Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 496376, 11 pages
http://dx.doi.org/10.1155/2014/496376

Research Article

Adaptive EWMA Method Based on Abnormal Network Traffic for LDoS Attacks

Dan Tang, Kai Chen, XiaoSu Chen, HuiYu Liu, and Xinhua Li

School of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan, Hubei 430074, China

Correspondence should be addressed to Kai Chen; kchen@hust.edu.cn

Received 19 March 2014; Revised 15 June 2014; Accepted 16 June 2014; Published 3 August 2014

Academic Editor: Abbas Saadatmandi

The low-rate denial of service (LDoS) attacks reduce network services capabilities by periodically sending high intensity pulse data flows. For their concealed performance, it is more difficult for traditional DoS detection methods to detect LDoS attacks; at the same time the accuracy of the current detection methods for LDoS attacks is relatively low. As the fact that LDoS attacks led to abnormal distribution of the ACK traffic, LDoS attacks can be detected by analyzing the distribution characteristics of ACK traffic. Then traditional EWMA algorithm which can smooth the accidental error while being the same as the exceptional mutation may cause some misjudgment; therefore a new LDoS detection method based on adaptive EWMA (AEWMA) algorithm is proposed. The AEWMA algorithm which uses an adaptive weighting function instead of the constant weighting of EWMA algorithm can smooth the accidental error and retain the exceptional mutation. So AEWMA method is more beneficial than EWMA method for analyzing and measuring the abnormal distribution of ACK traffic. The NS2 simulations show that AEWMA method can detect LDoS attacks effectively and has a low false negative rate and a false positive rate. Based on DARPA99 datasets, experiment results show that AEWMA method is more efficient than EWMA method.

1. Introduction

The low-rate denial of service (LDoS) [1] attack is a new type of DoS attack, which periodically sends high intensity pulse data flows to reduce network services capabilities by using the vulnerability of TCP congestion control mechanism. The duration time of each pulse attack flow is short, while the time of silence in each period is long, so that the average rate of the LDoS attacks traffic is low, and therefore it is difficult to distinguish from the normal traffic. So the LDoS attacks are more covert and cannot be detected by traditional DoS detection methods.

Currently, some progress has been made in the field of detection methods of the LDoS attacks [2–4], for example, the wavelet analysis method [5], the DTW method [6], the HAWK method [7], the STM method [8], the UDP-frequency-domain-based detection method [9], and so on [10–12]. Wavelet analysis method [5], which can detect attack flows on the key routers, principally aims at the AIMD-targeted attacks. Nonetheless, it is ineffective to the non-AIMD-targeted LDoS attacks. The DTW method [6] and the HAWK method [7] focus on the periodicity of attack traffic and abnormality of network data traffic, get the abnormal characteristics of flow on time domain, and then compare and identify the LDoS attacks. STM method [8] is a distributed collaborative filtering detection method based on power spectral density. It has a higher detection rate but occupies large storage resources. UDP-frequency-domain-based detection method [9] needs time/frequency transformation which functions less efficiently. These detection methods [10–12] for the LDoS attacks have still some deficiencies as the low accuracy, the high false negative rate, the high false positive rate, the weak reliability, and so on.

Some detection methods which are based on traditional traffic characteristics [13, 14] are proposed in recent years. These methods detect the LDoS attacks by searching and identifying the abnormal network traffic [15, 16] caused by the LDoS attacks. For example, the EWMA method [15, 16] which is based on the EWMA algorithm can detect most kinds of the LDoS attacks. While the EWMA algorithm may smooth not only the normal traffic but also the abnormal traffic. This will affect the detection accuracy for the LDoS attacks.

In this paper, a new adaptive EWMA method is proposed on the basis of the EWMA method. This method adopts the AEWMA algorithm which is a kind of improved EWMA algorithm. The AEWMA algorithm can retain the abnormal traffic and smooth the normal traffic at the same time, so this AEWMA method can highly efficiently detect the LDoS attacks. To develop this detection method for the LDoS attacks, firstly, the abnormal distribution of ACK traffic caused by the LDoS attacks is described and analyzed. Secondly, the abnormal characteristics of ACK traffic under the LDoS attacks are summarized. Thirdly, the AEWMA algorithm is introduced, and the advantages of the AEWMA algorithm compared with the EWMA algorithm are proved. Lastly the important parameters of the AEWMA detection method are analyzed. NS2 simulations show that this AEWMA detection method has a high accuracy rate, a lowfalse negative rate, and a low false positive rate for the LDoS attacks. Based on DARPA99 datasets, the experiment results show that the efficiency of this method has improved compared with the EWMA method.

2. Description and Analysis

2.1. The Model Description of LDoS Attack. The congestion control mechanism, which is a very important adaptive mechanism of the internet network, has some obvious defects. For example, when the network congests, the congestion control mechanism is triggered, resulting in the rapid shrink of the send window and the buffer queue, as well as the quick decline of the service capability of the network. The LDoS attacks exploit this flaw and periodically send high intensity pulse attack flows, making a constant switch of the network system states between inefficient and normal. Thereupon, the network cannot provide normal services, namely, denial of service.

The model of the LDoS attacks and the affection of the system performance under the LDoS attacks are shown in Figure 1, where the LDoS attacks usually have three important parameters: (1) the cycle of attack: T_{attack}, (2) the duration time of attack: t_{attack}, and (3) the intensity of attack pulse: R_{attack}. Figure 1(a) depicts the model of the LDoS attacks. As these three parameters, the average traffic of the LDoS attacks can be denoted as $R_{\text{attack}} \times (t_{\text{attack}}/T_{\text{attack}})$. In general, the LDoS attacks periodically send high intensity pulse data flows. In order to congest the network, the intensity of attack pulse R_{attack} must meet: $R_{\text{attack}} > C_{\text{b-link}}$, where $C_{\text{b-link}}$ is the network bottleneck bandwidth. At the same time, the duration time of each pulse attack flow is short while the time of silence in each period is long, so the average traffic of the LDoS attacks is lower than the network bottleneck bandwidth $C_{\text{b-link}}$ $((R_{\text{attack}} \times (t_{\text{attack}}/T_{\text{attack}})) < C_{\text{b-link}})$, as shown in Figure 1(a). Figure 1(b) shows that the system performance of the network has suffered heavy losses.

