverlapping blocks. Each block is of L length. Let $y(i)_m^{(L)}(n)$ be the series with aggregated level L in the mth segment of the nth section ($m = 0, 1, \ldots, M-1$; $n = 0, 1, \ldots, N-1$). Let $H_m(n)$ be the H value of $y(i)_m^{(L)}(n)$. Let $r(k; H_m(n))$ be the measured ACF of $y(i)_m^{(L)}(n)$ in the normalized case. The theoretic ACF form corresponding $y(i)_m^{(L)}(n)$ in the fGn sense is given by

$$R\left(k; H_m(n)\right) = 0.5\left[\left||k|+1\right|^{2H_m(n)} - 2|k|^{2H_m(n)} + \left||k|-1\right|^{2H_m(n)}\right]. \tag{2.9}$$

The above expression exhibits the multifractal property of traffic as can be seen from [13].

Let

$$J\left(H_m(n)\right) = \sum_k \left[R\left(k; H_m(n)\right) - r\left(k; H_m(n)\right)\right]^2 \tag{2.10}$$

be the cost function. Then one has

$$H_m(n) = \arg\min J\left[H_m(n)\right]. \tag{2.11}$$

Averaging $H_m(n)$ in terms of index m yields

$$H(n) = \frac{1}{M} \sum_{m=0}^{M-1} H_m(n), \tag{2.12}$$

representing the H estimate of the series in the nth section.

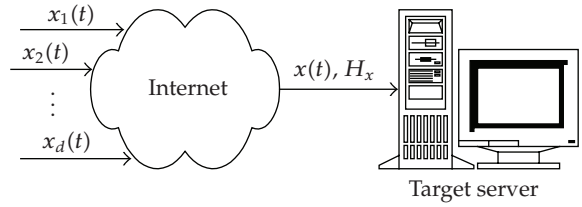

Figure 1: Normal traffic at input of a server.

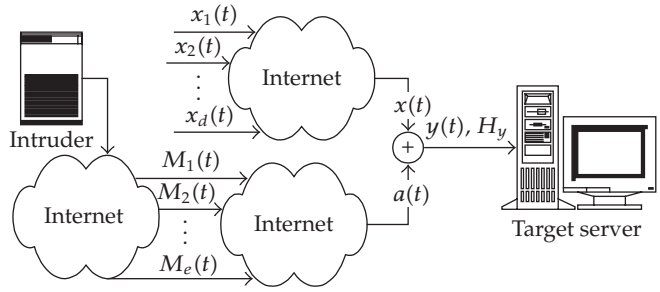

Figure 2: Illustration of abnormal traffic.

Usually, $H(n_1) \neq H(n_2)$ for $n_1 \neq n_2$. However, stationarity of traffic time series implies that $H(n)$ at a specific site is a number falling within a certain confidence interval [5, Paragraph 5, Section 5, page 966]. In practical terms, a normality assumption for $H(n)$ is quite accurate in most cases for $M > 10$ regardless of probability distribution function of H [14]. Thus we take

$$H_x = E\left[H(n)\right] \tag{2.13}$$

as a mean estimate of H of x, where E is the mean operator. It can be taken as a template of H of x for the purpose of statistical detection. The appendix gives a case of the H estimation of a real-traffic series to clarify the reasonableness of H in featuring traffic time series.

2.2. Characterizing traffic time series with H

Let x be normal traffic time series. Normally, the site serves x peacefully though x may sometimes be unpleasantly delayed because of the normal traffic jam. The arrival traffic x is contributed by many connections distributed all over the world. Figure 1 shows x contributed by traffic from d connections. From previous discussions, we see that x can be characterized by the Hurst parameter and we denote it as H_x.

Assume that the site is intruded by DDOS flood attacking. Then actual arrival traffic (abnormal traffic) consists of normal traffic x and attack traffic a, see Figure 2, where a is contributed by e connections. We use H_y as a feature of y.

3. Detection method and system structure

To explain our detection principle, we introduce three terms. Correctly recognizing an abnormal sign is termed *detection*; failing to recognize it, *miss*; mistakenly recognizing a normal as abnormal is *a false alarm*.

