Hindawi
Security and Communication Networks
Volume 2021, Article ID 6694264, 14 pages
https://doi.org/10.1155/2021/6694264

Research Article

Coherent Detection of Synchronous Low-Rate DoS Attacks

Zhijun Wu,[1] **Yue Yin**,[2] **Guang Li**,[1] **and Meng Yue**[1]

[1]*School of Electronic Information & Automation, Civil Aviation University of China, Tianjin 300300, China*
[2]*School of Economics and Management, Civil Aviation University of China, Tianjin 300300, China*

Correspondence should be addressed to Zhijun Wu; caucwu@263.net

Received 15 October 2020; Revised 24 February 2021; Accepted 4 March 2021; Published 23 March 2021

Academic Editor: Mamoun Alazab

Low-rate denial-of-service (LDoS) attacks are characterized by low average rate and periodicity. Under certain conditions, the high concealment of LDoS attacks enables them to transfer the attack stream to the network without being detected at all before the end. In this article, plenty of LDoS attack traffic is spread to the victim end to detect LDoS attacks. Through experimental analysis, it is found that the attack pulses at the victim end have sequence correlation, so the coherence detection technology in spread spectrum communication is proposed to detect LDoS attacks. Therefore, this paper proposes an attack detection method based on coherent detection, which adopts bivariate cyclic convolution algorithm. Similar to the generation of receiving terminal phase dry detection code in spread spectrum communication, we construct a local detection sequence to complete the extraction of LDoS attack stream from the background traffic of the victim terminal, that is, the coherent detection of LDoS attacks. When predicting the features of an LDoS attack, how to construct the parameters of the detection sequence (such as period, pulse duration, amplitude, and so on) is very important. In this paper, we observe the correlation of LDoS attacks and use coherence detection to detect LDoS attacks. By comparing calculated cross-correlation values with designed double threshold rules, the existence of attacks can be determined. The simulation platform and experiments show that this method has high detection performance.

1. Introduction

Low-rate denial-of-service (LDoS) attacks were first detected in 2001 and first announced in 2003 [1].Unlike DoS attacks which send a great quantity of traffic in a row, LDoS attacks send attack traffic to victims on a regular basis. For this reason, the target victim is constantly running from the congestion to the recovery or from the recovery to the congestion, so that it cannot function normally and satisfactorily. And the existing DoS attack detection and defense methods are not suitable for detecting LDoS attacks with low average attack rate. Over the past 16 years, LDoS attacks have caused a lot of harm, such as reduced quality (RoQ) [2] and fraudulent resource consumption (FRC) [3]. At the same time, various variations have evolved, such as slow attack [4], stealth DoS [5], and tail [6]. LDoS attacks generally have three properties.

(i) Wreak havoc on the Internet: LDoS attacks take advantage of vulnerabilities in a particular protocol or system in a network to prevent the network from working properly, such as low resource utilization, unstable systems, or poor quality of service.

(ii) Low cost: compared with flooding Dos (FDoS) attack with large traffic, LDoS attack can be launched with very few attack sources, and its harm is almost the same as the former.

(iii) Low average attack rate: the transmission rate is lower than that of legitimate users, which makes the LDoS attack very stealthy and difficult to be detected.

The TCP-targeted LDoS attack described in this article exploits the retransmission vulnerability in the transmission control protocol (TCP), and its type of attack is a ROT-(retransmission timeout-) based LDoS attack. Figure 1 shows the attack model [1, 7], where T is the attack cycle and the attack duration is L, which represents the attack traffic transmission duration. R is the attack rate.

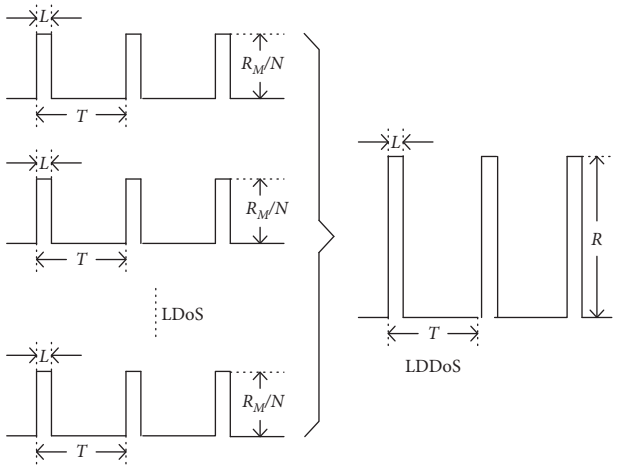


Figure 1: LDDoS attack schematic.

Macroscopically, LDDoS attack is a large attack pulse composed of many small distributed LDoS attack pulses. Assuming the LDDoS attack rate R_M is enough to make network congestion, the total attack pulse is N. From this, we get the average attack rate per LDoS, R_M/N.

As can be seen from Figure 1, when launching LDDoS attacks, each LDoS attacker needs to precisely control the pulse width L and attack period T because there is a certain relationship between them. Among them, the pulse width is directly related to the RTT (round-trip time), and attack cycle is also correlated with RTO to some extent. Therefore, the parameters of RTT and RTO both affect the time correlation of LDoS [8]. Thus, the small pulses of LDoS attack are highly correlated with each other.

According to the time characteristic of the LDoS pulse, LDoS attack detection based on RTO can be divided into synchronous detection and asynchronous detection. When an LDoS attack is initiated during a TCP retransmission, this exponential integer rate will inevitably cause TCP to remain in the retransmission timeout state. Therefore, synchronous attacks have the best effect. Next, we will focus on how to detect a synchronous LDoS attack.

The correlation of distributed LDoS pulse sequences is analyzed and a coherent detection method for LDoS attack is proposed. First, the time relationship of LDDoS attack pulses satisfying a specific target is studied. The detection sequence is constructed by cyclic convolution and coherence detection, and the correlation between it and the sampling sequence (sampled from network traffic) is obtained. In order to find the time correlation between each pulse, it is necessary to calculate the exact time when the attack pulse from different transmitting sources reaches the attack target (calculated by bivariate cyclic convolution algorithm). In addition, a new method is used to more accurately estimate the three characteristic parameters of an LDoS attack. Finally, the calculated cross-correlation values and the designed double threshold rule values are compared to detect LDoS attacks.

The major contributions of this paper are as follows:

(i) Considering LDoS attacks as pulse trains closely related to RTT, in this paper, the real-time cross-correlation between serial pulses is calculated to reveal the cross-correlation characteristics of signals. In order to better construct the detection sequence, we studied the relationship between signal cross-correlation and network traffic periodicity and designed and generated the detection sequence as coherent signal according to the relevant characteristics of LDoS attack pulses.

(ii) A coherent detection algorithm about LDoS attack is proposed. In this algorithm, cyclic convolution is used to calculate the exact time when the attack pulses of different transmission routes reach a specific target, and the cross-correlation between them is obtained. Then, we calculate the cross-correlation value between the LDoS attack pulse and the constructed detection sequence pulse. If the calculated result is greater than the threshold value, it will indicate that an LDoS attack has occurred. This new method uses a series of related operations to accurately detect LDoS attacks.

The related work is described in Section 2. In Section 3, a cross-correlation method for detecting LDoS attacks is proposed and the time-shifting relationship between attack pulses is discussed. Then, simulation is carried out in the experimental network environment to evaluate the performance of this method. In Sections 4 and 5, the experiment is introduced and theoretical analysis is carried out. Finally, practical issues and future work are discussed in Section 6.

2. Related Work

Kuzmanovic and Knightly primarily simulated a TCP-based LDoS attack [1]. Guirguis et al. [2] and Luo et al. [9], respectively, named this attack RoQ and PDoS. Although we use different names for these LDoS attacks, they all have a pattern of periodic pluses. Other platforms such as cloud computing, software-defined networks (SDNs), and information-centric networks (ICNs) also have LDoS attacks. FRC [3] is a low-speed attack for a long time. It takes advantage of on-demand pricing in cloud computing to expose cloud consumers to huge losses through deceptive use of cloud resources such as bandwidth.

There are two different LDoS attack implementation methods commonly found in SDN, that is, the low-speed stream table overflow attack [10] and the slow triad content addressable memory (TCAM) [11] exhaustion attack, which both exploit the vulnerability of timeout mechanism in open flow. That is, the attacker periodically installs malicious rules, which are always full and cannot install legitimate rules because the streamer will not uninstall any rules.

Now the research on LDoS attack detection has made plenty of achievements. Because it is difficult to detect LDoS attacks with low average rate using time domain statistical analysis, a new method of detecting LDoS attacks with frequency domain spectral analysis is proposed.