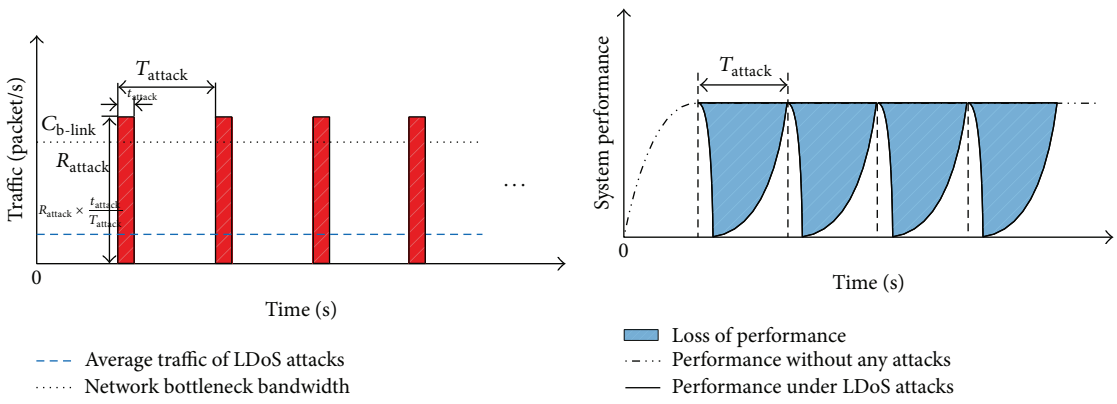
The influence of the TCP traffic under the LDoS attacks is shown in Figure 2. When the network is normal without any attacks, the TCP traffic is stable with small fluctuations, and then the average of TCP traffic is large. While, when the network is abnormal under the LDoS attacks, the TCP traffic fluctuates acutely, the average of TCP traffic is on the decline. Figure 2 shows that the LDoS attacks can significantly reduce the average TCP traffic.

2.2. The Characteristics Analysis of LDoS Attacks. The LDoS attacks usually occur in a *busy* network in order to get the better effect of the attacks. In the *busy* network, the LDoS attacks can cause a significant impact which is quite different from other attacks on the network traffic. According to the focus of this paper, we propose three kinds of representative scene of the network as follows. (1) Scene 1: the normal network which doesn't have any attacks; (2) Scene 2: there exist other attacks which have made an impact on TCP traffic except the LDoS attacks (e.g., the DDoS attacks in this paper); (3) Scene 3: there exist the LDoS attacks. At the same time, each scene has a sufficient number of TCP connections and background data traffic. According to the LDoS attacks principles, the legitimate TCP traffic and the corresponding ACK traffic will change significantly when the attacks have occurred. As the actual network TCP connection uses the *piggybacking* and the *cumulative acknowledgment* scheme, in order to improve the detection efficiency, the ACK traffic is used to analyze and to detect the LDoS attacks.

The ACK traffic distribution of the three scenes is shown in Figure 3. The μ_i $(i = 1, 2, 3)$ and σ_i $(i = 1, 2, 3)$ denote the average and the variance of the ACK traffic in the three scenes. Figure 3 shows that, in the Scene 1, the network occasionally congests, so the ACK traffic is more stable, and then μ_1 is large and σ_1 is small. In the Scene 2, TCP connections can hardly be established under the DDoS attacks, so the ACK traffic's μ_2 approaches to zero and σ_2 fluctuates in a very small manner. In the Scene 3, the TCP traffic waves hugely and the ACK traffic fluctuates acutely, so the ACK traffic's μ_3 is small but σ_3 sharply rises. Therefore, we can get $\mu_1 > \mu_3 > \mu_2 \approx 0$, and $\sigma_3 > \sigma_1 > \sigma_2$.

According to analysis above, in the Scene 3, because the LDoS attacks have convulsed the ACK traffic, its distribution is more discrete and has a significant abnormal change in comparison with the Scene 1. In the Scene 2, because the DDoS attacks lead the ACK traffic drop to be close to zero, its distribution has a significant abnormal change too compared with the Scene 1, but it is much different from the change of the Scene 3. Therefore, the LDoS attacks led the significant abnormal change of the distribution of the ACK traffic, and the distribution of the Scene 3 is very different from the distribution of the Scene 1, and it is much different from the distribution of the Scene 2 too. So the LDoS attacks can be detected by measuring and analyzing the distribution characteristics of the ACK traffic.

2.3. Measuring Abnormal Distribution of ACK Traffic. A large number of experiments have proved that, according to the central limit theorem, the Gaussian distribution could describe most of the real network data traffic distribution [17]. So the Gaussian distribution is used to express the ACK traffic probability distribution function (PDF for short) of the three different scenes, such as $\Phi_1(x, \mu_1, \sigma_1)$, $\Phi_2(x, \mu_2, \sigma_2)$, and $\Phi_3(x, \mu_3, \sigma_3)$. Figure 3 indicates that $\mu_1 > \mu_3 > \mu_2$ and



(a) model of LDoS attacks

(b) affection of system performance under LDoS attacks

Figure 1: The model and the influence of LDoS attacks.

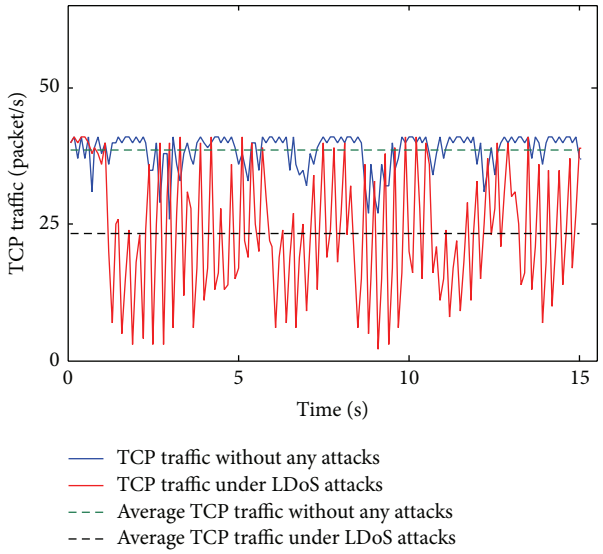


Figure 2: The influence of TCP traffic under LDoS attacks.

$\sigma_3 > \sigma_1 > \sigma_2$. Therefore, the probability distribution function of Φ_1, Φ_2, and Φ_3 are shown in Figure 4.

Figure 4 shows that $x = \mu_i$ $(i = 1, 2, 3)$ is the symmetry axis of function Φ_i $(i = 1, 2, 3)$. The characteristics of the Gaussian distribution show that the center of its distribution is highly concentrated and then quickly divergent trend. The dispersion degree is directly proportional to its variance, and the greater the variance, the more emanative the divergence. In order to contrast the divergence conveniently of the ACK traffic PDF in three scenes, we normalize the functions Φ_1, Φ_2, and Φ_3, make the symmetry axis of the three functions accordant, and set $x' = x - \mu_i$, which have been shown in Figure 5.

Figure 5 shows that there are some differences of the distribution of the functions Φ_1, Φ_2, and Φ_3 after being normalized. The differences manifest that, there is such an interval outside of which Φ_1 and Φ_2 have a low probability (<1%), but Φ_3 has a high probability ($\gg 1\%$). The probability of outside this interval has the greater *deviation* between function Φ_3 with functions Φ_1 and Φ_2; we call this *deviation* as the abnormal distribution which is caused by the LDoS attacks. Therefore, we can distinguish the Scene 3 from the Scene 1 and the Scene 2 through exploring the distribution characteristics of ACK traffic.

