# Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic

Zhengmin Xia, Songnian Lu and Jianhua Li
Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
E-mail: miaomiaoxzm@sjtu.edu.cn, snlu@sjtu.edu.cn, lijh888@sjtu.edu.cn

Junhua Tang
School of Information Security Engineering, Key Lab of Information Security Integrated Management Research, Shanghai Jiao Tong University, Shanghai 200240, China
E-mail: junhuatang@sjtu.edu.cn

**Keywords:** network security, statistical detection, self-similarity, fuzzy logic

**Received:** February 1, 2010

*Distributed denial-of-service (DDoS) flood attack remains great threats to the Internet. This kind of attack consumes a large amount of network bandwidth or occupies network equipment resources by flooding them with packets from the machines distributed all over the world. To ensure the network usability and reliability, real-time and accurate detection of these attacks is critical. To date, various approaches have been proposed to detect these attacks, but with limited success when they are used in the real world. This paper presents a method that can real-time identify the occurrence of the DDoS flood attack and determine its intensity using the fuzzy logic. The proposed process consists of two stages: (i) statistical analysis of the network traffic time series using discrete wavelet transform (DWT) and Schwarz information criterion (SIC) to find out the change point of Hurst parameter resulting from DDoS flood attack, and then (ii) adaptively decide the intensity of the DDoS flood attack by using the intelligent fuzzy logic technology to analyze the Hurst parameter and its changing rate. The test results by NS2-based simulation with various network traffic characteristics and attacks intensities demonstrate that the proposed method can detect the DDoS flood attack timely, effectively and intelligently.*

*Povzetek: Opisan je postopek za prepoznavo spletnega napada DDoS s pomočjo mehke logike.*

## 1 Introduction

Distributed denial-of-service (DDoS) attack has been one of the most frequently occurring attacks that badly threaten the stability of the Internet. According to CERT Coordination Center (CERT/CC)[1], there are mainly three categories of DDoS attacks: flood attack, protocol attack and logical attack. This paper mainly focuses on flood attack. In the DDoS flood attack, an intruder bombs attack packets upon a site (victim) with a huge amount of traffic so as to actually jam its entrance and block access by legitimate users or significantly degrade its performance[2]. Therefore, a real-time and accurate detection of these attacks is critical to the Internet community.

Usually, the attack detection methods are classified into two categories. One is misuse detection and the other is anomaly detection. Misuse detection is based on a library of known signatures to match against network traffic. Hence, unknown signatures from new variants of an attack mean 100% miss. Anomaly detection does not suffer from this problem. Considering that DDoS flood attack is a process changing dynamically and frequently, anomaly-based detectors play a key role in detecting this kind of attack. As far as anomaly detection is concerned, quantitatively characterizing statistic of network traffic without attack is fundamental[2].

As shown by Leland[3] et al., and supported by a number of later research [4-5], the measurements of local and wide-area network traffic, wire-line and wireless network traffic all demonstrate that network traffic possesses self-similarity characteristic in large time-scale. Self-similarity is the property associated with the object whose structure is unchanged at different scales, and its degree can be described by the Hurst parameter.

Several studies show that DDoS flood attack can exert remarkable influence on the self-similarity of network traffic. Thus, this kind of attack can be effectively detected by monitoring the change of the Hurst parameter[6-7]. Existing flood attack detection methods based on the self-similarity nature of network traffic divide the network traffic into non-overlapping segments. The Hurst parameter of each segment is estimated, once the Hurst parameter changes beyond a pre-defined fixed threshold, the loss of self-similarity (LoSS) occurs and the DDoS flood attack is detected. However, the DDoS flood attack may take place at arbitrary moment whenever the traffic changes its self-similarity characteristic. The intensity of DDoS flood attack is also varying, which leads to changing Hurst parameter. Therefore, these existing fixed threshold detection methods lack flexibility and self-adaptability.

In this paper, we propose a DDoS flood attack detection method using discrete wavelet transform (DWT) and Schwarz information criterion (SIC) to determine the change point of self-similarity. The SIC[8] statistic is based on the maximum likelihood function for the model, and can be easily applied to change point detection by comparing the likelihood of the null hypothesis (i.e., no change in the variance series) against the alternative hypothesis (i.e., a change is present). This paper presents the SIC algorithm working with the DWT to detect the change point of self-similarity in real-time. After the change point detection, we use the fuzzy logic[9-15] to adaptively determine the intensity of the DDoS flood attack. We also design a set of decision rules for the fuzzy logic to determine the intensity of the DDoS flood attack. As a result, this proposed attack detection method can accurately detect not only the moment when the flood attack happens, but also the intensity of the attacks.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 gives a brief introduction to self-similarity and the relationship between the wavelet coefficients and the Hurst parameter. Section 4 first deduces the basic detection principle, and then presents the outline of the whole detection process. Section 5 describes the on-line self-similarity change point identification in detail. In section 6, the decision rules of the attack intensity are given. Section 7 discusses the performance of our method by NS2-based simulation with various network traffic characteristics and attack intensities. Finally, a brief summary of our work and future research are provided in section 8.

# 2 Related work

Several anomaly detection methods have been proposed against DDoS flood attack in the literature[16-18]. In these methods, the network traffic activity is captured and then a profile representing its stochastic behavior is created. This profile is mainly based on metrics such as the network traffic rate, the number of packets or bytes for each protocol, the rate of connections, the number of different IP addresses, etc. Any activity that deviates from the profile is treated as a possible attack.

There is a serious problem with these statistical anomaly detection methods. That is, it is hard to decide the appropriate metric on the global scale, because the linear superposition of these micro-based detection methods can not cope with the complex behavior of whole network. In 1993，Leland[3] et al. first found that the network traffic is self-similar and this attribute is one of the basic natures of the network traffic. Later, the work in [19] pointed out that the self-similarity of Internet traffic is attributed to a mixture of the actions of a number of individual users, and 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.

The research done by Li[20] first mathematically proved that there is a statistically significant change in the average Hurst parameter under DDoS flood attack. Allen[21] et al. and W.Schleifer[22] et al. proposed a method using Hurst parameter to identify attack, which causes a decrease in the traffic's self-similarity. Those methods consider the normal range of Hurst parameter to be [0.5, 0.99], and there is an attack when the Hurst parameter runs out of this range. The experiment results demonstrate that the method proposed in [21-22] has an average detection rate of 60% to 84% depending on the intensity of the attack. Ren[23] et al. proposed using the wavelet analysis method to estimate the Hurst parameter, and consider there is an attack when the Hurst parameter runs out of the range [0.6, 0.9]. The cut down of normal range of Hurst parameter can be more efficient in detecting the low-rate DDoS flood attack. Nevertheless, all of these existing detection methods can only detect the presence of attack after the attack occurs, they can not identify at what time the attack happened.