In terms of detection based on frequency domain, Chen et al. used spectrum analysis to identify DoS attacks [12]. The packet arrival number of the traffic is used as the signal with

fixed time interval to estimate the power spectral density of the signal. This prevents normal traffic from slowing down or stopping and reduces the rate of false positives. He et al. used wavelet multiscale analysis to convert network traffic into fifth-order wavelet coefficients based on the characteristics of different LDoS features [13]. The system is called wavelet analysis- (DSBWA-) based detection system, and the BP neural network after training is used for comprehensive diagnosis. Once an attack is detected, the system locates illegal attack pulses. Zhang et al. proposed a method of using adaptive nuclear principal component analysis (KPCA) to defend against LDoS attacks [14]. Based on the wavelet multiscale analysis method, this method reconstructs the low-frequency and high-frequency network traffic groups with continuous sampling, aiming to study a new method to reject invalid hypothesis or detect LDoS attack. Chen and Huang proposed a coordinated shrew DDoS attack detection method using normalized cumulative amplitude spectrum (NCAS) to calculate the distance between TCP traffic distribution curve and shrew traffic [15, 16]. In [15, 16], the authors proposed the use of collaborative detection filtering method and DSP technology to detect attacks hidden in network background traffic. The advantage of these two methods is that they reduce the burden of normal operation of routers, and the method of collaborative detection across multiple routers has strong robustness and more intelligent detection process.

In the time-domain detection method, Chen et al. combined Zigbee wireless sensor network and trust assessment to detect LDoS attacks in Zigbee network sensors [17]. Experiments show that the method is effective. Tripathi et al. used chi-square (χ^2) test under the HTTP/2 model to calculate the difference in profile between normal and abnormal traffic to detect attacks [18]. In literature [19], the authors used the routing fast packet matching method to detect LDoS attacks. Wu and Yue proposed an LDoS attack detection method based on Kalman filter [20], which first calculated the error between the one-step prediction result and the optimal estimation of the time series of LDoS attack flow, and then used the error as the standard to judge whether the attack occurred. Some scholars have also made achievements in the study of relevant detection methods to detect LDoS attacks. Wei et al. observed that during a DDoS attack, the packet transmission rate of a convergent response stream may have a linear relationship with other response streams and proposed a rank-dependent detection (RCD) algorithm to detect attacks by calculating the correlation coefficient between attack streams and comparing it with the set threshold [21]. Bhuyan et al. also proposed the partial rank correlation detection method (PRCD) [22]. The principle is the same as the rank-correlation-based detection method. They both calculate the correlation between attack traffic and no longer rely on the protocol type to identify the attack traffic. This detection method of sampling the traffic through the router and testing its correlation can not only effectively detect LDoS but also detect high-rate DoS attacks. The advantages of these two methods are low computational complexity and strong independence. In [23], Kaur and Agrawal proposed two methods, CUSUM and Shiryaev, to detect LDoS attacks. Both methods are generally classified as "fastest point-of-change detection QCD" [23]. Different from the attack traffic detection of inclusion in the mixed flow, the "fastest point-of-change detection QCD" method dynamically detects the abnormal change of attack traffic in the legitimate flow. The experimental results show that the method has high reliability and fast detection speed. Khan et al. presented an effective multi-layer traffic classification method by applying machine learning classifiers on features of network traffic [24]. They designed a framework based on decision trees which effectively detects P2P botnets by using machine learning classifiers, and a decision tree algorithm is applied for feature selection to extract the most relevant features and ignore the irrelevant features. Swarna et al. studied an effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in Internet of medical things (IoMT) architecture [25]. They used a deep neural network (DNN) to develop effective and efficient intrusion detection system (IDS) in the IoMT environment to classify and predict unforeseen cyberattacks.

We summarize the classic related work as shown in Table 1.

Many scholars have studied the application of autocorrelation detection in detecting abnormal network traffic [21, 22]. Studies show that malicious traffic will cause significant changes in network traffic characteristics, which will cause large fluctuations in the correlation coefficient of overlapping data. At this time, the autocorrelation detection method can effectively detect attacks. However, in another case, since LDoS attack is deeply hidden in large-scale network background traffic, it is difficult to observe the changes in network traffic characteristics, so autocorrelation detection is not applicable. Therefore, according to the strict temporal relation of LDoS attack, we will explore the correlation of LDoS attack pulse based on coherence detection and detect the attack.

3. Coherent Detection of LDoS Attacks

The idea of using coherence detection to detect LDoS attacks originates from communication systems. That is, if the LDoS attack pulse is seen as a useful signal, then the sender's noise is the network background traffic. In the transmission process, useful signals (attack flow) are hidden in the noise (background flow), and coherent detection is used to detect the attack flow with high concealment at the receiving end.

3.1. Principle of Coherent Detection. Figure 2 shows the basic principle of using coherent detection to detect LDoS attacks [26].

Figure 2 shows a direct spread spectrum system (DS-SS), in which the LDoS attack flows $x(n)$ (useful signal) are spread and hidden in normal TCP flows (background signal). A local generated correlation detection signal $y(n)$ is used to do correlation operation with the received network traffic $m(n)$ at victim end. Once $m(n)$ contains LDoS attacks, if $y(n)$ is correctly modeled, $x(n)$ will be detected correctly.

Table 1: Summary of related work.

	Detection method	Summary
Frequency-domain	NCAS [16]	Using normalized cumulative amplitude spectrum (NCAS) to calculate the distance between TCP traffic distribution curve and attack traffic
	Rank-dependent [21]	A rank-dependent detection (RCD) algorithm to detect attacks by calculating the correlation coefficient between attack streams and comparing it with the set threshold
Time-domain	Kalman filter [20]	Calculating the error between the one-step prediction result and the optimal estimation of the time series of LDoS attack flow and then using the error as the standard to judge whether the attack occurred
	Multilayer [24]	An effective multilayer traffic classification method by applying machine learning classifiers on features of network traffic
	Hybrid PCA-GWO [25]	Using a deep neural network (DNN) to develop effective and efficient intrusion detection system (IDS) in the IoMT environment to classify and predict unforeseen cyberattacks

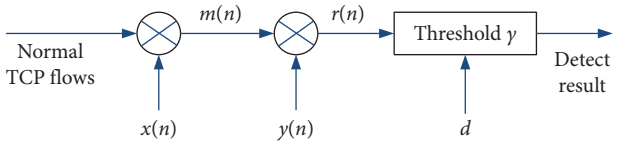


Figure 2: Principle of coherent detection of LDoS attacks.

In the principle of spread spectrum communication, Figure 2 is a correlated receive system, and $y(n)$ is called the coherent signal, which represents the coherence of $x(n)$ in special marks, such as attack rate R (amplitude), period T (frequency), and duration L (phase). This coherence means $x(n)$ and $y(n)$ have a particular relationship with a time variable. Therefore, according to the principle of spread spectrum communication, to retrieve a specific transmitted signal $x(n)$ from a communication channel, the user extended code $y(n)$ needs to be used to despread the total signal $m(n)$ in the channel, where $y(n)$ is the signal related to $x(n)$. In addition, when $y(n)$ are orthogonal to each other, the received signal can be associated with a specific user extended code, thus enhancing only the required user signals associated with the specific extended codes, while the remaining signal users are not enhanced.

3.2. Analysis of Network Traffic. A large number of research results show that LDoS attacks mainly utilize UDP protocol. Therefore, it is rational to use TCP stream and UDP stream as normal traffic and attack stream, respectively, in the analysis of this article. The UDP stream injected into the normal network environment by the attacker is regarded as the LDoS attack traffic. Thus, the legitimate UDP stream in the network is detected from the perspective of the receiver's noise detection.

Experienced researchers recommend setting the minimum repass timeout (minRTO) to 1 second for the generation of LDoS attacks. The reason for this is that RTT tends to be less than a second in milliseconds. Therefore, in the experiment and analysis, the attack duration (pulse width L) and the attack period T within a period were set to 200 ms and 1200 ms, respectively.

Normal network traffic is sampled every 10 ms. Time-domain statistics are shown in Figure 3 [27–29].

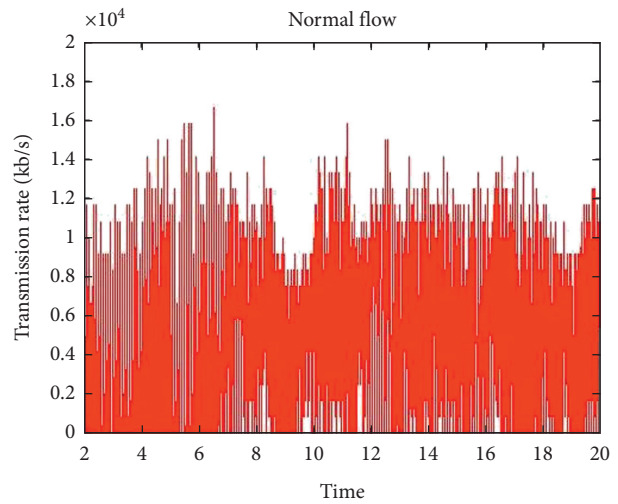


Figure 3: Normal TCP traffic.

The synchronous attack flow used in this article is shown in Figure 4 [27–29]. The pulses of the synchronized LDoS attack are kept at intervals of RTO, 2RTO, ..., 2^nRTO, respectively.

Figure 3 shows a direct view of the network traffic under real conditions. Comparing the nearly identical Figures 3 and 5 [27–29], it can be found that the attack flows are completely hidden in the legitimate traffic. Because of this, the traditional statistical average method in the time domain is difficult to detect LDoS attacks with high concealment.

