Correlation-based Detection of LDoS Attack

Wu Zhi-jun
School of Electronics & Information, Engineering, Civil Aviation University of China, Tianjin, China
Email: zjwu@cauc.edu.cn

Wang Minghua
China Computer Emergency Response Term, Beijing, China
Email: wmh@cert.org.cn

Zhang Haitao, Liu Xingchen
School of Electronics & Information, Engineering, Tianjin University, Tianjin, China
Email: haitao_mail@yahoo.com.cn; liu19850119@gmail.com

***Abstracts*—Low-rate Denial of Service (LDoS) attack and TCP flows are simulated in the time and frequency domain for the purpose of analyzing their signatures and extracting period T and duration L of LDoS attack, which are two correlative parameters used in the proposed detecting approach. In the correlation operation, the reference signal is the simulated traffic of LDoS attack, which are built based on the extracted parameters of T and L. The incoming signal is the hybrid signal (TCP flows plus Real LDoS attacks). A detect threshold is established to be compared with the results of correlation operation. If the correlation value exceeds the threshold, the LDoS attack is determined. The proposed method has been tested both in network simulation NS-2 platform and network testbed environment with different parameters of T and L. Experimental results show that the proposed approach reaches the good performance with higher detect rate P_D , and lower false negative alarm rate P_{FN} and false positive alarm rate P_{FP} .**

***Index Terms*—LDoS, correlation, detection, period, duration**

I. INTRODUCTION

Low-rate Denial of Service (LDoS) attack is a new class of DoS attacks[1]. LDoS attack uses network protocol adaptation mechanism of system security vulnerabilities, by sending periodic pulse attack flow to the target, making the victim end network throughput decreased, and the result is that the performance of its quality of services (QoS) reduced. From the signal processing point of view, LDoS attack is usually a periodic square wave signal[1], the main parameter is a triple: *L* is the pulse width, *T* is the pulse period, R is the transmission rate. Therefore, the average rate of the LDoS attack is *RL*/*T*. LDoS attacks remain silent (did not attack during the pulse) in most of the time, and only activities in the short period of time (pulse duration of attacks) to send high-intensity pulse, this feature of intermittent attacks makes the average data flow rate of attack very low, so the traditional DoS detection methods will be ineffective. In this paper, based on the analysis of LDoS attack model, utilizing its two important parameters: *T* and *L* to reconstruct LDoS attack signals on the affected side, we proposed parameters related based LDoS attack detection methods.

Since LDoS was found in 2001, it has attracted the concern of many researchers, Kuzmanovic and Knightly[1] first gave detailed analysis of the principle of LDoS, and conducted a deep research in characteristic of the periodic pulse of LDoS, mined the LDoS overflow attack methods, proposed network-based defense method; Cheng[2] first proposed a method to detect LDoS attack in the frequency domain by using the cumulative normalized power spectrum density; Barford. P. and Kline. J.[3] proposed a method to detect abnormal traffic by using signal processing; Gabriel Maciá-Fernández[4] and Y. Zhang, Z. M. Mao, and J. Wang[5] completed the method of detecting LDoS attack in frequency domain, and simulated in NS-2 environment; Xiapu Luo[6] and He Yanxiang[7] simulated and tested the performance of the LDoS attack by using wavelet in the frequency domain. That system focusing on the number of arriving packets at the monitoring node, extracts five feature indices of LDoS flows through wavelet multi-scale analysis. Then a synthesis diagnosis is made by a trained BP neural network; Qiao Zhu, Zhang Yizhi, and Xie Chuiyi[8] studied the LDoS attack and TCP-oriented prevention strategies. Macia-Fernandez, G., Diaz-Verdejo, J.E., and Garcia-Teodoro, P.[9] have researched the mathematical model for LDoS attacks against application servers[10].

In the LDoS attack detection methods using signal analysis theory, the results of the Sun H. B[11], Yu Chen[12] and HE Yan-Xiang[7] are representative. Sun H. B[17] proposed data flow through the sampling and feature extraction, which is commonly used in speech recognition using dynamic time warping (DTW) method to match the data and samples; Yu Chen[12] fitted curve of the normalized cumulative power spectral density which whether they are the attacks to find the optimal threshold.

doi:10.4304/jsw.7.10.2341-2348

II. MODEL OF LDOS ATTACK AND NORMAL TCP TRAFFIC FLOW IN TIME-FREQUENCY DOMAIN

A unified LDoS mathematical model in the time domain and frequency domain, and give the characteristics in the time domain and frequency domain from the perspective of mathematics. For the convenience of analysis, study in the paper focuses on one single TCP flow and one LDoS attack.