Fuzzy logic is one of the most popular methods used in attack detection for it can deal with the vague and imprecise boundaries between normal traffic and different levels of attacks[10]. Wang[24] et al. proposed to use the fuzzy logic to analyze the Hurst parameter and estimate the time duration of DDoS attack. However, the work in [24] didn't consider the intensity of the attack traffic compared with the background traffic, therefore cannot accurately reflect the level of damage that is caused by the attack.

The major contributions of this paper are: (i) considering the inherent relationship between DWT and self-similarity, we propose to use SIC combined with DWT to detect the *occurrence* of the DDoS flood attack, therefore real-time DDoS attack detection is achieved; (ii) we propose a fuzzy set and its implementation to decide the intensity of DDoS flood attack *against the background traffic* dynamically and intelligently, which provides an accurate indication of the possible damage caused by the attack.

# 3 Self-similarity

## 3.1 A brief review of self-similarity

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

Network traffic arrival process is a discrete time process, so the discrete time self-similarity definition will be used here. Let $X = \{x_i, i \in \square_+\}$ be a wide-sense stationary discrete stochastic traffic time series with constant mean $\mu$, finite variance $\sigma^2$, and autocorrelation

function $r(\tau), (\tau \in \mathbb{R}_+)$. Let $X^{(m)} = \{x_i^{(m)}, i, m \in \mathbb{R}_+\}$ be an $m$-order aggregate process of $X$, then

$$x_i^{(m)} = (x_{mi-m+1} + \cdots + x_{mi})/m . \quad (1)$$

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

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

$$r^{(m)}(\tau)=r(\tau), \quad (2)$$

where $r(\tau) = [(\tau+1)^{2-\beta} - 2\tau^{2-\beta} + (\tau-1)^{2-\beta}]/2$.

**Definition 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

$$\lim_{m\to\infty} r^{(m)}(\tau) = r(\tau) . \quad (3)$$

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

### 3.2 Wavelet-based Hurst parameter estimation

Currently, 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. However, the wavelet-based estimator[25] of the Hurst parameter stands out as one of the most reliable estimators in practice since it is more robust with respect to smooth polynomial trends and noise.

In this section, an on-line Hurst parameter estimation is proposed using the multiple resolutions feature of wavelet analysis. The estimation process is summarized as follows:

- **Wavelet decomposition:** For a given traffic trace time series $X$, we compute the wavelet coefficients $d(j,k)$ using a pyramidal filter bank in an on-line fashion for each scale $j$ and position $k$, as shown in Figure 1. At each level in the recursive structure, the bandpass (BP) output wavelet coefficients $d(j,\cdot)$, and the lowpass (LP) output scale coefficients $a(j,\cdot)$, occur at half rate of the input $a(j\text{-}1,\cdot)$.

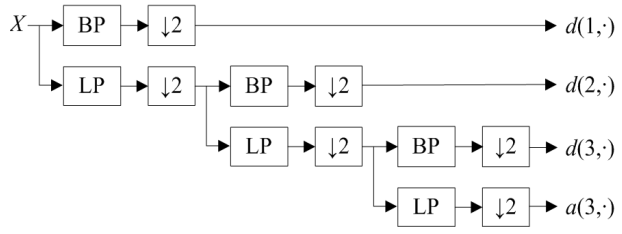


Figure 1: Pyramidal filter bank.

- **Detail variance estimation:** Let the current stored sum of squares calculated from the available wavelet coefficients at scale $j$ be

$$S_j = \sum_{k=1}^{n_j} d^2(j,k) , \quad (4)$$

where $n_j$ means the number of wavelet coefficients available at scale $j$. Assume that the arrival of a new traffic sample results in the new wavelet coefficient $d(j,n_j+1)$ at scale $j$ from the filter bank. The sum is then updated as follows:

$$\begin{aligned} n_j &\leftarrow n_j + 1 \\ S_j &\leftarrow S_j + d^2(j,n_j) \end{aligned} . \quad (5)$$

When the variance estimation at scale $j$ is required for the next step, it can be calculated as $\varepsilon_j=S_j/n_j$.

- **Analysis using the Logscale diagram:** We make a plot of $\log_2(\varepsilon_j)$ versus scale $j$ and apply a weighted linear regression over the curve region that looks linear, and then compute the slope $\alpha$. There is no need to compute the Logscale diagram every time a new traffic sample is acquired, since they may be recalculated only when needed.
- **Hurst parameter estimation:** The Hurst parameter $H$ can be estimated according to

$$H=(\alpha+1)/2 . \quad (6)$$

This on-line wavelet-based Hurst parameter estimation is performed in an accumulative way, that is, it returns the updated Hurst parameter computed over all available samples from beginning to current time. We can see that this estimation method is accumulative but not dynamic, thus can not be used directly in detecting the change point of self-similarity in the network traffic. Therefore, a change point detection method combined with DWT is proposed and discussed in detail in section 5.

## 4 Attack detection process

### 4.1 Attack detection principle

Let $X = \{x_i, i \in \mathbb{R}_+\}$ and $Y = \{y_i, i \in \mathbb{R}_+\}$ be normal and abnormal traffic respectively, and $Z = \{z_i, i \in \mathbb{R}_+\}$ be the attack traffic during transition process of attacking. $X$ and $Z$ are uncorrelated[2], so $Y$ can be abstractly expressed by $Y$=$X$+$Z$.

Figure 2 illustrates the components of normal and abnormal traffic. $x_i(p)$ represents the number of bytes sent out by node $p$ at time $i$ for normal network services, and $z_i(q)$ represents the number of bytes sent out by node $q$ at time $i$ for network attack, and $y_i$ is the total traffic the target received at time $i$.

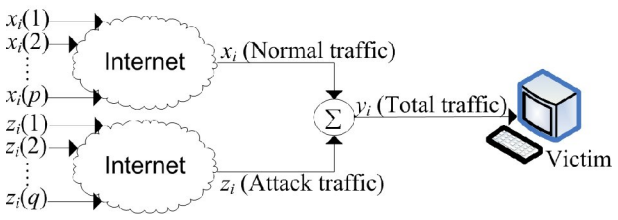


Figure 2: Composition of normal and attack traffic.