The attack pulses in Figures 4 and 5 are both periodic square waves with the same attack rate R and pulse width L. Observation of Figures 4 and 5 shows that although LDoS attacks are completely hidden in network traffic, you can still see these attacks with temporal characteristics in Figure 5. This further confirms that there is a strict temporal correlation between synchronous LDoS attack pulses. Through above analysis, we proposes a bivariate cyclic convolution algorithm to distinguish the periodic signals with strict temporal relationship from the mixed network traffic, so as to detect LDoS attacks.

3.3. Two-Variable Cyclic Convolution Algorithm. Degree of correlation refers to evaluating the correlations observed

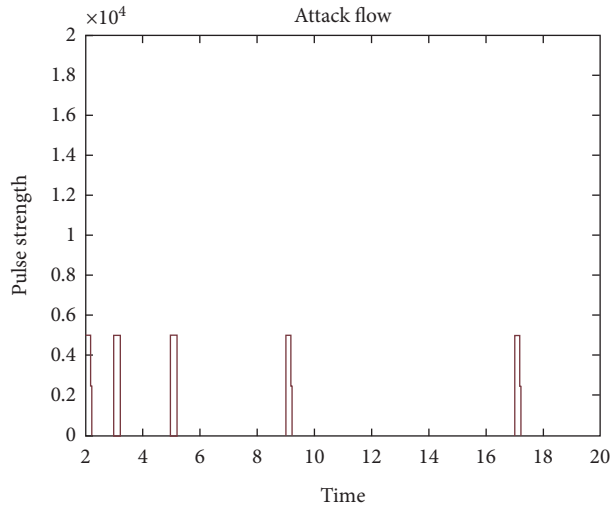


Figure 4: Synchronous LDoS attack flows.

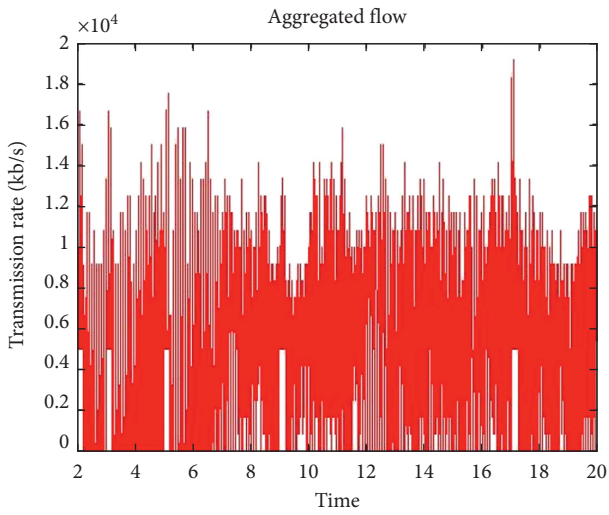


Figure 5: Mixed network traffic (containing synchronous LDoS attack flows).

between pairs of time sequences of LDoS attacks, i.e., it is to study the time evolution of these correlations.

Assuming that $x(n)$ and $y(n)$ represent two different LDoS attack sequences, X and Y are their distribution functions, respectively, where $n = 1, 2, \ldots, N-1$, the correlation coefficient between $x(n)$ and $y(n)$ is r_{xy}, and the calculation relationship is shown in the following formula [27–29]:

$$r_{xy} = \frac{\sum_n (x(n) - \overline{x})(y(n) - \overline{y})}{\sqrt{\sum_n (x(n) - \overline{x})^2 \sum_n (y(n) - \overline{y})^2}}, \quad (1)$$

where $\overline{x}$ and $\overline{y}$ are the mean values of sequences $x(n)$ and $y(n)$, respectively.

In the actual situation, there is a delay d among the LDoS attack traffic coming from various paths, so formula (1) is insufficient to describe the correlation between the two attack sequences. Therefore, in order to take the delay factor into account, the correlation $r(d)$ of the sequence is redefined, and the correlation between $x(n)$ and $y(n)$ is calculated by the following formula [27–29]:

$$r_{xy}(d) = \frac{\sum_n (x(n) - \overline{x})(y(n-d) - \overline{y})}{\sqrt{\sum_n (x(n) - \overline{x})^2 \sqrt{\sum_n (y(n-d) - \overline{y})^2}}}, \quad (2)$$

where $d = 0, \pm 1, \pm 2, \ldots, \pm (N-1)$.

The correlation between the sequences under different time delays is shown in Figure 6 [30–32].

For the two curves in the upper part of Figure 6, the X-axis represents the number of sampling points with a sample interval of 10 ms (for example, if the number of sampling points is 1200, it means 1200∗10 ms = 12000 ms). The Y-axis is the attack rate, and the unit is kb/s. For the single curve in the lower part of Figure 6, the X-axis d denotes the relative time shift of n in convolution computation. The step for time shift is 10 ms, it is consistent with the sampling interval (for example, if d is −100, it means −100∗10 ms = −1000 ms), and the Y-axis is the correlation coefficient without unit (note: in following similar figures, the X and Y axes are the same as defined).

As can be seen from Figure 6, $r(d)$ can embody the characteristics of LDoS attack. Therefore, attacks in TCP background traffic can be detected by extracting LDoS attack features (such as T and L) from the $r(d)$ sequence [33–35].

Through analyzing the sequence characteristics of LDoS attack sequences, it is found that the adjacent peak interval is T and the pulse width of $r(d)$ is $2L$. Here,

$$r(d) = \begin{cases} \text{maximum when } d = iT, & i = 0, 1, \ldots, \left(i < \dfrac{N}{T}\right), \\ \text{minimum when } d = iT \pm L, & i = 0, 1, \ldots, \left(i < \dfrac{N}{T}\right). \end{cases} \quad (3)$$

Figure 6 shows that the peak value of $r(d)$ sequence will decline with the increase of the delay $|d|$ between sequences. This will hinder the extraction of feature T and L to some extent. The operation of the molecular part of equation (2) is

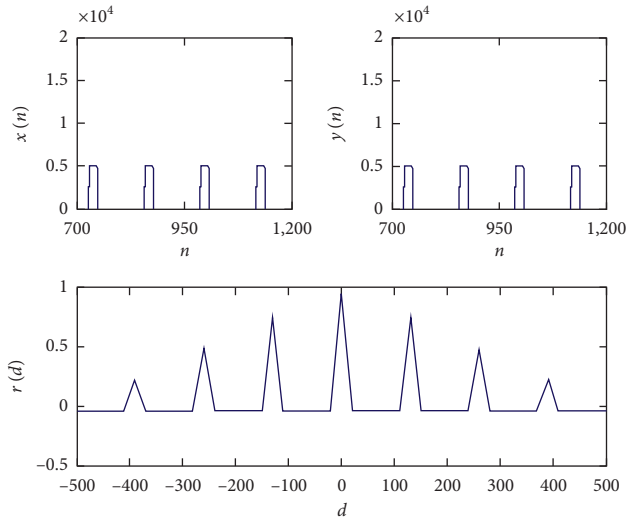


Figure 6: $r(d)$ for two great allies of LDoS attack sequences.

the cause of the attenuation caused by the linear convolution calculation.

Assuming that the length of the finitely long sequences $x(n)$ and $y(n)$ is N, their cyclic convolution is computed as follows. The purpose of using circular convolution instead of linear convolution is that the time shift of the sequence will cause the effect peak attenuation of the latter computation junction. The cyclic convolution calculation between two sequences is shown in the following formula [27–29]:

$$h(d) = x(n) \otimes y(n) = R_N(d) \sum_n x(n) * \tilde{y}(n-d), \tag{4}$$

where $\tilde{y}(n-d)$is the periodization of $y(n)$.

(i) Calculate the convolution of the finite sequence $x(n)$ (length N) and the infinite sequence $\tilde{y}(n-d)$ (period T) to get the infinite sequence $\tilde{h}(d)$ (period T).

(ii) The main value sequence $h(d)$ is calculated by $\tilde{h}(d)$ according to the relative time shift d.

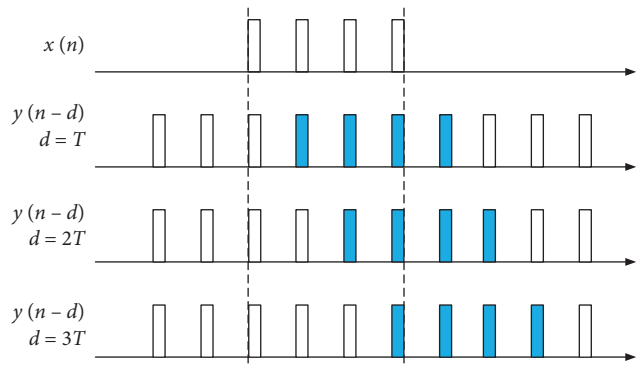


Figure 7: Calculation process of circular convolution.

