Low-Rate DoS Attacks Detection Based on Network Multifractal

Zhijun Wu, Liyuan Zhang, and Meng Yue

Abstract—Low-rate denial of service (LDoS) attacks send periodic pulse sequences with relative low rate to form aggregation flows at the victim end. LDoS attack flows have the characteristics of low average rate and great concealment. It is hard to detect LDoS attack flows from normal traffic due to low rate property. Network traffic measurement shows that aggregate network traffic is multifractal. In order to characterize and analyze network traffic, researchers have developed concise mathematical models to explore complex multifractal structure. Although the LDoS attack flows are very small, it will inevitably lead to the change of multifractal characteristics of network traffic. This paper targets at exploiting and estimating the changes in multifractal characteristics of network traffic for detecting LDoS attack flows. The algorithm of multifractal detrended fluctuation analysis (MF-DFA) is used to explore the change in terms of multifractal characteristics over a small scale of network traffic due to LDoS attacks. Through wavelet analysis, the singularity and bursty of network traffic under LDoS attacks are estimated by using Hölder exponent. The difference values (D-value) of Hölder exponent of network traffic between normal and under LDoS attack situations are calculated. The D-value is used as the basis to determine LDoS attacks. A detection threshold is set based on the statistical results. The presence of LDoS attacks can be confirmed through comparing D-value with detection threshold. Experiments on detection performance have been performed in the test-bed network and simulation platform. The extensive experimental results are congruent with the theoretical analysis.

Index Terms—Low-rate denial of service (LDoS), Multifractal detrended fluctuation analysis (MF-DFA), Hölder exponent, singularity and bursty, D-value

1 Introduction

IT has been 15 years since the first distributed Denial of service (DDoS) attacks were detected. So far, DDoS attacks have not been addressed properly [1]. This situation is even worse when the cloud computing is widely applied. Low-rate Denial of Service (LDoS) attack is a new type of DoS attack [2]. LDoS attacks exhibit a periodic pulse sequence, which can be expressed in a triple of attack period T, attack duration L, and attack rate R, i.e.. $LDoS(T, L, R)$. Here, T is the interval between two successive attack pulses, and T can be obtained by estimating the execution duration of trusted source. The duration of the timer refers to RTO (retransmission timeout). L is the width of attack pulse. R is the intensity of attack pulse. R indicates the highest rate of attack flows [3], [4]. The successful LDoS attacks usually have the following characteristics: (i) T is the minimum RTO value or the integer times of RTO value. (ii) R is large enough to cause packet loss in legitimate TCP flows. (iii) L is long enough to cause retransmission. The attack period T can be adjusted by estimating the RTO value. But the attack duration L and attack rate R cannot exceed a certain value for the purpose of avoiding being found according to the detect mechanism. Hence, the average rate of LDoS attacks is $R \times L/T$. LDoS attacks attempt to deny bandwidth to TCP flows while sending at sufficiently low average rate to elude detection by counter-DoS mechanisms. The LDoS attacks may keep damaging the victim for a long time without being detected [2].

Research result [5] shows that the network traffic exhibits self-similarity over a large time scale while presenting multifractal characteristics over a small time scale. The parameter α in multifractal characteristics is defined as Lipschitz-Hölder exponent (hereafter referred to as Hölder exponent), it is also known as the singularity exponent [6], which presents the local singularity of a function. LDoS attacks send attack packets periodically in a short time interval. The network multifractal must be disrupted when LDoS attacks are launched suddenly. Hence, the Hölder exponent is abnormal. According to the above analysis, the approach of LDoS attacks detection based on network multifractal is proposed in this paper. Based on the essential attributes and features of network traffic, this approach calculates the value of Hölder exponent at all points, and the abnormal difference between the values of Hölder exponent is the basis of the LDoS attack detection.

2 Related Works

LDoS attacks have the feature of concealing, which makes LDoS attacks elude traditional DoS detection easily. DDoS-oriented detection methods are no longer suitable for the detection of LDoS attacks. At present, LDoS detection methods can be divided into two categories, in time domain and in frequency domain.

Yu et al. [7] proposed a collaborative approach of defense against periodic shrew DDoS attacks in the frequency domain. This approach detected shrew DDoS attacks using the frequency-domain characteristics from the autocorrelation sequence of Internet traffic streams. They used the normalized cumulative amplitude spectrums (NCAS) to

• *The authors are with the School of Electronics & Information Engineering, Civil Aviation University of China, Tianjin, China. E-mail: {zjwu, myue}@cauc.edu.cn, zhangliyuan8908@126.com.*

Manuscript received 3 June 2014; revised 19 May 2015; accepted 28 May 2015. Date of publication 10 June 2015; date of current version 2 Sept. 2016. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TDSC.2015.2443807

calculate the distance between distribution curves of TCP and shrew traffic for the purpose of determining the existence of attacks. This approach achieved collaborative detection across multiple routers and required only a few seconds for successful detection of shrew DDoS attacks. Barford et al. [8], and HE et al. [9] introduced the wavelet processing idea in detecting LDoS attacks by using the discrete wavelet transform (DWT) technology. This method transforms network traffic into high, middle, and low frequency components for the purpose of finding the attack traffic. Results showed that wavelet filters are quite effective in exposing the details of both ambient and anomalous traffic. Wu et al. [10] presented an LDoS attack detection method using the technique of one step prediction Kalman filtering. This method explored the characteristics of network traffic observed at the victim end when the attack started. The error between one step prediction and the optimal estimation is used as the basis for detection.

Macia-Fernandez et al. [4] and Jingtang et al. [11] have proposed a mathematical model for the LDoS attacks. This model is helpful in evaluating the performance of LDoS attacks in dynamics network. They have validated the model by comparing the given performance values with those obtained in a simulated environment. Yang et al. [12] proposed information metric to quantify the differences of network traffic with various probability distributions. Two information metrics, generalized entropy metric and the information distance metric, are used to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. This method tracks IP address of attackers by using information distance, which can track the attack sources in time. Wu et al. [13] treated the LDoS attack flows as a periodic small signal and presented an LDoS attack detection method based on a small signal model in 2012. In this method, averaging multiple samplings based on missing sampling (MSABMS) is used to record the packets arriving in 30 seconds (sampling time is 10ms, with a total of 3,000 sampling points), and the statistical result is compared with the characteristic judging value, which is settled as a threshold to indicate the difference between normal flow and attack flow. An eigenvalue estimating matrix is established to estimate the attack period after LDoS attacks being detected.