Based on the theorems in reference [26], we can get the conclusion that no matter whether $Z$ is a self-similar process, if $X$ is a second-order stationary self-similar

process, then $Y$ will still be a self-similar process, but the degree of self-similarity may be changed. Let $r_X$, $r_Z$ and $r_Y$ be the autocorrelation functions of $X$, $Z$ and $Y$ respectively. During the attack, $\|r_Y - r_X\|$ is noteworthy[2], and $r_Y = r_X + r_Z$. For each value of $H \in (0.5,1]$, there is exactly one autocorrelation function with self-similarity[27]. Thus, the consequence is that $\|H_Y - H_X\|$ is considerable, where $H_Y$ and $H_X$ are average Hurst parameters of $Y$ and $X$, respectively. Hence, $H$ is a parameter that can be used to describe the abnormality of network traffic.

### 4.2 Outline of the attack detection process

The whole process of the DDoS flood attack detection is displayed in Figure 3.

From Figure 3, we can see that the whole detection process consists of two stages: on-line attack moment identification and intelligent attack intensity decision. In the part of attack moment identification, the wavelet coefficients and SIC statistic will be updated along with the incoming of new traffic samples, then the change point detection will re-run in every scale to find out whether there is a change point. It will signal a change point of self-similarity in network traffic if change points exist in enough scales at the same moment. After the attack moment identification, we then segment the network traffic into pieces around the identified attack moment. After that, we can decide the intensity of the attack using intelligent fuzzy logic technology. According to the Hurst parameter and its changing rate (the difference between the Hurst parameters of traffic pieces prior to and after the identified attack moment), we can determine the intensity of the DDoS flood attack using the fuzzy decision rules. The next two sections present the detailed implementation of attack moment identification and attack intensity decision.

## 5 Change point estimation with SIC

### 5.1 SIC

The SIC is a powerful approach in detecting the change point of self-similarity in network traffic[8]. The principle of SIC is that a sequence with a variance change point has higher entropy than a sequence with constant variance.

Given a sequence of length $M$, and suppose there is only one change point at position $g$ ($1<g<M$). The way of simultaneously detecting the presence and location of this change point is to compute the entropy of the entire sequence and of the pairs of pieces ($f_1=1,\ldots, g$ and $f_2=g+1,\ldots, M$), compare their values and then decide if there is a change point at position $g$ according to whether the entropy of the pieces is significantly lower than the entropy of the entire sequence.

We test the null hypothesis $A_0$ (no change is present) against the alternative $A_1$ (a single change is present). Assuming gaussianity and independence[8], the SIC statistic for the two hypotheses is given by

$$A_0 : \mathrm{SIC}(M) = M\log 2\pi + M\log\hat{\sigma}^2 + M + \log M,$$

$$A_1 : \mathrm{SIC}(g) = M\log 2\pi + g\log\hat{\sigma}_1^2 + (M-g)\log\hat{\sigma}_2^2 + M + 2\log M,$$

where $\hat{\sigma}^2$, $\hat{\sigma}_1^2$ and $\hat{\sigma}_2^2$ are the unbiased maximum likelihood estimators (MLEs) of the variances of the entire sequence and of the first and second pieces, respectively.

Our decision will follow the principle of minimum information, that is, $A_0$ will not be rejected if

$$\mathrm{SIC}(M) \le \min_g \mathrm{SIC}(g),$$

otherwise $A_0$ will be rejected if

$$\mathrm{SIC}(M) > \mathrm{SIC}(g),$$

for some $g$. The change point at position $g$ can be estimated according to

$$\mathrm{SIC}(g) = \min_{1\le g<M} \mathrm{SIC}(g). \quad (7)$$

Reference [28] gives a proof that $g$ is a consistent estimator of the true change point, and it also gives the expression for computing the signification level of SIC statistic. The analytic study by Tian[29] et al. shows that the Hurst parameter has close relationship with variance structure of wavelet coefficients. The SIC has the merit of detecting the change point in the variance structure of the sequence, so the combination of DWT and SIC can be used to detect the change point of Hurst parameter in the network traffic.

### 5.2 Connecting DWT and SIC

In this section, we apply the SIC change point detection to the wavelet coefficients $d(j,k)$ at each scale $j$. It will signal a change point of Hurst parameter if we find the same variance change position across all or a significant number of scales. A change in variance at a single scale only tells us of non-stationary in the variance at that scale

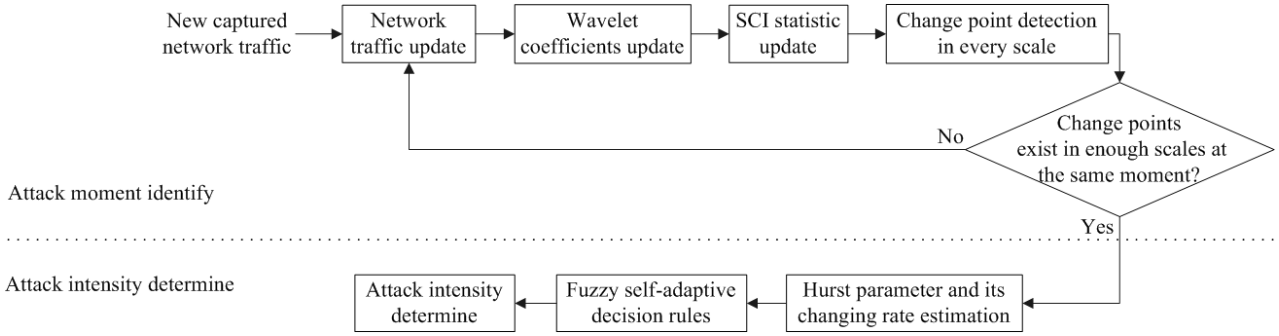


Figure 3: Diagram of DDoS flood attack detection

For the DWT, the number of wavelet coefficients at each scale is not the same, since each branch of the filter bank suffers a different number of decimations. Let $n_j$ be the number of available wavelet coefficients at scale $j$ and $n_{j+1}$ be the number of wavelet coefficients at scale $j$+1, then the relationship between adjacent scales of $n_j$ and $n_{j+1}$ satisfies $n_j=2n_{j+1}$. Figure 4 (a) shows the temporal relationship between the wavelet coefficients of each scale. We can see that the wavelet coefficients of each scale in the dotted line correspond to certain length of network traffic. In order to provide a good estimation of the change point at all available scales, a phase correction should be applied to higher scales, with a scale dependent delay as illustrated in Figure 4 (b). This phase correction aligns the position of the wavelet coefficients with a scale-dependent delay and with their zone of influence to the change point detection.