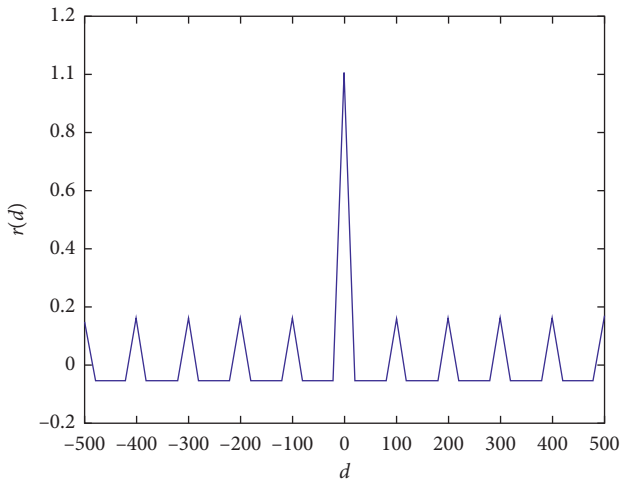


Figure 8: Sequence $r(d)$ for synchronous LDoS.

The circular convolution calculation is shown in Figure 7.

Two-variable cyclic convolution algorithm is defined as follows [27–29]:

$$r_{xy}(d) = \frac{(R_N(d) + R_N(-d-1))\sum_n (x(n) - \overline{x}) * (\tilde{y}(n-d) - \overline{y})}{\sqrt{\sum_n (x(n) - \overline{x})^2} \sqrt{\sum_n (y(n-d) - \overline{y})^2}}. \tag{5}$$

The great allies of sequences $x(n)$ and $y(n)$ and sequence $r(d)$ for synchronous attacks are calculated by using formula (5), and results are shown in Figure 8.

The bivariate cyclic convolution is calculated by formula (4). As can be seen from Figure 8, the sequence $r(d)$ calculated is a periodic sequence whose period is T and pulse width is L. Period T and pulse width L are two important features needed for the detection of LDoS attack. Extracting these two features from $r(d)$ is a crucial step for the detection of LDoS attack. This is also why the sequence $r(d)$ is computed using the bivariate cyclic convolution algorithm instead of linear convolution [36, 37].

3.4. LDoS Attack Detection by Using the Two-Variable Cyclic Convolution Algorithm. The low-rate nature of LDoS attack pulses in real network environments makes them well hidden from normal traffic (Figure 5). If the attack-added signature can be extracted using the bivariate circular convolution algorithm in the mixed stream, then the LDoS attack can be identified.

Let us say the mixing flow is $m(n)$, and we have [27–29]

$$m(n) = x(n) + c(n), \tag{6}$$

where $c(n)$ represents TCP traffic and its probability distribution pattern is the same as that of TCP flow.

According to formula (6) and Figure 2, the detection of LDoS attack from network traffic is the same as detecting $x(n)$ from $m(n)$. However, the high degree of concealment of $x(n)$ makes it difficult to be detected. In order to successfully detect $x(n)$ using the coherence method, we will construct the detection sequence $y(n)$, whose distribution is the same as $x(n)$. A detailed description of the sequence $y(n)$ is expanded in Section 3.5.

Coherent detection of mixed signal $m(n)$ was performed, and the result was [27–29]

$$r_{my} = \frac{\operatorname{cov}(M, Y)}{\sqrt{DM}\sqrt{DY}}, \tag{7}$$

where DM is obtained through statistical calculation of sampling values of mixed flows.

As can be seen from $M = X + C$, it is reasonable to consider that X and Z are independent of each other. Hence [27–29],

$$\operatorname{cov}(M, Y) = \operatorname{cov}(C, Y) + \operatorname{cov}(X, Y). \tag{8}$$

Since the rate, period, and duration of $y(n)$ are theoretically the same as $x(n)$, DX and DY are approximately equal.

Substituting formula (8) into formula (7), we have [27–29]

$$r_{my} = \frac{\sqrt{DX}}{\sqrt{DM}} \frac{\operatorname{cov}(X, Y)}{\sqrt{DX}\sqrt{DY}} + \frac{\sqrt{DC}}{\sqrt{DM}} \frac{\operatorname{cov}(C, Y)}{\sqrt{DC}\sqrt{DY}}. \tag{9}$$

A merge relationship is obtained as follows [27–29]:

$$r_{my} = \frac{\sqrt{DX}}{\sqrt{DM}} r_{xy} + \frac{\sqrt{DC}}{\sqrt{DM}} r_{zy}. \tag{10}$$

It is obvious that the degrees of correlation among C, X, and Y are very small. So, it is acceptable that

$$r_{cy} \approx 0. \tag{11}$$

As shown in Figure 9, the correlation between $c(n)$ and $y(n)$ is approximately zero through correlation calculation according to formula (11) [27–29].

Then,

$$r_{my} \approx \frac{\sqrt{DX}}{\sqrt{DM}} r_{xy}, \tag{12}$$

$$r_{my}(d) = k r_{xy}(d) + \sigma, \tag{13}$$

where

$$k \approx \frac{\sqrt{DX}}{\sqrt{DM}}, \quad \sigma \approx r_{hy}, \qquad r_{xy}(d) \approx \frac{1}{k} r_{my}(d). \tag{14}$$

According to formulas (12)~(14), $r_{xy}(d)$ can be obtained by calculating the cross-correlation between $y(n)$ and $m(n)$. By extracting the features related to LDoS attacks in $r_{xy}(d)$, the attacks will be detected.

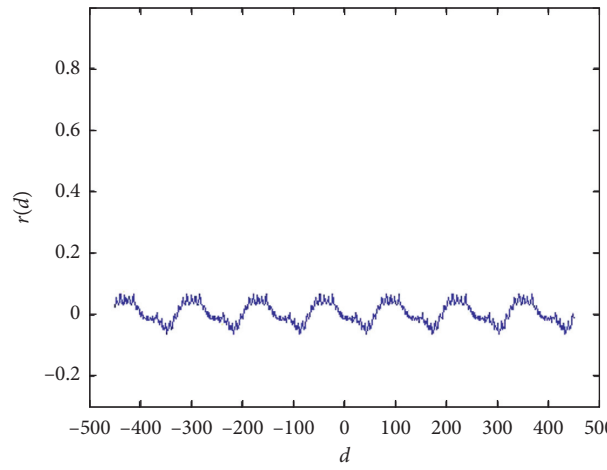


Figure 9: The correlation between $c(n)$ and $y(n)$.

After calculating $r_{xy}(d)$, design decision rules are needed to determine whether to inject an LDoS attack pulse into a mixed stream. The following is the definition of the characteristic parameter.

(i) Sample window N, a fixed time window: it should contain enough abnormal sample points.

(ii) Counter Co, statistical exception range.

(iii) Sensitivity coefficient, a judgment threshold: the correlation coefficient is abnormal when it exceeds the threshold value.

(iv) Threshold T_D, a decision tree threshold: determine if an LDoS attack exists.

Figure 10 shows the flow diagram of coherent detection method to detect LDoS attack.

The steps of the coherent detection method are described as follows.

(i) The traffic of the victim's last hop route is sampled at an interval of t seconds, and the $x(n)$ (length N) is obtained, with a sampling period of $t * N$ seconds.

(ii) Construct $y'(n)$(period estimation sequence) and estimate the attack period T by bivariate cyclic convolution algorithm.

(iii) The bivariate cyclic convolution algorithm is used to calculate the cross-correlation sequence $r_{xy}(d)$.

(iv) Solve for all values of $r_{xy}(d), d = 0, \pm 1, \pm 2, \ldots, \pm (N-1)$. The $r_{xy}(d)$ values are compared with the sensitivity coefficient γone by one. When $r_{xy}(d) > \gamma$, the counter Co will increase by 1; otherwise, the counter C will decrease by 1.

(v) Compare the value of counter Co with the decision threshold T_D. If $Co > T_D$, it indicates that $r_{xy}(d)$ is continuously greater than γ, which means that LDoS attack exists.

3.5. Detection Sequence Construction. LDoS attack sequences exist in the form of periodic square waves. The accurate estimation of the pulse amplitude R, pulse width L, and

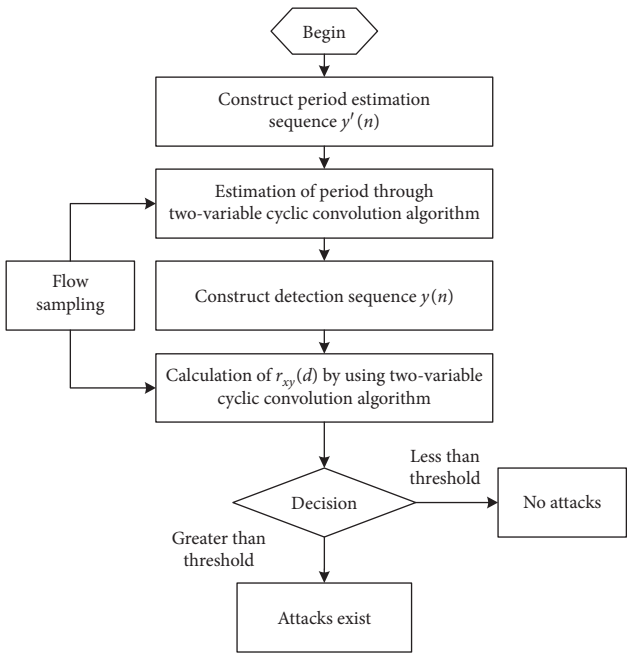


Figure 10: The flow diagram of coherent detection approach.

period T of the attack sequence is a key to determine whether $y(n)$ can guarantee the detection performance. The performance of detecting LDoS attacks depends on the error between the actual and estimated values.