The known research methods have some defects, such as, (i) the accuracy and the efficiency of entropy calculation will be greatly reduced with the expansion of network scale and the increase of network bandwidth. (ii) lower detection rate, and higher false positive rate and higher false negative rate. (iii) higher computational complexity.

At present, multifractal characteristics of network traffic are used in internet traffic measurement. Many network researchers studied the degree of long-range dependence (LRD) in network traffic, which has been referred to as self-similar, fractal, and multi-fractal behavior. Nogueira et al. [14] researched on modeling network traffic with multifractal behavior. They analyzed the complexity of multifractal structure of network traffic, and developed concise mathematical model for the characterization and analysis of network traffic. This model is used in studying the implications of LRD traffic on the quality of service (QoS) of network infrastructure. Vieira and Lee [15] presented effective bandwidth estimation and QoS aware bandwidth provisioning for multifractal network traffic. They developed an adaptive wavelet-based multifractal model (AWMM) by using properties of the wavelet coefficients of multifractal cascade processes, and derived an analytical expression for the bandwidth estimation of AWMM traffic.

This paper applies the theory of network traffic measurement [16] into detecting LDoS attacks. This study is based on the fact that LDoS attacks can lead to abnormal flows which will change the multifractal characteristics of the network traffic. Hence, the difference in Hölder exponents between attack and non-attack situations is the basis of detecting LDoS attacks [17].

This paper is organized as follows. Section 1 introduces the research background which includes the analysis of LDoS attacks. Section 2 reviews the world-wide academic researches on LDoS attack detection by using signal processing technique and analyzes the existing problems. Section 3 presents the proposed approach of LDoS attack detection based on multifractal. MF-DFA algorithm is used to analyze the multifractal of network traffic in this section. This approach applies the wavelet to estimate the Hölder exponent. Section 4 describes the experiments in both NS2 simulation platform and test-bed network environment. This section also highlights the verification of the network traffic multifractal, the detection of LDoS attacks, and the analysis of detection performance. Section 5 provides summary and discussion of detection performance as the conclusion of this paper.

3 Multifractal-Based LDoS Attacks Detection

At present, more and more complex network traffic is described by using a traffic model in network traffic measurement. The discovery of self-similar feature of traffic gives an impulse to perform further intensive research. But researchers found that the self-similar model with its single scaling parameter is not enough as a multiple scaling on fine timescales. Therefore, multifractal model comes into being to illustrate the complex features of network traffic in detail. Available research result [18] reveals that the network traffic presents self-similarity on a large time scale and multifractal characteristic on a small time scale.

Network traffic measurement research [19] shows that most of the network traffic uses the TCP protocol. The primary reason is that the growing number of Internet users, the widespread availability of easy-to-use web browsers, and the proliferation of web sites with rich multimedia content combine to contribute to the exponential growth of Internet TCP traffic [15], while LDoS attack usually uses the UDP protocol.

It is found that most of network services possess the multifractal characteristic, such as TCP, IP and HTTP, whereas UDP services have monofractal characteristic [16]. When LDoS attacks have been launched, a large number of UDP attack packets will appear in the network. This status will change the Hölder exponent which is used to measure local singularity of network traffic. A new approach of detecting LDoS attacks is proposed by monitoring the abrupt change of Hölder exponent through wavelet analysis.

3.1 Wavelet Analysis of Multifractal Characteristics

Given a function $\psi(t) \in L^2(R)$, $\Psi(\omega)$ is the Fourier transform of $\psi(t)$. If the function $\psi(t)$ satisfies the admissible condition [20],

$$C_\psi = \int_R \frac{|\Psi(\omega)|^2}{\omega} d\omega < +\infty. \quad (1)$$

Then, $\psi(t)$ is called a mother wavelet. $\{\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-b}{a}), a > 0, b \in R\}$ is the translation b and dilatation a of $\psi(t)$. A signal $f(t)$ can be decomposed by binary wavelet [20],

$$f = \sum_{j,k} d_{j,k}\psi_{j,k}, \quad (2)$$

where, $d_{j,k} = \langle f, \psi_{j,k} \rangle$ denotes the wavelet coefficients of the signal at the point k and on the scale j, and $\psi_{j,k}(t) = 2^{-j/2}\psi(2^{-j}t - k), j, k \in Z$.

The fractal characteristic of network traffic is verified by multifractal detrended fluctuation analysis (MF-DFA) algorithm [17] in this paper. The DFA algorithm is widely used in verifying the scale characteristic of monofractal and in detecting the long-range correlation of noisy nonstationary sequences.

By using the MF-DFA algorithm [17], researchers can achieve the multifractal spectrum easily and analyze the multifractal characteristic of nonstationary sequences effectively.

The procedures of calculating a time sequence $\{x(k), k = 1, 2, \ldots N\}$ by using MF-DFA algorithm are as follows [17].

Step 1: Computing the "profile",

$$Y(i) = \sum_{k=1}^{i} (x(k) - \bar{x}), i = 1, 2, \ldots N, \quad (3)$$

where, $\bar{x} = \frac{1}{N}\sum_{j=1}^{N} x(j)$.

Step 2: Dividing $Y(i)$ into non-overlapping segments N_s of equal size s, with N_s being the integral of N/s, and repeating the divide procedure starting from the opposite end. Thus, $2N_s$ segments will be obtained.

Step 3: Fitting local trend polynomial $y_v(i)$ by using least-square method for each segment $v, v = 1, 2, \cdots 2N_s$,

$$y_v(i) = a_0 + a_1 i + \cdots + a_{n-1} i^{n-1} + a_n i^n i = 1, 2, \ldots s; n = 1, 2, \ldots \quad (4)$$

Determining the variance as,

$$F^2(v, s) = \frac{1}{s}\sum_{i=1}^{s} \{Y[(v-1)s + i] - y_v(i)\}^2 v = 1, 2, \ldots N_s \quad (5)$$

and

$$F^2(v, s) = \frac{1}{s}\sum_{i=1}^{s} \{Y[N - (v - N_s)s + i] - y_v(i)\}^2 \quad v = N_s + 1, \ldots 2N_s \quad (6)$$

Step 4: Calculating the q^{th} order fluctuation function by averaging over all segments,

$$F_q(s) = \left\{ \frac{1}{2N_s} \sum_{v=1}^{2N_s} \left[F^2(v, s)\right]^{q/2} \right\}^{1/q} q \neq 0 \quad (7)$$

$$F_q(s) = \exp\left\{ \frac{1}{4N_s} \sum_{v=1}^{2N_s} \ln\left[F^2(v, s)\right] \right\} q = 0, \quad (8)$$

where, the index q can be any real value.

