Change trend of averaged Hurst parameter of traffic under DDOS flood attacks. Computer & Security, 25, 8

ARTICLE *in* COMPUTERS & SECURITY · MAY 2006

Impact Factor: 1.03 · DOI: 10.1016/j.cose.2005.11.007 · Source: DBLP

1 AUTHOR:

Ming Li
East China Normal University
108 PUBLICATIONS **1,344** CITATIONS

SEE PROFILE

Computers & Security (2006) **25**, 213–220

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Change trend of averaged Hurst parameter of traffic under DDOS flood attacks

Ming Li*

School of Information Science and Technology, East China Normal University, No. 3663, Zhongshan Bei Road, Shanghai 200026, PR China

Received 22 November 2004; revised 15 November 2005; accepted 15 November 2005

KEYWORDS
Hurst parameter;
Traffic;
Time series;
Distributed denial-of-service flood attacks;
Anomaly detection

Abstract Distributed denial-of-service (DDOS) flood attacks remain great threats to the Internet though various approaches and systems have been proposed. Because arrival traffic pattern under DDOS flood attacks varies significantly away from the pattern of normal traffic (i.e., attack free traffic) at the protected site, anomaly detection plays a role in the detection of DDOS flood attacks. Hence, quantitatively studying statistics of traffic under DDOS flood attacks (abnormal traffic for short) are essential to anomaly detections of DDOS flood attacks.

References regarding qualitative descriptions of abnormal traffic are quite rich, but quantitative descriptions of its statistics are seldom seen. Though statistics of normal traffic are affluent, where the Hurst parameter H of traffic plays a key role, how H of traffic varies under DDOS flood attacks is rarely reported. As a supplementary to our early work, this paper shows that averaged H of abnormal traffic usually tends to be significantly smaller than that of normal one at the protected site. This abnormality of abnormal traffic is demonstrated with test data provided by MIT Lincoln Laboratory and explained from a view of Fourier analysis.

Introduction

The Internet is the infrastructure that supports computer communications. It has actually become the ''electricity'' of the modern society because its use in modern society is so pervasive and many people rely on it so heavily. For instance, employees in the modern society would rather give up access to their telephone than give up their access to their email. Nevertheless, it is subject to electronic attacks (Coulouris et al., 2001), e.g., distributed denial-of-service (DDOS) flood attacks (Sorensen, 2004). The threats of DDOS attacks to the individuals are severe. For instance, any denial-of-service of a bank server implies a loss of money, disgruntling or losing customers. Hence, intrusion

* Tel.: +86 21 62233389; fax: +86 21 62232517.
E-mail addresses: mli@ee.ecnu.edu.cn, ming_lihk@yahoo.com.
URL: http://www.ee.ecnu.edu.cn/teachers/mli/js_lm(Eng).htm.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.11.007

detection system (IDS) and intrusion prevention system (IPS) are desired (Kemmerer and Vigna, 2002; Householder et al., 2002; Schultz, 2004; Sorensen, 2004; Gong, 2003; Li, 2004; Streilein et al., 2003; Bencsath and Vajda, 2004; Feinstein et al., 2003; Oh and Lee, 2003; Liston, 2004).

There are several categories of denial-of-service (DOS) attacks (Gong, 2003). The CERT Coordination Center (CERT/CC) divides DOS attacks into three categories: (1) flood (i.e., bandwidth) attacks, (2) protocol attacks, and (3) logical attacks. This paper considers flood attacks.

A DDOS flood attack sends attack packets upon a site (victim) with a huge amount of traffic, the sources of which are distributed over the world so as to effectively jam its entrance and block access by legitimate users or significantly degrade its performance. It never tries to break into the victim's system, making security defenses at the protected site irrelevant (DDoS; Dittrich-a; Dittrich-b; Dittrich-c; Dittrich-d; Dietrich et al.; Geng et al., 2002).

Usually, IDSs are classified into two categories. One is misuse detection and the other anomaly detection. Solutions given by misuse detection are primarily based on a library of known signatures to match against network traffic. Hence, unknown signatures from new variants of an attack mean 100% miss. Therefore, anomaly detectors play a role in detection of DDOS flood attacks. As far as anomaly detection is concerned, quantitatively characterizing abnormalities of statistics of abnormal traffic is fundamental.