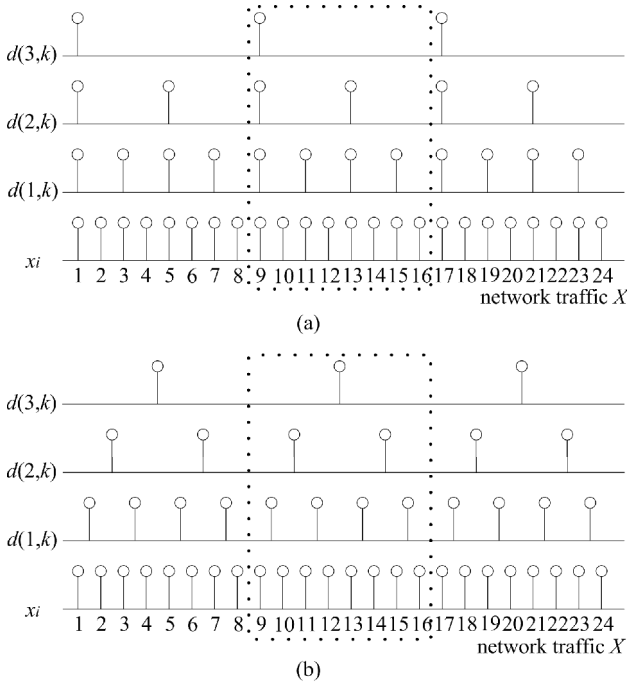


Figure 4: Temporal relationship between: (a) wavelet coefficients; (b) phase corrected wavelet coefficients.

There are two main requirements for the attack detection performance, one is accurate detection and the other is real-time detection. In the subsequent section, a real-time detection method is emphasized, which performs DWT and SIC statistics in sequential fashion, and with a slide-window to detect the change point of self-similarity on-line.

## 5.3 On-line change point estimation

The on-line detection scheme of the change point of self-similarity in network traffic comprises three steps: network traffic update using slide-window, wavelet coefficients update using pyramidal filter bank and SIC statistic update with new wavelet coefficients available at each scale.

- **Network traffic update:** Let $l$ represent the original number of network traffic time series used to detect the change point of self-similarity, and $h$ represent the size of slide-window. The process of updating network traffic is displayed in Figure 5. When $h$ samples of new traffic are acquired, we add these new traffic samples into the tail of original traffic and discard the same number of old samples at the head of original traffic simultaneously, so the reserved network traffic for the next detection is $l$-$h$. This process is iterated whenever new samples are acquired. By doing so, we can guarantee that there is only one change point of self-similarity in this finite length of traffic before we perform the detection.

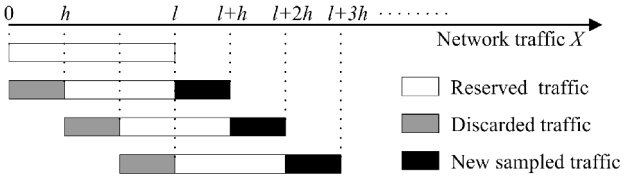


Figure 5: Network traffic update.

- **Wavelet coefficients update:** For the new acquired $h$ traffic samples, we feed them into the pyramidal filter bank displayed in Figure 1. The transforms give the new wavelet coefficients corresponding to the convolution of the new acquired $h$ samples and the memory of the filter. For example, let $h$ be 64 ($2^6$), then only wavelet coefficients at scales 1~5 need to be updated. Therefore, the change points in the variance structure will appear progressively in the higher scales as new samples are acquired. For the discarded traffic, we only need to discard the wavelet coefficients of each scale related to the discarded traffic, as we can see in Figure 4 (b).
- **SIC statistic update:** The update of SIC statistic is relatively simple to implement, since it only requires the variance of the new wavelet coefficients at each scale to be added and the variance of the discarded wavelet coefficients at each scale to be discarded. We then re-test the null hypothesis $A_0$ against the alternative $A_1$ at each scale to find out whether there are change points in the variance structure.

A decision that there is a change point of self-similarity in network traffic can be made if change points in the wavelet coefficients variance structure exist in enough scales at the same moment. A change in the wavelet coefficients variance structure in one scale or a few scales only tells us the non-stationary at that scale. After the change point of self-similarity detection in network traffic, we then segment the network traffic into pieces around the identified change moment. After that, we can determine the intensity of DDoS flood attack using intelligent fuzzy logic technology, which takes the Hurst parameter and its changing rate as decision-making basis.

# 6 Attack intensity decision with intelligent fuzzy logic

## 6.1 Intelligent fuzzy logic

Intelligent fuzzy logic decision disposes information based on fuzzy or non-fuzzy reasoning rules[10-12]. It makes self-adaptive decision in light of mature experience. The general fuzzy decision process consists of three parts: fuzzy quantitative disposal, fuzzy decision rules and fuzzy decision. The fuzzy quantitative disposal makes the real input parameter as a fuzzy set, and then the fuzzy decision carries out the output calculation based on the fuzzy set and fuzzy operators defined at fuzzy decision rules. This section will describe in detail how fuzzy logic can be utilized in DDoS flood attack intensity decision.

## 6.2 Attack intensity decision

Based on the basic theory and method of fuzzy mathematics, we propose an intelligent DDoS flood attack intensity decision system. DDoS flood attack intensity itself includes fuzziness, because the boundary between the light attack, moderate attack and severe attack is not well defined. So when judging the intensity of attack, one should take the intensity of background traffic into consideration. For example, a DDoS flood attack is considered as light attack if it causes slight decline of the network performance when the traffic load is high, but is considered as severe attack if it causes serious decline of the network performance when the network load is light.

In the proposed decision system, the DDoS flood attack intensity decision rules and operations are expressed by fuzzy sets, and then we feed these fuzzy decision rules and related information into knowledge repository. The network elements take the dynamic process of actual attack into consideration, and then use fuzzy reasoning to determine the intensity of attack dynamically and intelligently.

In this paper, the structure of fuzzy decision is two-dimensional input and one-dimensional output. The two inputs are the Hurst parameter and its changing rate. The Hurst parameter reflects the influence of dynamic normal traffic on attack intensity and the changing rate reflects the influence of attack on normal traffic. The output is the intensity of the attack. As shown in Figure 6, the fuzzy decision process of the intensity of the attack consists of three parts: Hurst parameter and its changing rate fuzzification, fuzzy decision rules of attack intensity and fuzzy reasoning of attack intensity.