Step 5: Analyzing log-log plots $F_q(s)$ versus s for each q. If the sequence $\{x(k), k = 1, 2, \cdots N\}$ is long-range power-law correlated, $F_q(s)$ increases, for large values of s, as a power-law,

$$\ln F_q(s) = h(q) \ln s + \ln A. \quad (9)$$

Step 6: If $\{x(k), k = 1, 2, \cdots N\}$ is a stationary and normalized sequence, the scaling exponent $\tau(q)$ is $qh(q) - 1$. Using the Legendre transformation, the multifractal spectrum $f(\alpha)$ and singularity exponent α can be expressed as,

$$f(\alpha) = q\alpha - \tau(q) \text{ and } \frac{d\tau(q)}{dq} = \alpha. \quad (10)$$

The results obtained by MF-DFA algorithm to verify the multifractal characteristic of network traffic will be presented in detail in Section 4.1.2 and 4.2.2.

3.2 Hölder Exponent Estimation

Hölder exponent, a fractal parameter of the network traffic, is used to characterize the bursty of network traffic at a certain point. The smaller the Hölder exponent α is, the "burstier" the network traffic at the point is [14]. Hence, when LDoS attacks have been launched, the multifractal characteristics of network traffic are changed, which indicates the bursty of network traffic. Through the estimation of Hölder exponent α, the bursty of network traffic is measured. Therefore, the LDoS attacks can be detected by Hölder exponent.

Vieira et al. [15] have proved that local signals' singularity can be characterized by the wavelet transformation, and put forward Lipschitz exponent of signals' singularity, which can be estimated by tracking the cross-scale change of wavelet transform modulus maxima (WTMM) in the cone of influence (COI). But the algorithm has some drawbacks. It can only be applied to isolated non-oscillating singularities, and the robustness and the accuracy of the algorithm are greatly reduced when WTMM curve fluctuates.

Based on the analysis above, a robust approach of estimating the pointwise Hölder exponent is presented in this paper, whether the point is an oscillating singularity or not.

Considering a positive process $X(t)$, the burst strength of X at time t can be characterized by [14]

$$\alpha(t) = \lim_{k_n 2^{-n} \to t} \alpha_{k_n}^n, \quad (11)$$

where, $\alpha_{k_n}^n = -\frac{1}{n}\log_2|X((k_n + 1)2^{-n}) - X(k_n 2^{-n})|$ and $k_n = 0, \ldots, 2^n - 1$.

$\alpha(t)$ is called the local Hölder exponent [14], which indicates the change in multifractal characteristics of network traffic due to LDoS attacks. Hence, the estimation of $\alpha(t)$ is the key step of LDoS attack detection.

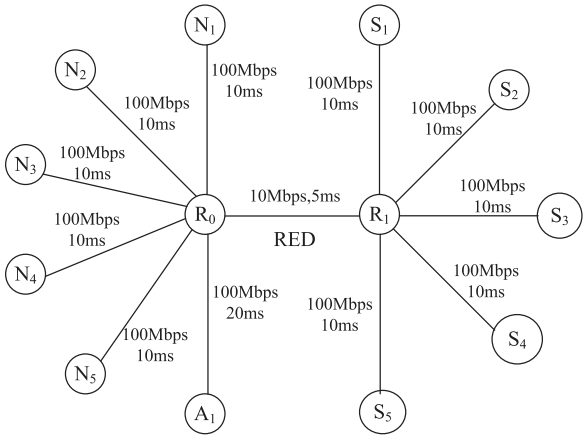


Fig. 1. The simulation topology in NS-2.

The network packets are modeled as a discrete time signal with samples of $n = 2^m$. The Hölder exponent at the point k_0 is estimated by using the algorithm as follows [21].

Step 1: Plotting the parametric curve on the same graph, for each j ($0 < j \leq m$),

$$x_j(k) = \log_2(2^{-j} + |k - k_0|/2^m) = x(j,k) \tag{12}$$

$$y_j(k) = \log_2(|d_{j,k}|). \tag{13}$$

Step 2: Finding each straight line $D : y = \alpha x + C$ such that, D is an upper-bound for all the plotted points $(x_j(k), y_j(k))$, i.e.,

$$\forall j, \forall k \, y_j(k) \leq \alpha x_j(k) + C. \tag{14}$$

There exists a sequence of pairs (j_i, k_i) such that,

$$\lim_{i \to \infty} y_{j_i}(k_i) - (\alpha x_{j_i}(k_i) + C) = 0. \tag{15}$$

Step 3: Finding the maximum of the slops $\alpha_{\max}$ over all lines D satisfying both formulas (14) and (15). The slope $\alpha_{\max}$ is the Hölder exponent of the signal at the point k_0.

4 Experiments and Results Analysis

For evaluating the performance of the proposed detection algorithm, experiments are conducted in both NS2 simulation platform and test-bed network environment.

LDoS attack generation tool exploits the Linux TCP-kernel source code of Shrew attack [22]. By using UDP-based software, the LDoS attack flows are generated in the following experiments [22].

During the experiments, network packets are sampled. Then, the multifractal characteristic of network traffic is verified by MF-DFA algorithm, and experimental results are analyzed in detail.

4.1 Experiments in NS2 Simulation Platform

A simulation network is designed in NS2 simulation platform for carrying out related experiments.

4.1.1 NS2 Experiment Environment

The topology of experiment network in NS-2 simulation platform is shown in Fig. 1.

