Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2010, Article ID 962435, 14 pages
doi:10.1155/2010/962435

Research Article

Note on Studying Change Point of LRD Traffic Based on Li's Detection of DDoS Flood Attacking

Zhengmin Xia,[1] Songnian Lu,[1,2] and Junhua Tang[2]

[1] *Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[2] *School of Information Security Engineering, Key Laboratory of Information Security Integrated Management Research, Shanghai Jiao Tong University, Shanghai 200240, China*

Correspondence should be addressed to Zhengmin Xia, miaomiaoxzm@sjtu.edu.cn

Received 7 February 2010; Accepted 11 March 2010

Academic Editor: Ming Li

Distributed denial-of-service (DDoS) flood attacks remain great threats to the Internet. To ensure network usability and reliability, accurate detection of these attacks is critical. Based on Li's work on DDoS flood attack detection, we propose a DDoS detection method by monitoring the Hurst variation of long-range dependant traffic. Specifically, we use an autoregressive system to estimate the Hurst parameter of normal traffic. If the actual Hurst parameter varies significantly from the estimation, we assume that DDoS attack happens. Meanwhile, we propose two methods to determine the change point of Hurst parameter that indicates the occurrence of DDoS attacks. The detection rate associated with one method and false alarm rate for the other method are also derived. The test results on DARPA intrusion detection evaluation data show that the proposed approaches can achieve better detection performance than some well-known self-similarity-based detection methods.

1. Introduction

DDoS flood attacks have been one of the most frequently occurring attacks that badly threaten the stability of the Internet. For DDoS flood attack, an intruder undermines the availability of computer systems or services by exploiting the inherent weakness of the Internet system architecture, and overwhelming the target with a huge amount of traffic flows launched through multiple zombies. The attack process is a relatively simple, yet very powerful technique to attack the Internet resources. Therefore, accurate detection of these attacks is critical to the Internet community.

As shown by Leland et al. [1], and supported by a number of later research [2–7], the measurements of local and wide-area network traffic, wire-line and wireless network

traffic all demonstrate self-similarity and long range dependence (LRD) characteristics at large time scales. The work in [8] points out that self-similarity of the Internet traffic is attributed to a mixture of the actions of a number of individual users, hardware and software behaviors at their originating hosts, multiplexed through an interconnection network. In other words, this self-similarity always exists regardless of the network type, topology, size, protocol, or the type of services the network is carrying. On the other hand, it is reported in [9–15] that when DDoS attack happens, the self-similarity of network traffic will change significantly. Thus, by monitoring the change of the Hurst parameter, the key parameter to describe the self-similarity of a self-similar process, DDoS attacks may be detected.

Much work has been done to detect DDoS attack by recognizing the pattern of self-similarity in the literature. In [16], Li deduced the statistical characteristic of network traffic autocorrelation function under normal condition and DDoS attack and gave the detection threshold based on the preselected detection rate and false alarm rate. In [11], Li quantitatively described the statistics of abnormal traffic and suggested that the Hurst parameter of network traffic under DDoS attack tends to be significantly smaller than that of normal traffic. Li also demonstrated in [11] that the average Hurst parameter of fixed number of normal traffic pieces follows Gaussian distribution at large time scales and when the attack occurs, this statistical property may in general change.

Based on Li's work, we propose a DDoS detection method by monitoring the Hurst variation. Specifically, we use an autoregressive (AR) system to estimate the Hurst parameter of normal traffic. If the actual Hurst parameter varies significantly from the estimation beyond a threshold, we assume that DDoS attack happens. Then we propose two methods to determine the change point of Hurst parameter, that is, to determine the threshold of Hurst variation that is used to distinguish attack traffic from normal traffic. The detection rate associated with one method and false alarm rate for the other method are also derived. The experiment results on Defense Advanced Research Projects Agency (DARPA) data sets indicate that the proposed detection methods are effective in detecting DDoS flood attacks, and can achieve better detection performance than some well-known self-similarity-based detection methods.

The rest of this paper is organized as follows. Section 2 briefly introduces the concept of self-similarity and the Hurst parameter estimation. Section 3 explains the proposed detection process based on the Hurst variation. Section 4 discusses the two methods for determining the change point of LRD traffic. Section 5 presents the performance evaluation and analysis of the proposed detection methods with traffic data from DARPA, followed by a brief conclusion in Section 6.

2. Preliminaries

2.1. Self-Similar Network Traffic

Self-similarity means that the sample paths of the process $B(t)$ and those of rescaled version $\delta^H B(t/\delta)$, obtained by simultaneously dilating the time axis t by a factor $\delta > 0$, and the amplitude axis by a factor δ^H, cannot be statistically distinguished from each other. Equivalently, it implies that an affine dilated subset of one sample path cannot be distinguished from its whole. H is called the Hurst parameter. For a general self-similar process, H measures the degree of self-similarity.