In the following analysis of the model, research on data of the TCP traffic and LDoS attacks stream which is extracted from NS-2 simulation, sampling the flow of inlet to the router with period of 10ms to constitute the sense stationary discrete sequence. According to the Nyquist criterion, the sampling interval is 10ms, the signal spectrum can get 0-50Hz, which is enough to analyze the signal characteristics. Also, due to the 10ms interval for the sample can reduce the normal TCP traffic suddenly, making it more smooth and easy on the signature analysis for LDoS. LDoS attack flow is mainly User Data Protocol (UDP) stream.

A. LDoS model in Time Domain

The intent of establishing the model of LDoS attack in time domain is to reveal the biggest difference between the normal TCP signal and LDoS attack signal--periodicity, which is one of bases for the relevant parameters detection[10][14].

A basic time-domain waveform of LDoS attack is shown in Fig 1.

The model of the attack flow can be expressed as:

$$x(n) = a(n) + G \quad (1)$$

Here, $a(n)$ is approximately periodic square wave, G is the background noise.

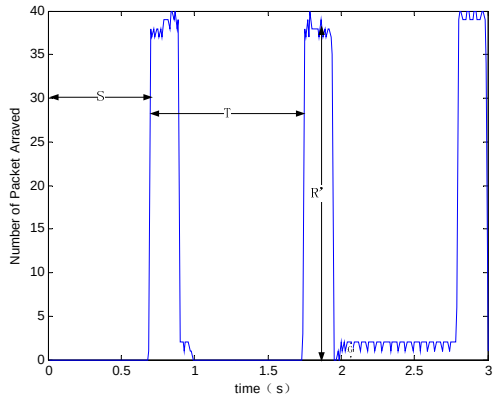

Figure 1. Waveform of LDoS attack in time-domain

Periodic square wave can be expressed as:

$$a(n) = R'*u(n-k*T-l-S) - R'*u(n-k*T-S) \quad (2)$$

Among them $k = 1, 2, \cdots$, $u(n)$ is step signal; S is signal delay of the step signal; R' is the peak of the received signal, determined by the peak R of LDoS attack; l is the length of signal pulse, determined by the pulse length of LDoS attack; T is the signal cycle, determined by LDoS pulse period[15].

Because there are single rate, variable rate (multi-rate) and other forms of LDoS attack[13], in order to clarify the characteristics of LDoS attack, in this paper we establish

As mentioned in above model, the discrete sequence of number packet of export port of the attacked router time-domain was determined by characteristics of the main parameters of the LDoS attack. Although the received signal at the receiving end was influenced by the middle of forwarding device queue management algorithms and preemption of other streams, but the main features of the signal must depend on the behavior of sending flow. Within a short time, normal TCP traffic signals does not like LDoS attack, it does not have the characteristic of periodic.

If within a certain sampling time, the signal can reflect periodic of LDoS attacks, so we must select the appropriate sampling interval. In order to reflect the periodicity of the LDoS attack signal better, the paper simulate the sample data in NS-2 environment. In the simulation, we established the low rate of UDP flow as LDoS attack flow, and let a single TCP stream and single low-speed UDP attack traffic through the same router. Configuration and parameter settings of experiment are shown in Table I.

TABLE I.
THE CONFIGURATION AND PARAMETER SETTINGS OF LDOS ATTACKS PERIODIC SIGNAL SIMULATION

Project	Configuration and Parameters
TCP flow congestion control	reno
Router queue management algorithm	RED（Random Early Detection）
Bottleneck link bandwidth	1.5M

The simulation results of periodic response of LDoS attack are shown in Fig 2.

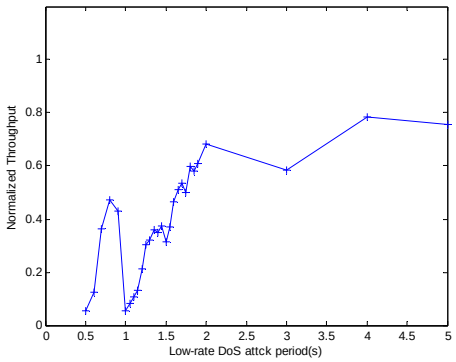

Figure 2. The simulation results of periodic response of LDoS attack

The simulation results from Fig 2 can be shown in Table II.