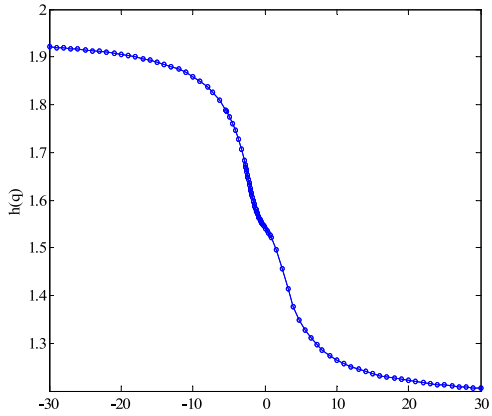


Fig. 2. The relationship between Hurst exponent $h(q)$ and order q.

The simulated network has an asymmetrical dumb-bell topology. It consists of Router R_1 (Node R_1), Router R_2 (Node R_2), five pairs of legitimate TCP senders (Node N_1 to N_5) and TCP receivers (Node S_1 to S_5), and a UDP LDoS attacker (Node A_1). The links connecting router R_1, senders, and attacker are at rate of 100 Mbps, the same as the links between router R_2 and the receivers. Both routers are connected through a bottleneck link of 10 Mbps with the random early detection (RED) queue management. The minRTO is set to be 1000 ms. The configuration of link delay is shown in Fig. 1.

The simulation period is 1,000 seconds, and the attack begins at 400$^{\text{th}}$ second and ends at 600$^{\text{th}}$ second. A triple $LDoS(T, L, R) = (1100 \text{ ms}, 200 \text{ ms}, 10 \text{ Mbps})$ is used to describe the LDoS attacks.

4.1.2 Verification of Network Traffic Multifractal

Set the X_1 represent the flow sequence without LDoS attacks, and X_2 express the flow sequence with LDoS attacks. Two sequences X_1 and X_2 are obtained by sampling the packets arriving at router R_2.

The relationship curves between Hurst exponent $h(q)$ and order q, scaling exponent $\tau(q)$ and order q, and multifractal spectrum $f(\alpha)$ and singularity exponent α are obtained individually by using the MF-DFA algorithm introduced in Section 3.2 for analyzing the sequence X_1. The results are shown in Figs. 2, 3, and 4.

Based on analysis of experimental results in NS2 simulation, Fig. 2 shows that there is a strong nonlinear dependence of $h(q)$ upon q, indicating the multifractal characteristic of

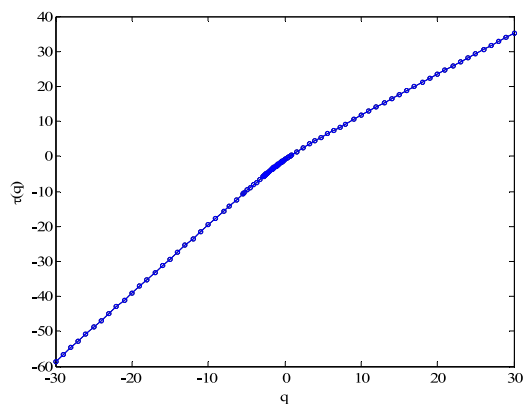


Fig. 3. The relationship between scaling exponent $\tau(q)$ and order q.

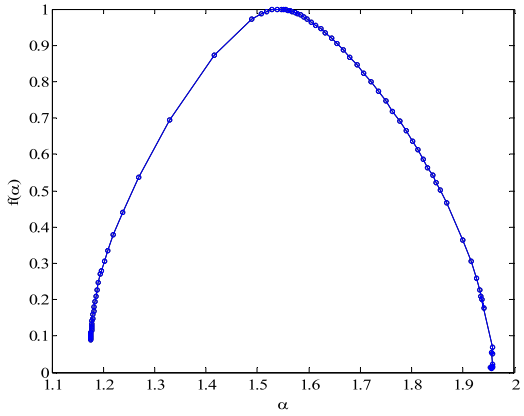


Fig. 4. The relationship between multifractal spectrum $f(\alpha)$ and singularity exponent α.

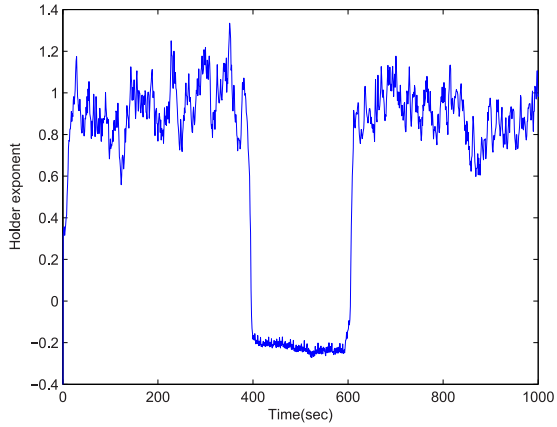


Fig. 6. Hölder exponent.

network traffic. The same is true of the dependence of $\tau(q)$ on q in Fig. 3. In Fig. 4, the relationship between multifractal spectrum $f(\alpha)$ and α exhibits the shape of one peak, which also proves the multifractal characteristic of network traffic. The wider the bell shape is, the stronger the intensity of multifractal is.

4.1.3 Detection of LDoS Attacks

Fig. 5 shows the network packet sequence X_2. The packet number increases sharply at the start of LDoS attacks.

For the sequence, pointwise Hölder exponents are estimated by the algorithm introduced in Section 3.2. Results are shown in Fig. 6.

The Hölder exponent changes abnormally by time with LDoS attacks. When the LDoS attacks start, the Hölder exponent falls quickly. When the LDoS attacks end, the Hölder exponent rises rapidly to the normal level. The abnormal change of singularity value of network traffic provides a new way to detect LDoS attacks.

The procedure of LDoS attack detection is put forward, where the pointwise Hölder exponents of the sampled network packet sequence are estimated, and then the difference value of Hölder exponent $|\Delta H\ddot{o}lder|$ is calculated as normalized.

In Fig. 7, there are two peaks in normalized $|\Delta H\ddot{o}lder|$ that occurred when LDoS attacks begin and end. Threshold σ is set based on the statistical analysis. If normalized $|\Delta H\ddot{o}lder|$ is larger than the detection threshold σ, LDoS attacks are considered to exist. Otherwise, there is no LDoS attack in the network.

