photonics

Article

Low-Rate Denial-of-Service Attack Detection: Defense Strategy Based on Spectral Estimation for CV-QKD

Enze Dai [1], Duan Huang [2] and Ling Zhang [1,*]

[1] School of Automation, Central South University, Changsha 410083, China; 8207191105@csu.edu.cn
[2] School of Computer Science and Engineering, Central South University, Changsha 410083, China; duanhuang@csu.edu.cn
* Correspondence: lingzhang2019@csu.edu.cn

Abstract: Although continuous-variable quantum key distribution (CVQKD) systems have unconditional security in theory, there are still many cyber attacking strategies proposed that exploit the loopholes of hardware devices and algorithms. At present, few studies have focused on attacks using algorithm vulnerabilities. The low-rate denial-of-service (LDoS) attack is precisely an algorithm-loophole based hacking strategy, which attacks by manipulating a channel's transmittance T. In this paper, we take advantage of the feature that the power spectral density (PSD) of LDoS attacks in low frequency band is higher than normal traffic's to detect whether there are LDoS attacks. We put forward a detection method based on the Bartlett spectral estimation approach and discuss its feasibility from two aspects, the estimation consistency and the detection accuracy. Our experiment results demonstrate that the method can effectively detect LDoS attacks and maintain the consistency of estimation. In addition, compared with the traditional method based on the wavelet transform and Hurst index estimations, our method has higher detection accuracy and stronger pertinence. We anticipate our method may provide an insight into how to detect an LDoS attack in a CVQKD system.

Keywords: CVQKD; LDoS attack; spectral estimation

Citation: Dai, E.; Huang, D.; Zhang, L. Low-Rate Denial-of-Service Attack Detection: Defense Strategy Based on Spectral Estimation for CV-QKD. *Photonics* **2022**, *9*, 365. https://doi.org/10.3390/photonics9060365

Received: 10 April 2022
Accepted: 17 May 2022
Published: 24 May 2022

1. Introduction

Humans have been giving great importance to cryptography since ancient times. With the development of computer technology, a massive amount of sensitive data called for more advanced encryption techniques to ensure security. Key distribution is the crucial issue of encryption techniques, and there have been many key distribution methods, such as RSA algorithms [1] of asymmetric encryption. However, all classical encryption techniques based on high computational complexity are decipherable and are unable to detect the disclosure of keys [2]. Thankfully, the progress of quantum key distribution (QKD) makes it possible for two remote communicating parties to share secure keys through an unsafe quantum channel controlled by an eavesdropper [3,4], since the Heisenberg uncertainty principle [5] and no-cloning theorem [6] of quantum mechanics guarantee QKD's unconditional information security and the detectability of eavesdroppers. Compared with discrete-variable (DV)QKD, continuous-variable (CV)QKD has the merits of low-cost implementation for it is compatible with the current telecom networks and components such as homodyne and heterodyne detectors and has other advantages [7,8]. Specifically, the Gaussian-modulated coherent state (GMCS) protocol, the most developed CVQKD protocol, has been proven secure against collective attacks and coherent attacks theoratically [9–13].

By contrast, the imperfection of hardware devices and algorithms lead to security loopholes in CVQKD systems.

A great deal of research has put forward various practical attack strategies by exploiting hardware defects, and examples include the wavelength attack, the calibration attack, the local oscillator (LO) fluctuation attack and the saturation attack [14–18]. P. Huang et al. proposed an asynchronous countermeasure strategy without structural modifications of the conventional CVQKD scheme to defend against the above-mentioned attacks [19]. In stark contrast, there are few studies on the practical security analysis of the algorithms. Y. Li et al. proposed a denial-of-service (DoS) attack strategy aimed at the parameter estimation method in the communication process [20]. Under the DoS attack, eavesdroppers' slight manipulation of the channel transmittance results in great underestimation of the secure transmittance distance, and subsequently the two sides of communication consider the channel insecure and thus terminate the communication process.

The low-rate denial-of-service (LDoS) attack is a more stealthy type of DoS attacks because it sends short-time but high-rate burst attack traffic periodically to maintain the average attack rate low, so as to escape from detection [21]. The LDoS attack, in the narrow sense, is TCP protocol oriented, while in GMCS protocol, the LDoS attack can be considered as short-time, high-rate and periodic burst attack on the parameter estimation. According to the periodicity of LDoS attacks and the characteristic differences between periodic signals and aperiodic signals in the frequency domain, the rule that the power spectral density (PSD) of the LDoS attack traffic in low frequency band is higher than normal is then obtained [22]. On the basis of this rule, the issue of LDoS attacks detection transforms into the spectral estimation of the stochastic sequence.

In this paper, to detect LDoS attacks and guarantee the consistency of spectral estimation, we proposed a detection method based on Bartlett's spectral estimation approach (average periodogram). Spectral estimation is the issue of estimating the power spectrum of a stochastic process given partial data, usually only a finite number of samples of the autocorrelation function [23]. It detects whether the network traffic contains LDoS attack traffic by estimating the power spectral density in low frequency band. There are two broad categories of approaches in spectral estimation, the classical approaches (non-parametric approaches) and the modern approaches (parametric model-based approaches). The former consists mainly of the periodogram and its improved approaches, including data windowed periodogram, average periodogram, etc., and the typical models of the latter are autoregressive (AR), moving average (MA) and autoregressive moving average (ARMA) models [24–26]. The structure of the paper is as follows. Firstly, the strategy of LDoS attacks based on the GMCS protocol is briefly introduced. Secondly, we discuss three different spectral estimation approaches, autocorrelation estimation with rectangular window, periodogram with Bartlett window and the Bartlett approach (average periodogram), and then analyze their estimation results. Finally, we carry out the related experiences and it is demonstrated that the proposed method can effectively detect LDoS attacks.