From the above results we can see that although the experiment using a more advanced router RED queue management algorithm[16], but the effect can be seen from the attacks, mainly against time (1s, 1.5s) range, the results are the same as KUZMANOVIC's[1], it demonstrates that if choose the appropriate configuration and the right parameters, the periodic nature of LDoS attack can reflect within a short time.

TABLE II.
LDOS ATTACK PERIODIC SIGNAL SIMULATION RESULTS

Project	Results
minimum round-trip time of the Link	132ms
periodic range of low-rate attack	0.5s—5s
pulse length of Low-rate attack	L＝0.15s

B. LDoS Model in Frequency Domain

At the receiving end, LDoS attack traffic signal does not show a strictly periodic signal. Because the intermediate forwarding device queue management algorithms and preemption of other streams, its periodicity cannot be got from the time domain. Therefore, we must analyze the periodicity in the frequency domain. This approach is to make discrete LDoS attack flow sequence to do Discrete Fourier Transform (DFT)[17], and normalize the spectrum of LDoS attack, then analyze the periodic characteristics of LDoS attack flows. The DFT operation as follows:

$$X(k) = DFT(x(n),k) = \frac{1}{N}\sum_{n=0}^{N-1} x(n) e^{-j2\pi kn/N} \qquad (3)$$

Through the equation (1), the traffic model of LDoS attacks is the approximate addition of periodic square wave and the background noise. Apply equation (1) model in equation (3), the result is:

$$\begin{aligned} X(k) &\approx X'(k) = DFT(x'(n),k) = \frac{1}{N}\sum_{n=0}^{N-1} x'(n) e^{-j2\pi kn/N} \\ &= \frac{1}{N}\sum_{n=0}^{N-1} (a(n)+N) e^{-j2\pi kn/N} \\ &= \frac{1}{N}\sum_{n=0}^{N-1} a(n) e^{-j2\pi kn/N} + \frac{1}{N}\sum_{n=0}^{N-1} G e^{-j2\pi kn/N} \\ &= A(k) + G' \end{aligned} \qquad (4)$$

When LDoS attacks occur on the export port of router, the characteristics of the number of data packets is a discrete sequence in time-domain mainly formed by the LDoS attack, as $a(n)$ is much larger than G. Therefore, the discrete spectrum of attack sequence number on the export port of the router packet $X(k)$ mainly shows features of $A(k)$.

Simulation is expressed as:

$$A(k) = \frac{R'l}{T}\mathrm{Sa}(k\frac{\pi l}{T}) \qquad (5)$$

Results show that the discrete spectrum of attack packet number sequence on the export port of the router is discrete *Sa* function. The spectrum of LDoS attack flow is shown in Fig 3.

Fig 3 indicates that the interval of discrete spectral lines is determined by $1/T$, $1/l$ determined the width of the first zero. Since $T \in (1\text{s}, 1.5\text{s}]$, the spectral interval is $l \in [0.66\text{Hz}, 1\text{Hz})$. Therefore, in Fig 3, LDoS attack models of the two most important parameters: T and l can be obtained in the frequency domain. Therefore, the parameters like period and pulse width can not be obtained in the time domain, but we can get them in the frequency domain. It can be built against the time domain signal, as the relevant benchmark, for LDoS attack detection.

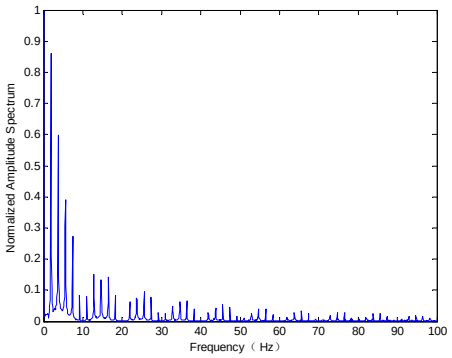

Figure 3. Spectrum of LDoS

To test the accuracy of the LDoS period by estimating attack flow T in frequency domain, the paper designs the experimental environment with the NS-2. Experimental configuration and parameter settings are the same as the test of LDoS period response simulation, as shown in Table I and Table II. The extracting flow of signal from the LDoS attack is 5s signal and the data do 500 points DFT. Signal period is estimated in the frequency domain, the results of the estimation error of period, as shown in Table III.

C. The Model of the Normal TCP Flow in Time Domain

The experiment of Normal TCP flow model in time domain, uses the same simulation with the above, the configuration and parameter settings and the results shown in Table I and Table II, but did not join with LDoS attack flow.