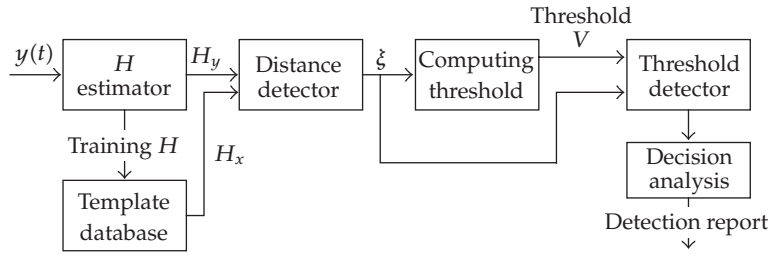

Figure 3: System diagram.

Let $\xi = \|H_x - H_y\|$. Then ξ represents the deviation of H of monitored traffic time series. Let $V > 0$ be the threshold. Then the detection hypotheses are as follows. $\xi > V$, implies detection, while $\varsigma = \|H_x - H_{xl}\| > V$ represents false alarm, where H_{xl} stands for H which is not used as the template but obtained when there is no attacking. Clearly, ξ and ζ are random variables. Mathematically, there are many distance measures available [15–17], but the following works well:

$$\xi = E\left[\sum_k \left|\frac{H_y}{H_x} - \log\frac{H_y}{H_x} - 1\right|\right]. \tag{3.1}$$

According to the previous discussions, we give the system diagram in Figure 3. The measured arrival traffic first passes through an H estimator. The result of H estimator goes to template database to produce the template H_x. In addition, it outputs an online estimate of H_y. H_x and H_y are compared in the distance detector. The comparison result ξ is fed into threshold detector to compare with a given threshold V. In the stage of decision analysis, the output of the threshold detector is analyzed and its output gives a sign of detection according to preset detection probability and false alarm probability.

4. Performance analysis

With the partition explained in Section 2, we see that there is a value of ξ representing the deviation of H of y in each segment. Therefore, in each section, ξ is a random sequence of M length. Denote $\bar{\xi}$ as the expectation of ξ in each section. Then $\bar{\xi}$ is a random sequence of N length. In the case of $N \geq 10$, $\bar{\xi}$ well obeys Gaussian distribution [14]. For the simplicity, we still denote $\bar{\xi}$ as ξ.

4.1. Detection probability

Let μ_ξ and σ_ξ^2 be the expectation and the variance of ξ, respectively. Then

$$\xi \sim N\left(\mu_\xi, \sigma_\xi^2\right) = \frac{1}{\sqrt{2\pi}\sigma_\xi} e^{-(\xi-\mu_\xi)^2/2\sigma_\xi^2}. \tag{4.1}$$

Let

$$\Phi(t) = \int_{-\infty}^{t} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt. \tag{4.2}$$

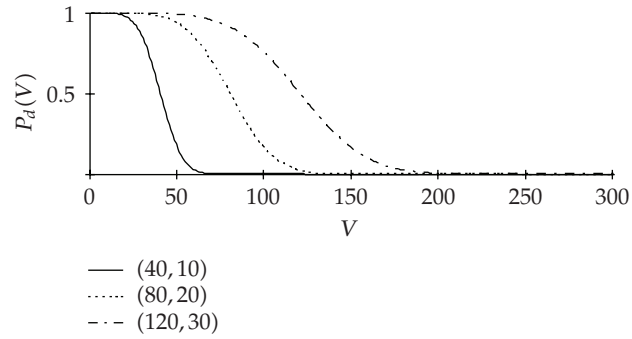

Figure 4: Detection probability.

Then detection probability is given by

$$P_d = P\{V < \xi < \infty\} = \int_{(V-\mu_\xi)/\sigma_\xi}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = 1 - \Phi\left[\frac{V-\mu_\xi}{\sigma_\xi}\right]. \tag{4.3}$$

4.2. False alarm probability

Let μ_ζ and σ_ζ^2 be the mean and the variance of ζ. Then false alarm probability is given by

$$P_f = P\{V < \zeta < \infty\} = \int_{(V-\mu_\zeta)/\sigma_\zeta}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = 1 - \Phi\left[\frac{V-\mu_\zeta}{\sigma_\zeta}\right]. \tag{4.4}$$