To further determine the beginning or the ending of LDoS attacks, t hypothesis test [10] is used as follows,

$$\begin{cases} H_0 : \mu \geq \mu_0 & the\ end\ of\ LDoS\ attack \\ H_1 : \mu < \mu_0 & the\ beginning\ of\ LDoS\ attack \end{cases}, \tag{16}$$

where, value μ_0 indicates the mathematical expectation of Hölder exponent without LDoS attacks.

The result of the inspection is either the beginning or the ending of LDoS attacks. The test statistic is:

$$t = \frac{\bar{X} - \mu_0}{s/\sqrt{n}}, \tag{17}$$

where, $\bar{X}$ indicates the average value of Hölder exponent in the hypothesis test. The critical region is $t_\alpha(n-1)$.

According to the t value of statistical result, the probability P of hypothesis test is determined. If P is not larger than α, hypothesis H_1 is true, i.e., LDoS attacks have just started, otherwise, H_0 is true, i.e., LDoS attacks have ended. The hypothesis test period and sample period are set to be 20 and 0.5 s individually.

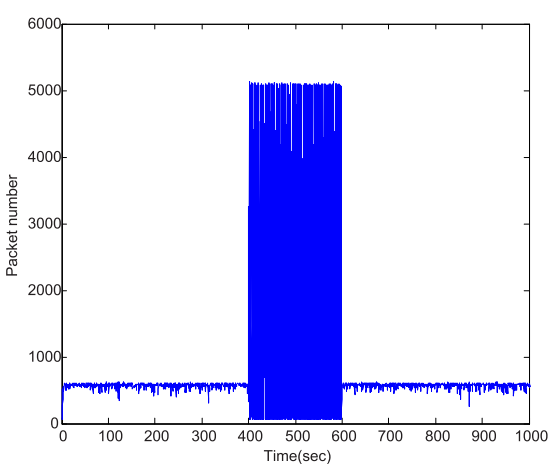


Fig. 5. Packet number in the NS2 link.

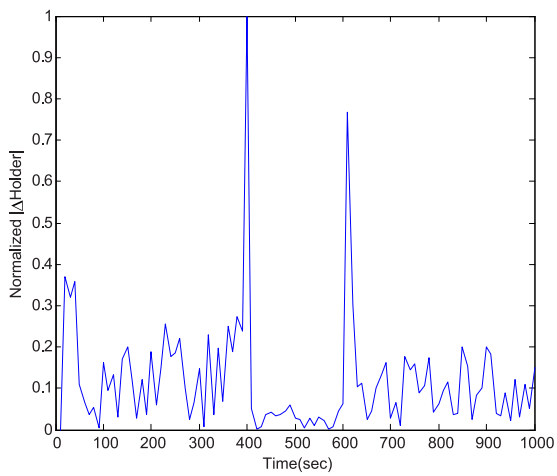


Fig. 7. Normalized $|\Delta H\ddot{o}lder|$.

TABLE 1
Performance of Different Detection Threshold

Threshold \ Performance	P_D	P_{FN}	P_{FP}
$\sigma = 0.4$	95%	5%	16%
$\sigma = 0.5$	93%	7%	12%
$\sigma = 0.6$	92%	8%	9%
$\sigma = 0.8$	86%	14%	11%

4.1.4 Analysis of Detection Performance

Indexes of the detection probability P_D, false positive rate P_{FP}, and false negative rate P_{FN} are critical indicators for evaluating attack detection performance. The value P_D is the correct detection probability, which is the proportion of all LDoS attacks correctly identified as attack traffic when the LDoS attacks exist. Here, detection means a test result that correctly indicates the presence of an LDoS attack. The value P_{FP} is error detection probability, which is the proportion of all normal or interference traffic that is incorrectly identified as LDoS attacks. Here, false positive means a test result that wrongly indicates the presence of an LDoS attack. In other words, false positive is mistaking the normal or interference traffic as attack flows when LDoS attack does not exist. The value P_{FN} is missing detection probability, which is the proportion of all LDoS attacks falsely identified as normal or interference traffic. Here, false negative means a test result showing no attacks when LDoS attacks actually exist. In other words, false negative is an incorrect result that falsely indicates the absence of an LDoS attack.

Therefore, it is necessary to find an optimal detection threshold σ that may achieve a high detection probability with acceptable false negative/positive rate. One hundred experiments have been conducted to test the performance of the detection approach proposed in the paper. The P_D, P_{FN} and P_{FP} with different detection thresholds are shown in Table 1.

For different thresholds, when the threshold σ is set to be 0.4 or 0.5, the detection algorithm can achieve higher detection probability, but the false probability P_{FP} is also higher. Otherwise, the detection probability is lower if the threshold σ is set to be 0.8 or larger. The P_D, P_{FN} and P_{FP} can reach the best compromise when the detection threshold σ is set to be 0.6. With LDoS attack detection based on multi-fractal, the detection probability reaches 92 percent, with the false positive rate of 9 percent and the false negative rate of 8 percent.

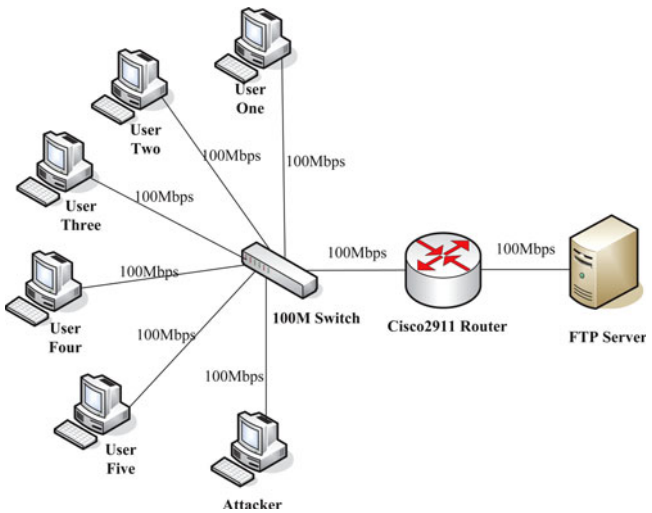


Fig. 8. The topology of test-bed network.

