Characterization of the Imaged R/S Pox Diagram for Low-rate DoS Attack

Akinori TAKAHASHI*, Ryuji IGARASHI*, Kazuto SASAI**, Hiroshi UEDA***, Yukio IWAYA****, Tetsuo KINOSHITA** and Masashi HASHIMOTO*

*Department of Mathematical Science and Electrical-Electronic-Computer Engineering, Graduate School of Engineering Science, Akita University, 1-1, Tegata Gakuen-machi, Akita-shi, Akita 010-8502, Japan
**Research Institute of Electrical Communication, Tohoku University
***Academic Center for Computing and Media Studies, Kyoto University
****Faculty of Engineering, Tohoku Gakuin University
E-mail: akinori@ie.akita-u.ac.jp

A low-rate denial of service (LDoS) attack can degrade the quality of TCP communication with fewer attack traffic. The LDoS attack transmits such network traffic that conforms to the minimum value of TCP retransmission timeout. This provides periodic features to the traffic concerned. We consider the application of an R/S Pox Diagram characteristic which can represent the LDoS attack periodicity. An R/S Pox Diagram shows a characteristic plot shape against the periodicity of the LDoS attack. The distinct shape of the plot is quantified as shape features of the two-dimensionally imaged R/S Pox Diagram. Our proposal in this paper is to positively make use of the shape features of the two-dimensionally imaged R/S Pox Diagram. We show the effectiveness of the shape features utilization by showing their detection performance to pieces of simulating LDoS attack.

Keywords: Low-rate DoS Attack, Imaged R/S Pox Diagram, plot shapes

1 INTRODUCTION

According to the development of network and systems environment, there are growing concerns about various threats on networking. Since many of those threats are caused by unauthorized access from the network, early detection of them is important as security measures. DoS attacks such as TCP SYN Flood [1] attack and smurf attack [2] waste network resources by sending a large number of packets to the victim and stop the victim’s network service. The Flooding attack is relatively easy to detect since it has a characteristic of high rate with respect to the network band. In recent years, however, it has been pointed out that DoS attacks that use attack packets exposed to inadequate detection comparing to conventional methods existed [3]. A low-rate denial of service (LDoS) attack can degrade the quality of TCP communication with fewer attack traffic. LDoS attacks are those that exploit TCP retransmission time out (RTO) which is one of the network congestion control agent of TCP communication. An attack that transmits bursty traffic with the same time interval of the minimum value of RTO causes instantaneous network congestion and packet losses. When a packet loss occurs, TCP communication performs congestion control, resulting in deterioration in quality such as throughput reduction. It has been proved difficult to detect them with the method developed for traditional DDoS attacks, since the attack is hard to distinguish from normal congestions [3,4].

LDoS attacks have a periodicity because bursty traffic transmitted at 1 second interval provides victims a great effect.

Various methods have been proposed for detecting attacks by focusing on the periodicity. In Ref. [5], a method is proposed to apply an autocorrelation function to a periodic pulse sequence which includes attack traffic. In Ref. [6], a method is proposed to discriminate patterns of attack traffic from flow level traffic. Detection method by signal processing using the DSP technique has been proposed, and there are methods based on wavelet analysis [7,8] and methods based on multifractal characteristics of network traffic [9]. In addition, a chaos-based approach [10] is proposed to detect LDoS attack by using the technology of weak signal detection.

We have proposed a detection method using R/S pox leg-line characteristics [11] against long-term port scanning attacks with periodic features like LDoS attacks. The R/S pox leg-line characteristic is a feature value obtained from a graph called an R/S Pox Diagram which is used for estimating self-similarity of a time series. This feature value has superiority over the conventional method because it can quantify change of attack state such as attack-start and attack-end in addition to periodic component detection. The leg-line characteristic is quantified from the slope of the characteristic plots which appears in the R/S Pox Diagram. Since the shape of the plot, from the viewpoint of a two-dimensional image, is considered to have various image properties, it is thought to be useful to quantify other shape features of R/S pox leg-line characteristics.