Network traffic arrival process; is a discrete time process, so the discrete time self-similarity definition is given below. Let $X = \{x_i, i \in \mathbf{Z}_+\}$be a wide-sense stationary discrete stochastic traffic time series with constant mean μ, finite variance σ^2, and autocorrelation function $r(\tau)$, $(\tau \in \mathbf{Z}_+)$. Let $X^{(m)} = \{x_i^{(m)}, i, m \in \mathbf{Z}_+\}$ be an m-order aggregate process of X; then

$$x_i^{(m)} = \frac{x_{mi-m+1} + \cdots + x_{mi}}{m}. \tag{2.1}$$

For each $m, X^{(m)}$ defines a wide-sense stationary stochastic process with autocorrelation function $r^{(m)}(\tau)$.

Definition 2.1. A second-order stationary process X is called exact second-order self-similar (ESOSS) with Hurst parameter $H = 1 - \beta/2$, $0 < \beta < 1$ if the autocorrelation function satisfies

$$r^{(m)}(\tau) = r(\tau), \tag{2.2}$$

where $r(\tau) = [(\tau+1)^{2-\beta} - 2\tau^{2-\beta} + (\tau-1)^{2-\beta}]/2$ and $m \in \mathbf{Z}_+$.

Definition 2.2. A second-order stationary process X is called asymptotical second-order self-similar (ASOSS) with Hurst parameter $H = 1 - \beta/2$, $0 < \beta < 1$ if the autocorrelation function satisfies

$$\lim_{m \to \infty} r^{(m)}(\tau) = r(\tau), \tag{2.3}$$

where $r(\tau) = [(\tau+1)^{2-\beta} - 2\tau^{2-\beta} + (\tau-1)^{2-\beta}]/2$ and $m \in \mathbf{Z}_+$.

In the field of network traffic theory, it is more practical to use ASOSS.

2.2. Hurst Parameter Estimation

To date, several methods have been proposed to estimate the Hurst parameter. Some of the most popular ones include the aggregated variance, local whittle, and the wavelet-based methods [17–21]. In this paper, we use the method proposed by Li [11] to estimate the Hurst parameter of network traffic. The estimation process is summarized as follows. For more information please refer to [11].

Let $r(\tau)$ be the autocorrelation function of x_i. Then

$$r(\tau) \sim c\tau^{(2H-2)}, \tag{2.4}$$

where $\sim$ stands for the asymptotical equivalence under the limit $\tau \to \infty$, $c > 0$, and $H \in (0.5, 1)$.

By taking fractional Gaussian noise as an approximate model of x_i, one has

$$\sigma^2_{x_i^{(m)}} \approx m^{2H-2}\sigma^2_{x_i}, \tag{2.5}$$

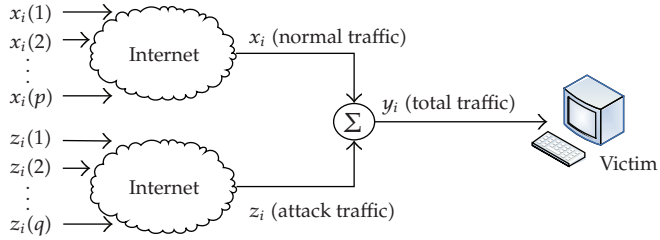

Figure 1: Composition of normal and attack traffic.

where $\sigma^2_{x_i^{(m)}}$ and $\sigma^2_{x_i}$ are the variances of m-order aggregate process $x_i^{(m)}$ and x_i.

Divide the traffic series x_i into N nonoverlapping sections, and each section is further divided into W nonoverlapping segments. Then the autocorrelation function of the wth segment in the nth section is given by

$$r(\tau; H_w(n)) = 0.5\left[|\tau+1|^{2H_w(n)} - 2|\tau|^{2H_w(n)} + |\tau-1|^{2H_w(n)}\right], \tag{2.6}$$

where $H_w(n)$ is the Hurst parameter of the wth segment in the nth section traffic piece. Let $J[H_w(n)] = \sum_\tau [r(\tau; H_w(n)) - r(\tau)]^2$ be the cost function. Then one has

$$H_w(n) = \arg\min J[H_w(n)]. \tag{2.7}$$

Averaging $H_w(n)$ in terms of w yields

$$H(n) = \frac{1}{W}\sum_{w=1}^{W} H_w(n), \tag{2.8}$$

where $H(n)(n = 1, \ldots, N)$ represents the Hurst parameter in the nth section.