A traffic stream is a packet flow. A packet consists of a number of fields, such as protocol type, source IP, destination IP, ports, flag setting (in the case of TCP or UDP), message type (in the case of ICPM), timestamp, and data length (packet size). Each may serve as a feature of a packet. The literature discussing traffic features is rich (see e.g. Li, 2004; Streilein et al., 2003; Bencsath and Vajda, 2004; Feinstein et al., 2003; Oh and Lee, 2003; Cho and Park, 2003; Cho and Cha, 2004; Lan et al., 2003; Paxson and Floyd, 1995; Li et al., 2003; Beran, 1994; Willinger and Paxson, 1998; Willinger et al., 1995; Csabai, 1994; Tsybakov and Georganas, 1998; MIT; Garber, 2000; Kim et al., 2004; Mahajan et al., 2002; Kim et al., 2004; Bettati et al., 1999). For instance, Mahajan et al. (2002) consider flow rate, Kim et al. (2004) use head message, Oh and Lee (2003) alone consider 86 features of traffic (not from a statistics view though), and so on. To the best of our knowledge, however, taking into account the Hurst parameter H in characterizing abnormality of traffic series in packet size under DDOS flood attacks is rarely seen except for Li (2004), where autocorrelation function (ACF) of traffic series in packet size (traffic for short) with long-range dependence (LRD) is taken as its statistical feature. As a supplementary to Li (2004), this paper specifically studies how H of traffic varies under DDOS flood attacks. In this regard, the following two questions are fundamental.

(1) Whether H of traffic when a site is under DDOS flood attacks (abnormal traffic for short) is significantly different from that of normal one (i.e., attack free traffic)?
(2) What is the change trend of H of traffic when a site suffers from DDOS flood attacks?

We will give the answers to the above questions from the point of views of processing data traffic and theoretic inference and analysis.

In the rest of paper, section ''Test data sets'' is about test data. We brief data traffic and use a series of normal traffic in ACM to explain how its H normally varies in section ''Brief of data traffic''. The answer to the question (1) is given in section ''Using H to describe abnormality of traffic under DDOS flood attacks''. Then, in section ''Change trend of traffic under DDOS flood attacks'', we use a pair of series (one is normal traffic and the other abnormal one) that is provided by MIT Lincoln Laboratory to demonstrate that averaged H of abnormal traffic tends to be significantly smaller than that of normal one and briefly discusses this abnormality of abnormal traffic from a view of Fourier analysis. The answer to the question (2) is given in this section. Section ''Conclusions'' concludes the paper.

Test data sets

Three series of test data are utilized in this paper. The first one is an attack free series measured at the Lawrence Berkeley Laboratory from 14:00 to 15:00 on Friday, 29 January 1994. It is named LBL-PKT-4, which has been widely used in the research of general (normal traffic) traffic pattern (see e.g. Paxson and Floyd, 1995; Li et al., 2004). We use it to show a case how H of normal traffic varies. The second is Outside-MIT-week1-1-1999-attack-free (OM-W1-1-1999AF for short) (MIT). It was recorded from 08:00:02, 1 March (Monday) to 06:00:02, 2 March (Tuesday), 1999. The third is Outside-MIT-week2-1-1999-attack-contained (OM-W2-1-1999AC for short) (MIT), which was collected from 08:00:01, 8 March (Monday) to 06:00:49, 9 March (Tuesday), 1999. Two MIT series are used to

demonstrate a case how H of traffic varies under DDOS attacks. Though whether or not MIT test data are in the sense of standardization is worth further discussion as stated in McHugh (2000), they are valuable and can yet be test data for the research of abnormality of abnormal traffic due to available data traffic under DDOS flood attacks being rare.

Brief of data traffic

Denote $x(t_i)$ a traffic series, indicating the number of bytes in a packet at time t_i, $i = 0, 1, 2, \ldots$. From a view of discrete series, we write $x(t_i)$ as $x(i)$ implying the number of bytes in the ith packet. Let $r(k)$ be the ACF of $x(i)$. Then,

$$r(k) \sim ck^{2H-2} \text{ for } c > 0, \quad H \in (0.5, 1), \tag{1}$$

where $\sim$ stands for the asymptotical equivalence under the limit $k \to \infty$ and H the Hurst parameter.

The ACF in Eq. (1) is non-summable for $H \in (0.5, 1)$, implying LRD. Hence, H is a measure of LRD of traffic.