The purpose of this study is to propose a method to quantify the features of the plot shape of R/S Pox Diagrams and to evaluate...
the detection performance of the shape variations of the R/S Pox Diagrams concerned with respect to LDoS attacks. The main procedure of the proposed method is to visualize the plot shape of the R/S Pox Diagram and to calculate the area, the perimeter and the circularity of the closed curve obtained from the image-processed R/S Pox Diagram. Evaluation of the proposed method is practiced by using simulation time series generated by R language [12]. Section 2 describes the mechanism of TCP retransmission timeout and an overview of LDoS attacks. Section 3 describes the imaging procedures of R/S Pox Diagram and calculation method of plot shape features. Section 4 presents simulation results, and Section 5 concludes the results and discussions.

2 LOW-RATE TCP ATTACK

In this section, we overview the TCP retransmission timeout, which is one of the important times of TCP congestion control, and the LDoS attack which exploits its properties.

2.1 TCP retransmission timeout

TCP congestion control in order to ensure communication quality is executed when packet loss occurs. If an ACK packet for a transmitted segment does not return even after a certain period of time, the same segment is transmitted again. This waiting time is called Retransmission Time Out(RTO), and its initial value is obtained from the round-trip time(RTT) as represented in Eq. (1).

\[ RTO = \max \{\minRTO, \text{(smoothed RTT)} + \max \{\text{(clock granularity)}, 4(\text{RTT variation})\}\} \tag{1} \]

Here, “minRTO” is the minimum value of RTO being recommended to set it to 1 second in RFC 6298[13] and “clock granularity” is the shortest interval of time measurement available from the clock. The second term of the function that compares the maximum value of Eq. (1) is obtained from the RTT. Since RTT time, however, is very small in most cases, the initial value of RTO is set to “minRTO”. When packet loss occurs RTO, in order to avoid congestion, is re-set as in Eq. (2).

\[ RTOi = 2 \times RTO_{i-1} \tag{2} \]

If the communication becomes normal between new RTO, it is reset to the initial value by Eq. (1). When the packet loss continues to occur, however, the value of RTO is increased each time.

2.2 Overview of Low-rate DoS Attack

Figure 1 shows the traffic model of an LDoS attack [3] which exploits the retransmission timeout described in Section 2.1. In Figure 1 the horizontal axis represents the time elapsed and the vertical axis represents traffic volume. In the traffic model below, \(L_p\) is the pulse width of the burst traffic, \(R\) is the traffic volume, and \(T\) is the period of the attack. LDoS attacks are shaped like periodic square waveforms which periods conform to minRTO and the burst traffic having these periods instantaneously causes a congestion.

When the attack begins, most TCP communication fails due to the first burst traffic and is retransmitted after the RTO passes. Because the RTO of most communications is set to minRTO, the retransmission will be synchronized to the next burst traffic. If the next retransmission also fails, the RTO is doubled by Eq.(2). However, RTO only becomes an integral multiple of minRTO. Therefore, retransmission continues to fail with repeatedly incoming burst traffic. Even in the case it becomes possible to communicate without overlapping the burst traffic due to communication fluctuation, there is a high possibility that the communication will fail again during the attack, and the communication quality is deteriorated.

3 PROPOSED METHOD

In this section, we describe the imaging method of R/S Pox Diagram and the way to derive shape features from the plot configuration of the imaged R/S Pox Diagram. The processing procedure of the proposed method is divided into the following three stages. The first is the processing of the R/S Pox Diagram obtained from arbitrary traffic time series, the second is to transform the graphical R/S Pox Diagram into a two-dimensional image, and, at the final stage, the feature characteristics of the transformed curve of the R/S Pox Diagram are derived.