3. DDoS Detection Based on Hurst Variation

Given discrete network traffic trace time series $X = \{x_i,\ i \in \mathbf{Z}_+\}$, $Y = \{y_i,\ i \in \mathbf{Z}_+\}$ and $Z = \{z_i,\ i \in \mathbf{Z}_+\}$, let X and Y be normal traffic and abnormal traffic, respectively and Z the DDoS flood attack traffic during transition process of attacking. X and Z are uncorrelated [11], so Y can be expressed as $Y = X + Z$.

Figure 1 illustrates the components of normal traffic, attack traffic, and abnormal traffic. $x_i(p)$ represents the number of bytes sent out by node p at time i for normal network services, $z_i(q)$ stands for the number of bytes sent out by node q at time i for DDoS flood attack, and y_i is the total traffic the target received at time i.

Based on the theorems in [22], we understand that no matter whether Z is a self-similar process or not, as long as X is a second-order stationary self-similar process, Y will be a self-similar process, but the degree of self-similarity may change. Let r_X, r_Z, and r_Y be the autocorrelation functions of X, Z, and Y, respectively. Li in [11] proved that during the transition process of attacking, $\|r_Y - r_X\|$ is significant, where $r_Y = r_X + r_Z$. For each

value of Hurst parameter in the range of $H \in (0.5, 1)$, there is exactly one corresponding autocorrelation function [23]. Therefore, $\|r_Y - r_X\|$ is significant means that $\|H_Y - H_X\|$ changes significantly when attack occurs, where H_Y and H_X are the Hurst parameters of Y and X, respectively. Based on this observation, we propose a DDoS detection method by monitoring the Hurst variation $\Delta H = \|H_Y - H_X\|$ in this paper. The details of the detection process are explained as follows.

After the Hurst parameter estimation of each section using (2.7), we apply autoregressive (AR) model to determine the self-similarity of traffic without attacks. That is,

$$\widehat{H}(n) = \sum_{k=1}^{Q} b_k H(n-k), \tag{3.1}$$

where $\widehat{H}(n)$ is the estimated Hurst parameter of normal traffic section n, Q is the order of AR model, and $\{b_k\}$ are the coefficients of AR model, which can be obtained by using the least-squares method [24]. Other models such as moving average (MA) model and autoregressive moving average (ARMA) model also can be used in our method in the same way.

Since the Hurst parameter $H(n)$ without any attack follows Gaussian distribution in most cases for $W > 10$ [11], the probability distribution function of $H(n)$ is given by

$$p(H(n)) = \frac{1}{\sqrt{2\pi}\sigma_H} e^{-[H(n)-\mu_H]^2/2\sigma_H^2}, \tag{3.2}$$

where

$$\begin{aligned} \mu_H &= \frac{1}{N}\sum_{n=1}^{N} H(n), \\ \sigma_H^2 &= \frac{1}{N}\sum_{n=1}^{N} [H(n) - \mu_H]^2, \end{aligned} \tag{3.3}$$

where N is the number of traffic section. μ_H and σ_H^2 are the mean and variance of the Hurst parameter $H(n)$, respectively.

Using linear estimation, the change of self-similarity $\Delta H(n)$ is given by

$$\Delta H(n) = \widehat{H}(n) - H(n) = \sum_{k=1}^{Q} b_k H(n-k) - H(n), \tag{3.4}$$

which can be regarded as the sum of independent Gaussian variables. So $\Delta H(n)$ also follows Gaussian distribution. The mean and variance of $\Delta H(n)$ are obtained by

$$\mu_{\Delta H} = \mu_H \sum_{k=1}^{Q} b_k - \mu_H = \mu_H \left(\sum_{k=1}^{Q} b_k - 1 \right),$$
$$\sigma_{\Delta H}^2 = \sigma_H^2 \sum_{k=1}^{Q} b_k^2 + \sigma_H^2 = \sigma_H^2 \left(\sum_{k=1}^{Q} b_k^2 + 1 \right). \tag{3.5}$$

So the probability distribution function of $\Delta H(n)$ is expressed by

$$p(\Delta H) = \frac{1}{\sqrt{2\pi}\sigma_{\Delta H}} e^{-[\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2}. \tag{3.6}$$

The attack detection can be formulated as the following hypothesis testing problem.

(A0) The change of self-similarity $\Delta H(n)$ is within a threshold indicating normal network traffic.

(A1) The change of self-similarity $\Delta H(n)$ is outside the threshold indicating abnormal network traffic caused by DDoS attacks.

It can be seen that a proper threshold of $\Delta H(n)$ is the key to successfully detect DDoS attacks. The threshold is also the change point of Hurst parameter whereby Hurst variation beyond this point implies DDoS attack. In the next section, we propose two methods for change point detection, one based on order statistic and the other based on maximum likelihood estimate.