According to the research in traffic engineering, fractional Gaussian noise (FGN) is an approximate model of traffic (Paxson and Floyd, 1995; Li et al., 2003; Beran, 1994; Willinger and Paxson, 1998; Willinger et al., 2002; Li et al., 2004; Paxson, 1997; Li and Chi, 2003; Michiel and Laevens, 1997; Adas, 1997; Leland et al., 1994; Beran et al., 1995; Stallings, 1998; Carmona et al., 1999; Pitts and Schormans, 2000; MaDysan, 2000). The ACF of FGN is given by

$$R(k; H) = 0.5\sigma^2 \left[|k+1|^{2H} - 2|k|^{2H} + |k-1|^{2H} \right], \tag{2}$$

where,

$$\sigma^2 = \frac{\Gamma(2-H)\cos(\pi H)}{\pi H(2H-1)}$$

(Mandelbrot, 2001; Muniandy and Lim, 2001).

By taking FGN as an approximate model of $x(i)$, we consider another series given by $x(i)^{(L)} = 1/L \sum_{j=iL}^{(i+1)L-1} x(j)$. According to the analysis in self-similar processes (see e.g. Beran, 1994; Mandelbrot, 2001; Beran et al., 1995), one has

$$\mathrm{Var}\left(x^{(L)}\right) \approx L^{2H-2} \mathrm{Var}(x),$$

where Var implies the variance operator. Thus, traffic has the property of self-similarity measured by H. Consequently, H characterizes the properties of both LRD and self-similarity of traffic.

In practice, measured traffic is of finite length. Let x be a series of P length. Divide x into N non-overlapping sections. Each section is divided into M non-overlapping segments. Divide each segment into K non-overlapping blocks. Each block is of L length. Let $x(i)_m^{(L)}(n)$ be the series with aggregated level L in the mth segment in the nth section $(m = 0, 1, \ldots, M-1; \quad n = 0, 1, \ldots, N-1)$. Let $H_m(n)$ be the H value of $x(i)_m^{(L)}(n)$. Let $r(k; H_m(n))$ be the measured ACF of $x(i)_m^{(L)}(n)$ in the normalized case. Then,

$$R(k; H_m(n)) = 0.5\Big[|k+1|^{2H_m(n)} - 2|k|^{2H_m(n)} + |k-1|^{2H_m(n)} \Big]. \tag{3}$$

The above expression exhibits the multi-fractal property of traffic as that explained from a mathematics view (Muniandy and Lim, 2001; Muniandy and Lim, 2000).

Let $J(H_m(n)) = \sum_k [R(k; H_m(n)) - r(k)]^2$ be the cost function. Then, one has

$$H_m(n) = \arg\min J[H_m(n)]. \tag{4}$$

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

$$H(n) = \frac{1}{M} \sum_{m=0}^{M-1} H_m(n), \tag{5}$$

representing the H estimate of the series in the nth section. 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 (Bendat and Piersol, 1986). Thus,

$$H_x = E[H(n)] \tag{6}$$

is taken as a mean estimate of H of x, where E is the mean operator.

Let σ_H be the standard deviation of $H(n)$. Then,

$$\mathrm{Prob}\left[z_{1-\alpha/2} < \frac{H(n) - H_x}{\sigma_H} \le z_{\alpha/2} \right] = 1 - \alpha,$$

where $(1-\alpha)$ is the confidence coefficient. The confidence interval of $H(n)$ with $(1-\alpha)$ confidence coefficient is given by $\left(H_x - \sigma_H z_{\alpha/2}, \; H_x + \sigma_H z_{\alpha/2}\right)$. The following demonstration exhibits $H(n)$ of traffic series LBL-PKT-4.

Demonstration 1: The first 1024 points of the series $x(i)$ of LBL-PKT-4 are indicated in Fig. 1 (a). Consider the first 524 288 (=P) points of $x(i)$. The partition settings are as follows. $L = 32$, $K = 16$, $M = 32$, $N = 32$, and $J = 2048$. Computing H in each section yields $H(n)$ as shown in Fig. 1(b). Its histogram is indicated in Fig. 1(c).