TABLE III.
STIMATE ERROR OF THE SIGNAL PERIOD IN FREQUENCY DOMAIN

Conge. Control \ Period	1	1.1	1.2	1.3	1.4	1.5
Reno	0s	0.02s	0.01s	0.01s	0.02s	0.03s

In simulation, the sampling interval is taken to be 10ms. It reduces the mutation factors of TCP flow, so that the normal TCP flow model becomes very flat. Normal TCP flow model in time domain can be expressed as:

$$y(n) = u(n) + H \qquad (6)$$

Here, $u(n)$ is the step signal, H is the other frequency components except zero frequency.

Simulation of the normal TCP flow signal in time-domain is shown in Fig 4.

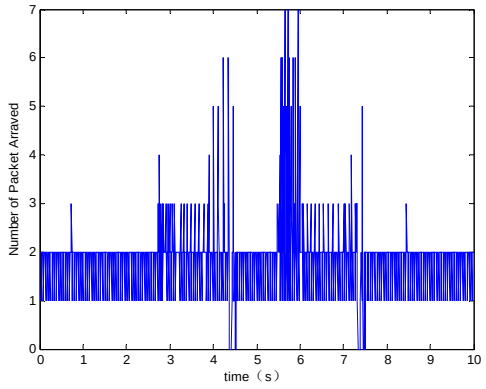

Figure 4. Normal TCP in time-domain

Fig 4 shows that $y(n)$ is shocking about 2, the flow in the receiver, $u(n)=2$ at that time $n>0$.

D. The Model of Normal TCP Flow in Frequency Domain

From the analysis above, TCP flow model in time domain can be expressed by equation. (6) .In frequency domain, the spectrum of $y(n)$ is composed with $u(n)$ and H two parts: the zero-frequency component is from $u(n)$; the other frequency components are from H. Normal TCP traffic through the simulated spectrum is shown in Fig 5.

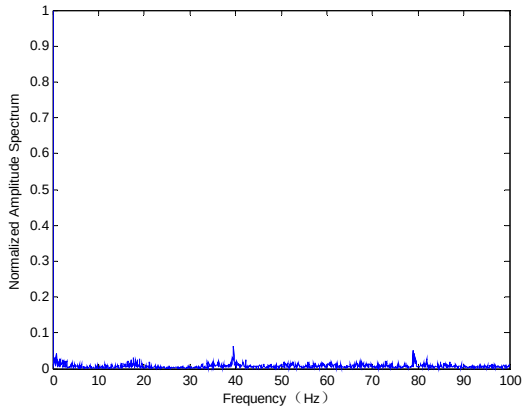

Figure 5. Normal TCP Spectrum

In Fig 5, there is a big difference between the component of zero-frequency and the other frequency. Normal TCP flows mainly focus in zero frequency, but other frequency components is very small, and relatively uniform, and continuous. That is, $u(n)$ accounting for most of the energy, and H is small.

Fig 3 shows that the frequency spectrum of LDoS attack is the *Sa* function, in addition to a large zero frequency component. Because of its periodic nature, LDoS attack signals in the frequency domain is discrete. So comparing Fig 3 and Fig 5, it can be concluded: normal TCP flow and LDoS attacks in the frequency domain with a very different, you can estimate and reconstruct periodic rectangular wave signals of LDoS with two key parameters: period T and pulse width l, and then do correlate detection.

III. DETECTION LDOS BASED ON CORRELATIVE PARAMETERS

From the analysis above, there is a large gap between the normal traffic and LDoS attack traffic, and a little resemblance exists between the two. Contrast the signal characteristics of LDoS attack traffic flow through the receiver, we can see the similarity between them and determine whether it is LDoS attack. A high degree of similarity occurs when LDoS attack happens[18].

Similarity between two discrete sequences can be expressed by the correlation function. Therefore, for LDoS attack traffic sequences $x(n)$ and normal TCP flows discrete sequence $y(n)$, the similarity between $x(n)$ or $y(n)$ and detecting comparing signal can be expressed by the cross-correlation $R_{xw}[m], R_{yw'}[m]$:

$$R_{xw}[m]=\sum_{m=-\infty}^{\infty}(x[n]w[n+m])$$
$$R_{yw'}[m]=\sum_{m=-\infty}^{\infty}(y[n]w'[n+m]) \quad (7)$$

Practically, the sampling time to obtain signal are limited, so we must use time limited signal to estimate the overall correlation of the signals. The two methods are: biased estimation and unbiased estimation. With regard to unbiased estimation, we select unbiased estimator:

$$R_{xw}[m]=\frac{1}{N-m}\sum_{m=-N}^{N}(x[n]w[n+m])$$
$$R_{yw'}[m]=\frac{1}{N-m}\sum_{m=-N}^{N}(y[n]w'[n+m]) \quad (8)$$

Where, $w(n)$ is the comparison signal; $R_{xw}[m]$ is the correlation between $x(n)$ and $w(n+m)$, $w(n+m)$ is comparison signal $w(n)$ by the delay m.