From a detection point of view, the attack parameters are unpredictable. Therefore, constructing a detection sequence is an effective method. This ensures that the error in the parameter estimate is acceptable for the test results falling within this range.

3.5.1. The Pre-Estimation of R. The value of $y(n)$ is affected by the value of R. Let us say $C = nY$; then [27–29],

$$r_{xc} = \frac{\operatorname{cov}(X, C)}{\sqrt{DX}\sqrt{DC}} = \frac{n\operatorname{cov}(X, Y)}{\sqrt{DX}\sqrt{n^2 DY}} = r_{xy}. \tag{15}$$

From formula (15), we can see that the statistical estimation of R shows that the error $\delta_R(\delta_R = \widehat{R} - R)$ has small influence on the detection of LDoS attack. Therefore, the value of R is to take the bottleneck link bandwidth.

3.5.2. The Pre-Estimation of L. Next, we will analyze the effect of L estimation error on the $r(d)$ sequence waveform. According to the characteristics of LDoS attack waveform, a mathematical model is established, as shown in the following equation [27–29]:

$$x(n) = \begin{cases} R, & iT \le n < iT + L, \\ 0, & iT + L \le n < (i+1)T, \end{cases} \tag{16}$$

where $i = 0, 1, 2, \ldots$.

The correlation calculation formula of two sequences with the same parameters is shown in the following equation [27–29]:

$$r(d) = \frac{a\sum_{n=0}^{T}(x(n) - \overline{x})(y(n-d) - \overline{y})}{a\sqrt{\sum_{n=0}^{T}(x(n) - \overline{x})^2}\sqrt{\sum_{n=0}^{T}(y(n-d) - \overline{y})^2}} = \frac{\sum_{n=0}^{T}(x(n) - \overline{x})(y(n-d) - \overline{y})}{\sqrt{\sum_{n=0}^{T}(x(n) - \overline{x})^2}\sqrt{\sum_{n=0}^{T}(y(n-d) - \overline{y})^2}}, \tag{17}$$

where N is the size of the sampling window and a is the number of pulses in a sampling window.

According to equation (17), the influence of the mean values of $\overline{x}$ and $\overline{y}$ on the correlation between $x(n)$ and $y(n)$ can be ignored. The mean values of $\overline{x}$ and $\overline{y}$ are set to zero in order to simplify the calculation. Finally, the maximum value about $r(d)$ is 1.

In the actual situation, it is difficult to accurately estimate RTT, but since L is closely related to RTT, the estimation of L may be biased in the process of building $y(n)$ ($\widehat{L}$ is the estimated pulse width of $y(n)$ and it is not equal to the true value of L). Through comparative analysis, the optimal estimate of $\widehat{L}_{\text{opt}}$ can be determined [27–29].

When $\widehat{L} > L$, we have [27–29]

$$\max r(d) = \frac{LR^2}{\sqrt{LR^2}\sqrt{\widehat{L}R^2}} = \frac{L}{\sqrt{L\widehat{L}}}. \tag{18}$$

When $\widehat{L} < L$, we have [27–29]

$$\max r(d) = \frac{\widehat{L}R^2}{\sqrt{LR^2}\sqrt{\widehat{L}R^2}} = \frac{\widehat{L}}{\sqrt{L\widehat{L}}}. \tag{19}$$

Let δ_L be the estimation error of $L(\delta_L = \widehat{L} - L)$. Formula (20) analyzes the influence of δ_L on $r(d)$ peak value [27–29].

$$\max r(d) = \begin{cases} \dfrac{L}{\sqrt{L(L + \delta_L)}}, & \text{when } \delta_L > 0, \\ \dfrac{L + \delta_L}{\sqrt{L(L + \delta_L)}}. & \text{when } \delta_L < 0. \end{cases} \tag{20}$$

When $L = 200$ ms, the relation between $\max r(d)$ and various δ_L is calculated by using formula (20). The result is shown in Figure 11.

In Figure 11, it is shown that the theoretical analysis result is similar to those of experiments.

In real networks, RTT is usually less than 100 ms, and the duration of a single LDoS attack pulse is typically 2 to 3 times that of RTT. When an LDoS attack pulse lasts long enough, it can be considered a traditional DoS attack. Therefore, in order to make a reasonable analysis of LDoS attack, the value range of L is controlled within 1 to 3 times the RTT value when building $y(n)$. It can be seen that the theoretical error of L is usually 2 to 3 times the RTT.

Therefore, we can come to the conclusion that when the estimated error δ_L is within the acceptable range, the influence of L on $r(d)$ and the performance of the detection method are not significant.

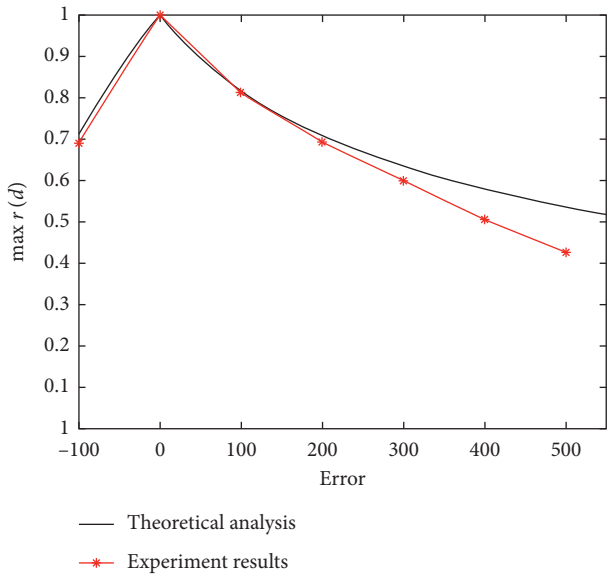


Figure 11: The effect of δ_L on max r (d).

3.5.3. The Pre-Estimation of T. The attack model of LDoS is periodic square wave. Therefore, T must be accurately estimated when constructing $y(n)$.

The cycles of synchronous LDoS attacks increase exponentially with RTO as the low number. Therefore, the pulse interval of $y(n)$ should be set to RTO, 2RTO, 4RTO, . . ., 2^nRTO according to the target network.

Usually, there is an estimated error of the period, which is defined as $\delta_T = T - \widehat{T}$, but it is reasonable. When δ_T changes in a small range, it has no obvious influence on the periodic characteristics, and its main influence is concentrated on max $r(d)$.

4. Experiment and Result Analysis

In this paper, a real simulation network is established in the NS-2 platform for experiments, and relevant experiments are carried out to test the algorithm for detecting LDoS attacks.

4.1. Experimental Environment Setting. Figure 12 shows the simulation experiment network of NS-2 platform [27–29].

In the network model shown in Figure 12, user 1 is the legitimate user, which is the host transmitting the noise stream $m'(n)$.The attacker launches a pulse attack with an attack rate of 5 Mbps, a pulse width of 200 ms, and a cycle of 1.2 s, and the attack traffic is aggregated at router A. The bottleneck link bandwidth between router A and router B is 15 mbps. Users 1, 9, and 10 form a normal TCP link together with routers A and B. The traffic of legitimate user 3 to legitimate user 8 is the background traffic of LDoS attack. In order to ensure that background traffic and attack traffic are independent from each other, legitimate users (users 3–8 and 11) do not establish legitimate TCP links through attack path, for example from A to B, but the link is established through a path where there is no attack, such as from A to C.

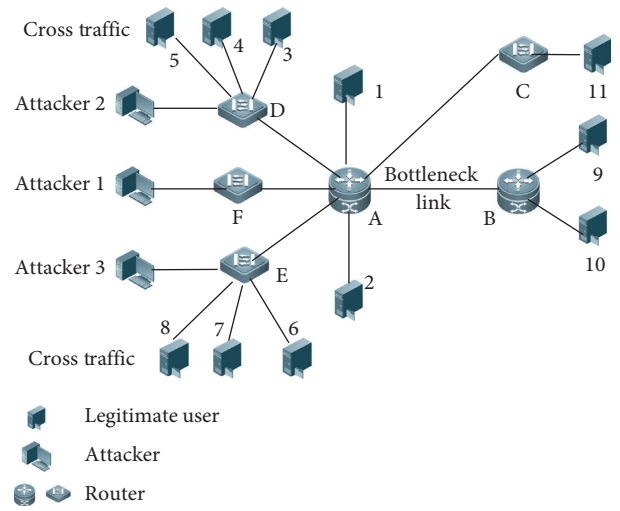


Figure 12: Experimental network environment.

Take the traffic of Attacker 1 as the benchmark traffic for analysis. Attackers 2 and 3 launch LDoS attacks that mix with normal network background traffic. Legitimate users 2 and 11 establish normal TCP connections through routers A and C. In this case, no attack traffic passes through the legitimate user 2 because it will not be subject to LDoS attacks. Therefore, in order to make the experimental environment more complex, the flow of user 2 was used as the noise signal in the detection process.