4. Determining Change Point of LRD Traffic

In the following discussion, the change point of self-similarity is equivalent to the threshold that is used to distinguish attack traffic from normal traffic. We propose two methods to determine the change point and calculate the associated detection rate for one method and false alarm rate for the other method.

4.1. Order Statistic-Based Detection

For order statistic-based detection, $\Delta H(n)$ $(n = 1, 2, \ldots, N)$ are first sorted in an increasing order to N reference cells as

$$\Delta H(1) \leq \Delta H(2) \leq \cdots \leq \Delta H(\varsigma) \leq \cdots \leq \Delta H(N). \tag{4.1}$$

The detection threshold is obtained by selecting the ζth-order-ranked $\Delta H(\varsigma)$ to represent the normal traffic plus measured noise. The input is multiplied to that cell by a scalar factor λ, and the threshold θ_{OS} is expressed by

$$\theta_{OS} = \lambda \Delta H(\varsigma). \tag{4.2}$$

The traffic in section n is considered normal if the change of self-similarity $\Delta H(n) < \theta_{OS}$; otherwise, the traffic is considered abnormal, indicating possible attacks in that section. $\Delta H(\varsigma)$ is a random variable, and its probability distribution function is expressed by

$$p[\Delta H(\varsigma)] = \varsigma \binom{N}{\varsigma} [P(\Delta H)]^{\varsigma-1} [1 - P(\Delta H)]^{N-\varsigma} p(\Delta H), \tag{4.3}$$

where $p(\Delta H)$ is the probability distribution function of $\Delta H(n)$, and $P(\Delta H)$ is the distribution function of $\Delta H(n)$.

We define the term detection as correctly recognizing an abnormal sign. The detection rate p_d is obtained by averaging the conditional probability of detection under the given threshold θ_{OS} over all possible values of the threshold. That is,

$$p_d = \int_{\theta_{OS}}^{+\infty} \left[\int_{\theta_{OS}}^{+\infty} p(\Delta H) d\Delta H \right] p[\Delta H(\varsigma)] d\Delta H(\varsigma). \tag{4.4}$$

Substituting (3.6) and (4.3) into (4.4) yields

$$\begin{aligned} p_d = {} & \varsigma \binom{N}{\varsigma} \int_{\theta_{OS}}^{+\infty} \left[\int_{\theta_{OS}}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{\Delta H}} e^{-[\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2} d\Delta H \right] \\ & \times \left[\int_{-\infty}^{\Delta H} \frac{1}{\sqrt{2\pi}\sigma_{\Delta H}} e^{-[\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2} d\Delta H \right]^{\varsigma-1} \\ & \times \left[1 - \int_{-\infty}^{\Delta H} \frac{1}{\sqrt{2\pi}\sigma_{\Delta H}} e^{-[\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2} d\Delta H \right]^{N-\varsigma} \frac{1}{\sqrt{2\pi}\sigma_{\Delta H}} e^{-[\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2} d\Delta H. \end{aligned} \tag{4.5}$$

4.2. Maximum Likelihood Estimate-Based Detection

Considering the independence between $\Delta H(n)$ and $\Delta H(n')$, $(n \neq n')$, the joint probability density function of ΔH is obtained by

$$p_{\text{joint}}(\Delta H) = \prod_{n=1}^{N} p[\Delta H(n)] = \frac{1}{(2\pi)^{N/2}\sigma_{\Delta H}^N} e^{-\sum_{n=1}^{N} [\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2}. \tag{4.6}$$

Taking the natural logarithm on both sides of (4.6), we have

$$\begin{aligned} \ln\left[p_{\text{joint}}(\Delta H)\right] &= \ln\left(\frac{1}{(2\pi)^{N/2}\sigma_{\Delta H}^N} e^{-\sum_{n=1}^{N} [\Delta H(n)-\mu_{\Delta H}]^2/2\sigma_{\Delta H}^2} \right) \\ &= -\left(\frac{N}{2} \ln(2\pi) + N \ln \sigma_{\Delta H} + \frac{1}{2\sigma_{\Delta H}^2} \sum_{n=1}^{N} \left[\Delta H(n) - \mu_{\Delta H}\right]^2 \right). \end{aligned} \tag{4.7}$$

In order to get the maximum likelihood estimate (MLE) of $\mu_{\Delta H}$ and $\sigma^2_{\Delta H}$, we have

$$\begin{aligned}\frac{\partial \ln\left[p_{joint}(\Delta H)\right]}{\partial \mu_{\Delta H}} &= \frac{1}{\sigma^2_{\Delta H}}\sum_{n=1}^{N}\left[\mu_{\Delta H} - \Delta H(n)\right] = 0,\\ \frac{\partial \ln\left[p_{\text{joint}}(\Delta H)\right]}{\partial \sigma^2_{\Delta H}} &= \frac{1}{2\left(\sigma^2_{\Delta H}\right)^2}\sum_{n=1}^{N}\left[\Delta H(n) - \mu_{\Delta H}\right]^2\frac{N}{2\sigma^2_{\Delta H}} = 0.\end{aligned} \tag{4.8}$$