Here, the comparison signal is:

$$w(n)=u(n-k*T'-l'/2)-u(n-k*T'+l'/2) \quad (9)$$

Note that, LDoS attack has two important parameters: period T' and pulse width l', which can be got from the frequency domain analysis.

Obtained from the frequency domain, the delay S is in $x(n)$, $R_{xw}[S+l'/2]$ is apparently the maximum of $R_{xw}[m]$ at the moment $S+l'/2$, that is, after a delay of $S+l'/2$, $x(n)$ is the most similar with $w(n+S+l'/2)$. As in the frequency domain taking the modulus of the frequency, eliminate the phase effect caused by the delay S. The time-domain signals are obtained by processing inverse transform on the frequency-domain sequence. If the delay is 0, the cross-correlation can reach the maximum value, which means it has the maximized similarity.

Also, because $R_{xw}[0]=\frac{1}{N}\sum_{k=-N/2}^{N/2}[X(k)W(k)]$, so for the different delay S, just multiplying the comparing signal

spectrum $W(k)$ and $X(k)$ point by point can obtain the maximum value $R(0)$, to avoid the sliding operation. For the normal TCP flow $y(n)$ and its comparison signals $w'(n)$ generated by the cross-correlation, computational methods are the same.

Therefore, simply follow the reconstruction of the spectrum model of the spectrum signal, it does not need to reconstruct the time domain signal.

For a limited signal transform, compared with the overall signal, the more points to be taken to form discrete signals, the greater the variance is; less the points, the smoother variance. More time needs learning and processing, the higher the complexity. So take the appropriate number of points to transform is very important. We take 500 points here, the 5s period of time to transform the signal. Whichever is the reconstructed signal parameter, were correlated.

Due to TCP flows follow a relatively fixed model in statistical, when the received normal TCP flows signals and reconstruction correlated, the distribution of the correlation coefficient should be mainly concentrated in the vicinity of its mean value; and LDoS attack traffic and the reconstructed signal is very similar, they centered on the correlation coefficient near 1. Hence in the selecting of threshold, it should be possible to search it between the correlation coefficient mean value of TCP traffic and the reconstructed signal and 1.

IV. Simulation and Analysis

To verify the effect of detection algorithm, we built a NS-2 network environment to execute simulation. The performance analysis for proposed detection algorithm focused on two aspects: (i) test false positive rate of correlation detection algorithm for different congestion control; (ii) test false positive alarm rate under different periods.

Network topology of detection used in experiments is shown in Fig 6.

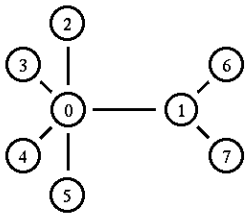

Figure 6. Network topology in NS-2 environment simulation test

Fig 6 shows that the test network is a non-symmetrical "dumbbell" shape. Where: "0" and "1" are the transmitter and receiver routers; "2", "3" and "4" are the three normal TCP flow; "5" constitutes a low-speed UDP attack traffic; "6" and "7" are the two target terminals. The network routing link between the target and attacker is built by using routers "0" and "1"; three TCP flows and one low-speed UDP attack traffic go through the same router.

Test network configuration is shown in Table IV; other configuration parameters are shown in Table II.

In Table IV, the TCP flows with 3 different methods of congestion control are used to test different false positive rates of the correlation detection algorithm with congestion control.

TABLE IV.
Test Network Configuration

Project	Configuration
TCP congestion control flow method	Reno, NewReno, and Sack
queue management algorithm	RED
the link bandwidth between TCP Sender, attacker and router	10 Mb/s
the link bandwidth between receiver and router "1"	100Mb/s
the link bandwidth between router "0" and router "1" (entire network bottleneck)	1.5 Mb/s

A. Detection Threshold

According to the test model shown in Fig 6, set LDoS attack period T = 1.1s; pulse width l = 0.15s; attacks start from 20ths. Extract 5s long (500points) signals and update once every 5s. Reconstruction Mixed with normal TCP signals, and there are 1500 experiments in total. Distribution to the Reconstruction related experiments is shown in Fig 7.