The description of each part of the fuzzy decision process is as follows:

- **Hurst parameter and its changing rate fuzzification:** Fuzzification makes the real input parameters of Hurst parameter and its changing rate as fuzzy sets. According to the change scope of Hurst parameter and its changing rate, we define the universe of discourse of the Hurst parameter as $UH$={0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0, 1.1}; the universe of discourse of the changing rate as $UHC$={0.05, 0.10, 0.15, 0.20, 0.25, 0.30, 0.35, 0.40, 0.45, 0.50}. The fuzzy sets of $UH$ and $UHC$ are $H'$={$S$, $M$, $B$} and $HC'$={$S$, $M$, $B$}, where "$S$" stands for small, "$M$" the moderate, and "$B$" the big. The variable's membership degree function of each fuzzy language satisfies normality assumption
$$\mu(x)=\exp\left[-(x-v)^2/b^2\right], \quad (8)$$
where $v$ and $b^2$ are the mean and variance of the membership degree function. Through Eq. (8), we can obtain fuzzy judgment model of every parameter as well as the membership degree assignments of every fuzzy subset.
- **Fuzzy decision rules of attack intensity:** The decision rules take note of the relationship between input fuzzy sets and output fuzzy sets. Define the fuzzy decision result of DDoS flood attack intensity as a variable $L$, and the fuzzy set of $L$ as $L'$={$LA$, $MA$, $SA$}, where "$LA$", "$MA$" and "$SA$" represent light DDoS flood attack, moderate DDoS flood attack and severe DDoS flood attack, respectively. Considering the relationship between Hurst parameter, its changing rate and DDoS flood attack intensity, we can get the fuzzy decision rules displayed in Table 1.

Table 1. The fuzzy decision rules of the DDoS flood attack.

| $HC'$ | $H'$ | | |
|---|---|---|---|
| | $S$ | $M$ | $B$ |
| $S$ | $MA$ | $LA$ | $LA$ |
| $M$ | $SA$ | $MA$ | $LA$ |
| $B$ | $SA$ | $SA$ | $MA$ |

- **Fuzzy reasoning of attack intensity:** After fuzzifying the input parameters Hurst parameter and its changing rate, we can reason the intensity of attack according to decision rules presented in Table 1. For example, when the Hurst parameter is considered moderate, we infer there is a light DDoS flood attack if the changing rate of the Hurst parameter is considered small. In a similar way, there is a moderate DDoS flood attack if the changing rate of the Hurst parameter is moderate, and severe DDoS flood attack if the changing rate of the Hurst parameter is big.

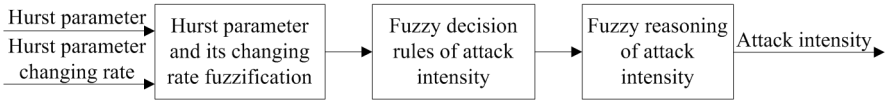


Figure 6: Intelligent fuzzy decision process.

# 7 Experiments and analysis

## 7.1 Simulation environment

The test traffic time series is constructed using NS2 simulator with varying parameters (e.g. the self-similarity degree of normal traffic and the attack intensity). The simulated traffic model is shown in Figure 2, and we let the number of nodes that provide normal service is $p$=100, and the number of nodes that implement the attack is $q$=100.

We conducted our simulation in two steps: First we generate the normal traffic using fractional Gaussian noise (=fGn) model with Hurst parameter $H$={0.6, 0.7, 0.8, 0.9}. The FGN model was first introduced by Mandelbrot and Van Ness[30], and now it is widely used in network traffic modeling for its simplicity and mathematically attractive. Other traffic models also can be used in this simulation in the same way. Second we inject constant rate attack traffic at time 600 (second) with maximum attack intensity varying from 100KBps to 500KBps. The constant rate attack achieves its maximum rate immediately and lasts for about 400 seconds. The normal traffic will persist for another 200 seconds after the attack stops.

The simulated abnormal traffic trace with different self-similarity degree and attack intensity is displayed in Figure 7. The merging time scale is 100 ms.

In Figure 7, every piece of traffic in the same column has same self-similarity degree with Hurst parameter displayed at the top of the column, and every piece of traffic in the same row suffered from same attack intensity. From the first row to the last row, the attack intensity is 100KBps, 200KBps, 300KBps, 400KBps, and 500KBps, respectively.

## 7.2 Test results and analysis

We use Daubechies(3) as mother wavelet and set the decomposition level to 6. In the experiment, the size of slide-window is $h$=64, and $l$=8$h$. Under the condition of significance equal to $10^{-5}$, we can identify the change points of Hurst parameter at points 6000 and 10000 as shown in Figure 8. In the simulation, point 6000 is when attack happens and point 10000 is when attack stops.

Figure 8 shows the results of phase corrected 6-level DWT-SIC statistics analysis of the simulated traffic trace. For normal traffic with same degree of self-similarity, we can see that: (i) At lower scales, the change points caused by both light DDoS flood attack and severe DDoS flood attack are clearly identified; (ii) At higher scales, the change points caused by light DDoS flood attack disappear because the DWT lacks temporal accuracy. Under the condition of same attack intensity, we can see that more change points appear at higher scales when self-similarity degree is higher, which means the higher degree of traffic self-similarity, the more sensitive the network is to DDoS flood attack.