3.1 R/S Pox Diagram

What is called an R/S analysis is a graphical method having conventionally been used to estimate the self-similarity parameter \(H\) of statistical events. This method, at first, was introduced for the analysis of Nile River flow fluctuations by H. E. Hurst [14]. Mathematical basis thereafter was established by B. B. Mandelbrot [15] and the analysis has been widely used in various walks of research fields. An application to communication fields especially for packet traffic communications was first practiced by Leland et al. [16] in the late 20th century. An R/S, the ratio of cumulative range \(R\) to the standard deviation \(S\) of a time series, is a statistic and the self-similarity parameter \(H\) named after Hurst is estimated graphically by using an R/S Pox Diagram [16], [17], [18].

A packet flow interpreted as random points placed on a time axis is captured for every small time interval \(\Delta t\) and then the count is transformed to a discrete time series \(X_i\), \(t = 1, 2, \cdots, N\). When employing the R/S analysis, a requirement is so introduced to divide the time series into non-overlapped \(n\) blocks. Here, \(n\) represents the size of a non-overlapped block. Then, a cumulative range \(R\) and a standard deviation \(S\) are calculated for all the blocks concerned by Eq. (3)-(6), where each \(X_i\) represents the magnitude of the event at \(k\), \(W_i\) represents the deviation of cumulative sum \(\sum X_i\) to the averaged sum \(k\bar{X}\), \(R_i\) represents the cumulative range, and \(S\) represents the standard deviation.

\[
\bar{X}_n = \frac{1}{n} \sum_{i=1}^{n} X_i \tag{3}
\]

\[
W_i = \sum_{j=t}^{n} X_j - k\bar{X}_i \tag{4}
\]

\[
R_i = \max \{0, W_i, \cdots, W_i, \cdots, W_n\} - \min \{0, W_i, \cdots, W_i, \cdots, W_n\} \tag{5}
\]

Figure 1 shows the traffic model of LDoS attack traffic.
When calculation is completed in all the blocks, the same calculation process is repeated while increasing the data size \( n \) of the block 1 through \( N \). An R/S Pox Diagram shows the variation of \( \log(R_n/S_n) \) to \( \log(n) \). Figure 2 shows an example of R/S Pox Diagram. The Pox Diagram of an FGN (Fractional Gaussian Noise), theoretically constructed 2nd order self-similar process [16], shows a monotone variation as depicted in Figure 2 (a). When a periodic sequence of period \( T = 100 \) is superimposed on the FGN, the plot shape of the Pox Diagram changes at block size \( n = 100 \) \( \{ \log(n) = 2.0 \} \) as depicted in Figure 2 (b). The variation point \( n = 100 \) corresponds to the period \( T = 100 \) in the R/S Pox Diagram concerned. In case the LDoS attack is attempted with period \( T = 100 \), the plot shape provides a definite change at this point.

In our study, packet time series are generated by setting the calculation process is repeated while increasing the data size \( n \) of the block 1 through \( N \). An R/S Pox Diagram shows the variation of \( \log(R_n/S_n) \) to \( \log(n) \). Figure 2 shows an example of R/S Pox Diagram. The Pox Diagram of an FGN (Fractional Gaussian Noise), theoretically constructed 2nd order self-similar process [16], shows a monotone variation as depicted in Figure 2 (a). When a periodic sequence of period \( T = 100 \) is superimposed on the FGN, the plot shape of the Pox Diagram changes at block size \( n = 100 \) \( \{ \log(n) = 2.0 \} \) as depicted in Figure 2 (b). The variation point \( n = 100 \) corresponds to the period \( T = 100 \) in the R/S Pox Diagram concerned. In case the LDoS attack is attempted with period \( T = 100 \), the plot shape provides a definite change at this point.

In our proposal below, a trade-off attention is laid to the pixel size. Therefore, in our proposal the closing process [19] applied to pixel size \( \Delta x \) and \( \Delta y \) sizes are changed to 0.02, 0.04, 0.05, 0.1. The results are shown in Figure 4(a)-(d).

In order to maintain a definite resolution of the image, smaller size of the pixel is preferred. For too smaller pixels as in Figure 4(a) and Figure 4(b), however, the image may lose peripheral continuity and may be divided into several domains, thus becomes useless with respect to our current purpose. When we set the pixel size too large as in Figure 4(d), however, periphery resolution becomes low and the smoothness of the curve disappears. In the present attempt, we set the pixel size as 0.05 for both \( \Delta x \) and \( \Delta y \) according to our preliminary exercise so far.