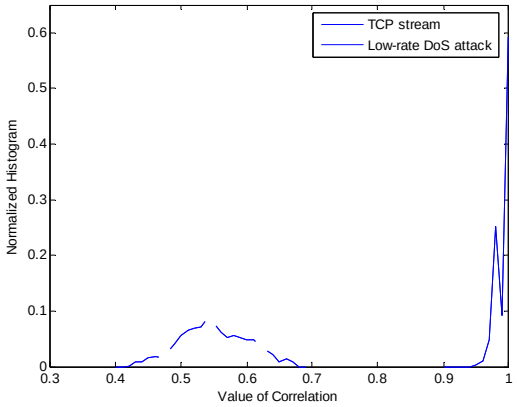

Figure 7. The normal TCP and T = 1.1s and l = 0.15s attack signal distribution comparison

Fig 7 indicates the distribution of cross correlation of TCP flow is closed to normal distribution and the mean of which is 0.54; distribution of cross correlation LDoS attacks are concentrated in a vicinity of 1. Therefore, the selecting of threshold should try equidistant between the mean of TCP flow correlation coefficient and 1. By setting different detection thresholds, the test results of False Positive Alarm Rate P_{FP} and False Negative Alarm Rate P_{FN} are shown in Table V.

TABLE V.
P_{FP} and P_{FN} for Different Threshold

Threshold / Detection	0.70	0.75	0.80
P_{FP}	0.2%	0.4%	0.8%
P_{FN}	1.1%	0.3%	0.2%

Because the detection probability, must trade-off

between P_{FP} and P_{FN}, we should select an appropriate threshold. The difficulty of this approach is to select the appropriate detection threshold, which needs statistical analysis to determine.

Therefore, we did a lot of experiment statistics, and got P_{FP} and P_{FN} under different thresholds, to determine the appropriate threshold.

Table V analysis showed that P_{FN} is high when threshold is selected at 0.70, and by taking threshold of 0.80, although P_{FP} dropped by 0.1%, but the P_{FN} increased significantly. Therefore, considering the P_{FN} and P_{FP}, we set detection threshold at 0.75. At this point, P_{FN} is less than 0.3%, P_{FP} is less than 0.4%, which can achieve higher detection performance.

B. The Performance of Detection Algorithm in Different Periods

To test P_{FP}, under different attacks period, we can also use the simulation network topology, the network configuration parameters are shown in Table IV. The period of LDoS attack were set at 1s, 1.2s and 1.5s; pulse width l=0.2s; attacks start from 20ths. Test the link we obtained the minimum Round-Trip Time (RTT) =132ms. Similar with the treatment of getting threshold, we extract 5s long (500 points) from LDoS attack flow and update once every 5s. With the normal TCP, the 1500 experiment, P_{FN} and P_{FP} test results are shown in Table VI.

TABLE VI.
CORRELATION DETECTION METHOD RESULTS UNDER DIFFERENT NETWORK ENVIRONMENT

Period / Conge. control	period 1s		period 1.2s		period 1.5s	
	P_{FN}	P_{FP}	P_{FN}	P_{FP}	P_{FN}	P_{FP}
Reno	0.3%	0.3%	0.3%	0.4%	0.3%	0.3%
NewReno	0.4%	0.4%	0.4%	0.3%	0.4%	0.4%
Sack	0.4%	0.4%	0.4%	0.4%	0.4%	0.4%

The experiment on P_{FN} and P_{FP} under different congestion control mechanism with a certain attack period have executed, test results show that the proposed detection algorithm for LDoS attacks reached lower P_{FN} and P_{FP}, which are less than 0.4%.

V. EXPERIMENTAL SETUP FOR NETWORK TEST

In the last section, the algorithm simulation experiments demonstrate the feasibility of the algorithm. In this section, to further test the algorithm, the actual network is used to test its practical effect and reliability.

A. Test Environment

The test environment for testing detection system is shown in Fig 8, where an attacker sends LDoS attacks. Normal user 1, 2 simulate to access the server's with normal traffic.

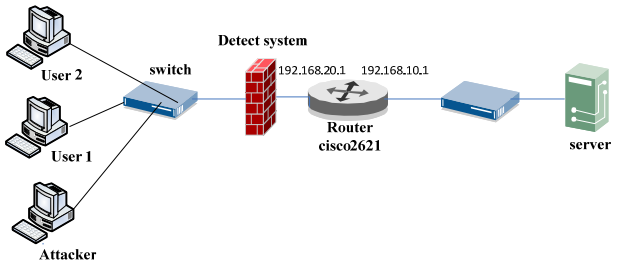

Figure 8 Test Environment

Linux-based server systems provide Web, Ftp service, and Web uses Apache, FTP uses Proftp. Other equipment is shown in Table VII.