The interval is called *Confidence Interval* (CI for short), defined as $\text{CI} = [\mu_i - h, \mu_i + h]$, where h is called the control line which determines the size of the CI. The range of CI is associated with μ_i and h. μ_i is the average ACK traffic of the *testing data* (where the network traffic which is going to be tested is called the testing data), and h is closely related to the variance σ_{normal} of the ACK traffic of the *training data* (where the network traffic which is obtained from the network without any attack in advance is called the training data). A reasonable CI is effective to analyze the abnormal distribution because it decides the discrimination of the abnormal distribution.

So, the LDoS attacks can be detected by observing the distribution and analyzing the deviation of the ACK traffic based on CI. The Adaptive Exponentially Weighted Moving Average (AEWMA for short) algorithm is used to describe the distribution of the ACK traffic.

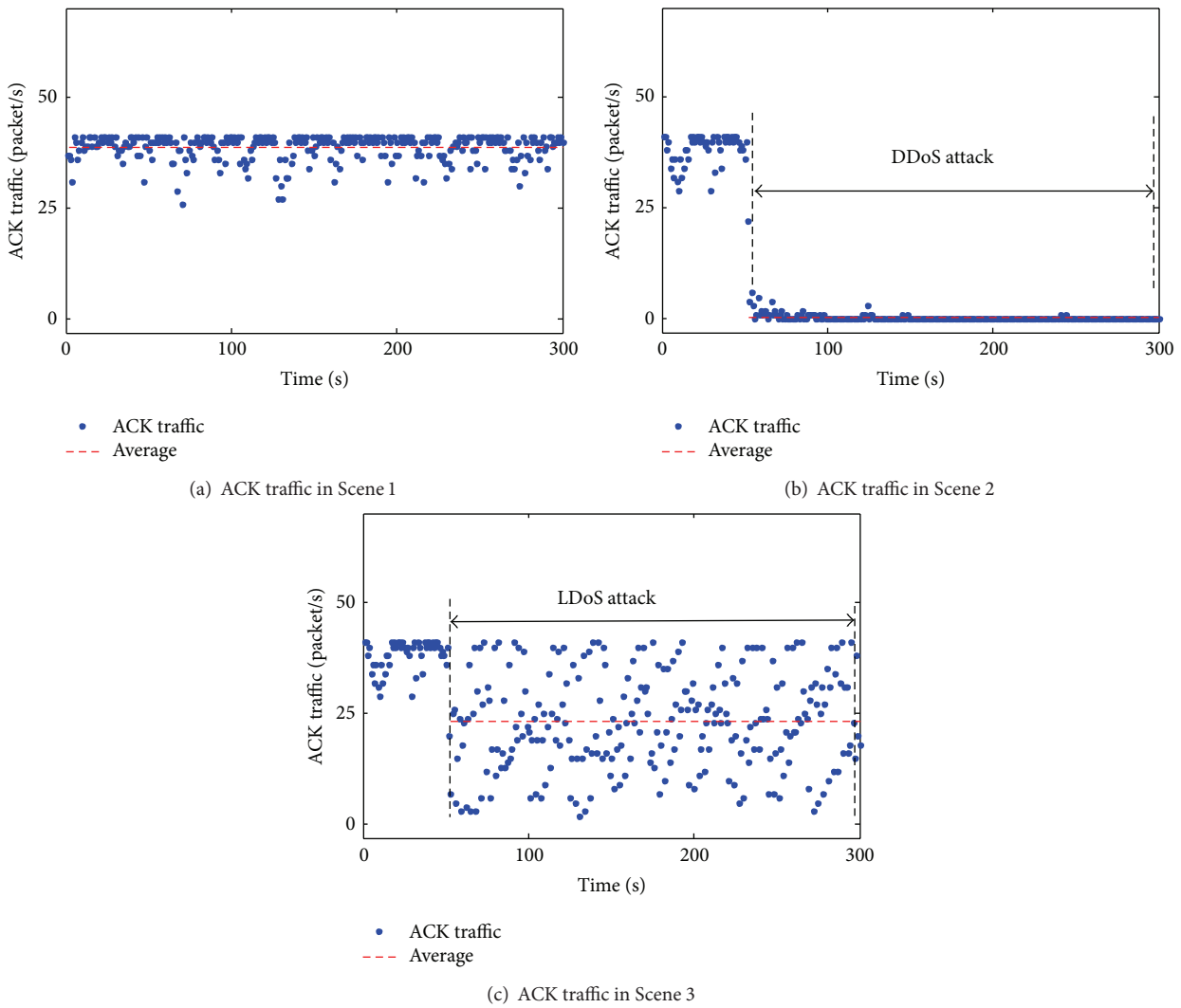
3. Adaptive EWMA Method for LDoS Attacks

3.1. The Adaptive EWMA Method. The LDoS attacks can be detected by analyzing and measuring the abnormal ACK traffic; in order to accurately describe and measure the distribution characteristics of ACK traffic, the AEWMA algorithm which is a kind of improved EWMA algorithm is used.

EWMA algorithm [18] was proposed by Roberts in 1959, which is defined as follows:

$$S_0 = 0,$$
$$S_i = (1 - \lambda_{\text{EWMA}}) S_{i-1} + \lambda_{\text{EWMA}} X_i, \tag{1}$$

where X_i is the ith sample values, S_i is the ith EWMA statistical value, λ_{EWMA} is a constant called smoothing parameter,



(a) ACK traffic in Scene 1

(b) ACK traffic in Scene 2

(c) ACK traffic in Scene 3

FIGURE 3: The ACK distribution of the three scenes.

and $\lambda_{\mathrm{EWMA}} \in (0, 1)$. Equation (2) is derived from (1). Consider

$$S_0 = 0,$$
$$S_i = S_{i-1} + \lambda_{\mathrm{EWMA}} \left(X_i - S_{i-1}\right). \tag{2}$$

For the EWMA algorithm, the smaller the λ_{EWMA}, the better the smoothness and the higher the accuracy of small *drift*, while the greater the λ_{EWMA}, the weaker the smoothness and the higher the accuracy of large *drift*. The EWMA algorithm is used widely in the field of the early product quality analysis, product anomaly detection, financial management, and other statistical areas. In recent years, The EWMA algorithm has been applied to the field of communications and network anomaly detection and determination.

However, it can be seen from (2) that the EWMA algorithm smoothes all of the original samples. This means that the EWMA algorithm not only smoothes the accidental error, but also smoothes the exceptional mutation too. In the LDoS attacks detection based on abnormal traffic, if the abnormal mutation which is always the research emphasis has been smoothed, it would lead the abnormal characteristics blurred or even lose. thereby reducing the detection accuracy. So in the LDoS attacks detection, there are some flaws and shortcomings if the EWMA algorithm is used to smooth the original samples.