According to Eq. (6), we have $H_x = 0.758$. The confidence interval with 95% confidence level is [0.750, 0.766]. Hence, we have 95% confidence to say that the H estimate in each section of that

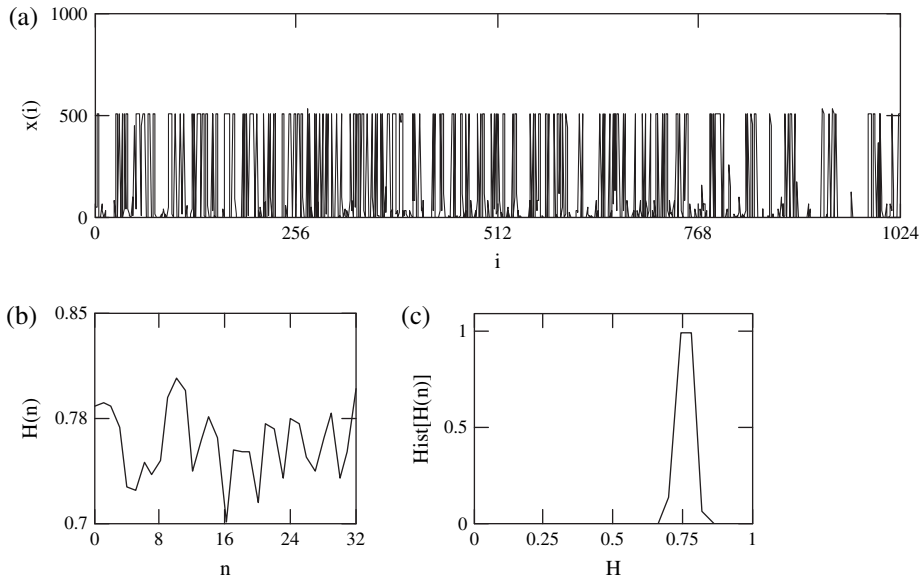

Figure 1 Demonstrating statistical invariable H. (a) A real-traffic time series; (b) estimate $H(n)$; (c) histogram of $H(n)$.

series takes $H_x = 0.758$ as its approximation with the fluctuation not greater than 7.431×10^{-3}.

Using H to describe abnormality of traffic under DDOS flood attacks

From the previous discussions, we see that H is a parameter to characterize the properties of both LRD and self-similarity of traffic. On the other hand, ACF is a statistical feature of a time series, which is used in queuing analysis of network systems (Livny et al., 1993; Li and Hwang, 1993). Hence, the following lemma.

Lemma: *Let x and y be normal traffic and abnormal traffic, respectively. Let r_{xx} and r_{yy} be the ACFs of x and y, respectively. During the transition process of DDOS flood attacking, $\|r_{yy} - r_{xx}\|$ is noteworthy* (*Li, 2004*).

Proof: A network system is a queuing system. Arrival traffic x of a queuing system has its statistical pattern r_{xx} (Livny et al., 1993; Li and Hwang, 1993). Suppose the site suffers from DDOS flood attacks. Suppose that $\|r_{yy} - r_{xx}\|$ is negligible in this case. Then, the site would be overwhelmed at its normal state even if there were no DDOS flood packets. This is an obvious contradiction. □

For each value of $H \in (0.5, 1)$, there is exactly one ACF of FGN with LRD as can be seen from Beran (1994, p. 55). Thus, a consequence of Lemma is that $\|H_y - H_x\|$ is considerable, where H_y and H_x are average H values of x and y, respectively. Hence, H is a parameter that can yet be used to describe abnormality of traffic under DDOS flood attacks. This gives the answer to the question (1) in Section ''Introduction''.

Change trend of H of traffic under DDOS flood attacks

Demonstrations

This subsection gives two demonstrations of $H(n)$. One is for normal traffic and the other abnormal one. Two demonstrations show that average value of H of abnormal traffic tends to be significantly smaller than that of normal one.

Demonstration 2 (attack free traffic): The first 1024 points of the series $x(i)$ of attack free traffic OM-W1-1-1999AF are indicated in Fig. 2(a). Its $H(n)$ is plotted in Fig. 2(b) and histogram in Fig. 2(c).

By computation, we obtain

$$H_x = 0.895, \tag{7}$$

its variance $= 5.693 \times 10^{-4}$, and the confidence interval with 95% confidence level [0.865, 0.895].

Demonstration 3 (abnormal traffic): The first 1024 points of the series $x(i)$ of attack contained traffic OM-W2-1-1999AC are indicated in Fig. 3(a).