B. Detection Performance

In the test, the normal user 1 gets a large file to download, attacker send LDoS attack. LDoS attack period=1.1s, pulse width l = 0.2s, attacks start from 20ths. The minimum RTT of the link equals 132ms. Extract 5s long (500 points) from composite flow, and update once every 5s. Signal with the normal TCP we got 200 experiments, P_{FN} and P_{FP} test results are shown in Table VIII, which shows that the detection method based on correlation has reached higher detection accuracy, and lower P_{FP} and P_{FN}.

TABLE VII.
TEST EQUIPMENT

No	IP address	operating system	CPU / memory	Usage
Attack	192.168.20.3	Fedora core9	P4 2.4G/512	send attack traffic
Server	192.168.10.3	Fedora core9	P4 2.4G/512	simulation services
Normal user 1	192.168.20.4	Fedora core9	P4 2.4G/512	simulate normal flow
Normal user 2	192.168.20.5	Windows XP	P4 2.4G/512	simulate normal flow

TABLE VIII.
DETECTION RATE IN THE ACTUAL NETWORK ENVIRONMENT

Congestion control / Period	Period 1s	
	P_{FN}	P_{FP}
Reno	0.5%	0.5%
NewReno	1%	0%

In this paper, the algorithm only use DFT once and one bit multiply, computational complexity is $O(n \operatorname{Log} n)$, and proposed the same algorithmic complexity as Yu Chen[12], but less than SUN. H. B[11] proposed for the computational complexity of dynamic time around DTW algorithm. This algorithm can be seen in the smaller case of computation and it obtained good detection results. DFT is also an important parameter to obtain LDoS attack, for the subsequent development of defense strategy and it provides a reasonable basis of the data.

VI. SUMMARY

In this paper, a detecting algorithm for the low-rate TCP attack (LDoS) s proposed. The waveform and

spectrum of LDoS attacks and normal TCP flow are analyzed in the time-domain and frequency-domain; using spectral intervals to period *T* and the using the first zero point to get pulse length *l* which are two important parameters, and reconstructed signal directly in the frequency domain; then bit multiplying signal reconstructed with original signal is used to detect LDoS attack.

Simulation results show that the detection algorithm has high detection performance and computational performance. Main features: (i) detection algorithm for this attack in different periods, the missing rate is very low (less than 0.5%), which makes the correlation detection algorithm can accurately detect attacks. At the same time, you can estimate the main characteristics of the attack - attack period T. This work lays a good foundation to the defense follow-up of attack; (ii) This detection algorithm for Reno, NewReno and Sack congestion control of several major false alarm rates are very low (less than 0.5%). And is widely used not only for the Reno algorithm by using the newer kernel algorithm, but also has a strong ability to adapt NewReno and Sack making a longer period of time in the future on the impact of normal network behavior is very small; (iii) the detection computational algorithm compared with the existing results, with the advantages of lower computational complexity.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their hard work. This work was supported in part by a grant from the National Natural Science Foundation of China (No. 61170328), and Natural Science Foundation of Tianjin (No. 12JCDZJC20900).

REFERENCES

[1] A. Kuzmanovic, E. W. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks- The Shrew vs. the Mice and Elephants [A]. Proceedings of ACM SIGCOMM 2003[C], Karlsruhe, Germany, Aug. 2003. Page(s):75-86.

[2] Cheng, C.-M., Kung, H., and Tan, K.-S., 2002. Use of spectral analysis in defense against DoS attacks. Proc. IEEE GLOBECOM, Taipei, China.

[3] Barford. P., Kline, J., Plonka, D., and Ron, A. 2002. A Signal Analysis of Network Traffic Anomalies. ACM Proc. Internet Measurement Workshop. Marseille, France, November Page(s): 6-8.

[4] Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo and Pedro García-Teodoro. Evaluation of a low-rate DoS attack against iterative servers. Computer Networks: The International Journal of Computer and Telecommunications Networking. 2007 51(4) : 1013-1030.

[5] Y. Zhang, Z. M. Mao, and J. Wang. Low-rate tcp-targeted dos attack disrupts internet routing. In Proc. 14th Annual Network & Distributed System Security Symposium, 2007.

