A New Detection Method based on AEWMA Algorithm 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, P. R. China
*Corresponding author, Email: d_tang@hust.edu.cn, kchen@hust.edu.cn

***Abstract*—The Low-rate Denial of Service (LDoS) attack is a new type of DoS (Denial of Service) attack, which produces the similar harmful effect as the DoS attack. It is more difficult for existing DoS detection methods to detect the LDoS attacks because of their distinct characteristics, at the same time the accuracy of the current detection methods for the LDoS attacks is relatively low. However, when the LDoS attacks occur, the characteristics of the ACK traffic have special changes. As the fact that the LDoS attacks led to abnormal traffic and abnormal distribution of the ACK traffic, a new LDoS detection method is proposed based on coefficient of variation and AEWMA algorithm by measuring the abnormal characteristics of the ACK traffic. The NS2 simulations show that this method can detect LDoS attacks effectively with a low false-negative rate and false-positive rate. Based on LBNL Datasets and MAWI Datasets, the experiment results show that this method is more efficient than the EWMA method.**

***Index Terms*—The Low-rate Denial of Service, Coefficient of Variation, AEWMA, Judgment Criterion**

I. INTRODUCTION

The Low-rate Denial of Service (LDoS) [1] attack is a new type of DoS attack, which produces the similar harmful effect as the DoS attack. The LDoS attacks use the vulnerability of TCP congestion control mechanism and periodically send high intensity pulse attack flows to reduce network services capabilities. Because of the much lower average attack traffic of the LDoS attacks it is difficult to distinguish from the normal traffic. Then the LDoS attacks are more covert and can't be detected by existing DoS detection methods.

Currently, some progress has been made in the field of the LDoS detection methods [2, 3], such as the min-TRO method [1], the wavelet analysis method [4], the DTW method [5], the HAWK method [6], the Vanguard method [7], and the EWMA method [8]. These methods are still some deficiencies as the low accuracy, the high false-negative rate, the high false-positives rate, the weak reliability and so on. For example, the EWMA method [8] which is proposed by Chen is based on the EWMA algorithm. This detection method can detect most kinds of the LDoS attack. 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, we analyze the abnormal traffic and abnormal distribution of ACK traffic caused by the LDoS attacks, then we provide a new LDoS detection method based on coefficient of variation and AEWMA algorithm. NS2 simulations show that this detection method for the LDoS attacks has a high accuracy rate, a low false-negative rate and a low false-positive rate. Based on LBNL Datasets and MAWI Datasets, the experiment results show that the efficiency of this detection method has improved compared with EWMA method.

II. DESCRIPTION AND ANALYSIS

A. The Model Description of LDoS Attack

The congestion control mechanism, which is a very important adaptive mechanism of the internet network, has an obvious defect. When the congestion control mechanism is be set to work, the send window and the buffer queue will be rapidly shrink, then the service capability of the network has been a sharply decline. The LDoS attacks exploit this flaw and periodically send high intensity pulse attack flows, then the network repeating congest and cannot provide normal services.

In order to reduce the service capability of the network, the LDoS attacks usually send high intensity pulse data flows. Then the power of the LDoS attacks can be defined as (1).

$$\phi(t)\Big|_{t_{Orig}}^{t_{End}} = \begin{cases} A(t) & (\ nT \le t < nT+\tau\ ) \\ S(t) & (\ nT+\tau \le t < nT+T\ ) \end{cases} \quad (\begin{cases} A(t) > C \\ S(t) < C \end{cases},\ n \in N^{+}, t_{Orig} \le t \le t_{End}\ ) \tag{1}$$

where function $A(t)$ denotes the intensity of pulse attack of this LDoS attack, $S(t)$ denotes the intensity of silent period, C denotes the bottleneck bandwidth, T denotes the cycle of attack, τ denotes the duration time of attack, and this LDoS attack last from t_{Orig} to t_{End}. Moreover in order to get the attack effect, function $A(t)$ and $S(t)$ must meet $A(t)>C$ and $S(t)<C$.