Figure 5(a) shows an example of a binary image of an R/S Pox Diagram. In this example, such pixels that include a noise reside. In our proposal, the closing process [19] was employed in order to remove the noise pixel. Closing process consists of a dilation process followed by an erosion process which is known to be valid to fill in holes and small gaps.

In the dilation process pixel value of the pixels all around the

\[
S_n = \sum_{k=1}^{N} X_k^2/n - X_n^2
\]

(6)

3.2 Imaging method

From the viewpoint of image construction, the plot of the R/S Pox Diagram can be interpreted as one two-dimensional shape. Since it is reasonably imagined that the periodicity of LDoS attack appears as a definite bend along the plotted pox in the R/S Pox Diagram, it is expected that two-dimensionally image-transformed configuration provides some useful pieces of information when we intend to detect the LDoS attack concerned. This is why we propose an image-transformed method to R/S Pox Diagrams. Figure 3 shows an example of the image construction (hereafter, imaging) method from an R/S Pox Diagram.

The size of one pixel on the logarithmic axis of the R/S Pox Diagram is set as represented in Eqs. (7) and (8).

\[
\Delta x = \Delta \log_2(n)
\]

(7)

\[
\Delta y = \Delta \log_2(R_n/S_n)
\]

(8)

A pixel value under a certain coordinate \((x, y)\) is so defined as \(\text{pixel}(x, y)\) in Figure 3. In the case when the plot shape of the Pox Diagram lies in the pixel concerned, \(\text{pixel}(x, y)\) is set to 1. To the contrary, in case there exists no plot, \(\text{pixel}(x, y)\) is set to 0.

In the present study, we intend to quantify the shape characteristics of an R/S Pox Diagram by using image features, the image being constructed from the R/S Pox Diagram configuration. In our proposal below, a trade-off attention is laid to the pixel size. In order to verify the change of shape feature by image resolution, we generated binary images of R/S Pox Diagram when \(\Delta x \) and \(\Delta y\) sizes are changed to 0.02, 0.04, 0.05, 0.1. The results are shown in Figure 4(a)-(d).
target pixel is set to 1 even in the case there is only a single pixel within the surrounding pixels. To the contrary, the erosion process sets the pixel value of all surrounding pixels to 0 even if there is only one pixel whose pixel value is 0. Figure 5(b) represents the binary image after closing process has been practiced with respect to the image in Figure 5(a).

3.3 Calculation of shape features

The area showing the plot shape in the binary image of an R/S Pox Diagram has properties as figures. We quantify the shape features of the plot area shape from the viewpoint of image processing. It is presumed that shape features of the plot area shape comprehensively express partial slopes of R/S Pox Diagram used in the R/S pox leg-line characteristics. Although there are various characteristics related to a figure shape, we employed in this study "area", "perimeter" and "circularity" as feature parameters as shown in Figure 6.

Area $A$ is plot amount representing the extension of a figure constructed from an R/S Pox Diagram and is obtained by counting the number of pixels included in the plotted figure. The plotted figure in Figure 6, for example, provides $A = 341$ pixels. Perimeter $L$ is determined from the circumference length of the plotted figure. The perimeter is represented by the number of pixels along the circumference line of the figure. Here an attention must be paid to the difference in $L$ which depends on the connectivity of the figure circumference concerned. This provides us different $L$ even in case the same figure is employed. In the present study, the weight $\sqrt{2}$ is provided to the perimeter. This is because a diagonal line is imagined with 8-neighborhoods contours between pixels. In Figure 6, the perimeter is obtained as 120.27 pixels. Circularity $C_L$ is a function of perimeter $L$ and area $A$ as represented in Eq. (9).

$$C_L = \frac{4\pi A}{L^2} \quad (9)$$

The circularity is a quantity that provides the value 1 for a true circle, and the value becomes smaller as it becomes an elongated, elliptic shape. With the plot shape in Figure 6, it provides about 0.30. Since the plot figure has an elliptical shape for the stationary time series and a bend shape for the introduction of periodic time series, it is anticipated that the circularity becomes small in the case of the LDoS attack.