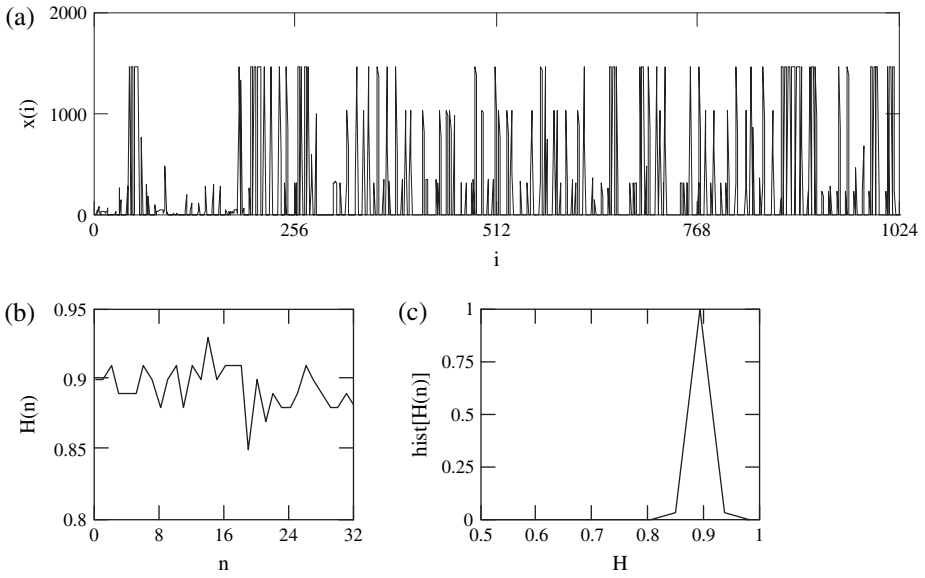

Figure 2 Demonstrating $H(n)$ of attack free traffic OM-W1-1-1999AF. (a) Time series of OM-W1-1-1999AF; (b) estimate $H(n)$ of OM-W1-1-1999AF; (c) histogram of $H(n)$ of OM-W1-1-1999AF.

Its $H(n)$ is plotted in Fig. 3(b) and histogram in Fig. 3(c).

By computation, we obtain

$$H_y = 0.774, \tag{8}$$

its variance $= 6.777 \times 10^{-4}$, and the confidence interval with 95% confidence level [0.723, 0.825].

Comparing the means of H in the above two demonstrations, we see

$$H_y < H_x. \tag{9}$$

The above inequality exhibits a case of the change trend of H of traffic under DDOS flood attacks. It actually follows a general rule as can be seen from the following analysis.

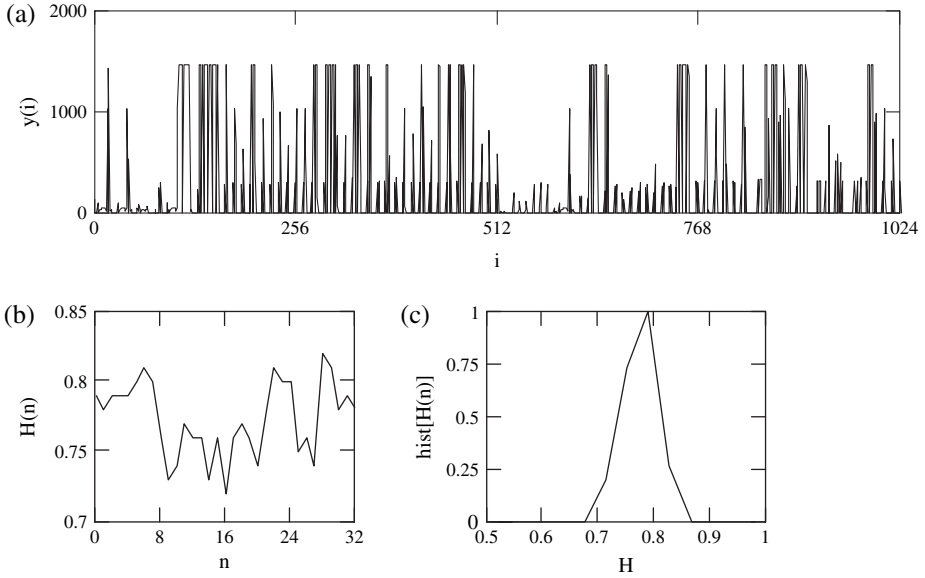

Figure 3 Demonstrating $H(n)$ of abnormal traffic OM-W2-1-1999AC. (a) Time series of OM-W2-1-1999AC; (b) estimate $H(n)$ of OM-W2-1-1999AC; (c) histogram of $H(n)$ of OM-W2-1-1999AC.