TABLE 2
Devices Configuration

Device	Configuration	IP address
User One	Windows 7	10.1.20.144
User Two	Windows 7	10.1.20.143
User Three	Windows 7	10.1.20.142
User Four	Windows 7	10.1.20.141
User Five	Windows 7	10.1.20.140
Attacker	Red Hat Linux 5.5	10.1.20.111
FTP Server	Windows Server 2003	10.1.10.11

4.2 Experiments in Test-Bed Network Environment

In order to better verify the detection performance of the proposed approach, experiments in test-bed network environment with five users are performed.

4.2.1 Test-Bed Experiment Environment

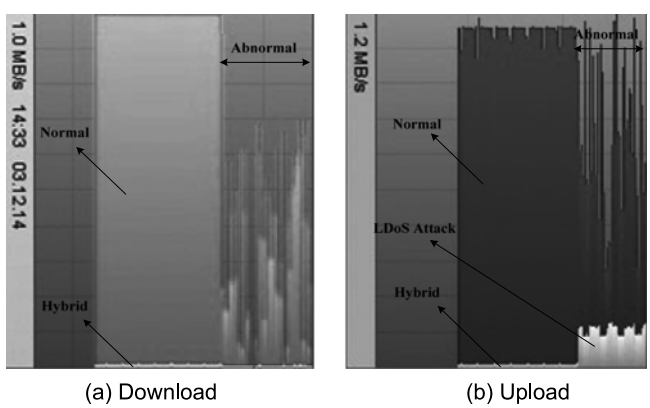
The test-bed network topology is shown in Fig. 8. It consists of a 100 M switch, a Cisco2911 router, five users, an attacker and a FTP server. The FTP server is configured as a victim.

Devices in the test-bed network are configured as shown in Table 2.

The FTP throughput is tested in the test-bed network (shown in Fig. 8) by using the UDP-based software. In the test scenario, the victim provides FTP service, and the user downloads a file from a FTP Server. Once the normal FTP traffic is steady, the LDoS attack, with T of 1,100 ms, L of 200 ms, R of 10 Mbps starts.

As shown in Fig. 9, the **Normal** in Fig. 9 a represents the client's normal download traffic recorded in the user before the attacks, and the **Normal** in Fig. 9b is the server's upload traffic recorded in FTP server. Both **Normal** traffic are approximately equal. The **Hybrid** represents the combination of uploads and downloads in the client or server, and the **Abnormal** is the download or upload traffic during attacks.

During LDoS attacks, download and upload traffic are lower than normal state and amplitude fluctuates strongly.



(a) Download (b) Upload

Fig. 9. Traffic with LDoS attacks.

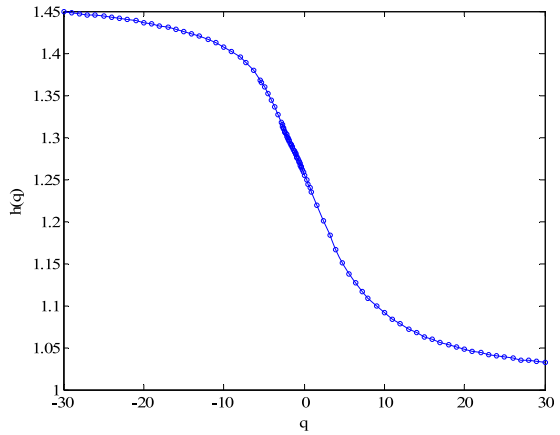


Fig. 10. The relationship between Hurst exponent $h(q)$ and order q.

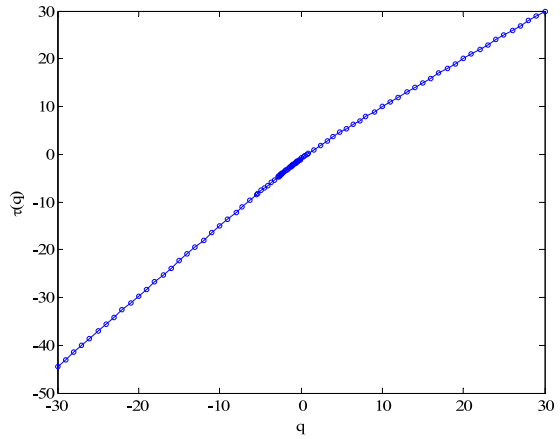


Fig. 11. The relationship between scaling exponent $\tau(q)$ and order q.

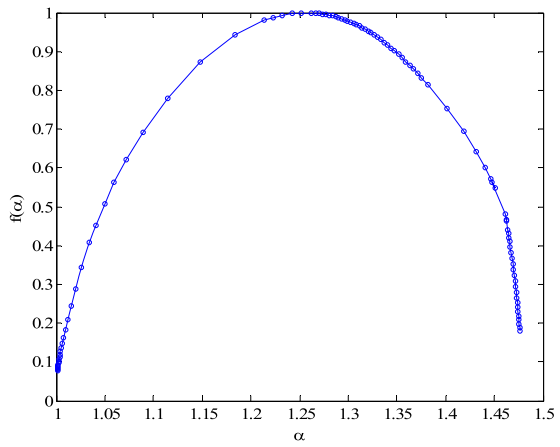


Fig. 12. The relationship between multifractal spectrum $f(\alpha)$ and singularity exponent α.

In Fig. 9b, the **LDoS Attack** denotes the attack traffic from the attackers. The rate of LDoS attacks is even lower than the attacked FTP traffic.

4.2.2 *Verification of Network Traffic Multifractal*

The packet number sequences Y_1 and Y_2 are respectively sampled at the FTP Server on two occasions, namely without and with LDoS attacks.

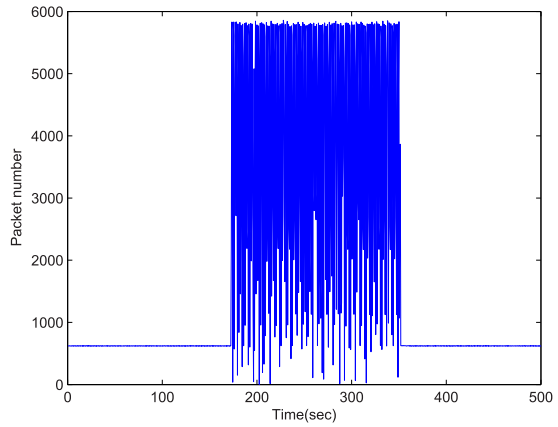


Fig. 13. Packet number in the test-bed link.