The AEWMA algorithm [19] which has an adaptive smoothing function was proposed by Capizzi and Masarotto in 2003. AEWMA algorithm is a kind of improved EWMA algorithm and is defined as follows:

$$S_0 = \frac{1}{n}\sum_{i=1}^{n} X_i \quad \left(n \in N^+\right),$$
$$S_i = \left(1 - w\left(e_i\right)\right) S_{i-1} + w\left(e_i\right) X_i, \tag{3}$$

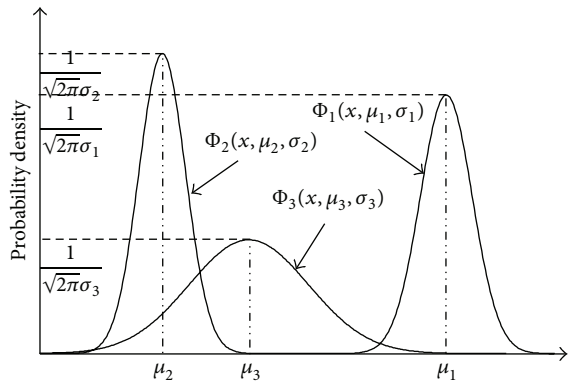


Figure 4: The PDF of ACK traffic in three scenes.

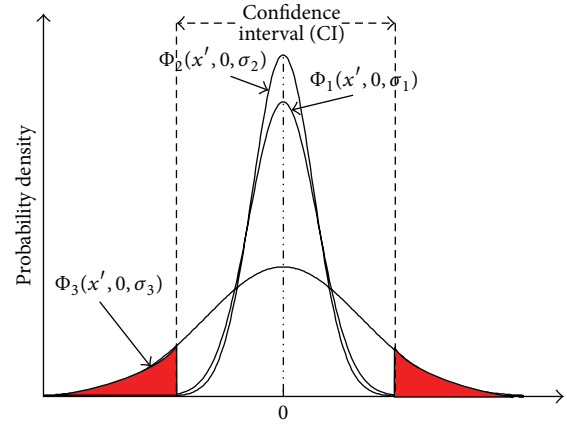


Figure 5: The Normalized PDF of ACK traffic.

where X_i is the ith sample values, S_i is the ith AEWMA statistical value, and $w(e_i)$ is an adaptive smoothing function. Equation (4) is derived from (3). Consider

$$S_0 = \frac{1}{n}\sum_{i=1}^{n} X_i \quad (n \in N^+),$$
$$S_i = S_{i-1} + w(e_i)(X_i - S_{i-1}). \tag{4}$$

Set $e_i = X_i - S_{i-1}$ and $\phi(e_i)$, called the score function, is defined as follows:

$$\phi(e_i) = w(e_i)(X_i - S_{i-1}). \tag{5}$$

Then (6) is derived from (4) and (5). One has

$$S_0 = \frac{1}{n}\sum_{i=1}^{n} X_i \quad (n \in N^+),$$
$$S_i = S_{i-1} + \phi(e_i). \tag{6}$$

For the AEWMA algorithm, it can be seen from (6) that if $\phi(e_i) = \lambda_{\text{EWMA}} e_i$, then the classic EWMA algorithm is obtained. Therefore EWMA algorithm is a special case of AEWMA algorithm and the AEWMA algorithm has the characteristics and advantages of the classical EWMA algorithm. Then the AEWMA algorithm, which uses the score function instead of fixed initial parameters, is apparently more adaptable to a wider range than the EWMA algorithm.

The score function $\phi(e)$ has the following characteristics: (1) $\phi(e)$ is a nondecreasing function; (2) $\phi(e)$ is an odd function; (3) when $|e|$ is small, $\phi(e) \approx \lambda e$; (4) when $|e|$ is great, $\phi(e) \approx e$. One score function is defined as follows [19]:

$$\phi(e) = \begin{cases} \left\{1 - (1 - \lambda_{\text{AEWMA}})\left[1 - \left(\frac{e}{k}\right)^2\right]^2\right\} \times e, & (|e| < k) \\ e, & (|e| \geq k), \end{cases} \tag{7}$$

where λ_{AEWMA} and k are parameters of the score function $\phi(e)$, λ_{AEWMA} is smoothing parameter for $\phi(e)$, and k is an important threshold for measuring the variable e.

The score function of the AEWMA algorithm and the fixed initial parameters λ_{EWMA} of the EWMA algorithm are shown in Figure 6. Figure 6 shows that the EWMA algorithm corresponding straight line $y = \lambda_{\text{EWMA}} \times x$ has a linear weighting, while the AEWMA algorithm corresponding curve line has a nonlinear weighting. $\phi(e)$ equals straight line $y = x$, when the variable e is large ($e \geq k$), and $\phi(e)$ closes straight line $y = \lambda_{\text{EWMA}} \times x$, when the variable e is small ($e < k$). $\phi(e)$ intersects with straight line $y = x$ at the point (k, k). Therefore $\phi(e)$ can retain the exceptional mutation ($e \geq k$) and smooth the accidental error ($e < k$).

The statistics results of traffic based on the AEWMA algorithm and the EWMA algorithm are shown in Figure 7. Figure 7 shows that the AEWMA algorithm and the EWMA algorithm can effectively smooth the slight fluctuation of the traffic when the traffic without any attacks is normal. Two curves corresponding statistical values almost coincide. But when the traffic under attacks is abnormal, the EWMA algorithm smoothes the large fluctuation too, while the AEWMA algorithm can retain the abnormal characteristics of the sample value. Two curves corresponding statistical values are quite different. Therefore the AEWMA algorithm is more suitable than the EWMA algorithm for LDoS attacks detection based on the abnormal characteristics of traffic.

As can be seen from the above analysis, the AEWMA algorithm is a kind of improved EWMA algorithm. The fundamental principle of the EWMA algorithm is the more recent sample values, the more information and the more weight. Its statistical value is a weighted linear combination of the sample values. By using a nonlinear weight function, the AEWMA algorithm can retain the exceptional mutation and smooth the accidental error of the samples. When the LDoS attacks occur, lots of high intensity pulse attack flows result in a lot of abnormal traffic in the network. Then the AEWMA algorithm is more suitable than the EWMA algorithm for retaining the abnormal characteristics caused by the LDoS attacks, so the AEWMA algorithm is adaptable.

3.2. The Detection Judgment of LDoS Attacks. By using the AEWMA algorithm the accidental error is smoothed and the exceptional mutation is retained; then the LDoS attack can be exactly measured. When the LDoS attacks exist, the

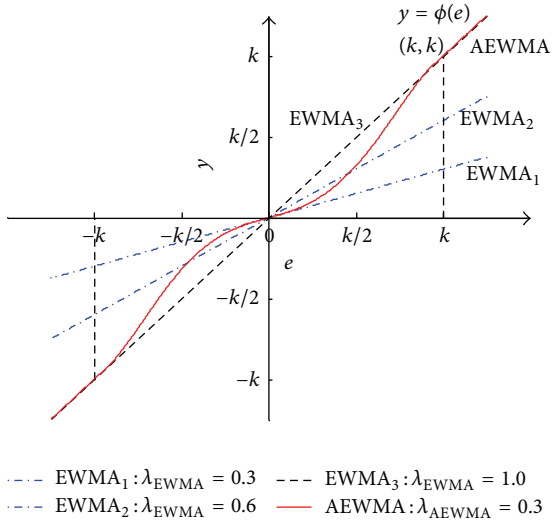


Figure 6: Score function of the AEWMA algorithm.