By solving (4.8), one has

$$\begin{aligned}\mu_{\Delta H_{\text{MLE}}} &= \frac{1}{N}\sum_{n=1}^{N}\Delta H(n),\\ \sigma^2_{\Delta H_{\text{MLE}}} &= \frac{1}{N}\sum_{n=1}^{N}\left[\Delta H(n) - \mu_{\Delta H\text{-MLE}}\right]^2.\end{aligned} \tag{4.9}$$

So the probability distribution function of $\Delta H(n)$ is expressed by

$$p(\Delta H_{\text{MLE}}) = \frac{1}{\sqrt{2\pi}\sigma_{\Delta H_{\text{MLE}}}}e^{-\left[\Delta H(n)-\mu_{\Delta H_{\text{MLE}}}\right]^2/2\sigma^2_{\Delta H_{\text{MLE}}}}. \tag{4.10}$$

Let the detection threshold be θ_{MLE}. The traffic in section n is considered normal if the change of self-similarity $\Delta H(n) < \theta_{\text{MLE}}$; otherwise, the traffic is considered abnormal, indicating possible attacks in that section.

Define false alarm as mistakenly recognizing a normal traffic as abnormal traffic. The false alarm rate p_f of the proposed detection system is expressed by

$$p_f = p(\theta_{\text{MLE}} < \Delta H(n)) = \int_{\theta_{\text{MLE}}}^{+\infty}\frac{1}{\sqrt{2\pi}\sigma_{\Delta H_{\text{MLE}}}}e^{-\left[\Delta H(n)-\mu_{\Delta H_{\text{MLE}}}\right]^2/2\sigma^2_{\Delta H_{\text{MLE}}}}d\Delta H. \tag{4.11}$$

So when given the preselected false alarm rate p_f, the detection threshold θ_{MLE} is given by

$$\theta_{\text{MLE}} = \mu_{\Delta H_{\text{MLE}}} + \Phi_{(1-p_f)}\sigma_{\Delta H_{\text{MLE}}}, \tag{4.12}$$

where Φ is the standard normal distribution function.

5. Experiments and Analysis

5.1. Data Preparation

To evaluate the proposed detection methods, we use two traffic data sets from DARPA 1999 [25]. The DARPA 1999 data sets are from the Information Systems Technology Group, MIT Lincoln Laboratory, under DARPA ITO and Air Force Research Laboratory. These traffic data sets are the first standard for the evaluation of computer network intrusion detection systems.

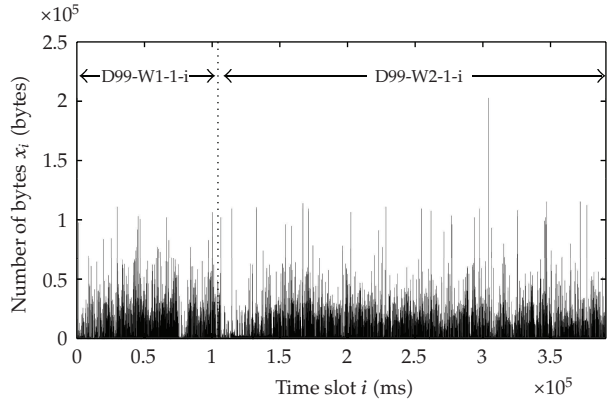

Figure 2: The two traffic traces used in the test.

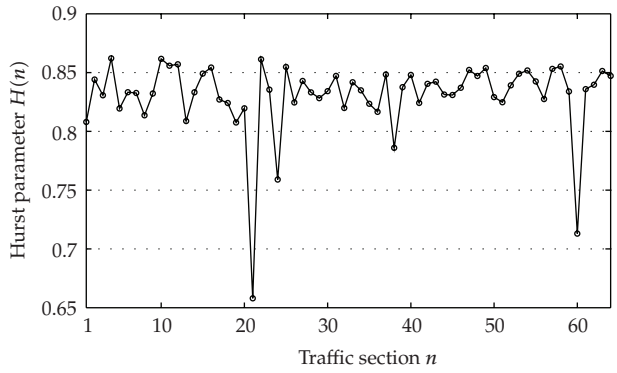

Figure 3: Hurst parameters of traffic D99.