4 EVALUATION BY SIMULATION

In this section, we examine the variation of the shape features obtained by our proposed method. In the procedure, the simulation time series based on the LDoS attack traffic model shown in Figure 1 was employed.

4.1 Periodic characteristics

As we have explained in section 2, LDoS attacks have a large impact on victims when the attack traffic is consecutively transmitted at the same 1 second interval. This interval is the minimum value of RTO. Taking into real traffic state into account, a procedure to focus the detection period only to 1s, however, deviates somewhat from reasonable one. This is because the cycle of attack varies depending on the communication state of the network. Considering this kind of situation, investigations of the shape features for various attack periods are required.

In view of above possibility, such a simulation that employ time series having varying period $T$ was practiced. With this procedure, we are able to examine the influence on the shape features explained in Sec.3.3. The simulation time series are generated by using fgnSim function of farm package [20], in which the long-range dependence model is defined by R language. The fgnSim function can generate FGN (Fractional Gaussian Noise) which is characterized by Hurst parameter $H$. The parameter $H$ is an indicator to the degree of self-similarity. Well known is that $H$ reveals such values as $0.5 < H < 1$ when a stochastic process exhibits a long-range dependence, which also is regarded to exhibit the self-similarity [16]. By taking this property into account we employed such date series that corresponds to stationary time series. The size $N$ of simulation data was chosen as $N = 1000$. In the simulation, assigned values respectively to $H$ are $H = 0.6, 0.7, 0.8, \text{and} \ 0.9$. All of the $H$ values are within $0.5 < H < 1$ so that they satisfy the condition to obey the self-similarity. These were provided as base time series. The shape features having been stated in Sec.3.3 are calculated by using simulation time series realized by superimposing periodic pulse trains onto the base time series. Parameters employed are the peak rate $R$, the length of the peak $L_p$, and the period $T$ of the pulse train which are represented in Figure 1. Concretely the values respectively were $R = 10, L_p = 7/2, T = 50$ to 150 increasing by 10.

The results are shown in Figure 7. Figure 7(a) shows the variations of area $A$ with respect to the period $T$. Similarly, Figure 7(b) shows the variations of perimeter $L$ and Figure 7(c) shows the variations of circularity $C_L$. In addition, the values in parentheses in the legends of respective figures indicate respective shape features obtained from the stationary time series with $H = 0.6, 0.7, 0.8, \text{and} \ 0.9$.

In order to compare the shape features of the periodic time series to the stationary ones, quantities below are introduced as
represented in Est. (10)-(12).

\[ P_{\text{Area}} = \sum_{H=0.8}^{H=0.6} \frac{A_H(100) - A_H(0)}{A_H(0)} \]  \hspace{1cm} (10)  

\[ P_{\text{Perimeter}} = \sum_{H=0.8}^{H=0.6} \frac{L_H(100) - L_H(0)}{L_H(0)} \]  \hspace{1cm} (11)  

\[ P_{\text{Circularity}} = \sum_{H=0.8}^{H=0.6} \frac{C_L_H(100) - C_L_H(0)}{C_L_H(0)} \]  \hspace{1cm} (12)  

\( A_H(100), L_H(100), C_L_H(100) \) are shape features at \( T=100 \) respectively and \( A_H(0), L_H(0), C_L_H(0) \) are those at \( T=0 \) which accordingly mean those for the stationary series. In Eqs. (10)-(12) \( P_{\text{Area}}, P_{\text{Perimeter}}, \) and \( P_{\text{Circularity}} \) exhibit the ratio of the magnitude of discrepancy between non-stationary time series and the stationary one. The ratios in Eqs. (10)-(12) becomes a kind of normalization to the stationary time series. Also, an attention should be paid in Eqs. (10)-(12) that the effect of \( H \) variation is totally incorporated in it as averages.