4.2. Synchronous Attack Detection. As shown in Figure 12, coherent detection measures are deployed on user 1. The traffic on the link between user 1 and router A is sampled (at a 10 ms interval). The sampled waveforms of background traffic (noise) $m'(n)$ (no attack) and mixed flows $m(n)$ (with attack) are shown in Figures 13 and 14.

Calculate the variance of $m(n)$ and $y(n)$, respectively, and we have the results that $DX = DY = 1.1887 * 10^6$, $DM = 2.0476 * 10^7$, and $k = \sqrt{DX}/\sqrt{DM} = 0.2409$. The correlation $r_{m'y}(d)$ between two sequences is calculated according to formula (13). Putting value k into formula (14), we get $r_{xy}(d)$, as shown in Figure 15.

The cross-correlation sequence $r_{my}(d)$ was calculated by formula (13). Putting value k into formula (14), we get $r_{xy}(d)$, as shown in Figure 16. From Figure 16, we can see that $r_{xy}(d)$ has a distinct peak. This is a typical attack pulse correlation sequence. Therefore, there is a high correlation between $m(n)$ and $y(n)$. Comparing Figure 8 with Figure 16, we can see that the synchronous cross-correlation sequence in Figure 16 is very close to that in Figure 8.

We find that if the number of experiments reaches a certain number, the distribution of peaks of related sequences roughly follows the normal distribution through the central limit theorem [15, 16].

Assuming that the peak distributions of the correlation sequences with no attack and with attack are $N(\mu_0, \sigma_0^2)$ and $N(\mu_1, \sigma_1^2)$, respectively, the probability density functions (PDFs) corresponding to them are shown in formulas (21) and (22) [27–29].

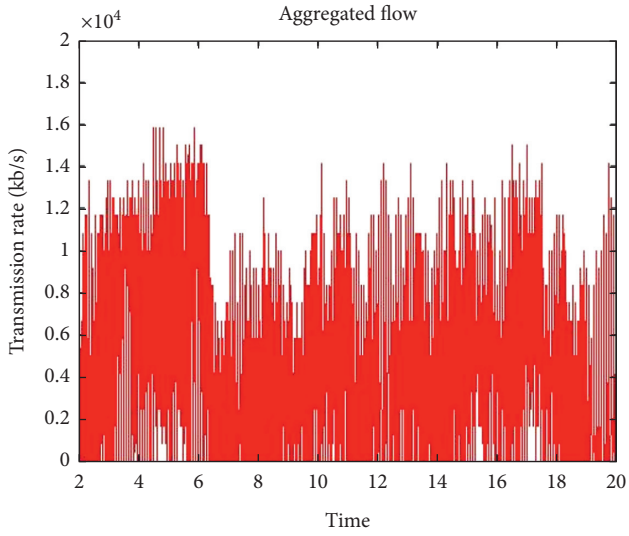


Figure 13: The noise $m'(n)$.

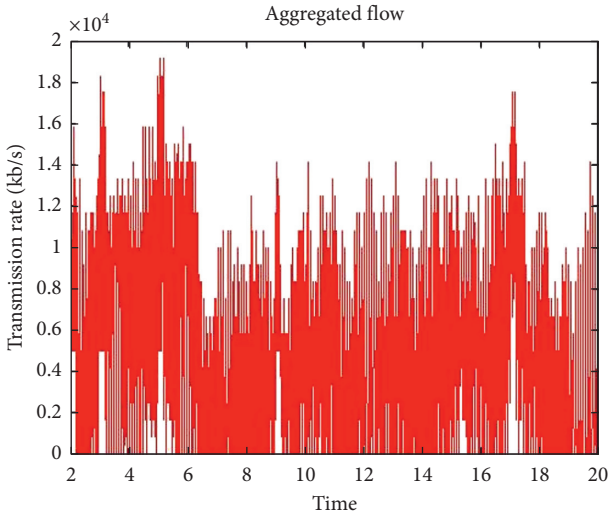


Figure 14: The mixed flows $m(n)$.

$$f_0(x) = \frac{1}{\sqrt{2\pi}\sigma_0}\exp\left\{-\frac{(x-\mu_0)^2}{2\sigma_0^2}\right\}, \quad (21)$$

$$f_1(x) = \frac{1}{\sqrt{2\pi}\sigma_1}\exp\left\{-\frac{(x-\mu_1)^2}{2\sigma_1^2}\right\}. \quad (22)$$

The mean value and variance of the peak distribution of correlation sequences were calculated by statistical method after 100 experiments. The results are as follows.

$\mu_0 = 0.4213, \sigma_0 = 0.1846$, without attacks.

$\mu_1 = 0.9315, \sigma_1 = 0.0829$, with attacks.

The probability density functions with and without attacks are shown in Figure 17, where the X-axis is the correlation coefficient without units.

Table 2 shows the experimental results of different sensitivity coefficient γ.

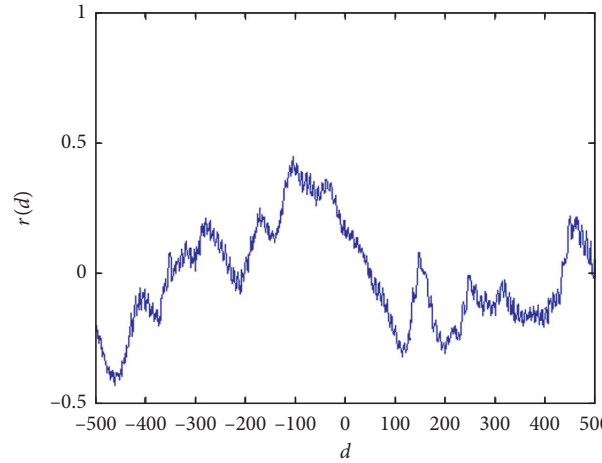


Figure 15: $r_{xy}(d)$ based on noise flow $m'(n)$.

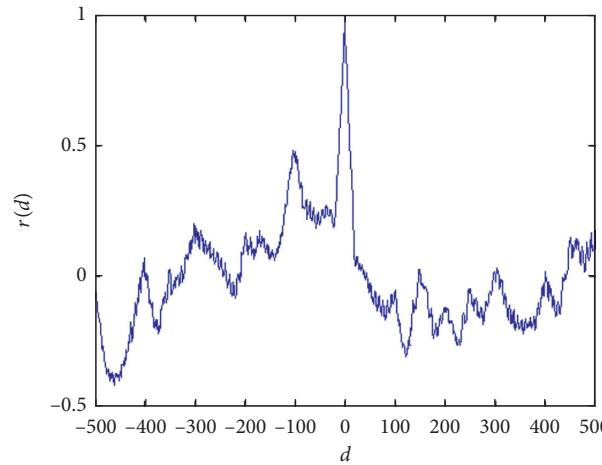


Figure 16: $r_{xy}(d)$ based on the mixed flow $m(n)$.

From Table 2, we can come to a conclusion that the detection performance is better when the sensitivity coefficient is within the range of 0.7–0.8.

4.3. Analysis of Experimental Results. The proposed method is compared with other DoS attack detection methods. From Table 3, we can see that the detection performance of this method is very close to that of the rank-dependent DDoS detection method [21] and parameter-dependent frequency-domain LDoS attack detection method [38]. By comparing this method with the normalized cumulative amplitude spectral density method (NCAS) [16], the detection rate of the coherent detection method used in this paper increases by about 5% and the detection error rate increases by about 2%.

5. Experiment and Performance Analysis

In order to test performance of two-variable circular convolution detection algorithm, a real experimental network was established.

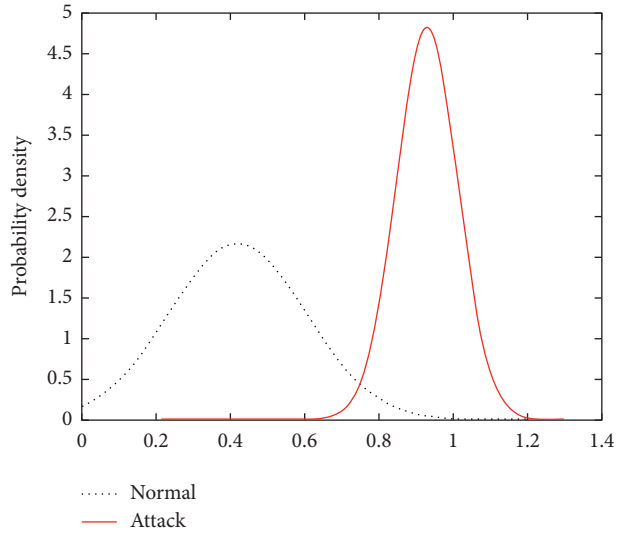


Figure 17: PDF for synchronous attack detection.

Table 2: Detection performance for synchronization attack under different γ.

Sensitivity coefficient γ	Detection rate P_D	False negative rate P_{FN}	False positive rate P_{FP}
0.60	100.00	0.00	18.75
0.70	99.78	0.22	7.65
0.75	98.78	1.22	4.46
0.80	95.03	4.97	2.44

Table 3: Performance comparison of different detection methods.