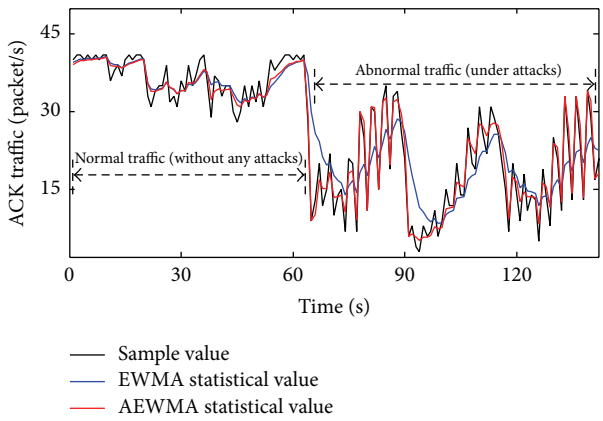


Figure 7: The statistics results of traffic based on AEWMA and EWMA algorithm.

distribution of the ACK traffic will deviate, and the specified CI is used to measure the dispersion degree. So the LDoS attacks can be detected by analyzing and contrasting the dispersion degree of ACK traffic's distribution.

In order to analyze the ACK traffic samples, we define the concept of the *testing windows* which is composed of the continuous on time scales for multiple samples, as follows.

Definition 1. A certain number of consecutive sample values of the ACK traffic compose a testing window, TW for short, and then the length of the sampling time corresponding to a TW denotes Time_{TW}.

In a TW, the S_i of the ACK traffic is named S_i^{ACK}. The mapping point in the two-dimensional coordinate system of the group $\langle i, S_i^{\text{ACK}} \rangle$ is named the AEWMA statistical point. If $S_i^{\text{ACK}} \in \text{CI}$, the AEWMA statistical point is called the normal point (NP for short); otherwise, it is called the abnormal point (AP for short). The congregation which is composed of a set of consecutive APs is called GP. Each GP contains at least one AP.

Definition 2. In a TW, the ratio of the number of AP to the number of all AEWMA statistical points is called APT, and the ratio of the number of GP to the number of all AEWMA statistical points is called GPT.

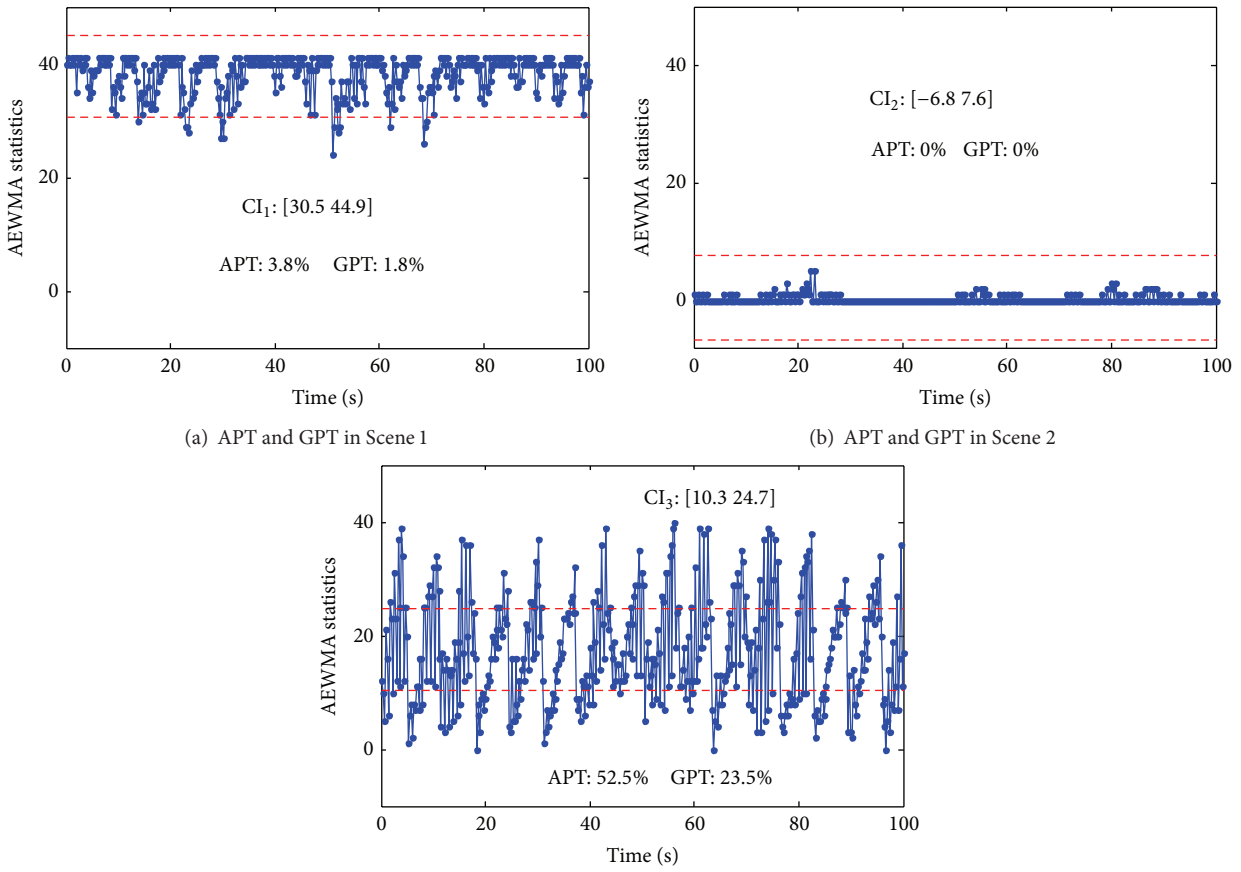
In the Scene 1, the ACK traffic is stable and S^{ACK} is normal distribution; namely, few S^{ACK}s are outside of CI. So NP is more and AP is less in all the AEWMA statistical points. Therefore APT and GPT are both small. In the Scene 2, DDoS attacks cause network the complete denial of service and the traffic is almost zero and the same as the S^{ACK}. So APT and GPT approach to zero. In the Scene 3, LDoS attacks cause the ACK traffic more volatile and the S^{ACK} anomalistic, so AP is more and APT is larger. At the same time GP and GPT are larger too for the frequent changes of the ACK traffic. Figure 8 shows the difference of ATP and GPT of the three scenes.

According to the characteristics of distribution of AEWMA statistics of ACK traffic on CI for the three scenes, the judgment criterion is given as follows.