2. System Description and Attack Detection

2.1. Attack Strategy against GMCS Protocol

In the GMCS protocol, Alice sends Bob a chain of coherent states $|x + ip\rangle$ where the quadratures (x, p) are randomly chosen from a Gaussian distribution of mean zero and variance $V_A N_0$, where N_0 means the shot noise variance. Then, Bob randomly chooses to measure either x or p by homodyne detection and announces overtly to Alice which one he measured, so that she discards the irrelevant data. After several rounds of exchanges, Alice and Bob will share a set of correlated Gaussian variables, which are employed for further secret key extractions by way of post-processing procedures, including parameter estimation, reverse reconciliation and amplification. The above-mentioned process can be seen in Figure 1. To maintain consistency, the reconciliation protocol has to be unidirectional (from Bob to Alice) [27–29]. As LDoS attacks mainly aim at the process of parameter estimation, we will introduce the principle of parameter estimation methods of GMCS protocol at length in the following part.

Some parameters in parameter estimation are determined by the instruments' characteristic and measured beforehand. The detector efficiency η and the electrical noise V_{el} of Bob's end are relatively stable in experimental repetition, thus we measure them in advance and treat them as constants during the communication. The shot noise can be expressed as $N_0 = K_{N_0} E_{LO}$, where K_{N_0} is a parameter that needs to be calibrated before communication, and E_{LO} is the power of the local oscillator.

Others, including channel transmittance T and channel excess noise ε, demand estimation in real time. Exploiting this loophole, Eve manipulates the parameters to cause estimation deviation till the communicating parties think the channel insecure and close it. In this way, an attack succeeds. In the GMCS protocol, some shared Gaussian variables are disclosed to estimate the channel transmittance and channel excess noise; others are used for key extraction and we generally estimate the above-mentioned parameters by means of statistical methods. In the classical parameter estimation method, Alice and Bob's data are associated with each other through the linear model $y = tx + z$, where $t = \sqrt{T} \in \mathbb{R}$ and z follows a centered normal distribution with unknown variance $\sigma^2 = 1 + T\varepsilon$.

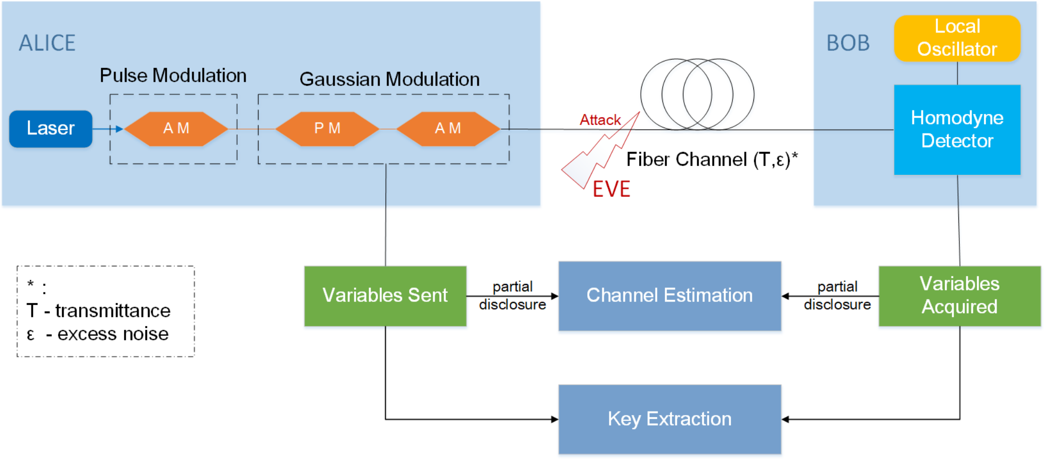


Figure 1. In the GMCS CVQKD protocol, Alice encodes the secret key information by modulating the quadratures x and p of coherent states with independent Gaussian distributions and sends them to Bob through an insecure channel controlled by Eve. Next, the homodyne detector on Bob's end obtains the transmitted information. Then, some of the shared Gaussian variables are disclosed for channel estimation. Lastly, shared Gaussian variables are used to extract keys.

According to the above linear model, adopting the maximum likelihood estimation method and neglecting the finite-size effect of limited data, we are able to estimate the value of the channel transmittance T and the channel excess noise ε as below

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2} \tag{1}$$

$$\hat{\sigma}^2 = \frac{1}{m} \sum_{i=1}^{m} (y_i - \hat{t} x_i)^2, \tag{2}$$

where $\hat{t}$ is the estimated value of $\sqrt{T}$, and $\hat{\sigma}^2$ is the estimated value of $1 + T\varepsilon$. Furthermore, $\hat{t}$ and $\hat{\sigma}^2$ comply with the normal distribution and chi-square distribution, respectively,

$$\hat{t} \sim \mathcal{N}(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_i^2}) \quad \hat{\sigma}^2 \sim \mathcal{X}^2(m-1), \tag{3}$$

where t and σ^2 are the true values of the parameters $\sqrt{T}$ and $1 + T\varepsilon$, respectively.

Using Equations (1) and (2), we can estimate the value of T and ε convincingly . The authors of [30] proposed a method under the condition of considering the finite-size effect, while for the sake of simplicity, we do not consider the effect as it only degrades the precision of results. In the rest of this section, we will analyze the impact caused by Eve's arbitrary manipulations in channel parameters under the framework of this parameter estimation method.

In the optical fiber transmission system, we generally treat the channel's transmittance as a constant when making parameter estimations. Nonetheless, in consideration of Eve's control of the channel, she can intentionally modify the characteristics of the channel, which will lead to deviations to parameter estimations. Such manipulation is a so-called denial-of-service attack, since it can make the actual secure channel perceived as insecure by two parties and lead to the communication discontinuance [20]. Now, we begin with Equations (1) and (2) to analyze the effects of DoS attacks.

As mentioned before, channel transmittance T and excess noise ε are the two parameters we lay stress on. We assume that Alice modulates X and Bob measures Y, where X is a cosine signal and Y is an X-distorted signal that is presented in the phase deviation and linear noise. Next, due to the phase compensation technique and the linear noise mean value of 0, the following formula can be obtained

$$\hat{t} = E(\sqrt{T}), \tag{4}$$

where we highlight the conclusion. From Equation (4) we can draw the following conclusions: if the transmittance T is a constant, the estimated $\hat{t}$ equals to the true value $\sqrt{T}$, while if not, there will be deviations in our estimation.