Analysis of change trend of H of traffic under DDOS flood attacks

In the case of multi-fractional FGN, we let H represent the mean estimate of the Hurst parameter as that in Eq. (6) for the sake of simplicity. As

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

is the finite second-order difference of $0.5\tau^{2H}$ (Beran, 1994; Mandelbrot, 2001; Li and Chi, 2003; Caccia et al., 1997), approximating it with 2-order differential of $0.5\tau^{2H}$ yields

$$0.5\left[(\tau+1)^{2H}-2\tau^{2H}+(\tau-1)^{2H}\right]\approx H(2H-1)\tau^{2H-2}. \tag{10}$$

In the domain of generalized functions (Lighthill, 1958, p. 43), we obtain

$$\mathcal{F}\left(|\tau|^{-(2-2H)}\right)=2\cos\frac{\pi(2H-1)}{2}(2H-2)!|\omega|^{-(2H-1)}, \tag{11}$$

where $\mathcal{F}$ is the operator of the Fourier transform.

As known, the frequency bandwidth of x is the width of its power spectrum $S(\omega)$, which is usually explained in the sense of the maximum effective frequency in engineering (Stalling, 1994). Hence, the following is a consequence of Eq. (11).

Corollary: *Let B_1 and B_2 be the bandwidths of LRD FGN x_1 and x_2, respectively. Let mean estimates of H of x_1 and x_2 be H_1 and H_2, respectively. Then, $H_2 < H_1$ if $B_2 > B_1$.*

As known, the data rate of abnormal traffic is usually greater than that of attack free traffic (Garber, 2000). Hence, the bandwidth of abnormal traffic is wider than that of attack free traffic according to the relationship between data rate and bandwidth (Stalling, 1994). Then, according to Corollary, we see that average H of abnormal traffic is smaller than that of attack free traffic, giving the answer to the question (2) in section''Introduction''. Eq. (9) is a case about this rule. As the larger the H the stronger the LRD as well as self-similarity (Beran, 1994; Mandelbrot, 2001), we note that LRD and self-similarity of abnormal traffic become weaker than those of attack free traffic.

In passing, Corollary gives the reason why Li (2004) designs the case study by assigning abnormal traffic's Hs smaller than that of normal one.

Conclusions

To reveal how a statistical feature of traffic varies under DDOS flood attacks is crucial to anomaly detection of DDOS flood attacks (Liston, 2004). As the Hurst parameter H (or equivalently autocorrelation function (Li, 2004; Paxson and Floyd, 1995; Li et al., 2003; Beran, 1994; Willinger and Paxson, 1998; Willinger et al., 1995; Tsybakov and Georganas, 1998; Willinger et al., 2002; Li et al., 2004; Mandelbrot, 2001; Paxson, 1997; Li and Chi, 2003; Michiel and Laevens, 1997; Adas, 1997; Leland et al., 1994; Beran et al., 1995; Stallings, 1998; Carmona et al., 1999; Pitts and Schormans, 2000; MaDysan, 2000; Mandelbrot, 1971) plays a key role in traffic analysis, this paper aims at revealing how H varies under DDOS flood attacks. We have explained that average H of abnormal traffic significantly differs from that of normal one as a consequence of Lemma, where H represents mean estimate in the case of multi-fractional series. We have given a corollary to show that average H of abnormal traffic is smaller than that of normal one. The results in theory are demonstrated and also validated with the test data provided by MIT Lincoln Laboratory.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under the project grant number 60573125. MIT Lincoln Laboratory is highly appreciated.

References

Adas A. Traffic models in broadband networks. IEEE Communications Magazine 1997;35(7):82—9.

Bencsath B, Vajda I. Protection against DDoS attacks based on traffic level measurements. In: International symposium on collaborative technologies and systems. Waleed W. Smari, William McQuay; 2004. p. 22—8.

Bendat JS, Piersol AG. Random data: analysis and measurement procedure. 2nd ed. John Wiley & Sons; 1986.

Beran J, Shernan R, Taqqu MS, Willinger W. Long-range dependence in variable bit-rate video traffic. IEEE Transactions on Communications February—April 1995;43(2—4):1566—79.

Beran J. Statistics for long-memory processes. Chapman & Hall; 1994.

Bettati R, Zhao W, Teodor D. Real-time intrusion detection and suppression in ATM networks. In: Proceedings of the first USENIX workshop on intrusion detection and network monitoring; April 1999.