Judgment Criterion. In a TW, if APT $> \Lambda_{\text{AP}}$ (which is called Condition 1, C1 for short) and GPT $> \Lambda_{\text{GP}}$ (which is called Condition 2, C2 for short), then the LDoS attacks exist in this TW. where Λ_{AP} and Λ_{GP} are accessed from the training data ($0 < \Lambda_{\text{GP}} \leq \Lambda_{\text{AP}} < 1$).

3.3. The Important Parameters. The AEWMA algorithm can be used to detect the LDoS attacks; then the reasonable λ_{AEWMA} and k are very important for the AEWMA algorithm. The algorithm that is required not only can filter the random error of the normal network traffic such as the *white noise*, but also can maintain a certain degree of sensitivity for the abnormal network traffic. Smoothing parameter λ_{AEWMA} impacts smoothness of the AEWMA algorithm, and then the AEWMA statistics S_is are smoother when the smoothing parameter λ_{AEWMA} is small; therefore it is propitious to filter the random error such as the *white noise*. The parameter k is an important threshold for measuring the variable e. The AEWMA algorithm can retain e when e is large ($e \geq k$), while retaining smooth e when e is small ($e < k$). So the reasonable λ_{AEWMA} and k are needed for the AEWMA algorithm to retain the exceptional mutation and smooth the random error.

In general, the reasonable λ_{AEWMA} and k need to meet the requirements of the two different situations: the low APT in normal network traffic without any attacks and the high APT in abnormal network traffic under attacks. The λ_{AEWMA} and k which meet these two conditions are the optimal parameters. The solving of the optimal parameters λ_{AEWMA} and k are shown in Figure 9, where λ_{AEWMA} is the x-axis, k is the y-axis, and APT is the z-axis. Figure 9(a) shows that in normal network traffic without any attacks, the APT is low and meets APT $\leq \alpha$ (where α is constant); the suitable parameters are shown in A area. Figure 9(b) shows that in abnormal network traffic under attacks, the APT is high and meets APT $\geq \beta$

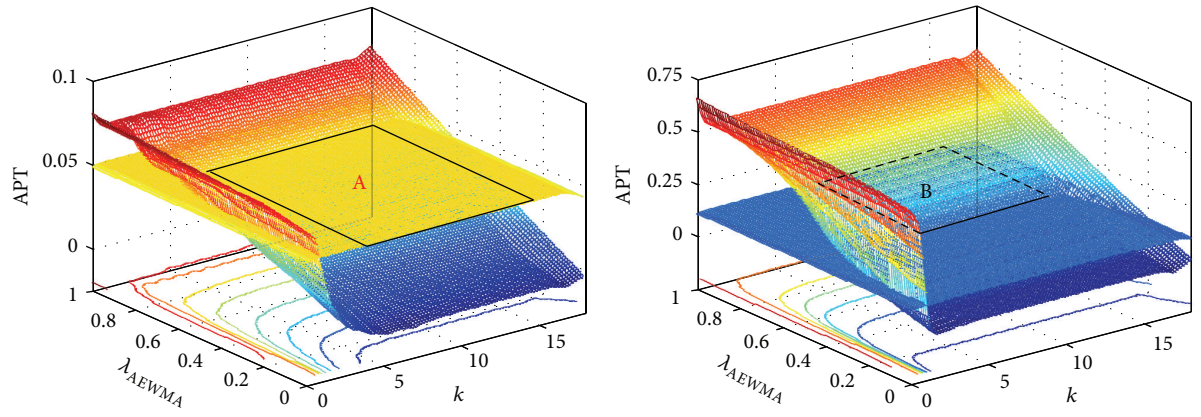


(a) APT and GPT in Scene 1

(b) APT and GPT in Scene 2

(c) APT and GPT in Scene 3

Figure 8: APT and GPT of three scenes.



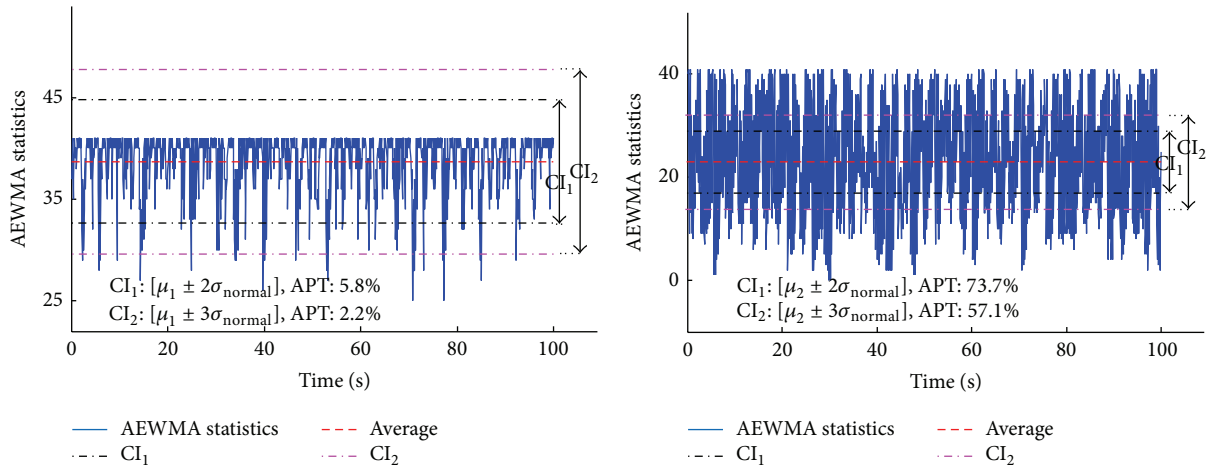
(a) Normal network without any attacks

(b) Abnormal network under attacks

Figure 9: λ_{AEWMA} and k for the AEWMA algorithm.

(where β is constant); the suitable parameters are shown in B area. Finally, the optimal parameters are shown in the A ∩ B area.

The control line h is essential for determining AP. Figure 10(a) shows the changes of APT in confidence intervals $\text{CI}_1[\mu_1 - 2\sigma_{\text{normal}}, \mu_1 + 2\sigma_{\text{normal}}]$ and $\text{CI}_2[\mu_1 - 3\sigma_{\text{normal}}, \mu_1 + 3\sigma_{\text{normal}}]$ in normal network traffic without any attacks (where μ_1 is the average and σ_{normal} is the variance of the *training data*). It can be seen from Figure 10(a) that the smaller the h, the narrower the CI and the higher the APT and therefore the higher false positive rate in normal network traffic. Figure 10(b) shows the changes of APT in confidence intervals $\text{CI}_1[\mu_2 - 2\sigma_{\text{normal}}, \mu_2 + 2\sigma_{\text{normal}}]$ and $\text{CI}_2[\mu_2 - 3\sigma_{\text{normal}}, \mu_2 + 3\sigma_{\text{normal}}]$ in abnormal network traffic under



(a) Normal network without any attacks

(b) Abnormal network under attacks

FIGURE 10: Control line h for CI.