Similarly, by using the equivalent relations in Equation (4) and equation $V_A = E(X^2)$, we can rewrite Equation (2)

$$\hat{\sigma}^2 = E(T)\varepsilon + 1 + E(T)V_A - (E(\sqrt{T}))^2 V_A. \tag{5}$$

Likewise, if the transmittance T is a constant, the estimated $\hat{\sigma}^2$ equals to the true value $1 + T\varepsilon$, while if not, $E(T)V_A \neq (E(\sqrt{T}))^2 V_A$ which will bring about inaccuracy in excess noise estimation.

Through the above brief analysis, Eve's DoS attack strategy, namely making the parameter estimation deviates from the true value by manipulating the channel transmittance T, has been demonstrated. For the detailed derivation process, refer to Appendix A. As for the LDoS attack, it is one type of DoS attacks and conforms to their basic principles, characterized by the good quality of concealment.

2.2. Detection Principle of LDoS Attack by Spectral Estimation

Though Y. Li et al. suggested a countermeasure based on post-selection to suppress the DoS attack [20], there is still a vacancy in the detection of LDoS attacks. Y. Chen et al. analyzed the PSD distribution over the frequency domain to find that LDoS attacks are mainly distributed in the low-frequency band rather than broadband distribution of the normal traffic [22]. Hence, we can use such feature to effectively detect an LDoS attack and the flow chart of the detection method is shown in Figure 2.

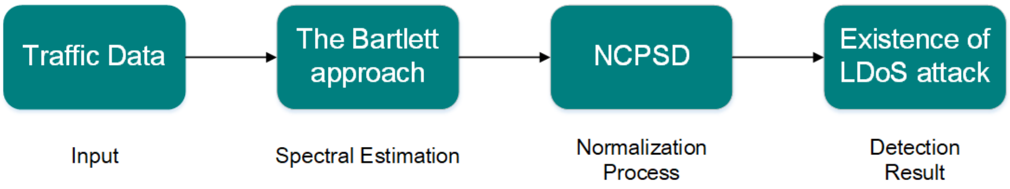


Figure 2. The flow chart of LDoS attack detection. The Bartlett approach is used to obtain the PSD of traffic data, and then normalized cumulative power spectrum density (NCPSD) is gained after the normalization process. Judge whether there is an attack by analyzing the distribution of NCPSD in low frequency domain at last.

The power spectrum gives us an insight into the characteristics of the generalized stationary stochastic process in frequency domain, such as periodicity, peak position, frequency range, etc. The power spectrum of zero-mean generalized stationary stochastic process $\{x_n\}$ is defined as

$$S_x(e^{jw}) \equiv \sum_{m=-\infty}^{+\infty} R_x(m)e^{-jwm}, \tag{6}$$

namely Wiener–Khinchin theorem, where the autocorrelation sequence $R_x(m)$ is defined as

$$\begin{aligned} R_x(m) &\equiv E[x(n)x^*(n+m)] \\ &\equiv \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-N}^{N} x(n)x^*(n+m), \end{aligned} \tag{7}$$

where N means the length of sample data. It is noteworthy that Equations (6) and (7) are only of theoretical significance for reasons as follows: first, there is no way to collect infinite data, and second, there is always noise mixed in our data. In any event, the spectral estimation of $\{x_n\}$ is then transformed into the estimation of its autocorrelation sequence $R_x(m)$. With regard to the stochastic process whose mean value is not equal to 0, its power spectrum will not change after eliminating the mean value, and thus only discussing the case where the mean value is 0 does not lose the conclusions' generality [31]. In this section, we are going to compare three spectral estimation approaches from the perspective of consistency of estimations and discuss whether they are unbiased estimations.

2.2.1. Autocorrelation Estimation with Rectangular Window

Since it is impossible to get unlimited data, we can intercept a certain length of data by using the window function. Here, the rectangular window is our first consideration. We assume that $x(n)$ is a sampling sequence of stochastic process $\{x_n\}$ and we intercept a segment of $x(n)$ as

$$x_N(n) = w_R(n)x(n) = \begin{cases} x(n), & 0 \le n \le N-1 \\ 0, & else, \end{cases} \tag{8}$$

where $w_R(n)$ is a rectangular window of length N

$$w_R(n) = \begin{cases} 1, & 0 \le n \le N-1 \\ 0, & else. \end{cases} \tag{9}$$

When the length of sample data is N, the autocorrelation $R_x(m)$ is estimated as

$$\hat{R}_x(m) = \begin{cases} \sum\limits_{n=-\infty}^{+\infty} \dfrac{x_N(n)x_N^*(n+m)}{N-\mid m\mid}, \mid m \mid\le N-1 \\ 0, \quad else, \end{cases} \tag{10}$$

which can be simplified as

$$\hat{R}_x(m) = \begin{cases} \sum\limits_{n=0}^{N-1-|m|} \dfrac{x(n)x^*(n+m)}{N-\mid m\mid}, \mid m \mid\le N-1 \\ 0, \quad else. \end{cases} \tag{11}$$