[6] Xiapu Luo and Rocky K. C. Chang, Optimizing the Pulsing Denial-of-Service Attacks, Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)

[7] He Yanxiang, Cao Qiang, A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform, Software, Page(s): 2009.04.

[8] Qiao Zhu; Zhang Yizhi; Xie Chuiyi; Research and survey of low-rate Denial of Service attacks; 2011 13th International Conference on Advanced Communication Technology (ICACT), 2011: 1195 – 1198.

[9] Yang Xiang, Ke Li, and Wanlei Zhou; Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics; IEEE Transactions on Information Forensics and Security, 2011, 6(2): 426-437.

[10] Macia-Fernandez, G.; Diaz-Verdejo, J.E.; Garcia-Teodoro, P.; Mathematical Model for Low-Rate DoS Attacks Against Application Servers; IEEE Transactions on Information Forensics and Security; 2009, 4(3): 519 – 529.

[11] SUN, H. B., LUI, J. C. S., and YAU, D. K. Y. 2004. Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection. Proc. IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, October, Page(s): 5-8.

[12] Yu Chen, and Kai Hwang. Collaborative Detection and Filtering of Shrew DDoS Attacks Using Spectral Analysis. Journal of Parallel and Distributed Computing, special issue on Security in Grids and Distributed Systems, 2006, 66(9), Page(s): 1137-1151.

[13] Kumar, V.; Jayalekshmy, P.; Patra, G.; Thangavelu, R.; On remote exploitation of TCP sender for low-rate flooding denial-of-service attack; IEEE Communications Letters; 2009, 13(1): 46 – 48.

[14] Xiaodong Xu; Xiao Guo; Shirui Zhu; A queuing analysis for low-rate DoS attacks against application servers; 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010: 500 – 504.

[15] Zenghui Liu; Liguo Guan; Attack Simulation and Signature Extraction of Low-Rate DoS; 2010 Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI), 2010: 544 – 548.

[16] Changwang Zhang; Jianping Yin; Zhiping Cai; Weifeng Chen; RRED: robust RED algorithm to counter low-rate denial-of-service attacks; IEEE Communications Letters, 2010, 14(5) : 489 – 491.

[17] Efstathopoulos, P.; Practical study of a defense against low-rate TCP-targeted DoS attack; 2009. ICITST 2009. International Conference for Internet Technology and Secured Transactions, 2009: 1 – 6.

[18] Zhijun Wu; Limin Liu; Xingchen Liu; The approach of detecting LDoS attack based on correlative parameters; 2011 International Conference on Multimedia Technology (ICMT), 2011: 5587 – 5590.

Zhijun Wu was born in The Xinjiang Uygur Autonomous Region, China at May, 1965. He received the B.A. and M.A., degrees in electronics engineering from Xidian University, China, in 1988 and 1996 individually, and the Ph.D. degree in information security from Beijing University of Posts & Telecommunications, China, in 2004.

He is a professor in the department of Electronics & Information Engineering, Civil Aviation University of China. He is a supervisor of Ph.D candidates in the fields of Communication and Information System at Tianjin

University, China, and of Information Security at Beijing University of Posts & Telecommunications, China. From 2004 to 2006, he worked as a post-doctoral in China Education & Research Network Engineering Center, Tsinghua University, China, where he was involved in several research network security projects. His research was initially focused on Information Hiding but he is currently working on computer and network security, with special focus on denial of service attacks, intrusion detection, and reliable protocol design.

Minghua Wang was born in Shangqiu, Henan Province, China, at April, 1977. He received the M.A. and Ph.D degrees in information security from Beijing University of Posts & Telecommunications, China, in 2002 and 2005 individually.

He is the deputy director of China Computer Emergency Team (CNCERT), Center of Computer Network and Information Management of China. His research was initially focused on internet security but he is currently working on computer and network security, with special focus on network security management, and computer emergency response.

Haitao Zhang was born in Tianjin, China, in 1968. He received the B.A. and M.A. degrees in electronics & information engineering from Tianjin University, China, in 2004 and 2007 individually.

He is currently an Ph.D candidate in Tianjin University, China. His research area is network architecture and protocol.

Xingchen Liu was born in Shenyang, Liaoning Province, China, in 1986. He received the B.A. degrees in electronics & information engineering from Northeastern University, China, in 2008, and M.A., degrees in electronics & information engineering from Civil Aviation University of China, in 2011.

He is currently an associate engineer in SECWORLD Company, Beijing, China. His research was initially focused on network security but he is currently working on computer software, with special focus on computer management, and computer emergency response.