Detection method	Detection rate P_D	False negative rate P_{FN}	False positive rate P_{FP}	Space complexity	Time complexity
DDoS detection method based on cross-correlation [20]	99.82	0.18	0.10	$O(n \log_2 n)$	$O(n \log_2 n)$
Normalized cumulative amplitude spectrums (NCAS) [15]	94.80	5.00	10.0	$O(n)$	$O(n^2)$
Cross-correlation detection method in frequency [33]	99.50	0.50	0.50	$O(n^2)$	$O(n^2)$
Adaptive multilayer botnet detection [23]	98.70	1.30	3.00	$O(n)$	$O(n^2)$
Feature engineering for DNN using hybrid PCA-GWO [24]	99.80	0.20	0.00	$O(n^2)$	$O(n^2)$
Proposed coherent approach (LDoS (T, L, R) = (1100 ms, 200 ms, 10 Mbps))	99.80	0.22	7.65	$O(n \log_2 n)$	$O(n \log_2 n)$

5.1. Experimental Network Environment. The network topology used in this article is shown in Figure 12. The testbed network is consistent with the working principle and process configuration of the NS-2 platform. The testbed network consists of two Cisco2911 routers and four 100 M switches.

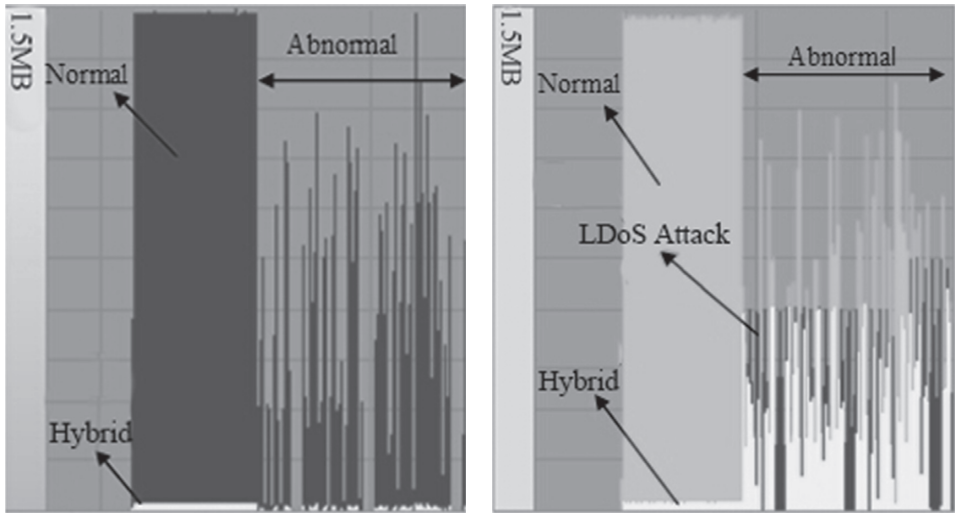
The LDoS generation tool used in this paper is the Linux TCP kernel source code [39], and the UDP-based software is used to generate LDoS attacks. LDoS attacks can be described as triple LDoS(T, L, R) = (1000 ms, 200 ms, 10 Mbps). The duration of the experiment is 1000 seconds, with attacks starting at 400 seconds and ending at 600 seconds.

This experiment uses UDP-based software to test FTP throughput. In the test scenario shown in Figure 12, the victim (the node connected to B and C) will provide an FTP service, and the host (the legitimate node connected to D and E) will download files from the FTP server. If FTP traffic is in a stable state, then start the LDoS attack at LDoS(T, L, R) = (1000 ms, 200 ms, 10 Mbps).

From the analysis of Figures 18(a) and 18(b) [27–29, 39, 40], it can be seen that when the attack did not start, the download traffic recorded by the host (**Normal**) and the upload traffic recorded by the FTP server (**Normal**) were approximately equal. In Figure 18(a), Hybrid represents the client download or server upload traffic, and the exception represents the presence of attack traffic.

When LDDoS attack exists, the fluctuation of download traffic and upload traffic is large and the traffic is lower than the normal level. In Figure 18(b), **Attack** represents the attack flow initiated by botnets, whose attack rate is even slower than the transfer rate of FTP [27–29, 39, 40].

5.2. LDoS Attack Detection Experiments. When experimenting in a test bed network, both synchronous and asynchronous LDoS attacks are injected into the network to make the simulation more realistic. Since the experimental process and steps on the test bed are exactly the same as



(a) (b)

Figure 18: Traffic with LDDoS attacks. (a) Download. (b) Upload.

those on the NS-2, the results are given directly by skipping the steps.

The correlation between $c(n)$ and $y(n)$ is shown in Figure 19. It can be seen from Figure 19 that the cross-correlation sequence of $c(n)$ and $y(n)$ has apparent periodic characteristics.

Figure 20 shows the calculation results of the cross-correlation sequence $r_{my}(d)$.

It is found in Figure 20 that the attack period T and attack pulse time L of LDoS attack can be estimated by observing the cross-correlation of sequences.

The performance of this method is tested on a real testbed network. The statistical analysis results after 100 experiments are shown in Table 4.

According to Table 4, P_D, P_{FN}, and P_{FP} are 96.33%, 3.67%, and 5.97%, respectively, when γ is 0.55. This is where the algorithm has the best performance.

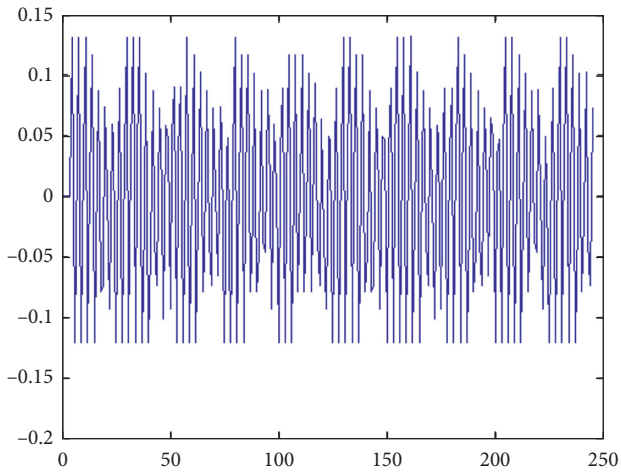


Figure 19: The correlation between $c(n)$ and $y(n)$.

5.3. Result Analysis. By testing the performance of this method on different experimental platforms, we find that when $\gamma = 0.7$, the NS-2 simulation platform has the best detection performance, and when the testbed network has the best detection performance, γ is 0.55. This is because the network environment of the simulation platform is simpler than the real network environment.

The performance and complexity of this method are compared with other methods, and the results are shown in Table 5.

In the NCAS method [16], P_D is 87.9%, P_{FP} is 15c.7%, and P_{FN} is 11.6%. The space complexity and time complexity are $O(n)$ and $O(n^2)$, respectively. P_D, P_{FP}, and P_{FN} of Kalman filter [20] are 88.7%, 11.9%, and 9.8%, respectively. The space complexity is $O(n^2)$, and the time complexity is the same as NCAS.

By comparing and analyzing the data in Table 5, we can draw the conclusion that P_D of LDoS attack detected by the coherent detection used in this article under the testbed

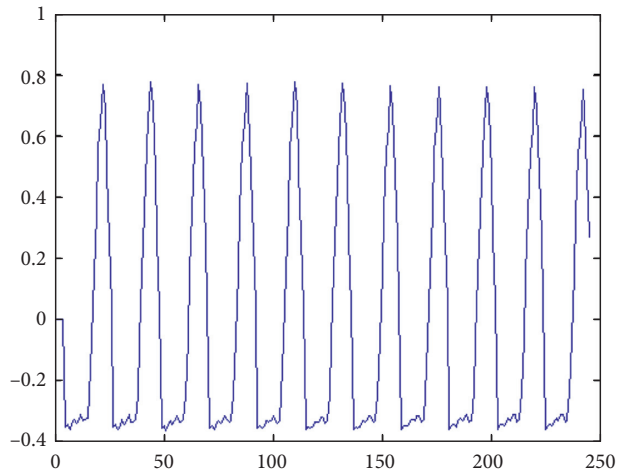


Figure 20: The cross-correlation sequence $r_{my}(d)$.

Table 4: Detection performance of real testbed network.

Sensitivity coefficient γ	Detection rate P_D (%)	False negative rate P_{FN} (%)	False positive rate P_{FP} (%)
0.55	96.33	3.67	5.97
0.60	91.94	8.06	4.06
0.65	84.42	15.58	2.68
0.70	73.33	26.67	1.72
0.75	59.23	40.77	1.06

Table 5: Comparison of different detection methods.

Items					
Method	Detection performance			Complexity	
	P_D (%)	P_{FN} (%)	P_{FP} (%)	Space complexity	Time complexity
NCAS [16]	87.9	11.6	15.7	$O(n)$	$O(n^2)$
Kalman [20]	88.7	9.8	11.9	$O(n^2)$	$O(n^2)$
Coherent	91.4	8.06	4.06	$O(n \log_2 n)$	$O(n \log_2 n)$

network is 91.4%, which is 3.5% higher than that of NCAS and 2.7% higher than that of Kalman. Although the spatial complexity of coherence detection is high, its time complexity is low.