4.3. Miss probability

Let P_m be miss probability. Then

$$P_m = P\{-\infty < \xi < V\} = \int_{-\infty}^{(V-\mu_\xi)/\sigma_\xi} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = \Phi\left[\frac{V-\mu_\xi}{\sigma_\xi}\right]. \tag{4.5}$$

Generally, $\mu_\zeta = 0$. Besides, the numeric computation in data processing can be arranged such that $\sigma_\zeta = \sigma_\xi = \sigma$. In this case, three probabilities are given by

$$\begin{aligned} P_d &= \int_{(V-\mu_\xi)/\sigma}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = 1 - \Phi\left[\frac{V-\mu_\xi}{\sigma}\right], \\ P_f &= \int_{V/\sigma}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = 1 - \Phi\left(\frac{V}{\sigma}\right), \\ P_m &= \int_{-\infty}^{(V-\mu_\xi)/\sigma} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = 1 - \Phi\left[\frac{V-\mu_\xi}{\sigma}\right]. \end{aligned} \tag{4.6}$$

Figures 4–6 show the curves of three distributions, respectively. As $P_d + P_m = 1$, high P_d implies low P_m and vice versa.

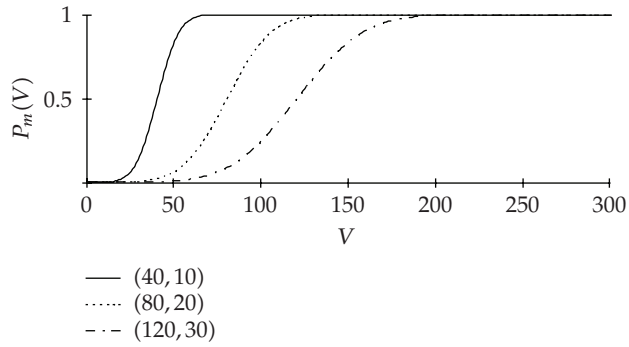

Figure 5: Miss probability.

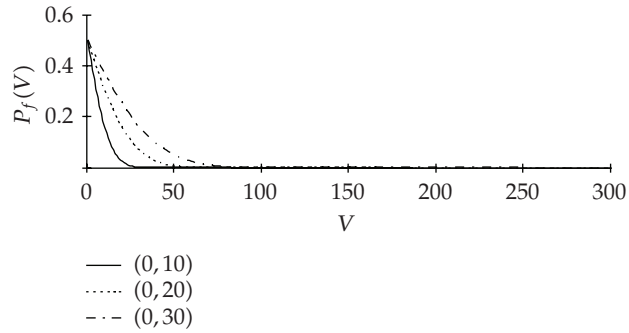

Figure 6: False alarm probability.

4.4. Threshold and detection region

As can be seen from the previous discussions, the selection of a threshold value is crucial to our system. In fact, given a false alarm probability f, we want to find the threshold V_f such that $P(V_f) \leq f$. Clearly,

$$V_f \geq -\sigma\Phi^{-1}(f). \tag{4.7}$$

If $f = 0$ and when the selected precision is 4, we obtain

$$V_f \geq 4\sigma. \tag{4.8}$$

Given a detection probability d, we want to find the threshold V_d such that $P_d(V_d) \geq d$. Clearly,

$$V_d \leq \mu_\xi - \sigma\Phi^{-1}(d), \quad \text{if } \mu_\xi - \sigma\Phi^{-1}(d) > 0. \tag{4.9}$$

In the case of $d = 1$,

$$V_d \leq \mu_\xi - 4\sigma, \quad \text{if } \mu_\xi - 4\sigma > 0. \tag{4.10}$$

Therefore, when $-\sigma\Phi^{-1}(f) < \mu_\xi - \sigma\Phi^{-1}(d)$ and $V \in [-\sigma\Phi^{-1}(f), \mu_\xi - \sigma\Phi^{-1}(d)]$, $P_d \geq d$ and $P_f \leq f$ are assured. That is,

$$\begin{matrix} P_d \geq d, \\ P_f \leq f, \end{matrix} \quad \text{if } V \in \left[-\sigma\Phi^{-1}(f), \mu_\xi - \sigma\Phi^{-1}(d)\right],\ \mu_\xi - \sigma\Phi^{-1}(d) > 0. \tag{4.11}$$