In the present simulation, \( P_{\text{Area}}, P_{\text{Perimeter}}, \) and \( P_{\text{Circularity}} \) respectively became 12.7% decrease, 5.2% increase, and 21.1% decrease against the stationary time series. From these results, it was confirmed that respective shape features could provide definite reactions to periodic time series. The highest sensitivity in the present case is obtained for \( P_{\text{Circularity}} \). The tendency of the shape features remained unchanged for various \( T \). This support the proposed shape features to appropriately be able to provide as detection parameters of LDoS attacks.

4.2 Time dependent characteristic

The simulation time series we employed correspond to 10s intervals in real time. As explained in Figure 8(a), the simulation series consists of two parts. One is a base series mentioned in Sec.4.1 and another is an attack series described in Figure 1. The

\[ X_p (p=1,2,...,N_p=7000) \]

\[ \text{LDoS attack traffic (T=100, L=50, R=10)} \]

\[ \text{Step size } \Delta p = 10 \]

\[ N_0=1000 \]

\[ A(t), L(t), C_L(t) \]

Figure 7: Variation of shape features \( A, L, C_L \) against the period \( T \)

Figure 8: Overview of simulation and examples of time-dependent characteristics of shape characteristics.
base series \( X_r [p: 1, 2, \cdots, N_r = 7000] \) consisted of an FGN series having \( H = 0.6 \). The attack series was \( T = 100, L = 50 \), and \( R = 10 \) respectively. Here \( T = 100 \) corresponds to 1s because one point in the time axis is set as 0.01s in real time.

The attack traffic comes after 2000 steps after the onset of the simulation as represented in Figure 8(a). Windows are prepared to derive \( A(t), L(t), \) or \( C(t) \) consecutively. The length of the window was set at 1000 points. The window step \( \Delta p \) is set to \( \Delta p = 10 \) points. Since the observation starts from \( p = 1000 \) points, the termination in \( t \) becomes \( t = 600 = 6000/\Delta p \). Obtained shape features \( A(t), L(t), \) and \( C(t) \) derived in this manner are represented in Figure 8(b).

The attack traffic is inserted between \( p = 2000 \) and 5000, which corresponds to \( t = 20 \) and 50s on real time axis. The overall sequence was as follows; \{attack onset, \( t = 20 \)s\}, \{attack duration, \( t = 20 \)s through 50s\}, \{base traffic duration, \( t = 0 \)s through 60s\}. Since the window length is set to 1000 points, the start point of \( A(t), L(t), \) and \( C(t) \) must have been laid at \( p = 1000 \) which corresponds to \( 10s = 1000\times0.01 \)s. This is why the duration of respective \( A(t), L(t), \) and \( C(t) \) becomes 600 points \( = (7000-1000)/0.01 \)s = 60s.

Represented in Figure 8(b) are time dependent shape features \( A(t), L(t), \) and \( C(t) \). All of them showed a definite variation with respect to \( t \). The variation appears immediately after the onset of the attack. This states us that the shape features may be used as estimators for change point detection. The change point here corresponds to the onset of the attack. Especially remarkable in Figure 8(b) are \( L(t) \) and \( C(t) \). Both of them showed a sudden change when the windows reached the onset point. This provides a favorable characteristic because the sudden change in other words a high sensitivity. From the statement above, it is said that the proposed shape features are useful as detection parameters of traffic state.

5 CONCLUSION

In this study, we proposed a method to treat R/S Pox Diagram as a two-dimensional image. Shape features Area \( A \), Perimeter \( L \), and Circularity \( C_l \) were defined in the image-converted R/S Pox Diagram. According to the simulation study in which LDoS (Low rate DoS) attack was assumed the usefulness of the shape features was confirmed.

In the future, we will consider a method for determining the attack state using the proposed shape features and compare it with other methods. Moreover, we will examine the effect of randomly placed LDoS attack where pulse trains no more reveal periodic appearance.