Next, we find the mathematical expectation of $\hat{R}_x(m)$

$$\begin{aligned} E[\hat{R}_x(m)] &= \sum_{n=0}^{N-1-|m|} \frac{E[x(n)x^*(n+m)]}{N-\mid m\mid} \\ &= \sum_{n=0}^{N-1-|m|} \frac{R_x(m)}{N-\mid m\mid} = R_x(m), \end{aligned} \tag{12}$$

which has values only if $\mid m \mid\le N-1$ and 0 in other cases. According to Equation (12), when $\hat{R}_x(m)$ is used as the estimate of $R_x(m)$, estimation bias $B = R_x(m) - E[\hat{R}_x(m)] = 0$, namely $\hat{R}_x(m)$ is the unbiased estimation. By the estimation of $R_x(m)$, the estimation of the power spectrum ($\hat{P}_x(\omega)$) can be obtained

$$\hat{P}_x(\omega) = \sum_{m=-(N-1)}^{N-1} \hat{R}_x(m)e^{-jwm}, \tag{13}$$

whose mathematical expectation is the convolution of frequency spectrum and rectangular window spectrum. When $N \to \infty$, the mean value is

$$\begin{aligned} \lim_{N\to\infty} E[\hat{P}_x(\omega)] &= \sum_{m=-\infty}^{+\infty} w_R(m)R_x(m)e^{-jwm} \\ &= \sum_{m=-\infty}^{+\infty} R_x(m)e^{-jwm} = P_x(\omega), \end{aligned} \tag{14}$$

from which $P_x(\omega)$ is the true value of power spectrum and we can see that $\hat{P}_x(\omega)$ is the asymptotic unbiased estimation, as when $N \to \infty$, $w_R(m) \to 1$.

However, the Fourier transform of rectangular window function

$$\begin{aligned} W_R(e^{jw}) &= \sum_{n=-(N-1)}^{N-1} w_R(n)e^{-jwn} \\ &= \sum_{n=-(N-1)}^{N-1} e^{-jwn} = \frac{sin(\frac{w(2N-1)}{2})}{sin(\frac{w}{2})} \end{aligned} \tag{15}$$

shows that it has values in negative number field which may lead to $\hat{P}_x(\omega)$ less than zero subsequently. As there is no physics meaning if $\hat{P}_x(\omega) < 0$, the autocorrelation estimation with rectangular window is not used to estimate the power spectrum generally.

2.2.2. Periodogram with Bartlett Window

Due to the defects of rectangular window that some results are inconsistent with physics meaning and the estimation error is comparatively large when the value of $\mid m \mid$ is close to N, we consider using Bartlett window to optimize,

$$w_B(m) = \begin{cases} 1 - \dfrac{\mid m \mid}{N}, & \mid m \mid \leq N-1 \\ 0, & else. \end{cases} \tag{16}$$

Thus, we get another estimate of $R_x(m)$

$$\hat{R}'_x(m) = \begin{cases} \displaystyle\sum_{n=0}^{N-1-|m|} \frac{x(n)x^*(n+m)}{N}, \mid m \mid \leq N-1 \\ 0, \quad else, \end{cases} \tag{17}$$

whose link with Equation (10) can be expressed as $\hat{R}'_x m = (N - \mid m \mid)\hat{R}_x(m)/N$. Therefore, the mathematical expectation of $\hat{R}'_x(m)$ can be easily obtained

$$\begin{aligned} E[\hat{R}'_x(m)] &= E[\frac{N- \mid m \mid}{N}\hat{R}_x(m)] \\ &= \frac{N- \mid m \mid}{N}R_x(m), \end{aligned} \tag{18}$$

which means $\hat{R}'_x(m)$ is the biased estimate of $R_x(m)$ because estimation bias $B = R_x(m) - \hat{R}'_x(m) = \mid m \mid R_x(m)/N$ is not equal to 0. While because of

$$\begin{aligned}\lim_{N\to\infty} E[R'_x(m)] &= \lim_{N\to\infty}\frac{N-\mid m\mid}{N}R_x(m)\\ &= R_x(m),\end{aligned} \tag{19}$$

hence the autocorrelation estimation based on Bartlett window is the asymptotic unbiased estimation.

More importantly, the Fourier transform of Bartlett window can be regarded as the conjugated product of the rectangular window's Fourier transform

$$\begin{aligned}W_B(e^{jw}) &= W_R(e^{jw})W_R^*(e^{jw})\\ &= \frac{1}{N}\left(\frac{sin(\frac{wN}{2})}{sin(\frac{w}{2})}\right)^2,\end{aligned} \tag{20}$$

which ensures the power spectrum estimation obtained later is greater than 0, thus being consistent with the physics meaning. Similarly, according to Equation (13), the mathematical expectation of power spectrum estimation can be deduced as

$$\begin{aligned}E[\hat{P}_x(\omega)] &= E[\sum_{m=-\infty}^{+\infty}\hat{R}_x(m)e^{-jwm}]\\ &= \sum_{m=-(N-1)}^{N-1} w_B(m)R_x(m)e^{-jwm}\\ &= \frac{1}{2\pi}W_B(\omega)*P_x(\omega)\\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi}W_B(\xi)P_x(\omega-\xi)d\xi,\end{aligned} \tag{21}$$

which demonstrates its mean value is the convolution of frequency spectrum and Bartlett window spectrum. When $N \to \infty$, referring to Equation (14), it is not hard to draw that $E[\hat{P}_x(\omega)] \to P_x(\omega)$.

Another indicator to measure estimation performance is estimate consistency, which can be represented by estimation variance

$$Var[\hat{P}_x(\omega)] \approx P_x^2\left[1+\left(\frac{sin(\omega N)}{Nsin\omega}\right)^2\right], \tag{22}$$

from which we can find spectral estimation with Bartlett window is not a consistent estimation. Based on the above analyses, it is appropriate to make spectral estimations by using autocorrelation estimations with Bartlett window, though the results are not consistent.

Regrettably, the approach based on Equation (6) is still not simple enough, and then the so-called direct calculation approach of periodogram is proposed,

$$\begin{aligned}&\hat{P}_x(\omega) = \textstyle\sum_{m=-\infty}^{+\infty}\hat{R}'_x(m)e^{-jwm}\\ &= \tfrac{1}{N}\textstyle\sum_{m=-\infty}^{+\infty}\sum_{n=-\infty}^{+\infty}x_N(n+m)x_N^*(n)e^{-jwm}\\ &\overset{n+m=k}{=} \tfrac{1}{N}\textstyle\sum_{n=-\infty}^{+\infty}\sum_{k=-\infty}^{+\infty}x_N(k)e^{-jwk}x_N^*(n)e^{jwn}\\ &= \tfrac{1}{N}\left|\textstyle\sum_{n=0}^{N-1}x(n)e^{-jwn}\right|^2\\ &= \tfrac{1}{N}\left|X_N(e^{jw})\right|^2,\end{aligned} \tag{23}$$

where $X_N(e^{jw}) = \sum_{n=0}^{N-1}x(n)e^{-jwm}$. In this way, we no longer need to estimate the autocorrelation function, but obtain spectral estimation by directly Fourier transforming the sequence data and then squaring their modulus.