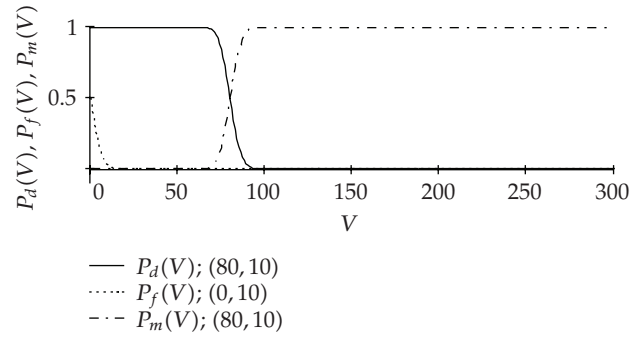

Figure 7: Intersection of three probability distributions: detection region.

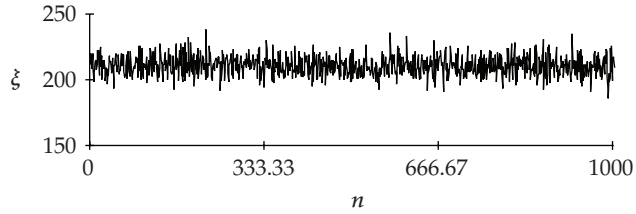

Figure 8: Random variable ξ.

In the case of $d = 1$ and $f = 0$,

$$\begin{aligned} P_d &= 1, \\ P_f &= 0, \end{aligned} \quad \text{if } V \in [4\sigma, \mu_\xi - 4\sigma],\ \mu_\xi - 4\sigma > 0. \tag{4.12}$$

The constraint of (4.12) is given by $\mu_\xi > 8\sigma$.

Obviously, the detection region is the intersection of three probability functions. Under the condition of $\mu_\xi = 80$ and $\sigma = 10$, the detection region is shown in Figure 7.

5. A case study

Suppose the template $H_0 = 0.7671$ as described in the appendix. Assume that the confidence level is 99.9999%. Thus we suppose y's $H \in (0.5000, 0.7669)$ or $(0.7673, 0.9900)$ during the transition process of intrusion. In this case study, 1000 points of Hs in $(0.5000, 0.7669)$ or (0.7673,0.9900) are randomly selected to simulate the abnormal traffic deviating from the normal one. The error sequence is indicated in Figure 8. By the numeric computation, we obtain $\mu_\xi = 210.3011$ and $\sigma = 7.7490$. Therefore, we obtain the probability distributions for detection, false alarm and miss as shown in Figure 9. Under the conditions of $P_d = 1$ and $P_f = 0$, we obtain $V_{\min} = 30.9951$ and $V_{\max} = 179.3052$. Hence when we select $V \in [30.9951, 179.3052]$, we have 99.9999% confidence to say that $P_d = 1$ and $P_f = 0$ are assured, which can be easily observed from Figure 9.

6. Discussions

Since Yahoo servers were successfully attacked in 2001, the issue of detecting DDOS flood attacking has been paid much attention to. Various methods and systems have been

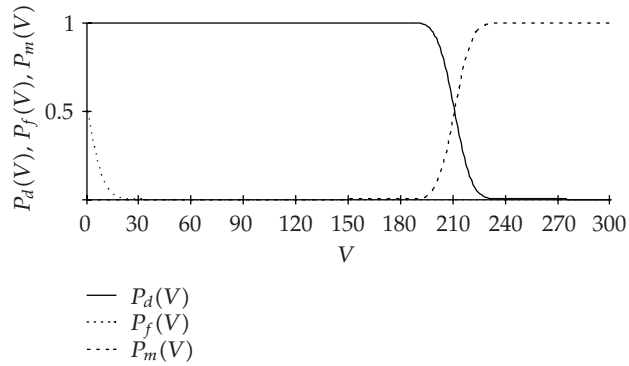

Figure 9: Case study: detection region.

proposed, see, for example, [18–25]. As known, traffic under DDOS flood attack must be significantly different from that of normal one [25]. Otherwise, DDOS flood attack would have no effect. From this point of view, the value of H of traffic under DDOS flood attacks is considerably different from that of normal one, see [12] for details.