Acknowledgment—This study was supported in part by the Nation-wide Cooperative Research Projects of Research Institute of Electrical Communication, Tohoku University (H27/A24).

References

[1] CERT Advisory CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks, https://www.cert.org/historical/advisories/CA-1996-21.cfm (1996).
[2] CERT Advisory CA-1998-01: “smurf” IP Denial of Service Attacks, https://www.cert.org/historical/advisories/CA-1998-01.cfm (1998).
[3] A. Kuzmanovic and E. W. Knightly, “Low-Rate TCP- Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants) ”, Computer Communication Review, 33(4), pp.75-88 (2003).
[4] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, “Reduction of Quality (RoQ) Attacks on Internet End Systems,” Proc. INFOCOM 2005 (2005).
[5] H. Sun, J.C.S. Liu and D.K.Y. Yau, “Defending Against low-rate TCP Attacks: Dynamic Detection and Protection”, In proc. OFICNP ’04, pp.196-205 (2004).
[6] A. Shevetkar, K. Anantharam and N. Ansari, “Low Rate TCP Denial-of-Service Attack Detection ad Edge Routers”, IEEE Communications Letters, Vol.9, No.4, pp.363-365 (2005).
[7] C. T. Huang, S. Thareja and Y.-J. Shin, “Wavelet-based Real Time Detection of Network Traffic Anomalies”, Int. J. of Network Security, Vol.6, No.3, pp.309-320 (2008).
[8] Y. X. He, Q. Cao, T. Liu and Q. Xiong, “Low-rate DoS detection method based on feature extraction using wavelet transform”, Jornal of Software, Vol.20, No.4, pp.930-941 (2009).
[9] Z. Wu, L. Zhang, and M. Yue, “Low-Rate DoS Attacks Detection Based on Network Multifractal”, IEEE Trans. on Dependable and Secure Computing, Vol.13, No.5, pp.559-567 (2016).
[10] W. Zhi-jun, L Jin, Y. Di, W. Ming-hua and S. M. Musa, "Chaos-based detection of LDoS attacks", Journal of System and Software, Vol.86, No.1, pp.211-221 (2013).
[11] A. Takahashi, R. Igarashi, H. Ueda, Y. Iwaya and T. Kinoshita, "R/S Pox Leg-line Characteristics", JPSJ Journal, Vol.54, No.6, pp.1761-1770 (2013).
[12] The R Project, https://www.r-project.org/
[13] V. Paxson, M. Allman, J. Chu and M. Sargent, “computing TCP’s Retransmission Timer”, Internet RFC 6298, IETF (2011).
[14] H. E. Hurst, "Long-Term Storage Capacity of Reservoirs", Trans. Amer. Soc. Civil Eng., Vol.116, pp.770-799 (1951).
[15] B.B. Mandelbrot and J.R. Wallis, "Robustness of the Rescaled Range R/S in the Measurement of Noncyclic Long-Run Statistical Dependence", Water Res. Res., Vol.5, No.5, pp.967-988 (1969).
[16] W.E. Leland, M.S.Taqqu, W. Willinger and D.V. Wilson: "On the Self-Similar Nature of Ethernet Traffic", Computer Communications Review, Vol.23, No.4, pp.183-193 (1993).
[17] J. Beran, R. Sherman, M. S. Taquu, and W. Willinger, “Long-Range Dependence in Variable-Bit Rate Video Traffic”, IEEE Transa- ctions on Communications, Vol.43, No.2/3/4, pp.1566-1579 (1995).
[18] M. S. Taquu, V. Teverovsky, and W. Willinger, "Estimators for Long-Range Dependence: An Empirical Study", Fractals, Vol.3, No.4, pp.785-798 (1995).
[19] M. Takagi and H. Shimoda, "Handbook of image analysis", University of Tokyo Press (1991).
[20] D. Wuerzt, et al., "Arma: ARMA Time Series Modelling", https://cran.r-project.org/web/packages/fArma/index.html (2013).