In a word, periodogram with Bartlett window guarantees the power spectrum greater than 0 and simultaneously the calculation is relatively simple, while the defect lies in the estimation inconsistency.

2.2.3. The Bartlett Approach

The result of periodogram is the asymptotic unbiased estimation, but not the consistent estimation of power spectrum. Inspired by Equation (14), if we could find the consistent estimation of $E[\hat{P}_x(\omega)]$, and correspondingly the consistent estimation of $P_x(\omega)$ is then gained.

According to the statistic theory, the arithmetic mean of a set mutually independent data of a stochastic variable is the consistent estimation of this variable's mathematical expectation. Consequently, we take several mutually independent sampling sequences of a stochastic process and average their periodogram results. The mean value so obtained would be the consistent spectral estimation of the stochastic process. Such approach is the so-called average periodogram, or the Bartlett approach.

Refer to the algorithm model in Figure 3, for data with N points, they are divided into L segments, each of which has M points, namely $N = L \times M$. For each segment, we perform periodogram with Bartlett window separately to estimate power spectrum

$$\hat{P}_i(\omega) = \sum_{m=-\infty}^{+\infty} \hat{R}_i(m)e^{-jwm}, \quad (1 \le i \le L) \tag{24}$$

and then average the total L segments' estimation results

$$\begin{aligned} \hat{P}_b(\omega) &= \frac{1}{L}\sum_{i=1}^{L} \hat{P}_i(\omega) \\ &= \frac{1}{L}\sum_{i=1}^{L}\sum_{m=-\infty}^{+\infty} \hat{R}_i(m)e^{-jwm} \\ &= \sum_{m=-\infty}^{+\infty}\left[\frac{1}{L}\sum_{i=1}^{L}\hat{R}_i(m)\right]e^{-jwm}, \end{aligned} \tag{25}$$

which means find out each segment's autocorrelation function, calculate the average value and then conduct Fourier Transform.

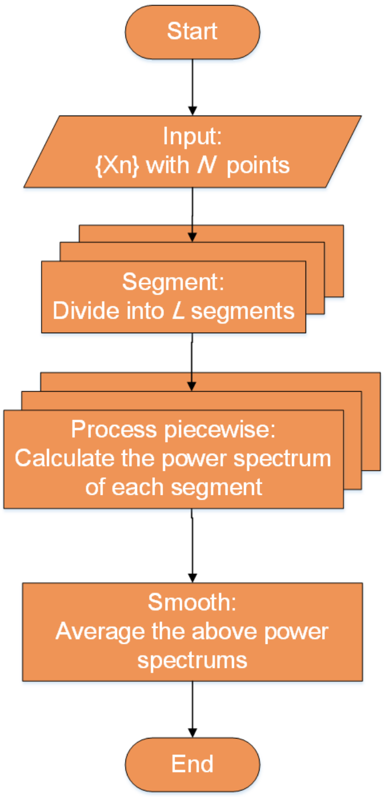


Figure 3. The algorithm model of the Bartlett approach.

$P_i(\omega)$ can be approximately regarded as mutually independent in the case of $M \gg 1$, hence the estimation variance of the Bartlett approach is

$$Var[\hat{P}_b(\omega)] \approx \frac{1}{L^2}\sum_{i=0}^{L} Var[\hat{P}_i(\omega)] = \frac{1}{L} Var[\hat{P}_i(\omega)]. \tag{26}$$

Considering the limiting case of $L \to \infty$, the variance $Var[\hat{P}_b(\omega)] \to 0$, demonstrating the Bartlett approach is the consistent estimation.

3. Performance

3.1. Comparison with the Wavelet Approach

The detection principle of the traditional method, based on wavelet feature extraction and Hurst index estimation [32], is such that when the DoS attack occurs, the Hurst index of network traffic will decrease. The Hurst index of normal network traffic is roughly between 0.75 and 1, and the larger the Hurst index, the stronger the burst of traffic [33]. When the channel is completely blocked, the network traffic tends toward a Poisson distribution, and the Hurst index becomes 0.5. However, as the DDoS and LDos attack both are a type of DoS attack and will cause the drop of the Hurst index in the same way, it is unattainable to achieve the goal of distinguishing these two attacks. Moreover, the complexity of the wavelet transform is higher than that of the power spectrum estimation.

Based on a NS-2 simulation environment from Rice University, the performance of the wavelet approach and the Bartlett approach in LDoS attack detection accuracy is compared in Table 1. Only DDoS and LDoS attacks are set in the simulation environment. It can be seen from Table 1 that the wavelet approach has almost no ability to distinguish these two attacks.

Table 1. Detection accuracy of LDoS attack.

Method	Accuracy
The wavelet approach with Hurst estimation	53%
The Bartlett approach with NCPSD	88%

3.2. Estimation Consistency and Detection Effect

To verify the validity of our proposed detection approach, we initially compare the performance of estimation consistency, then detect the traffic containing LDoS attack streams by analyzing the distribution of normalized cumulative power spectrum density (NCPSD) in frequency band to test the authenticity of our approach. The authors of [20] conducted relevant simulation experiments to prove that a slight change in transmittance T will result in the keyrate-distance product decrease. A typical experiment in Ref. [20] shows that, in the channel where T obeys a two-point distribution, when p, which means the probability that the channel transmittance is non-zero, drops from 1 to 0.99, the channel's secure transmission distance is reduced by more than half. Therefore, the LDoS attack stream in our experimental data mainly aims at tempering the transmittance T. As for the data used to test the estimation consistency, we adopt the filtered Gaussian white noise as the stochastic process sequence with a normalized center frequency (see Appendix B for definition) of 0.1 and a relative bandwidth (see Appendix B for definition) of 4%. Moreover, the sampling frequency is 100 Hz in the estimation consistency experiment.