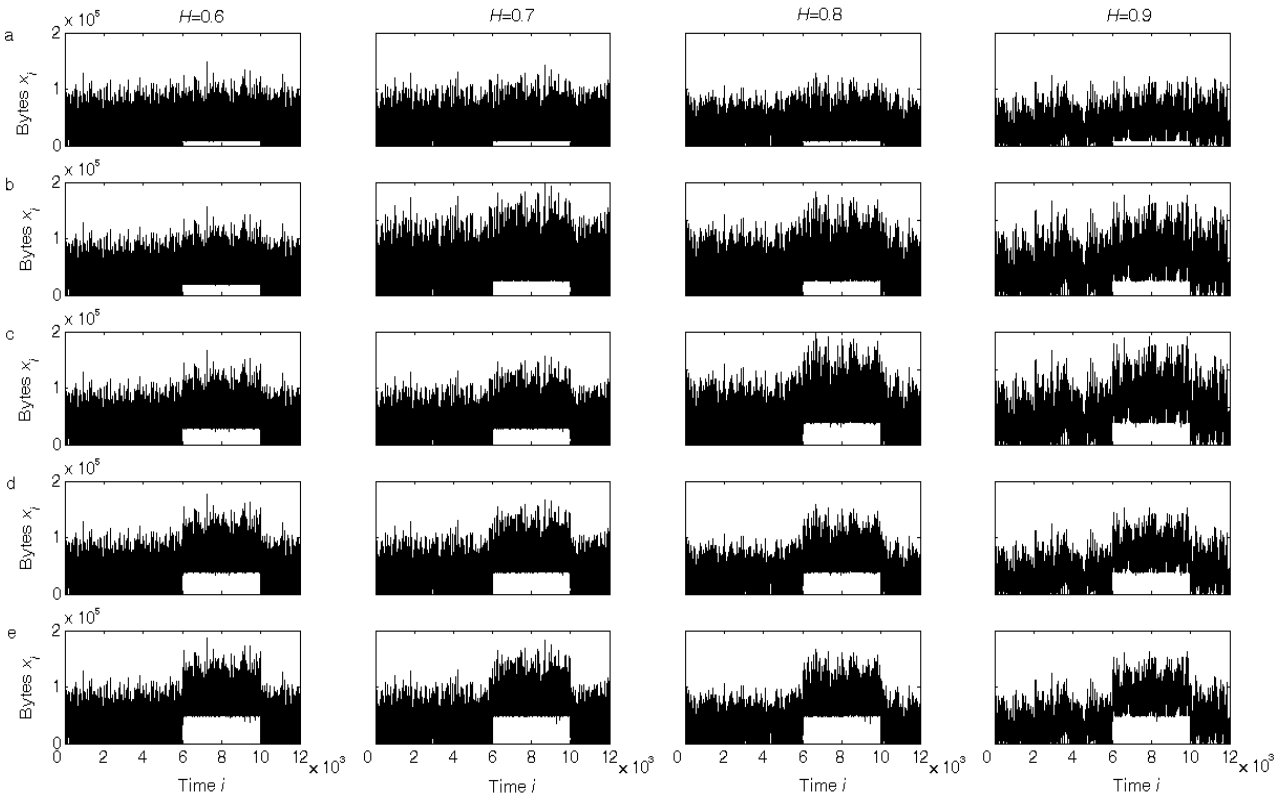


Figure 7: Simulated abnormal traffic trace: (a) attack intensity-100KBps; (b) attack intensity-200KBps; (c) attack intensity-300KBps; (d) attack intensity-400KBps; (e) attack intensity-500KBps.

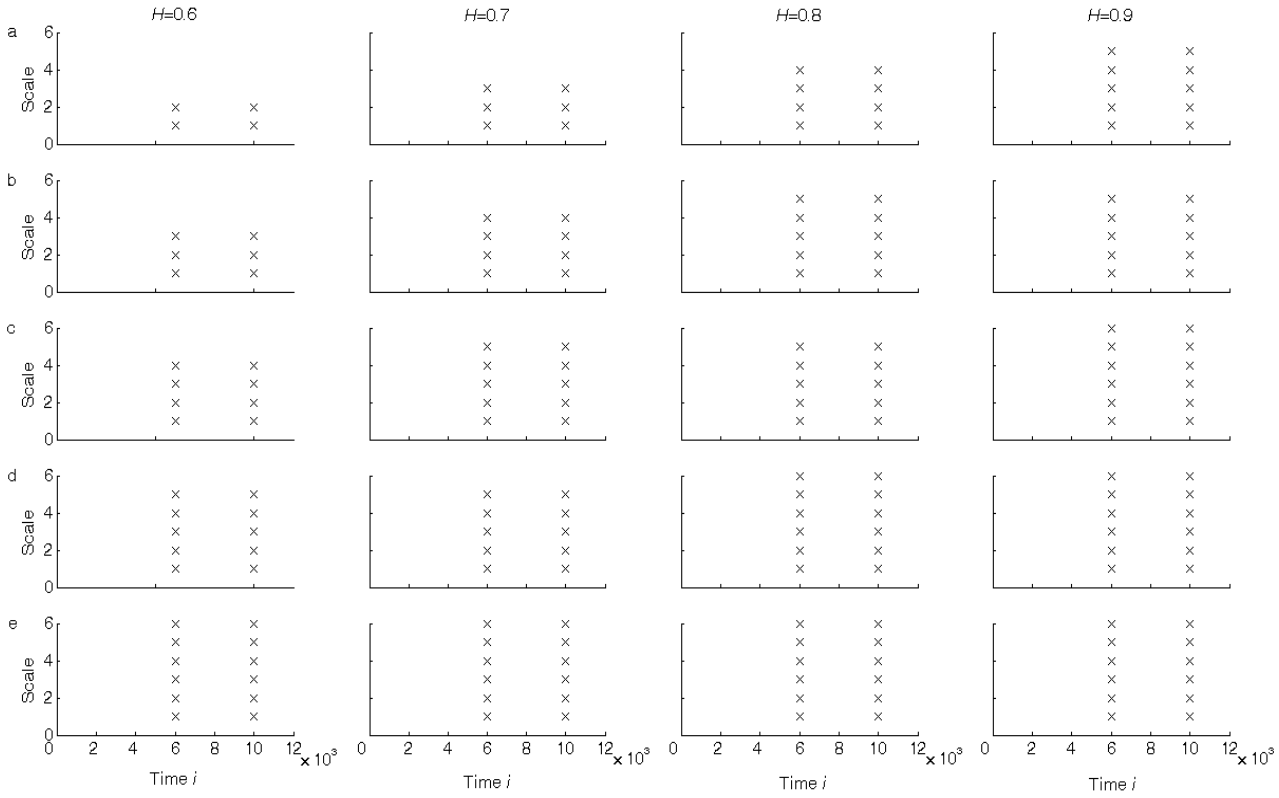


Figure 8: Change point candidates at each scale. The test traffic trace: (a) attack intensity-100KBps; (b) attack intensity-200KBps; (c) attack intensity-300KBps; (d) attack intensity-400KBps; (e) attack intensity-500KBps.

We segment the simulated abnormal traffic around the identified change points 6000 and 10000, and estimate the Hurst parameters of first and second traffic pieces. The changing rate of Hurst parameter can be computed by calculating the difference of these two Hurst parameters. Table 2 displays the changing rate of Hurst parameter under different degree of network traffic self-similarity and DDoS flood attack intensity.

Table 2. Input parameters in fuzzy decision of DDoS flood attack.

| Attack intensity | *H* | | | |
|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 |
| 100KB | 0.011 | 0.018 | 0.026 | 0.035 |
| 200KB | 0.030 | 0.043 | 0.061 | 0.088 |
| 300KB | 0.053 | 0.074 | 0.105 | 0.152 |
| 400KB | 0.082 | 0.119 | 0.170 | 0.248 |
| 500KB | 0.120 | 0.187 | 0.272 | 0.397 |

We select the input parameters *H* and *HC* in Table 2, and put them into the fuzzy logic decision process shown in Figure 6. We first fuzzify *H* and *HC* as fuzzy sets based on the membership degree function defined in Eq. (8). The mean and variance of the membership degree function is 0 and 1. According to the decision rules in Table 1, we can get the decision results of DDoS flood attack intensity shown in Table 3.