Caccia DC, Percival D, Cannon MJ, Raymond G, Bassingthwaighte JB. Analyzing exact fractal time series: evaluating dispersional analysis and rescaled range methods. Physica A 1997;246(3—4):609—32.

Carmona R, Hwang W-L, Torresani B. Practical time-frequency analysis: Gabor and wavelet transforms with an implementation in S. Academic Press; 1999. p. 244–7.

Cho S, Cha S. SAD: web session anomaly detection based on parameter estimation. Computers & Security 2004;23(4): 312–9.

Cho S-B, Park H-J. Efficient anomaly detection by modeling privilege flows using hidden Markov model. Computers & Security 2003;22(1):45–55.

Coulouris G, Dollimore J, Kindberg T. Distributed systems: concepts and design. 3rd ed. Addison-Wesley; 2001.

Csabai I. $1/f$ noise in computer network traffic. Journal of Physics A: Mathematical and General 1994;27(12):L417–21.

Data are available from: <http://www.acm.org/sigcomm/ITA/>.

Distributed denial of service (DDoS) attacks/tools, <http://staff.washington.edu/dittrich/misc/ddos/>.

Dietrich S, Long N, Dittrich D. An analysis of the 'Shaft' distributed denial of service tool, <http://www.adelphi.edu/~spock/shaft_analysis.txt>.

Dittrich D. The DoS project's 'Trinoo' distributed denial of service attack tool, <http://staff.washington.edu/dittrich/misc/trinoo.analysis> (Dittrich-a).

Dittrich D. The 'Tribe Flood Network' distributed denial of service attack tool, <http://staff.washington.edu/dittrich/misc/tfn.analysis.txt> (Dittrich-b).

Dittrich D. The 'Stacheldraht' distributed denial of service attack tool, <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt> (Dittrich-c).

Dittrich D. The 'Mstream' distributed denial of service attack tool, <http://staff.washington.edu/dittrich/misc/mstream.analysis.txt> (Dittrich-d).

Feinstein L, Schnackenberg D, Balupari R, Kindred D. Statistical approaches to DDoS attack detection and response. In: DARPA information survivability conference and exposition, vol. I, April 22–24, 2003. Washington, DC; 2003. p. 303–14.

Garber L. Denial-of-service attacks rip the Internet. Computer April 2000;33(4):12–7.

Geng X, Huang Y, Whinston AB. Defending wireless infrastructure against the challenge of DDoS attacks. Mobile Networks and Applications 2002;7:213–23.

Gong F. Deciphering detection techniques: part III denial of service detection. White Paper. McAfee Network Security Technologies Group; January 2003.

Householder A, Houle K, Dougberty C. Computer attack trends challenge Internet security. Supplement to Computer. IEEE Security & Privacy April 2002;35(4):5–7.

Kemmerer RA, Vigna G. Intrusion detection: a brief history and overview. Supplement to Computer. IEEE Security & Privacy April 2002;35(4):27–30.

Kim SS, Reddy ALN, Vannucci M. Detecting traffic anomalies at the source though aggregate analysis of packet header data. In: Proceedings of Networking 2004. LNCS, vol. 3042, Athens, Greece; May 2004. p. 1047–59.

Kim Y, Lau WC, Chuah MC, Chao HJ. PacketScore: statistics-based overload control against distributed denial-of-service attacks. In: IEEE Infocom 2004, Hong Kong; 2004.

Lan K, Hussain A, Dutta D. Effect of malicious traffic on the network. In: Proceedings of passive and active measurement workshop, April 2003, La Jolla, California; 2003.

Leland E, Taqqu M, Willinger W, Wilson DV. On the self-similar nature of ethernet traffic, (extended version). IEEE/ACM Transactions on Networking February 1994;2(1):1–15.

Li Ming, Chi C-H. A correlation-based computational method for simulating long-range dependent data. Journal of the Franklin Institute September–November 2003;340(6–7): 503–14.

Li S-Q, Hwang C-L. Queue response to input correlation functions: continuous spectral analysis. IEEE/ACM Transactions on Networking December 1993;1(6):678–92.

Li Ming, Zhao W, Jia WJ, Chi C-H, Long DY. Modeling autocorrelation functions of self-similar teletraffic in communication networks based on optimal approximation in Hilbert space. Applied Mathematical Modelling 2003; 27(3):155–68.