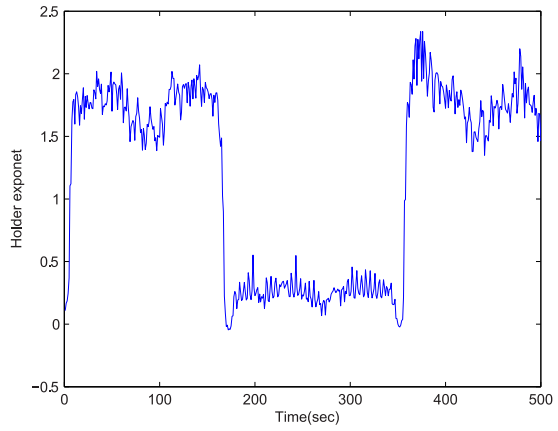


Fig. 14. Pointwise Hölder exponent.

The multifractal characteristics of the network traffic in the test-bed are also verified by using the MF-DFA algorithm [17]. The results are shown in Figs. 10, 11, and 12.

As can be seen from figures mentioned above, the nonlinear dependence of $h(q)$ upon q indicates multifractal characteristic of network traffic in the test-bed. The same information is included in the dependence of $\tau(q)$ on q. The relationship between multifractal spectrum $f(\alpha)$ and α indicates the shape with one peak, which also proves the multifractal characteristic of network traffic.

4.2.3 *Detection of LDoS Attacks*

Fig. 13 shows the packet number of real network sequence Y_2. As with the NS2 simulation results, the packet number increases sharply when the LDoS attack starts.

For sequence Y_2, pointwise Hölder exponents are estimated by the algorithm introduced in Section 3.2. Results are shown in Fig. 14.

As can be seen from Fig. 14, the range of the pointwise Hölder exponent value is different from that in the NS2 simulation, because different topologies are used in two experiment environments so that the multifractal intensity differs. Nonetheless, the change trend of the pointwise Hölder exponent is the same as that of NS2 simulation. Hölder exponent $\alpha(t) > 1$ indicates the real network traffic changes relatively smoothly. Reversely, Hölder exponent $\alpha(t) < 1$ shows that network traffic has a higher degree of bursty in

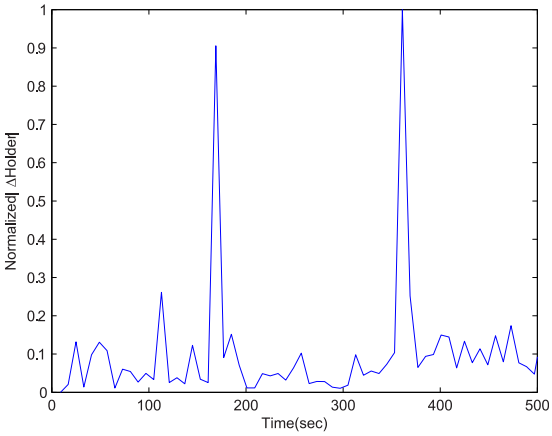


Fig. 15. Normalized $|\Delta H\ddot{o}lder|$.

the vicinity of t at all scales [23]. The normalized difference value of Hölder exponent $|\Delta H\ddot{o}lder|$ is shown in Fig. 15.

A threshold σ has to be set to detect LDoS attacks. If the normalized $|\Delta H\ddot{o}lder|$ is smaller than the detection threshold σ, there is no LDoS attack. Otherwise, LDoS attack is considered to exist.

4.2.4 Analysis of Detection Performance

Totally one hundred experiments are conducted in the test-bed to test the performance of the detection approach. The optimal detection threshold σ is set to be 0.6, then, the detection probability of 91 percent, the false positive rate of 10 percent and the false negative rate of 9 percent are obtained.

The detection performance in test-bed network environment is compared with that in NS2 simulation platform. The comparative analysis result is shown in Table 3.

Because NS2 simulation offers an ideal environment, which is different from the real test-bed influenced by complicate factors, the detection probability of the method used in the test-bed is lower than that of NS2 simulation.

The proposed approach in the paper is compared with other detection methods upon the detection performance and complexity. In order to make an objective and fair comparison analysis, two methods that have been tested in real network are chosen in this comparison. The first one is NCAS method, which was proposed by Chen et al. [7] in frequency domain. NCAS method achieves detection probability of 88 percent, false positive rate of 16.7 percent and false negative rate of 12 percent, with space complexity of $O(n)$ and time complexity of $O(n^2)$. The second method is based on Kalman Filtering [10], with detection probability of 89.6 percent, the false positive rate of 12.6 percent and the false negative rate of 10.4 percent, space complexity of $O(n^2)$ and time complexity of $O(n^2)$. The comparison results are shown in Table 4.

TABLE 3
Comparison of Different Experimental Platforms

Items / Name	P_D	P_{FN}	P_{FP}
Detection in NS2	92%	8%	9%
Detection in test-bed with five users	91%	9%	10%

TABLE 4
Comparison of Different Detection Methods

Items / Name	Detection performance			Complexity	
	P_D	P_{FN}	P_{FP}	Space	Time
NCAS	88%	12%	16.7%	$O(n)$	$O(n^2)$
Kalman	89.6%	10.4%	12.6%	$O(n^2)$	$O(n^2)$
Multifractal	91%	9%	10%	$O(n\log_2 n)$	$O(n\log_2 n)$

Table 4 indicates that LDoS attack detection based on multifractal in test-bed network obtains the detection probability of 91 percent, which is higher than that detection of NCAS in frequency [7] and the detection based on Kalman Filtering [10]. Although the approach presented in the paper has higher space complexity, it has lower time complexity. In summary, LDoS attack detection based on multifractal achieves good performance.

5 Conclusion

In this paper, a new approach of detecting LDoS attacks based on multifractal is proposed. Experiments in NS2 simulation platform as well as test-bed network environment are conducted to test the detection performance. It is proved that network traffic has the multifractal characteristic by using MF-DFA algorithm. Then, pointwise Hölder exponents are estimated based on wavelet analysis. And then, LDoS attacks are detected by comparing the Hölder exponent difference with the detection threshold, and the beginning or the ending of LDoS attacks are determined by t hypothesis test. The performance of the approach in the NS2 simulation is compared with that in test-bed network, and compared with other methods. The NS2 results show that the approach can achieve the detection probability of 92 percent and false positive rate of 9 percent. The test-bed results show the approach applied in the network of five or more users can reach the detection probability of 91 percent and false positive rate of 10 percent along with low complexity.