As shown in Figure 4, our experiment data are filtered from Gaussian white noise by FIR filter with Blackman window and the data length is 1800 points. We carefully select the order of filter to balance the signal distortion and filtering effect. In accordance with a sampling frequency of 100 Hz, it can be calculated that the analog frequency corresponding to the normalized frequency of 0.1 should be $0.1 \times 100\ \ \text{Hz}/2 = 5$ Hz.

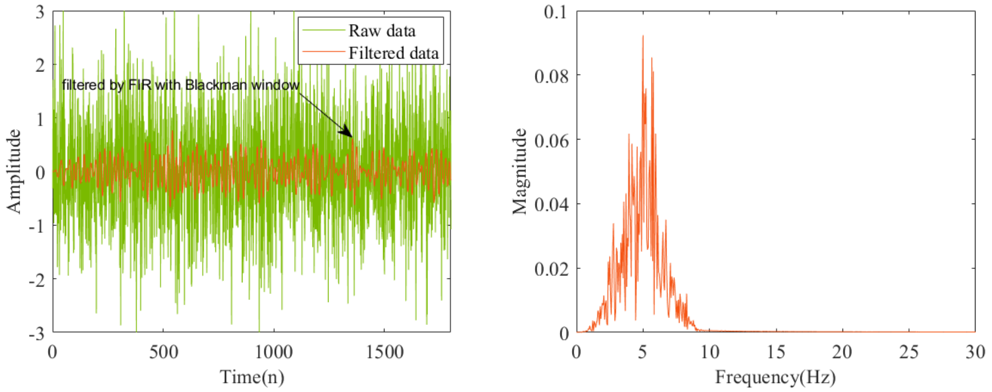
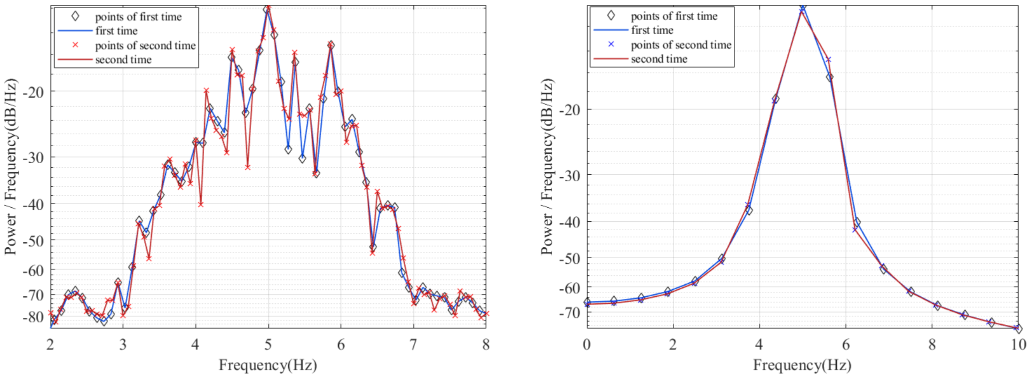


Figure 4. Data of estimation consistency experiment. Raw data is the Gaussian white noise with mean value of 0 and variance of 1. Filtered data is obtained by filtering the raw data with a high-order FIR filter. The figure on the right is the spectogram, distributed around 5 Hz, of filtered data.

After that, we successively used the periodogram with Bartlett window and the Bartlett approach to estimate the power spectrum of experiment data. In order to put stress on the estimation consistency, the power spectrum's details in the vicinity of the center frequency are magnified in Figure 5. Both spectral estimation approaches estimate twice to analyze the consistency of the estimation.



(**a**) (**b**)

Figure 5. Comparison of estimation consistency. (**a**) Adopting the periodogram with Bartlett window for spectral estimation. (**b**) Adopting the Bartlett approach (average periodogram) for spectral estimation.

Comparing the two figures in Figure 5, except the discovery that the performance in consistency of the Bartlett approach outperforms the periodogram with Bartlett window, we can also find that the curve of the Bartlett approach is smoother and its center frequency peak is more distinct. Hence, the Bartlett approach's estimation consistency has been strongly verified.

In the simulation experiment, the Bartlett approach is used for the spectral estimation. Using the NCPSD (see Appendix B for definition) calculation of the LDoS attack stream under different background traffic intensities, we test the feasibility of the proposed method to detect the LDoS attacks.

As shown in Figure 6a, the stream with the LDoS attacks has an energy distribution close to 70% of the total energy in the range of 0 to 50 Hz, while the normal stream has only 10% energy in this range. It, at the same time, proves that we can calculate the deviation of the NCPSD from the normal value to reflect whether the stream contains LDoS attacks.

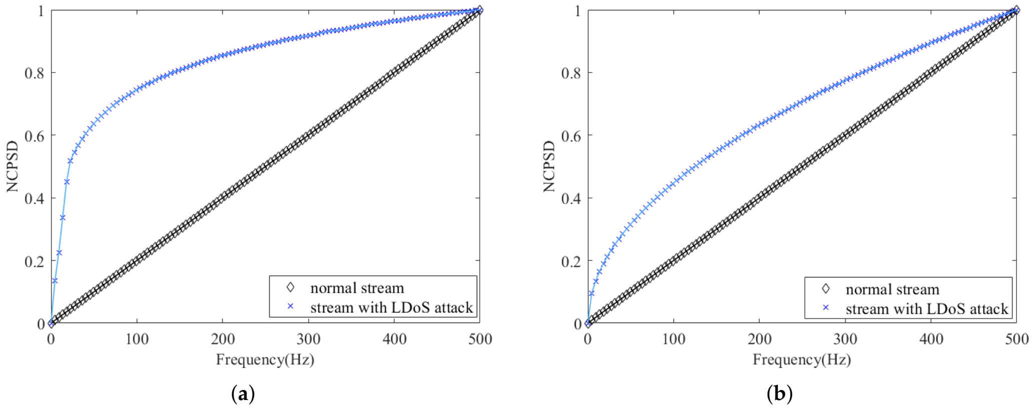


Figure 6. NCPSD under different background traffic intensity.(**a**) NCPSD of attack stream and normal stream under low background traffic. (**b**) NCPSD of attack stream and normal stream under high background traffic.