For a stationary random time series of finite length, ACF and power spectrum density (PSD) function are commonly used in engineering for feature extraction in statistical classifications [16, 17]. However, the PSD of traffic does not exist in the domain of ordinary functions since it has long memory [8]. To avoid such a difficulty in mathematics, consequently, ACF of traffic is considered for feature extraction in our early work [25]. This paper focuses on detection of local variations of traffic based on the self-similarity of traffic. Thus it suggests a new method that substantially develops the work of [25], from the point of view of traffic pattern matching, because feature extraction of traffic time series by using a single parameter H makes pattern matching more efficient.

7. Conclusions

We have discussed the characterization of the local irregularity of traffic by $H(n)$. We have explained a principle of statistical detection to capture signs of DDOS flood attacking with predetermined detection probability and false alarm probability based on the variation of the local irregularity of traffic.

Appendix

Demonstration of H estimation of a real-traffic series

This appendix gives a demonstration with a real-traffic series, named LBL-PKT-4 [26, 27]. Denote $x(i)$ as the series of LBL-PKT-4, indicating the number of bytes in the ith packet. The length of that series is 1.3 million. The first 1024 points of that series is plotted in Figure 10(a). Divide $x(i)$ into 32 nonoverlapping sections. Computing H in each section yields $H(n)$ $(n = 0, 1, \ldots, 31)$ as shown in Figure 10(b). Its histogram is indicated in Figure 10(c).

According to (2.13), we have $H_x = 0.7671$. The confidence interval with 95% confidence level is [0.7670,0.7672]. Hence we have 95% confidence to say that the H estimate in each section of that series takes $H_x = 0.7671$ as its approximation with fluctuation not greater than 1×10^{-4}. Further, it is easy to obtain that the confidence interval with 99.9999%

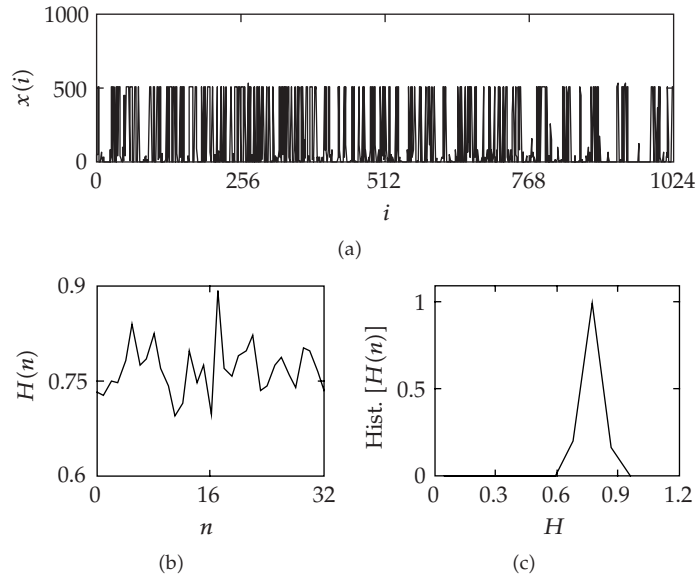

Figure 10: Verification of statistical invariable H. (a) A real-traffic time series; (b) estimate $H(n)$; (c) histogram of $H(n)$.

confidence level is [0.7669, 0.7673]. Hence we have 99.9999% confidence to say that the H estimate in each section of that series takes $H_x = 0.7671$ as its approximation with fluctuation not greater than 2×10^{-4}.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under the project Grant no. 60573125. Wei Zhao's work was also partially supported by the NSF (USA) under Contracts no. 0808419, 0324988, 0721571, and 0329181. Any opinions, findings, conclusions, and/or recommendations in this paper, either expressed or implied, are those of the authors and do not necessarily reflect the views of the agencies listed above.

References

[1] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems: Concepts and Design*, Addison-Wesley, Reading, Mass, USA, 3rd edition, 2001.

[2] E. G. Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response*, Intrusion.Net Book, Sparta, NJ, USA, 1999.