6. Conclusion

This paper first analyzes the periodicity of LDoS attack traffic. The difference between time domain and frequency domain of network traffic in the presence and absence of LDoS attack is studied. Then, an algorithm for detecting LDoS attacks, namely, correlation detection algorithm based on cyclic convolution, is proposed. First, it is important to construct the detection sequence and design the decision rules. Then, the aperiodic single-pulse prediction techniques are used to extract three important parameters from the correlation sequence: attack period T, pulse width L, and attack rate R. Finally, the correlation between the detection sequence and the sampling sequence is calculated to judge whether the LDoS attack exists. Through a series of data statistics and comparative analysis, it can be observed that the algorithm we have proposed has a good performance. In order to get closer to the real network environment, this paper also designs the construction method of LDoS attack model.

Future research work can be concentrated in two aspects. On the one hand, researchers can reveal new vulnerabilities that may be exploited by LDoS attacks in new situations, such as LDoS attacks in the cloud, LDoS attacks in ICN, and LDoS attacks in SDN. On the other hand, researchers can explore new LDoS attack detection and mitigation methods. For example, SDN technology, elastic mechanism, and game theory have important value in mitigation of LDoS.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew versus the mice and elephants," in *Proceedings of the ACM SIGCOMM Computer Communication Review*, pp. 75–86, Kalrushe, Germany, August 2003.

[2] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the transients of adaptation for RoQ attacks on Internet resources," in *Proceedings of the IEEE International Conference on Network Protocols*, pp. 184–195, Berlin, Germany, October 2004.

[3] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of fraudulent resource consumption in the cloud," in *Proceedings of the IEEE International Conference on Cloud Computing*, pp. 99–106, Honolulu, HI, USA, September 2012.

[4] E. Cambiaso, G. Papaleo, G. Chiola et al., "Slow DoS attacks: definition and categorisation," *International Journal of Trust Management in Computing and Communications*, vol. 3, no. 20, pp. 300–319, 2013.

[5] M. Ficco and M. Rak, "Stealthy denial of service strategy in cloud computing," *IEEE Transactions on Cloud Computing*, vol. 3, no. 1, pp. 80–94, 2015.

[6] H. S. Shan, Q. Y. Wang, and C. Pu, "Tail attacks on web applications," in *Proceedings of the ACM Conference Computer Communications Security*, pp. 1725–1739, Dallas, TX, USA, November 2017.

[7] Z. Wu, L. Zhang, and M. Yue, "Low-rate DoS attacks detection based on network multifractal," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 5, pp. 559–567, 2016.

[8] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014.

[9] X. Luo, E. Chan, and R. Chang, "Detecting pulsing denial-of-service attacks with nondeterministic attack intervals," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, no. 1, pp. 1–13, 2009.

[10] J. Cao, M. Xu, Q. Li, K. Sun, Y. Yang, and J. Zheng, "Disrupting SDN via the data plane: a low-rate flow table overflow attack," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 01, pp. 356–376, 2018.

[11] A. P. Tulio, G. D. Yuri, and E. F. Iguatemi, "Slow TCAM exhaustion DDoS attack," *IFIP Advances in Information and Communication Technology*, vol. 2, pp. 17–31, 2017.

[12] C. M. Cheng, H. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks," in *Proceedings of the IEEE Globecom*, vol. 3, pp. 2143–2148, Taipei, China, September 2002.

[13] Y. X. He, Q. Cao, T. Liu et al., "A low-rate DoS detection method based on feature extraction using wavelet transform," *Journal of Software*, vol. 20, no. 4, pp. 930–941, 2009.

[14] X. Y. Zhang, Z. J. Wu, J. S. Chen, and M. Yue, "An adaptive KPCA approach for detecting LDoS attack," *International Journal of Communication Systems*, vol. 30, no. 4, pp. 1–11, 2017.

[15] Y. Chen, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," *Journal of Parallel and Distributed Computing*, vol. 66, no. 9, pp. 1137–1151, 2006.

[16] Y. Hwang, K. Hwang, and Y. K. Kwok, "Filtering of shrew DDoS attacks in frequency domain," in *Proceedings of the IEEE Conference on Local Computer Networks (LCN 2005)*, pp. 786–793, Sydney, Australia, November 2005.

[17] H. S. Chen, C. X. Meng, Z. G. Shan, and Z. C. Fu, "Detection approach in ZigBee wireless sensor network by combining Hilbert-Huang transformation and trust evaluation," *IEEE Access*, vol. 7, pp. 32853–32866, 2019.

[18] N. Tripathi and N. Hubballi, "Slow rate denial of service attacks against HTTP/2 and detection," *Computers & Security*, vol. 72, pp. 255–272, 2018.

[19] Y. Hayashi, Y. Jia, and S. Nishiyama, "Method for detecting low-rate attacks on basis of burst-state duration using quick packet-matching function," in *Proceedings of the 2017 IEEE International Symposium on Local and Metropolitan Area Networks*, pp. 1-2, Osaka, Japan, June 2017.

[20] Z. J. Wu and M. Yue, "Detection of LDDoS attack based on kalman filtering," *Acta electronica sinica*, vol. 36, no. 8, pp. 1590–1594, 2008.

[21] W. Wei, F. Chen, Y. Xia, and G. Jin, "A rank correlation based detection against distributed reflection DoS attacks," *IEEE Communications Letters*, vol. 17, no. 1, pp. 173–175, 2013.

[22] M. H. Bhuyan, A. Kalwar, A. Goswami, D. K. Bhattacharyya, and J. K. Kalita, "Low-rate and high-rate distributed dos attack detection using partial rank correlation," in *Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies*, pp. 706–710, Gwalior, MP, India, April 2015.

[23] G. Kaur and P. Agrawal, "Detection of ldos attacks using variant of cusum and shiryaev - robertss algorithm," in *Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 363–369, Himachal Pradesh, India, December 2016.

[24] R. U. Khan, X. Zhang, R. Kumar et al., "An adaptive multi-layer botnet detection technique using machine learning classifiers," *Applied Sciences*, vol. 9, no. 2375, pp. 2–22, 2019.

[25] R. M. Swarna Priya, M. Parimala, T. R. SrinivasKoppu, C. LalChowdhary, and MamounAlazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Computer Communications*, vol. 160, pp. 139–149, 2020.

[26] E. Cambiaso, G. Papaleo, G. Chiola, and M. Aiello, "Designing and modeling the slow next DoS attack," *Advances in Intelligent Systems and Computing*, vol. 369, pp. 249–259, 2015.

[27] Z.-j. Wu, L. I. Guang, and M. YUE, "Detecting low-rate DoS attacks based on signal cross-correlation," *Acta Electronica Sinica*, vol. 42, no. 09, pp. 1760–1766, 2014.

[28] L. I. Guang, *Detecting LDoS Attacks Based on Signal Cross-Correlation*, Civil Aviation University of China, Tianjin, China, 2014.

[29] Z. Wu, Q. Pan, M. Yue, and L. Liu, "Sequence alignment detection of TCP-targeted synchronous low-rate DoS attacks," *Computer Networks*, vol. 152, pp. 64–77, 2019.

[30] L. Garg, E. Chukwu, N. Nasser, C. Chakraborty, and G. Garg, "Anonymity preserving IoT-based COVID-19 and other infectious disease contact tracing model," *IEEE Access*, vol. 8, pp. 159402–159414, 2020.

[31] Y. Shelke and C. Chakraborty, "Augmented reality and virtual reality transforming spinal imaging landscape: a feasibility study," *IEEE Computer Graphics and Applications*, 2020.

[32] M. Numan, F. Subhan, W. Z. Khan et al., "A systematic review on clone node detection in static wireless sensor networks," *IEEE Access*, vol. 8, pp. 65450–65461, 2020.

[33] M. Tang, M. Alazab, and Y. Luo, "Big data for cybersecurity: vulnerability disclosure trends and dependencies," *IEEE Transactions on Big Data*, vol. 5, no. 3, pp. 635–647, 2019.

[34] M. Mittal, C. Iwendi, S. Khan, and A. R Javed, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg–Marquardt neural network and gated recurrent unit for intrusion detection system," *Transactions on Emerging Telecommunications Technologies*, 2020.

[35] A. Rehman Javed, Z. Jalil, S. Abbas, and X. Liu, "Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. e4088, 2020.

[36] M. Ali, M. Asad, and A. Rehman Javed, "Robust early stage botnet detection using machine learning," in *Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1–6, Islamabad, Pakistan, March 2020.

[37] S. U. Rehman, M. Khaliq, S. I. Imtiaz et al., "Distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU)," *Future Generation Computer Systems*, vol. 118, pp. 453–466, 2021.

[38] X. Y. Dang, Z. T. Liu, B. L. Li, and Q. Li, "Noncoherent multiple symbol detection for continuous phase modulation in physical-layer network coding," *Journal of Electronics & Information Technology*, vol. 38, no. 04, pp. 877–884, 2016.

[39] W. Edward, "Knightly, aleksandar kuzmanovic, shrew attack linux code," 2004.

[40] Z. Wu and Y. Meng, "Research on the performance of low-rate DoS attack," *Journal on Communications*, vol. 29, no. 6, pp. 87–94, 2008.