The first traffic set collected from 8:20:00.0 to 11:10:39, 1 March (Monday), 1999, named DARPA1999-week1-Monday-inside, is an attack free series. The second traffic set collected from 8:20:00.0 to 16:24:41.5, 8 March (Monday), 1999, named DARPA1999-week2-Monday-inside, is an attack contained series. 3 types of DDoS attacks are contained in this data set, which are pod, back, and land separately. We rename the first-attack free traffic set as D99-W1-1-i and second attack contained traffic set as D99-W2-1-i for short. The traffic traces for these two data sets are displayed in Figure 2. The merging time scale is 100 ms.

5.2. Test Results and Analysis

After the 100 ms merging, the number of data in D99-W1-1-i is 102400 and the number of data in D99-W2-1-i is 290816. Combine these two traffic sets into one and name it as D99. D99 is divided into 64 sections ($N = 64$) and each section is further divided into 12 segments ($W = 12$). So the length of each traffic segment is 512. We use (2.7) to estimate the Hurst parameter $H_w(n)$ of the wth traffic segment in the nth section ($w = 1, 2, \ldots, W$ and $n = 1, 2, \ldots, N$), then average the $H_w(n)$ in terms of w. After that, we obtain the Hurst parameter $H(n)$ in the nth section, as shown in Figure 3.

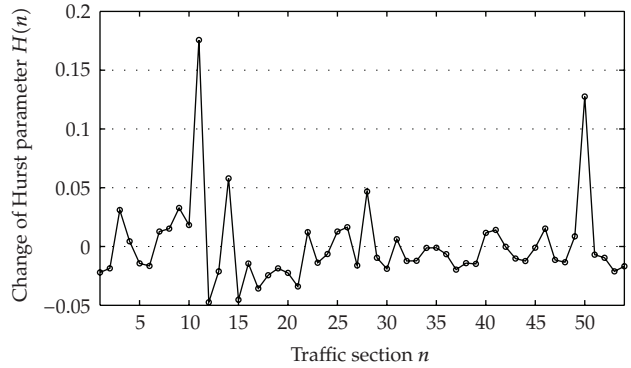

Figure 4: Hurst variation of traffic D99.

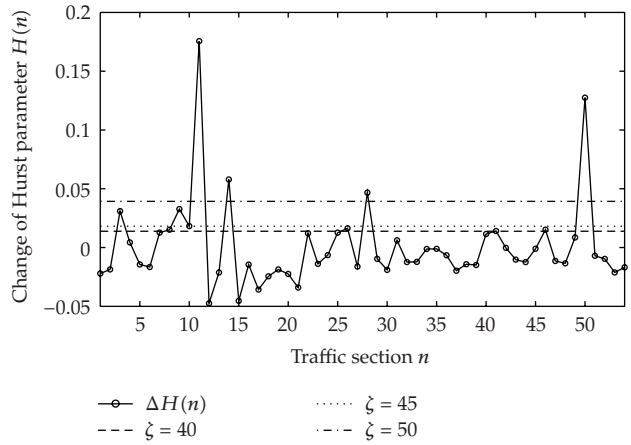

Figure 5: Detection thresholds based on order statistic.

We apply AR model with order Q ($Q = 10$) to estimate the Hurst parameter of the traffic. The Hurst variation $\Delta H(n)$ of the nth traffic section is obtained using (3.4). The results are shown in Figure 4.

For the order statistic-based detection method, we first sort $\Delta H(n)$ in an increasing order and then choose the scale factor $\lambda = 1.2$. After selecting a value ζ, the detection threshold θ_{OS} is calculated according to (4.2). Figure 5 shows the thresholds when ζ is 40, 45, and 50, respectively.

Form Figure 5, we can see that when ζ is smaller ($\zeta = 40$), the detection threshold is lower. In this case, more traffic sections will have Hurst variations above the threshold thus more attacks are declared. However, note that a smaller ζ may also introduce more false alarms, mistakenly recognizing more normal traffic as attack traffic.

For the maximum likelihood estimate-based detection, we compute the detection threshold θ_{MLE} using (4.12). Figure 6 shows the resulted thresholds when the pre-selected false alarm rate p_f is 1%, 5%, and 10%, respectively.

Form Figure 6, we can see that when the pre-selected false alarm rate p_f is higher ($p_f = 10\%$), the resulted threshold is lower. This is in accordance with our expectation because

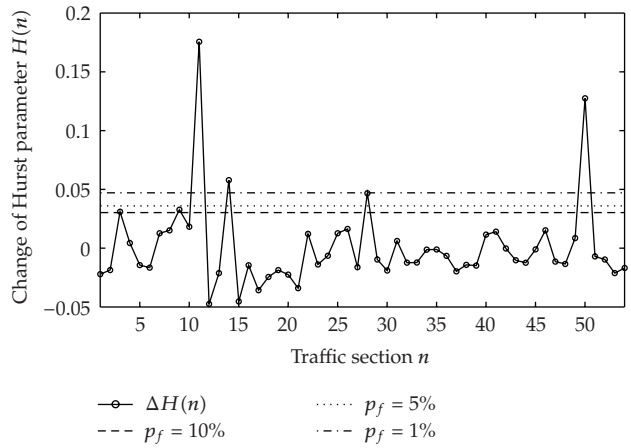

Figure 6: Detection thresholds based on maximum likelihood estimate.