Figure 6b shows the NCPSD curves of stream with the LDoS attack and the normal one. In spite of the narrowed difference between the two curves, there is 30% of the total energy distributed within the range of 0 to 50 Hz, which is still quite deviated from 10% of the normal stream. That is to say, under the high intensity of background traffic, the detection effect has declined to some extent, but it can still detect whether the stream contains LDoS attacks.

4. Conclusions

In our paper, a method based on Bartlett's approach of spectral estimation is proposed to detect LDoS attacks in the CVQKD communicating progress. The LDoS attack is an algorithm-aimed hacking strategy and related experiments have already demonstrated that a slight manipulation of a channel's parameters can trigger the communication interruption. What we pay attention to is the channel's transmittance T, as other parameters can be deduced from it. Taking advantage of the periodicity of LDoS attacks, we obtain the rule that the PSD of the LDoS attack stream is higher than normal in the low frequency domain, hence transforming the issue of the LDoS attack detection into the spectral estimation of stochastic sequence. Three of the spectral estimation approaches are discussed emphatically, including the autocorrelation estimation with rectangular window, periodogram with Bartlett window and the Bartlett approach, from the perspective of estimation consistency and estimation unbiasedness. Through mathematical deduction and experimental analysis, the Bartlett approach performs best among the three approaches. The simulation experiment results show that the Bartlett approach is consistent in its estimations and can effectively detect the LDos attacks.

Author Contributions: Conceptualization, E.D.; methodology, L.Z.; resources, L.Z.; data curation, E.D. and L.Z.; writing—original draft preparation, E.D.; software, E.D.; writing—review and editing, D.H. and L.Z.; supervision, D.H. and L.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

CVQKD	Continuous-variable quantum key distribution
DVQKD	Discrete-variable quantum key distribution
DoS	Denial-of-service
LDoS	Low-rate denial-of-service
PSD	Power spectral density
GMCS	Gaussian-modulated coherent state
LO	Local oscillator
TCP	Transmission control protocol
NCPSD	Normalized cumulative power spectral density
FIR	Finite impulse response

Appendix A. Detailed Derivation and Proof of the LDoS Attack Strategy

In Section 2.1, we have briefly explained the LDoS attack strategy against the GMCS protocol. In this part, the rigorous mathematical derivation is given. During a communication, Alice modulates X and Bob measures Y, both X and Y are Gaussian variables, and their expressions are as follows

$$X = Acos(\theta) \quad Y = \sqrt{T}Acos(\theta + \Delta\varphi) + A_N, \tag{A1}$$

where A is the amplitude of the coherent state that is modulated by AM, θ is the phase of the coherent state that modulated by PM, T is the channel transmittance, $\Delta\varphi$ is the phase deviation generated by the quantum channel and A_N is the linear error caused by the noise. Once again, the finite-size effect is left out of consideration and we regard detector efficiency η and electrical noise V_{el} as fixed values. Substitute Equation (A1) into Equation (1) and then the following formula can be obtained

$$\begin{aligned} \hat{t} &= \frac{\frac{1}{m}\sum_{i=1}^{m} x_i y_i}{\frac{1}{m}\sum_{i=1}^{m} x_i^2} = \frac{E(XY)}{E(X^2)} \\ &= \frac{E(\sqrt{T}A^2cos(\theta)cos(\theta+\Delta\varphi)) + E(A_N Acos(\theta))}{E(A^2cos^2(\theta))}. \end{aligned} \tag{A2}$$

Then, in view of the phase compensation technique could rectify the phase shift and the mean value of A_N caused by noise equals 0, we reckon that $\Delta\varphi \approx 0$ and $E(A_N Acos(\theta)) = E(A_N)E(Acos(\theta)) = 0$. Such being the case, we can simplify Equation (A2) to

$$\begin{aligned} \hat{t} &= \frac{E(\sqrt{T}A^2cos^2\theta)}{E(A^2cos^2\theta)} \\ &= \frac{E(\sqrt{T})E(A^2cos^2\theta) + cov(\sqrt{T}, A^2cos^2\theta)}{E(A^2cos^2\theta)} \\ &= \frac{E(\sqrt{T})E(A^2cos^2\theta)}{E(A^2cos^2\theta)} = E(\sqrt{T}). \end{aligned} \tag{A3}$$

The covariance $cov(\sqrt{T}, A^2cos^2\theta)$ equals 0 because the parameter T is irrelevant to Alice's modulation process. Ulteriorly, by using the equivalent relations in Equation (A3) and equation $V_A = E(X^2) = E(A^2cos^2\theta)$, we can get the $\hat{\sigma}^2$ as

$$\begin{aligned} &\hat{\sigma}^2 = E(Y - \hat{t}X)^2 = E(Y^2 - 2\hat{t}XY + \hat{t}^2X^2) \\ &= E(T\varepsilon) + 1 + E(TX^2) - 2\hat{t}E(XY) + \hat{t}^2E(X^2) \\ &= E(T)\varepsilon + 1 + E(T)V_A - (E(\sqrt{T}))^2V_A. \end{aligned} \tag{A4}$$

Equations (A3) and (A4) fully prove that T is a key parameter in channel estimation. Eve can carry out attacks by manipulating T.

Appendix B. Definition of Some Key Parameters

In this part, we give the definitions of key parameters that are not provided in the manuscript.