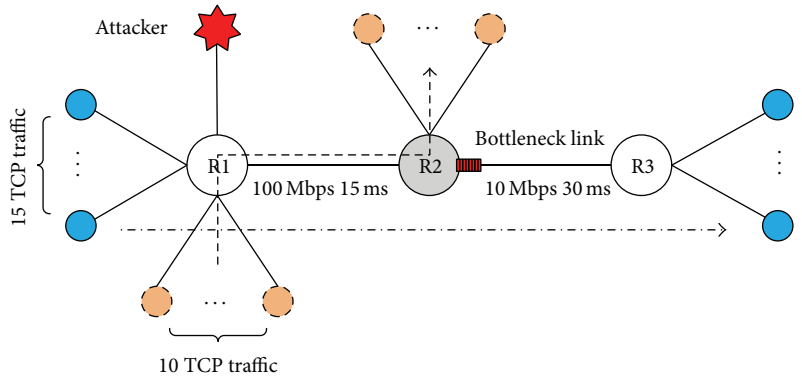


FIGURE 11: The network topology for NS2 experiments.

attacks (where μ_2 is the average and σ_{normal} is the variance of the *training data*). It can be seen from Figure 10(b) that the higher the h, the wider the CI and the lower the APT, and therefore the higher the false negative rate in abnormal network traffic. So the reasonable h is in need to meet the requirements of the two different situations: the low APT in normal network traffic without any attacks and the high APT in abnormal network traffic under attacks, which is the same as λ_{AEWMA} and k. Finally, the control line h which meets the above two conditions is the optimal parameter.

4. The Experiments

In this paper, Experiment I and Experiment II are designed to verify this AEWMA detection method for LDoS attacks. Experiment I which builds the environment of LDoS attacks based on Network Simulator 2 (NS2 for short) [20] proves the validity in detecting the LDoS attacks. Experiment II uses the DARPA99 datasets [21] to evaluate the false positive rate for LDoS attacks, and the AEWMA method is compared with the EWMA method.

4.1. Experiment I. In order to detect the feasibility and accuracy of the AEWMA detection method, the experiment system which is based on NS2 simulator platform is build. The network topology is shown in Figure 11, where R1, R2, and R3 are routers, and the link between R2 and R3 is the bottleneck link whose bandwidth is 10 Mbps and delay is 30 ms. All other links have 100 Mbps bandwidth and 15 ms delay. The network contains 25 TCP connections, in which 10 TCP connections are regarded as the background traffic. All TCP connections use the New Reno congestion control algorithm, and the minimum timeout is 1.0 s. The router queue management mechanism is Randomly Early Detection (RED) algorithm. Other network parameters use the default value of the NS2 simulation platform. Simulation time is from 0 s to 320 s and the background TCP traffic last from 0 s to 320 s, and the LDoS or the DDoS attacks last from 120 s to 220 s. Ten group experiments are designed to test the AEWMA detection method.

Experiment group 1 without any attacks in the network is used to validate the false positives of the Scene 1. Experiment group 2 containing the DDoS attacks (20 M attack pulse) is used to validate the accuracy of the Scene 2. From

Table 1: Experiment I scheme.

Number	Experiment group									
	1	2	3	4	5	6	7	8	9	10
T_{attack} (s)	—	—	1.0	1.0	1.0	1.0	2.0	2.0	2.0	2.0
t_{attack} (s)	—	—	0.1	0.1	0.3	0.3	0.1	0.1	0.3	0.3
R_{attack} (M)	—	20	20	30	20	30	20	30	20	30

Table 2: The detection results of the Experiment I.

Number	Meet C1: APT > Λ_{AP}	Meet C2: GPT > Λ_{GP}	Judgment (the LDoS attacks exist)
Group 1	None	None	None
Group 2	TW_6, TW_{11}	None	None
Group3	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 4	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 5	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 6	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 7	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 8	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 9	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}
Group 10	TW_6~TW_{11}	TW_6~TW_{11}	TW_6~TW_{11}

experiments group 3 to experiments group 10 are used to test the accuracy of the Scene 3. The LDoS attacks parameters (T_{attack}, t_{attack}, R_{attack}) are shown in Table 1.

The sampling time is 0.05 s and $Time_{TW}$ = 20 s. We set the detection time from 10 s to 310 s, so we get 15 TWs in each group, Where the LDoS attacks occur in the TW_6 (120 s~130 s), TW_7 ~ TW_{10}, and TW_{11} (210 s~220 s) of experiment group 3~10. We have got prior 20 groups training data for this network topology; each group training data lasts 3600 s and does not contain any attacks. Based on the training data, the available parameters of AEWMA algorithm are as follows: λ = 0.2, $k = 3\sigma_{normal}$, $h = 3\sigma_{normal}$, Λ_{AP} = 5.2%, and Λ_{GP} = 3.1%.

The experiment results are shown in Table 2. The 15 TWs of the experiment group 1 do not meet C1 and C2; only the TW_6 and TW_{11} of the experiment group 2 meet C1 but does not meet C2; and the TW_6 ~ TW_{11} of the experiment group 3~10 meet both C1 and C2. Therefore we determine that, the experiment group 1 and group 2 do not contain the LDoS attacks, while the TW_6 ~TW_{11} of the experiment group 3~10 contain the LDoS attacks. Experiment results show that the proposed method can accurately and efficiently detect the LDoS attacks.

4.2. Experiment II. Experiment II evaluates the false positive rate of the AEWMA method and the EWMA method when the network is normal (the Scene 1) or when there exist other attacks except LDoS attacks (the Scene 2). This experiment is based on the MIT Lincoln Laboratory's DARPA99 datasets. In DARPA99 datasets, the data of the first week, the second week, and the third week do not contain any attacks, and the

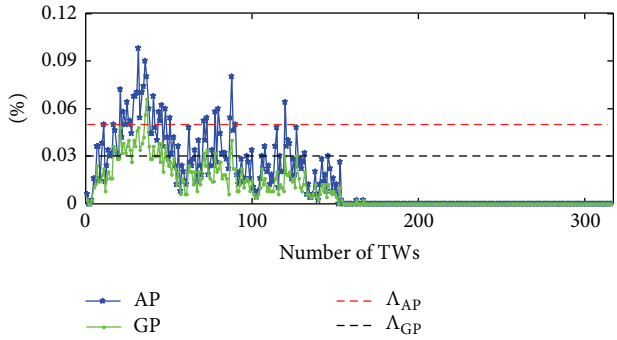


Figure 12: Detection results of Experiment II.