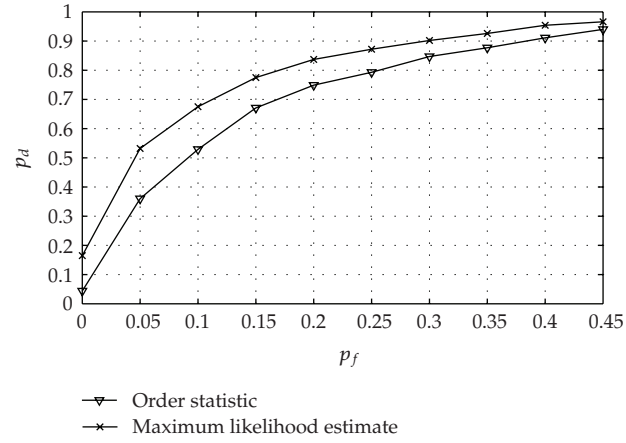

Figure 7: Detection performance.

when the pre-selected false alarm rate is high, it is allowed to mistakenly treat some normal traffic as attacks, thus the detection threshold is low.

Figure 7 shows the detection rate p_d versus false alarm rate p_f for both of the detection methods. We can see from the figure that both of the two detection methods can achieve reasonable detection rate, but the detection performance of maximum likelihood estimate-based method is better than the order statistic-based method. Meanwhile, we can see that for both detection methods, a minor increase of the p_f results in a significant increase in p_d when p_f is lower than 0.1. Which means if we allow a little bit more false alarm, the detection rate will be significantly improved. We can also observe from Figure 7 that when p_d is higher than 0.9, a minor increase in p_d will require a significant increase in p_f. That is, if we want to improve the detection rate in the range greater than 0.9, we have to tolerate much more false alarms.

Table 1: Comparisons of detection performance.

Detection method	p_f	p_d
Allen	34%	80%
Order statistic-based detection	34%	87%
Maximum likelihood estimate-based detection	34%	92%
Ren	38%	89%
Order statistic-based detection	38%	91%
Maximum likelihood estimate-based detection	38%	96%

5.3. Comparison with Existing Detection Methods

In this section, we compare our proposed two detection methods with Allen's method [26] and Ren's method [27], for these are two well-known self-similarity-based detection methods in the literature. Both of these methods define a range of Hurst parameter for normal traffic. For Allen's method, the Hurst range is (0.5, 0.99) and the range is (0.65, 0.85) in Ren's method. Traffic section with a Hurst outside the range is treated as abnormal traffic.

Table 1 compares the detection performance of Allen's method, Ren's method, and our proposed methods. Ren's detection method achieves higher detection rate p_d than Allen's method at the cost of slightly higher false alarm rate p_f. We first use the Allen's false alarm rate 34% as the false alarm rate of the proposed two detection methods. The proposed order statistic-based detection method can archive detection rate as high as 87%, and maximum likelihood estimate-based detection method archives detection rate as high as 92%, both higher than the detection rate of Allen's method. Similarly, we use the Ren's false alarm rate 38% as the false alarm rate of the proposed two detection methods. The detection rates of the proposed detection methods are also higher than that of the Ren's method.

6. Conclusion

In this paper, we have proposed a DDoS detection method by monitoring Hurst variation based on Li's work on DDoS attack detection. Meanwhile, we have discussed two methods for determining the change point of LRD traffic, which can be used to distinguish attack traffic from normal traffic. Experiments have been conducted to evaluate the performance of our proposed scheme, and the test results show that the proposed detection methods outperform existing self-similarity based detection methods, and can significantly enhance the reliability and robustness of the DDoS flood attack detection.

Acknowledgments

This work was supported in part by the National High Technology Research and Development Program of China under Grant no. 2007AA01Z473 and the National Natural Science Foundation of China (NSFC) under Grants no. 60573125, no. 60873264, no. 60605019 and no. 60702047. The authors would also like to thank the reviewers for their constructive comments that have considerably increased the quality of this paper.

References

[1] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the self-similar nature of ethernet traffic (extended version)," *IEEE/ACM Transactions on Networking*, vol. 2, no. 1, pp. 1–15, 1994.

[2] 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.