[3] L. Garber, "Denial-of-service attacks rip the Internet," *Computer*, vol. 33, no. 4, pp. 12–17, 2000.

[4] G. Toma, "Practical test functions generated by computer algorithms," in *Proceedings of the International Conference on Computational Science and Its Applications (ICCSA '05)*, vol. 3482 of *Lecture Notes in Computer Science*Lecture Notes in Computer Science, pp. 576–584, Singapore, May 2005.

[5] W. Willinger and V. Paxson, "Where mathematics meets the Internet," *Notices of the American Mathematical Society*, vol. 45, no. 8, pp. 961–970, 1998.

[6] M. Li, W. Zhao, W. Jia, D. Long, and C.-H. Chi, "Modeling autocorrelation functions of self-similar teletraffic in communication networks based on optimal approximation in Hilbert space," *Applied Mathematical Modelling*, vol. 27, no. 3, pp. 155–168, 2003.

[7] B. Tsybakov and N. D. Georganas, "Self-similar processes in communications networks," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1713–1725, 1998.

[8] A. Adas, "Traffic models in broadband networks," *IEEE Communications Magazine*, vol. 35, no. 7, pp. 82–89, 1997.
[9] B. B. Mandelbrot, *Gaussian Self-Affinity and Fractals*, Springer, New York, NY, USA, 2002.
[10] M. Li and S. C. Lim, "A rigorous derivation of power spectrum of fractional Gaussian noise," *Fluctuation and Noise Letters*, vol. 6, no. 4, pp. C33–C36, 2006.
[11] J. Beran, *Statistics for Long-Memory Processes*, vol. 61 of *Monographs on Statistics and Applied Probability* Monographs on Statistics and Applied Probability, Chapman and Hall, New York, NY, USA, 1994.
[12] M. Li, "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks," *Computers & Security*, vol. 25, no. 3, pp. 213–220, 2006.
[13] M. Li and S. C. Lim, "Modeling network traffic using generalized Cauchy process," *Physica A*, vol. 387, no. 11, pp. 2584–2594, 2008.
[14] J. S. Bendat and A. G. Piersol, *Random Data. Analysis and Measurement Procedures*, John Wiley & Sons, New York, NY, USA, 3rd edition, 2000.
[15] M. Basseville, "Distance measures for signal processing and pattern recognition," *Signal Processing*, vol. 18, no. 4, pp. 349–369, 1989.
[16] K. S. Fu, Ed., *Digital Pattern Recognition*, Springer, Berlin, Germany, 2nd edition, 1980.
[17] A. R. Webb, *Statistical Pattern Recognition*, Edward Arnold, London, UK, 1999.
[18] M. Li and W. Zhao, "A statistical model for detecting abnormality in static-priority scheduling networks with differentiated services," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '05)*, vol. 3802 of *Lecture Notes in Computer Science*Lecture Notes in Computer Science, pp. 267–272, Springer, Xi'an, China, December 2005.
[19] V. Paxson, "Bro: a system for detecting network intruders in real time," in *Proceedings of the 7th USENIX Security Symposium*, San Antonio, Tex, USA, January 1998.
[20] W. Yu, D. Xuan, and W. Zhao, "Middleware-based approach for preventing distributed deny of service attacks," in *Proceedings of IEEE Military Communications Conference (MILCOM '02)*, vol. 2, pp. 1124–1129, Anaheim, Calif, USA, October 2002.
[21] P. Innella and O. McMillan, "An introduction to intrusion detection systems, tetrad digital integrity, LLC," December 2001, http://www.securityfocus.com/infocus/1520/.
[22] http://en.wikipedia.org/wiki/Denial-of-service_attack/.
[23] http://www.sans.org/dosstep/index.php/.
[24] R. Bettati, W. Zhao, and D. Teodor, "Real-time intrusion detection and suppression in ATM networks," in *Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, Calif, USA, April 1999.
[25] M. Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition," *Computers & Security*, vol. 23, no. 7, pp. 549–558, 2004.
[26] http://www.acm.org/sigcomm/ITA/.
[27] V. Paxson and S. Floyd, "Wide area traffic: the failure of Poisson modeling," *IEEE/ACM Transactions on Networking*, vol. 3, no. 3, pp. 226–244, 1995.