Acknowledgements

This work was supported in part by National Natural Science Foundation of China under Grant No. 61170328 and U1333116, Key Project of Natural Science Foundation of Tianjin under Grant No. 12JCZDJC20900, the Civil Aviation Science and Technology Innovation Foundation in 2013 under Grant No. MHRD20130217, the Fundamental Research Foundation for the Central Universities of CAUC under Grant 3122013P007, 3122013D007, and 3122013D003, and the research laboratory construction foundation of Civil Aviation University of China (CAUC) in 2014-2016.

References

[1] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.

[2] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies," *IEEE/ACM Trans. Netw.*, vol. 14, no. 4, pp. 683–696, Aug. 2006.

[3] T. Yajuan, L. Xiapu, H. Qing, and R. K. C. Chang, "Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 339–353, Mar. 2014.
[4] G. Macia-Fernandez, J. E. Diaz-Verdejo, and P. Garcia-Teodoro, "Mathematical model for low-rate DoS attacks against application servers," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 519–529, Sep. 2009.
[5] A. Feldmann, A. Gilbert, and W. Willinger, "Data networks as cascades: Explaining the multifractal nature of internet traffic," in *Proc. ACM SIGCOMM*, Sep. 1998, pp. 42–55.
[6] Z. Xia, S. Lu, and J. H. Li, "DDoS flood attack detection based on fractal parameters," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, 2012, pp. 1–5.
[7] Y. Chen, K. Hwang, and Y.-K. Kwok, "Collaborative defense against periodic shrew DDoS attacks in frequency domain," USC Internet Grid Comput. Lab, Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. TR 2005–11, May 2005.
[8] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in *Proc. ACM SIGCOMM Internet Meas. Workshop*, Marseilles, France, 2002, pp. 71–82.
[9] H. Yan-Xiang, C. Qiang, L. Tao, H. Yi, and X. Qi, "A Low-Rate DoS detection method based on feature extraction using wavelet transform," *J. Softw.*, vol. 20, no. 4, pp. 930–941, Apr. 2009.
[10] W. Zhijun and Y. Meng, "Detection of LDDoS attack based on kalman filtering," *Acta Electronica Sinica*, vol. 36, no. 8, pp. 1590–1594, Aug. 2008.
[11] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, " On a mathematical model for low-rate shrew DDoS," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.
[12] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 426–437, Jun. 2011.
[13] Z.-J. Wu, H.-T. Zhang, M.-H. Wang, and B.-S. Pei, "MSABMS-based approach of detecting LDoS attack," *Comput. Security*, vol. 31, pp. 402–417, 2012.
[14] A. Nogueira, P. Salvador, R. Valadas, and A. Pacheco, "Modeling network traffic with multifractal behavior," *Telecommun. Syst.*, vol. 24, nos. 2–4, pp. 339–362, Oct. 2003.
[15] F. H. T. Vieira and L. L. Lee, "Adaptive wavelet-based multifractal model applied to the effective bandwidth estimation network traffic flows," *IET Commun.*, vol. 3, no. 6, pp. 906–919, Jun. 2009.
[16] C. Williamson, "Internet traffic measurement," *IEEE Internet Comput.*, vol. 5, no. 6, pp. 70–74, Nov./Dec. 2001.
[17] U. B. Desai, K. P. Murali, and V. M. Gadre, *Multifractal Based Network Traffic Modeling*. Norwell, MA, USA: Kluwer, Dec. 12, 2003.
[18] R. H. Riedi, M. S. Crouse, V. J. Ribeiro, and R. G. Baraniuk, "A multifractal wavelet model with application to network traffic," *IEEE Trans. Inf. Theory*, vol. 45, no. 3, pp. 992–1018, Apr. 1999.
[19] R. Caceres, P. Danzig, S. Jamin and D. Mitzel, "Characteristics of wide-area TCP/IP conversations," in *Proc. ACM Conf. Commun. Architect. Protocols*, Zürich, Switzerland, Sep. 1991, pp. 101–112.
[20] I. Daubechies, *Ten Lectures on Wavelets*. Philadelphia, PA, USA: SIAM, 1999, pp. 355–357.
[21] S. Seuret and A. Gilbert, "Pointwise Holder exponent estimation in data network traffic," presented at the ITC Specialist Seminar Workshop, Monterey, CA, USA, Sep. 2000.
[22] E. W. Knightly and A. Kuzmanovic. (2004). Shrew attack Linux code [Online]. Available: http://www.cs.northwestern.edu/~akuzma/rice/shrew/
[23] R. Mondragon, A. Moore, J. Pitts, and J. Schormans, "Analysis, simulation and measurement in large-scale packet networks," *IET Commun.*, vol. 3, no. 6, pp. 887–905, Jun. 2009.

Zhijun Wu received the BS and MS degrees in information processing from Xidian University, China, in 1988 and 1996, individually and the PhD degree in cryptography from the Beijing University of Posts & Telecommunications, China, in 2004. He is a professor in the Department of Communication Engineering, Civil Aviation University of China, and he teaches and directs research in network security and communication engineering. He is an external professor employed by Tianjin University and Beijing University of Posts & Telecommunications, China. He is the supervisor of Ph.D. candidates in the fields of Communication and Information System at Tianjin University, China, and of Information Security at the Beijing University of Posts & Telecommunications, China. His current research interests include denial-of-service attacks, and security in big data and cloud computing. His research is funded by the National Natural Science Foundation of China.

Liyuan Zhang received the BA degree in information & computing science from Ludong University, China, in 2012. She is a postgraduate in communication and information system in Civil Aviation University of China. Her current research interests are network and information security.

Meng Yue received the BS degree in electronics & information engineering from Hebei Science & Technology University, China, in 2006, and the MS degree in communication and information system from Civil Aviation University of China in 2009. He is currently with the College of Electronics & Information Engineering, Civil Aviation University of China. His research was initially focused on information security and cloud computing, with special focus on denial of service attacks, intrusion detection, and defense.