[3] O. Tickoo and B. Sikdar, "On the impact of IEEE 802.11 MAC on traffic characteristics," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 2, pp. 189–203, 2003.

[4] M. Li, "Fractal time series—a tutorial review," *Mathematical Problems in Engineering*, vol. 2010, Article ID 157264, 26 pages, 2010.

[5] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*. In press.

[6] M. Li and S. C. Lim, "Modeling network traffic using generalized Cauchy process," *Physica A*, vol. 387, no. 11, pp. 2584–2594, 2008.

[7] M. Li and W. Zhao, "Variance bound of ACF estimation of one block of fGn with LRD," *Mathematical Problems in Engineering*, vol. 2010, Article ID 60429, 14 pages, 2010.

[8] W.-B. Gong, Y. Liu, V. Misra, and D. Towsley, "Self-similarity and long range dependence on the internet: a second look at the evidence, origins and implications," *Computer Networks*, vol. 48, no. 3, pp. 377–399, 2005.

[9] W. Schleifer and M. Männle, "Online error detection through observation of traffic self-similarity," *IEE Proceedings: Communications*, vol. 148, no. 1, pp. 38–42, 2001.

[10] J. T. Wang and G. Yang, "An intelligent method for real-time detection of DDoS attack based on fuzzy logic," *Journal of Electronics*, vol. 25, no. 4, pp. 511–518, 2008.

[11] M. Li, "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks," *Computers and Security*, vol. 25, no. 3, pp. 213–220, 2006.

[12] C. S. Sastry, S. Rawat, A. K. Pujari, and V. P. Gulati, "Network traffic analysis using singular value decomposition and multiscale transforms," *Information Sciences*, vol. 177, no. 23, pp. 5275–5291, 2007.

[13] M. F. Rohani, M. A. Maarof, A. Selamat, and H. Kettani, "Continuous LoSS detection using iterative window based on SOSS model and MLS approach," in *Proceedings of the International Conference on Computer and Communication Engineering (ICCCE '08)*, pp. 1005–1009, Kuala Lumpur, Malaysia, May 2008.

[14] M. Li and W. Zhao, "Detection of variations of local irregularity of traffic under DDOS flood attack," *Mathematical Problems in Engineering*, vol. 2008, Article ID 475878, 11 pages, 2008.

[15] M. Li, J. Li, and W. Zhao, "Experimental study of DDOS attacking of flood type based on NS2," *International Journal of Electronics and Computers*, vol. 1, no. 2, pp. 143–152, 2009.

[16] M. Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition," *Computers and Security*, vol. 23, no. 7, pp. 549–558, 2004.

[17] C. Cattani and A. Kudreyko, "On the discrete harmonic wavelet transform," *Mathematical Problems in Engineering*, vol. 2008, Article ID 687318, 7 pages, 2008.

[18] C. Cattani and A. Kudreyko, "Application of periodized harmonic wavelets towards solution of eigenvalue problems for integral equations," *Mathematical Problems in Engineering*, vol. 2010, Article ID 570136, 8 pages, 2010.

[19] C. Cattani, "Harmonic wavelet analysis of a localized fractal," *International Journal of Engineering and Interdisciplinary Mathematics*, vol. 1, no. 1, pp. 35–44, 2009.

[20] E. G. Bakhoum and C. Toma, "Mathematical transform of traveling-wave equations and phase aspects of quantum interaction," *Mathematical Problems in Engineering*, vol. 2010, Article ID 695208, 15 pages, 2010.

[21] G. Toma, "Specific differential equations for generating pulse sequences," *Mathematical Problems in Engineering*, vol. 2010, Article ID 324818, 11 pages, 2010.

[22] S. Song, J. K. Y. Ng, and B. Tang, "Some results on the self-similarity property in communication networks," *IEEE Transactions on Communications*, vol. 52, no. 10, pp. 1636–1642, 2004.

[23] J. Beran, *Statistics for Long-Memory Processes*, vol. 61 of *Monographs on Statistics and Applied Probability*, Chapman and Hall, New York, NY, USA, 1994.

[24] D. He and H. Leung, "Network intrusion detection using CFAR abrupt-change detectors," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 3, pp. 490–497, 2008.

[25] http://www.ll.mit.edu/mission/communications/ist/index.html.

[26] W. H. Allen and G. A. Marin, "The LoSS technique for detecting new denial of service attacks," in *Proceedings of IEEE South East Conference*, pp. 302–309, Greensboro, NC, USA, March 2004.

[27] X. X. Ren, R. C. Wang, and H. Y. Wang, "Wavelet analysis method for detection of DDoS attack on the basis of self-similarity," *Frontiers of Electrical and Electronic Engineering in China*, vol. 2, no. 1, pp. 73–77, 2007.