Appendix B.1. NCPSD

The normalized cumulative power spectrum density is defined as

$$\phi(f) = \sum_{i=1}^{f} PSD(i) / \sum_{i=1}^{f_{max}} PSD(i),$$

where $PSD(i)$ means the power spectral density of ith frequency component. The value range of NCPSD is 0 to 1, and NCPSD reflects the proportion of different frequency components in the whole signal.

Appendix B.2. Normalized Frequency

The normalized frequency is defined as

$$\omega = \frac{2\pi f}{f_s},$$

where f means the analog frequency and f_s means the sampling frequency. It takes the sampling frequency as the reference value. In this way, a unified standard is achieved, which is conducive to comparing the distribution of various frequencies.

Appendix B.3. Relative Bandwidth

Relative bandwidth is defined as

$$f_{rb} = \frac{2(f_H - f_L)}{f_H + f_L},$$

where f_H and f_L are the upper and lower limit frequencies, respectively.

References

1. Rivest, A.; Shamir, L.; Adleman, T. A method for obtaining digital signature and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Kumar, A.; Garhwal, S. State-of-the-Art Survey of Quantum Cryptography. *Arch. Comput. Methods Eng.* **2021**, *28*, 2831–2868. [CrossRef]
3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.; Dusek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
4. Li, C.; Qian, L.; Lo, H.-K. Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources. *npj Quantum Inf.* **2021**, *7*, 150. [CrossRef]
5. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
6. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.; Ralph, T.; Shapiro, J.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2011**, *84*, 621–669. [CrossRef]
7. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072. [CrossRef]
8. Ye, W.; Guo, Y.; Xia, Y.; Zhong, H.; Zhang, H.; Ding, J.Z.; Hu, L.Y. Discrete modulation continuous-variable quantum key distribution based on quantum catalysis. *Acta Phys. Sin.* **2020**, *69*, 060301. [CrossRef]
9. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
10. Navascués, M.; Grosshans, F.; Acín, A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef]
11. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [CrossRef] [PubMed]

12. García-Patrón, R.; Cerf, N.J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
13. García-Patrón, R.; Cerf, N.J. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501.
14. Hao, Q.; Rupesh, K.; Romain, A. Saturation attack on continuous-variable quantum key distribution system. In Proceedings of the Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, Dresden, Germany, 29 October 2013; Volume 8899.
15. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.-M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [CrossRef]
16. Wiechers, C.; Lydersen, L.; Wittmann, C.; Elser, D.; Skaar, J.; Marquardt, C.; Makarov, V.; Leuchs, G. After-gate attack on a quantum cryptosystem. *New J. Phys.* **2011**, *13*, 013043. [CrossRef]
17. Ferenczi, A.; Grangier, P.; Grosshans, F. Calibration attack and defense in continuous variable quantum key distribution. In Proceedings of the European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference, Munich, Germany, 17–22 June 2007; p. 1.
18. Silva, T.; Xavier, G.; Temporäo, G.; von der Weid, J.P. Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems. *Opt. Express* **2012**, *20*, 18911. [CrossRef]
19. Huang, P.; Huang, J.; Wang, T.; Li, H.; Huang, D.; Zeng, G. Robust continuous-variable quantum key distribution against practical attacks. *Phys. Rev. A* **2017**, *95*, 052302. [CrossRef]
20. Li, Y.; Huang, P.; Wang, S.; Wang, T.; Li, D.; Zeng, G. A denial-of-service attack on fiber-based continuous-variable quantum key distribution. *Phys. Lett. A* **2018**, *382*, 3253. [CrossRef]
21. Kuzmanovic, A.; Knightly, E. Low-rate tcp-targeted denial of service attacks and counter strategies. *IEEE/ACM Trans. Netw.* **2006**, *14*, 683. [CrossRef]
22. Chen, Y.; Hwang, K. Collaborative detection and filtering of shrew ddos attacks using spectral analysis. *J. Parallel Distrib. Comput.* **2006**, *66*, 1137. [CrossRef]
23. Antonio, M.; Santiago, S.; Geert, L.; Alejandro, R. Stationary Graph Processes and Spectral Estimation. *IEEE Trans. Signal Process.* **2017**, *65*, 5911–5926.
24. Bai, J.; Ma, L. Detection of Range-Spread Target in Spatially Correlated Weibull Clutter Based on AR Spectral Estimation. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2021**, *E104.A*, 305–309. [CrossRef]
25. Konar, A.; Sidiropoulos, N.D.; Mehanna, O. Parametric Frugal Sensing of Power Spectra for Moving Average Models. *IEEE Trans. Signal Process.* **2015**, *63*, 1073–1085. [CrossRef]
26. Teles, P.; Sousa, P. The effect of temporal aggregation on the estimation accuracy of ARMA models. *Commun. Stat.-Simul. Comput.* **2018**, *47*, 2865–2885. [CrossRef]
27. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef]
28. Cerf, N.J.; Grangier, P. From quantum cloning to quantum key distribution with continuous variables: A review (Invited). *J. Opt. Soc. Am. B* **2007**, *24*, 324–334. [CrossRef]
29. Luo, H.; Wang, Y.; Ye, W.; Zhong, H.; Mao, Y.; Guo, Y. Parameter estimation of continuous variable quantum key distribution system via artificial neural networks. *Chin. Phys. B* **2022**, *31*, 2. [CrossRef]
30. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]
31. Yu, X.D.; Gühne, O. Detecting coherence via spectrum estimation. *Phys. Rev. A* **2019**, *99*, 062310. [CrossRef]
32. He, Y.X.; Cao, Q.; Liu, T.; Han, Y.; Xiong, Q. A Low-Rate DoS Detection Method Based on Feature Extraction Using Wavelet Transform. *J. Softw.* **2009**, *20*, 930–941.
33. Wu, Z.J.; Li, H.J.; Liu, L.; Zhang, J.A.; Yue, M.; Lei, J. Detection of LDoS Attacks Based on Wavelet Energy Entropy and Hidden Semi-Markov Models. *J. Softw.* **2020**, *31*, 1549–1562.