Li Ming, Chi C-H, Long DY. Fractional Gaussian noise: a tool of characterizing traffic for detection purpose. In: Content computing LNCS, vol. 3309. Springer; November 2004. p. 94–103.

Li Ming. An approach for reliably identifying signs of DDoS flood attacks based on LRD traffic pattern recognition. Computers & Security 2004;23(7):549–58.

Lighthill MJ. An introduction to Fourier analysis and generalised functions. Cambridge University Press; 1958.

Liston K. Intrusion detection FAQ: can you explain traffic analysis and anomaly detection? <www.sans.org/resources/idfaq/anomaly_detection.php>; 6 July, 2004.

Livny M, Melamed B, Tsiolis AK. The impact of autocorrelation on queuing systems. Management Science 1993;39:322–39.

MaDysan D. QoS & traffic management in IP & ATM networks. McGraw-Hill; 2000.

Mahajan R, Bellovin S, Floyd S, Ioannidis J, Paxson V, Shenker S. Controlling high bandwidth aggregates in the network. Computer Communications Review July 2002;32(3):62–73.

Mandelbrot BB. Fast fractional Gaussian noise generator. Water Resources Research 1971;7(3):543–53.

Mandelbrot BB. Gaussian self-affinity and fractals. Springer; 2001.

McHugh J. Testing intrusion detection systems: a critique of the 1988 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory. ACM Transactions on Information System Security November 2000;3(4):262–94.

Michiel H, Laevens K. Teletraffic engineering in a broad-band era. Proceedings of the IEEE December 1997;85(12):2007–33.

<http://www.ll.mit.edu/IST/ideval>.

Muniandy SV, Lim SC. On some possible generalizations of fractional Brownian motion. Physics Letters A 2000;266:140–5.

Muniandy SV, Lim SC. Modelling of locally self-similar processes using multifractional Brownian motion of Riemann–Liouville type. Physical Review E 2001;63:046104.

Oh SH, Lee WS. An anomaly intrusion detection method by clustering normal user behavior. Computers & Security 2003; 22(7):596–612.

Paxson V, Floyd S. Wide-area traffic: the failure of Poisson modeling. IEEE/ACM Transactions on Networking June 1995;3(3): 226–44.

Paxson V. Fast, approximate synthesis of fractional Gaussian noise for generating self-similar network traffic. Computer Communications Review October 1997;27(5):5–18.

Pitts JM, Schormans JA. Introduction to IP and ATM design and performance: with applications and analysis software. John Wiley; 2000. p. 287–93.

Schultz E. Intrusion prevention. Computers & Security 2004; 23(4):265–6.

Sorensen S. Competitive overview of statistical anomaly detection. White Paper. Juniper Networks Inc., www.juniper.net; 2004.

Stalling W. Data and computer communications. 4th ed. Macmillan; 1994.

Stallings W. High-speed networks: TCP/IP and ATM design principles. Prentice Hall; 1998 [chapter 8].

Streilein WW, Fried DJ, Cunninggham RK. Detecting flood-based denial-of-service attacks with SNMP/RMON. In: Workshop on statistical and machine learning techniques in computer intrusion detection. September 24–26, 2003. George Mason University; 2003.

Tsybakov B, Georganas ND. Self-similar processes in communications networks. IEEE Transactions on Information Theory September 1998;44(5):1713–25.

Willinger W, Paxson V. Where mathematics meets the Internet. Notices of the American Mathematical Society August 1998; 45(8):961–70.

Willinger W, Taqqu MS, Leland WE, Wilson DV. Self-similarity in high-speed packet traffic: analysis and modeling of ethernet traffic measurements. Statistical Science 1995;10(10): 67–85.

Willinger W, Paxson V, Riedi RH, Taqqu MS. Long-range dependence and data network traffic. In: Doukhan P, Oppenheim G, Taqqu MS, editors. Long-range dependence: theory and applications. Birkhauser; 2002.

Ming Li completed his undergraduate program in electronic engineering at Tsinghua University. He received the M.S. degree in mechanics from China Ship Scientific Research Center and Ph.D. degree in Computer Science from City University of Hong Kong, respectively. In March 2004, he joined East China Normal University (ECNU) as a professor after several years' experiences in National University of Singapore and City University of Hong Kong. He is currently a Division Head for Communications & Information Systems at ECNU. His current research interests include teletraffic modeling and its applications to anomaly detection and guaranteed quality of service, fractal time series, testing and measurement techniques. He has published over 50 papers in international journals and international conferences in those areas.