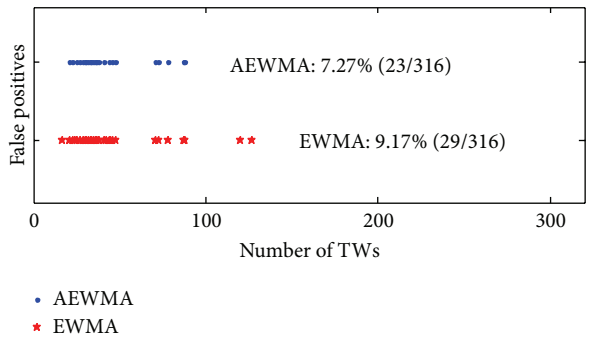


Figure 13: The false positives rate of AEWMA and EWMA.

data of the fourth week and fifth week contain a lot of attacks except the LDoS attacks. In this experiment the dataset of Tuesday in the first week (*inside data*, 0 s~79000 s) is regarded as the training data, and the dataset of Monday in the fifth week (*inside data*, 0 s~79200 s) is regarded as the testing data. The dataset of Tuesday in the first week does not contain any attacks. The dataset of Monday in the fifth week contains 16 kinds of attack types, a total of 84 attacks.

The sampling time is 0.5 s and $Time_{TW}$ = 250 s. The parameters of the AEWMA detection algorithm and the EWMA detection algorithm are shown in Table 3.

Experiment II produces a total of 316 TWs, and detection results are shown in Figure 12. By using the AEWMA method 23 false positive TWs are obtained, and the false positives rate is 7.27%.

While, by using the EWMA method 29 false positive TWs are obtained, the false positive rate is 9.17%. The false positive TWs of these two methods are shown in Figure 13. In Figure 13, the solid points are the false positive TWs. In the EWMA method, in order to measure the exceptional mutation caused by LDoS attacks the smoothing parameter λ_{EWMA} is much larger, and therefore the smoothness is weak. While in the AEWMA method the smoothing parameter λ_{AEWMA} is much smaller, which can keep the smoothness and filter part of the accidental error, and at the same time the exceptional mutation can be retained. So the false positive rate of AEWMA method is lower than that of the EWMA method.

Table 3: The parameters of AEWMA and EWMA.

	AEWMA method	EWMA method
Detection parameters	$\sigma_{\text{normal}} = 5.32$, $\lambda_{\text{AEWMA}} = 0.20$, $k = 3.0\sigma_{\text{normal}}$, $h = 3.0\sigma_{\text{normal}}$	$\sigma_{\text{normal}} = 5.32$, $\lambda_{\text{EWMA}} = 0.95$, $h = 3.0\sigma_{\text{normal}}$
Judgment parameters	$\Lambda_{\text{AP}} = 5.0\%$ $\Lambda_{\text{GP}} = 3.0\%$	$\Lambda_{\text{a}} = 38.9\%$ $\Lambda_{\text{b}} = 10.04\%$

5. Conclusions

In this paper, based the abnormal distribution of the ACK traffic caused by the LDoS attacks, the distribution characteristics of ACK traffic are summarized and a new LDoS attacks detection method is proposed based on the AEWMA algorithm. According to statistical analysis of the ACK traffic characteristics, the LDoS attacks which could lead to distribution deviation of the ACK traffic are concluded. Then the AEWMA algorithm is introduced and the advantage of this AEWMA algorithm compared with the EWMA algorithm is analyzed. Lastly the AEWMA method to detect the LDoS attacks is proposed and the important parameters of this method are analyzed. Experiments have proved that this LDoS attacks detection method is effective, and at the same time the false positive rate of the AEWMA method is lower than that of the EWMA method.

The abnormal network traffic caused by the LDoS attacks is not limited to the abnormal characteristics of ACK traffic. Therefore, more experiments are needed to present the abnormal network traffic caused by LDoS attacks. At the same time, in order to improve the detection accuracy, more detection methods are needed to collaboratively detect and analyze LDoS attacks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] K. Aleksandar and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," in *Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 75–86, 2003.

[2] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the transients of adaptation for RoQ attacks on internet resources," in *Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP '04)*, pp. 184–195, October 2004.

[3] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on internet end-systems," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, pp. 1362–1372, 2005.

[4] L. Mohan, M. G. Bijesh, and J. K. John, "Survey of low rate denial of service (LDoS) attack on RED and its counter strategies," in *Proceedings of the IEEE International Conference on Computational Intelligence & Computing Research (ICCIC '12)*, pp. 1–7, Coimbatore, India, 2012.

[5] X. Luo and R. K. C. Chang, "On a new class of pulsing denial-of-service attacks and the defense," in *Proceedings of the Network and Distributed System Security Symposium*, pp. 2–5, February 2005.

[6] S. Haibin, J. C. S. Lui, and D. K. Y. Yau, "Defending against low-rate TCP attacks: dynamic detection and protection," in *Proceedings of the 12th IEEE International Conference on Network Protocols*, pp. 196–205, 2004.

[7] K. Yu-Kwong, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks," in *Proceedings of the 3rd International Conference on Computer Network and Mobile Computing*, pp. 423–432, 2005.

[8] Y. Chen, K. Hwang, and Y.-K. Kwok, "Collaborative defense against periodic shrew DDoS attacks in frequency domain," *ACM Transactions on Information and System Security*, pp. 1–30, 2005.

[9] S. Sarat and A. Terzis, "On the effect of router buffer sizes on low-rate denial of service attacks," in *Proceedings of 14th International Conference on Computer Communications and Networks*, pp. 281–286, 2005.

[10] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426–437, 2011.

[11] M. Sean and O. Antonio, "Detecting low-rate periodic events in internet traffic using renewal theory," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal*, pp. 4336–4339, 2011.

[12] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, "Flow level detection and filtering of low-rate DDoS," *Computer Networks*, vol. 56, no. 15, pp. 3417–3431, 2012.

[13] X. Luo, E. W. W. Chan, and R. K. C. Chang, "Vanguard: a new detection scheme for a class of TCP-targeted denial-of-service attacks," in *Network Operations and Management Symposium*, pp. 507–518, 2006.

[14] L. Xiapu, E. W. W. Chan, and R. K. C. Chang, "Detecting pulsing denial-of-service attacks with nondeterministic attack intervals," *EURASIP Journal on Advances in Signal Process*, vol. 2009, Article ID 256821, 2009.

[15] K. Chen, H. Liu, and X. Chen, "Detecting LDoS attacks based on abnormal network traffic," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 7, pp. 1831–1853, 2012.

[16] K. Chen, H. Liu, and X. Chen, "EBDT: a method for detecting LDoS attack," in *Proceedings of the International Conference on Information and Automation (ICIA '12)*, pp. 911–916, Shenyang, China, June 2012.

[17] P. Abry and D. Veitch, "Wavelet analysis of long-range-dependent traffic," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 2–15, 1998.

[18] S. W. Roberts, "Control chart tests based on geometric moving averages," *Technometrics*, vol. 1, no. 3, pp. 239–250, 1959.

[19] G. Capizzi and G. Masarotto, "An adaptive exponentially weighted moving average control chart," *Technometrics*, vol. 45, no. 3, pp. 199–207, 2003.

[20] K. Fall and K. Varadhan, "The NS manual," 2009, http://www.isi.edu/nsnam/ns/.

[21] Cyber Systems and Technology Group, "1999 DARPA Intrusion Detection Evaluation DataSets," 1999, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html.