Table 3. Fuzzy decision results of DDoS flood attack.

| *HC* | *H* | | | |
|---|---|---|---|---|
| | 0.6 | 0.7 | 0.8 | 0.9 |
| 0.011 | *LA* | *LA* | *LA* | *LA* |
| 0.018 | *LA* | *LA* | *LA* | *LA* |
| 0.026 | *LA* | *LA* | *LA* | *LA* |
| 0.030 | *LA* | *LA* | *LA* | *LA* |
| 0.035 | *MA* | *LA* | *LA* | *LA* |
| 0.043 | *MA* | *LA* | *LA* | *LA* |
| 0.053 | *MA* | *MA* | *LA* | *LA* |
| 0.061 | *MA* | *MA* | *LA* | *LA* |
| 0.074 | *MA* | *MA* | *MA* | *LA* |
| 0.082 | *MA* | *MA* | *MA* | *LA* |
| 0.088 | *SA* | *MA* | *MA* | *LA* |
| 0.105 | *SA* | *MA* | *MA* | *MA* |
| 0.119 | *SA* | *MA* | *MA* | *MA* |
| 0.120 | *SA* | *MA* | *MA* | *MA* |
| 0.152 | *SA* | *SA* | *MA* | *MA* |
| 0.170 | *SA* | *SA* | *MA* | *MA* |
| 0.187 | *SA* | *SA* | *MA* | *MA* |
| 0.248 | *SA* | *SA* | *SA* | *MA* |
| 0.272 | *SA* | *SA* | *SA* | *MA* |
| 0.397 | *SA* | *SA* | *SA* | *SA* |

### 7.3 Comparison with existing detection method

In order to compare our proposed detection method with the existing self-similarity based detection methods, we carry out the following experiments. Firstly, we divide each network traffic with different degree of self-similarity into non-overlapping sections of length $l$=8$h$, where $h$=64. Secondly, we estimate the Hurst parameter of each section using Abry-Veitch wavelet-based estimator[31], and the Matlab source code for this estimator is available at [32]. The Hurst parameter of each section under different attacks intensity is displayed in Figure 9.

In Figure 9, we can see that the Hurst parameters of section 12 (corresponds to points 5633-6144) and section 20 (corresponds to points 9729-10240) are larger than the Hurst parameter before the attack happens. This is because at the beginning and ending moments of attack, the network traffic becomes more bursty and non-stationary, which leads to increase of the Hurst parameter. But during the attack, the normal traffic is overwhelmed by the attack traffic, and the Hurst parameter decreases (from section 13 to section 19, corresponding to points 6155-9728). Using the detection threshold proposed by Allen[21], we find that those attacks with severe intensity can be detected properly, but attacks with light or moderate intensity will be missed. Using the detection threshold proposed by Ren[23], we find that those attacks with severe or moderate intensity can be detected properly, but attacks with light intensity are missed. To make things even worse, in Ren's method, normal traffic with light degree of self-similarity and high degree of self-similarity are taken as attack behaviors. Our detection method takes the self-similarity degree of normal traffic into account, and study the influence of different attack intensities to the network traffic self-similarity. So our detection method can detect light, moderate and severe intensity of attacks accurately and intelligently.

In addition, in methods proposed by Allen and Ren, it is important to choose a proper length of the section($l$), because short section can not guarantee the amount of data required for estimating the Hurst parameter, and long section will result in prolonged detection latency. But our detection method does not suffer from this problem, because if there is a change point of self-similarity in network traffic, we only need to sample a few more data after the change point, then we can detect this change point timely by detecting the changes of wavelet coefficients variance structure at several scales. For example, if the wavelet decomposition level is 5, then we only need to sample another 64($2^6$) sample data to find out this change point.

## 8 Conclusion

In this paper, we proposed a method to detect the occurrence and intensity of DDoS flood attack based on the change of self-similarity in network traffic. To identify the DDoS flood attack, we adopt a kind of Schwarz information criterion that can not only find out the presence of attack in network traffic, but also its occurring moment. After the attack identification, we further propose a method to determine the intensity of attack based on intelligent fuzzy logic technology. To verify the effectiveness of our method, we conducted experiments using traffic trace constructed by NS2 simulator. The results demonstrate that the proposed method can detect the DDoS flood attack timely, effectively and intelligently. The future work will focus

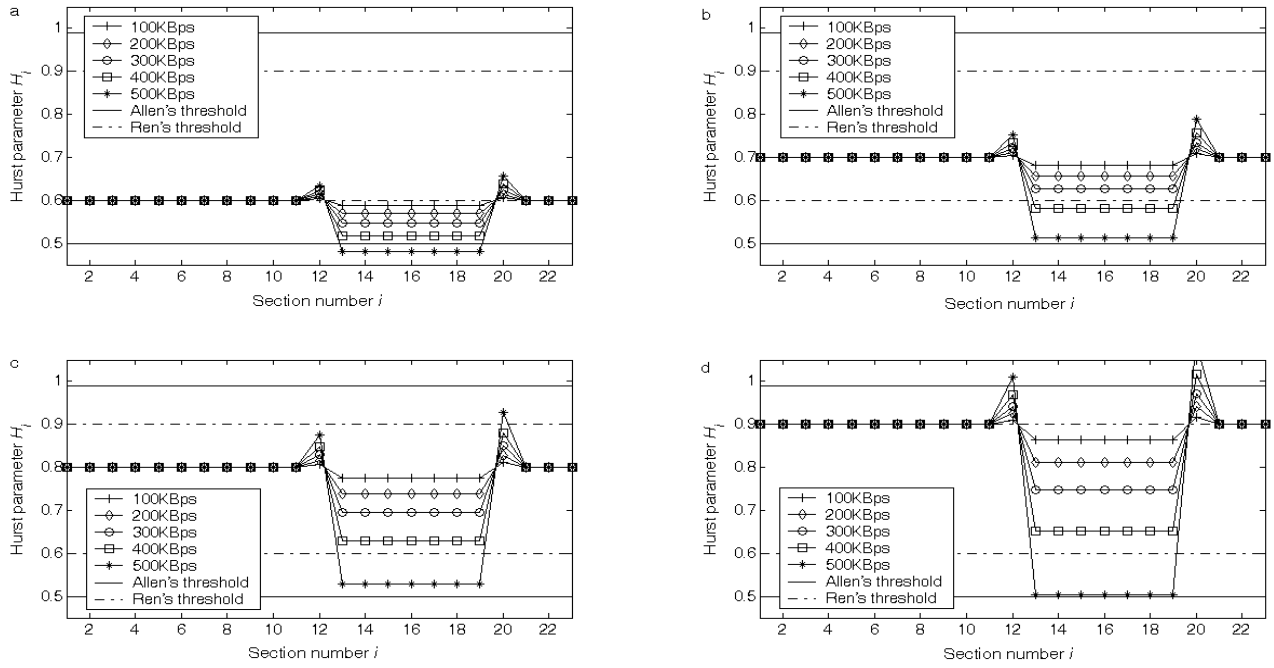


Figure 9: Change trend of Hurst parameter under different DDoS flood attack intensity. The degree of normal traffic self-similarity is: (a) 0.6; (b) 0.7; (c) 0.8; (d) 0.9.

on constructing fuzzy rule base by some learning techniques and testing this method on traffic trace from live networks.

## Acknowledgement

This work was supported in part by the National High Technology Research and Development Program of China under Grant No.2007AA01Z473; the National Natural Science Foundation of China under Grant No.60605019 and No. 60702047. The authors would also like to thank Patrice and Darryl for providing the Matlab source code and other members of Lab of Information Security Integrated Management Research for their valuable suggestions that have considerably increased the quality of this paper.

# References

[1] http://www.cert.org

[2] M. Li. An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition. *Computers & Security*, 23(7): 549-558, 2004.

[3] W.E. Leland, M.S. Taqqu and W. Willinger. On the self-similar nature of ethernet traffic (extended version). *IEEE/ACM Transactions on Networking*, 2(1): 1-15, 1994.

[4] V. Paxson and S. Floyd. Wide area traffic: the failure of Poisson modeling. *IEEE/ACM Transactions on Networking*, 3(3): 226-244, 1995.

[5] O. Tickoo and B. Sikdar. On the impact of IEEE 802.11 MAC on traffic characteristics. *IEEE Journal on Selected Areas in Communications*, 21(2): 189-203, 2003.

[6] C.S. Sastry, S. Rawat and A.K. Pujari. Network traffic analysis using singular value decomposition and multiscale transforms. *Information Sciences*, 177(23): 5275-5291, 2007.

[7] M.F. Rohani, M.A. Maarof and A. Selamat. Continuous LoSS detection using iterative window based on SOSS model and MLS approach. *In Proceedings of the International Conference on Computer and Communication Engineering*, Kuala Lumpur, Malaysia, May 2008.

[8] D. Rincón and S. Sallent. On-line segmentation of non-stationary fractal network traffic with wavelet transforms and Log-likelihood-based statistics. *LNCS*, 3375: 110-123, 2005.

[9] N. K. Swain. A survey of application of fuzzy logic in intelligent transportation systems (ITS) and rural ITS. *In Proceedings of the IEEE Southeast Conference,* March 2006.

[10] S.X. Wu and W. Banzhaf. The use of computational intelligence in intrusion detection systems: A review. *Applied Soft Computing*, 10: 1-35, 2010.

[11] L.A. Zadeh. Fuzzy sets. *Information and Control*, 8(3): 338-353, 1965.

[12] A. Abraham. Neuro-fuzzy systems: State-of-the-art modeling techniques, connectionist models of neurons, learning processes, and artificial intelligence. *LNCS*, 2084: 269-276, 2001.

[13] A. Meier and N. Werro. A fuzzy classification model for online customers. *Informatica,* 31(2): 175-182, 2007.

[14] J. Abonyi and B. Feil. Computational intelligence in data mining. *Informatica*, 29(1): 3-12, 2005.

[15] S. Avdoshin and V. Serdiouk. Some approaches to information security of communication networks. *Informatica*, 26(1): 1-10, 2002.

[16] C. Douligeris and A. Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5): 643-666, 2004.

[17] A. Patcha and J. M. Park. An overview of anomaly detection techniques: existing solutions and latest technological trends. *Computer Networks*, 51(12): 3448-3470, 2007.

[18] P. García-Teodoro, J. Díaz-Verdejo and G. Maciá-Fernández. Anomaly-based network intrusion detection: techniques, systems and challenges. *Computers & Security*, 28(1-2): 18-28, 2009.

[19] W.B. Gong, Y. Liu and V. Misra. Self-similarity and long range dependence on the internet: a second look at the evidence, origins and implications. *Computer Networks*, 48(3): 377-399, 2005.

[20] M. Li. Change trend of averaged Hurst parameter traffic under DDOS flood attacks. *Computers & Security*, 25(3): 213-220, 2006.

[21] W.H. Allen and G.A. Marin. The LoSS technique for detecting new denial of service attacks. *In Proceedings of IEEE South East Conference*, Greensboro, NC, March 2004.

[22] W. Schleifer and M. Männle. Online error detection through observation of traffic self-similarity. *In Proceedings of the IEE Communications Conference*, 148(1): 38-42, 2001.

[23] X.Y. 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*, 2(1): 73-77, 2007.

[24] J.T. Wang and G. Yang. An intelligent method for real-time detection of DDoS attack based on fuzzy logic. *Journal of Electronics (China)*, 25(4): 511-518, 2008.

[25] S. Stoev, M. Taqqu and C. Park. On the wavelet spectrum diagnostic for Hurst parameter estimation in the analysis of Internet traffic. *Computer Networks*, 48(3): 423-445, 2005.

[26] S. Song and K. Joseph. Some results on the self-similarity property in communication networks. *IEEE Transactions on Communications*, 52(10): 1636-1641, 2004.

[27] J. Beran. Statistics for long-memory processes. *Chapman & Hall*, New York, 1994.

[28] J. Chen and A. Gupta. Testing and Locating Variance Change points with Application to Stock Prices. *Journal of the* American *Statistical Association*, 92: 739-747, 1997.

[29] X. Tian, J. Wu and C. Ji. A unified framework for understanding network traffic using independent wavelet models. *In Proceedings of IEEE INFOCOM'*, June 2002.
[30] B. B. Mandelbrot and J. W. Van Ness. Fractional Brownian motions, fractional noises and applications. *SIAM Review*, 10(4): 422-437, 1968.
[31] A. Patrice and V. Darryl. Wavelet analysis of Long-Range-Dependence traffic. *IEEE Transactions on Information Theory*, 44(1): 2-15, 1998.
[32] http://www.cubinlab.ee.unimelb.edu.au/%7Edarryl