In order to get the much better attack efficiency with minimum cost, function $s(t)$ is usually set to $s(t)=0$. Then, the power of the LDoS attacks is usually shown as (2).

doi:10.4304/jnw.9.11.2981-2986

$$\varphi(t)\Big|_{t_{Orig}}^{t_{End}} = \begin{cases} A(t) & (\quad nT \quad \le t < nT+\tau\ ) \\ 0 & (\ nT+\tau \le t < nT+T\ ) \\ & (\ A(t) > C, t_{Orig} \le t \le t_{End}\ ) \end{cases} \qquad (2)$$

Then the three important parameters (T_{attack}, t_{attack}, R_{attack}) of the LDoS attacks can be defined as (3).

$$(T_{attack}, t_{attack}, R_{attack}) = (T, \tau, \int_0^{\tau} \frac{A(t)}{\tau} dt\ ) \qquad (3)$$

where T_{attack} denotes the cycle of attack, t_{attack} denotes the duration time of attack and R_{attack} denotes the average intensity of attack pulse. Then the average traffic of the LDoS attacks E denotes as $E = R_{attack} \times \frac{t_{attack}}{T_{attack}}$. The attack model and effect of the LDoS attacks is shown in figure 1. Fig. 1(a) shows that the high intensity pulse attack flows is more than the bottleneck bandwidth (R_{attack}>C), while the average traffic of the LDoS attacks is lower than the bottleneck bandwidth (E<C). The affection of the system performance under the LDoS attacks is shown in Fig. 1(b). Fig. 1(b) shows that the system performance of the network has suffered heavy losses when the LDoS attacks occur.

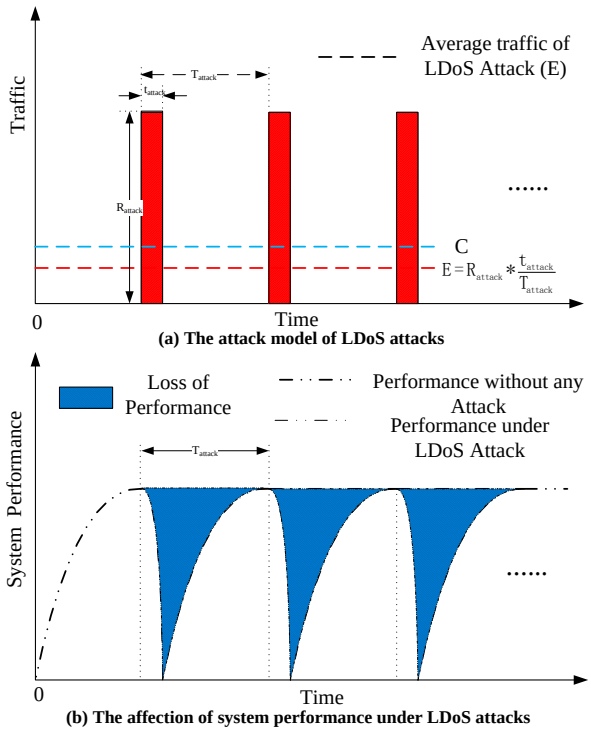

Figure 1. The attack model and effect of LDoS attacks

B. The Abnormal ACK Traffic

In order to get the better attack effect the LDoS attacks usually occur in a "busy" network. In this environment, the LDoS attacks can make a significant impact on network traffic and conceal themselves. According to the focus of this paper, we propose three kinds of representative scenes of the network as follows [8]: (1) Scene 1: the normal network without any attacks; (2) Scene 2: exist other attacks which have made a significant impact on network traffic but except the LDoS attacks, such as the DDoS attacks (3) Scene 3: 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 "effective" TCP traffic and the corresponding ACK traffic will change significantly when the LDoS attacks have occurred. As the actual network TCP connection uses the "Piggybacking" and the "Cumulative Acknowledgment" scheme, for increasing the detection efficiency, we analyze the ACK traffic to detect the LDoS attacks.

In three scenes, the $\mu_i (i=1,2,3)$ and $\sigma_i^2 (i=1,2,3)$ denote the average and the variance of the ACK traffic. In the Scene 1, because the network is normal although occasionally congest, the ACK traffic is more stable, then μ_1 is large and σ_1 is small. In the Scene 2, because TCP connections can hardly establish under the DDoS attacks, μ_2 approaches to zero and σ_2 fluctuates very small. In the Scene 3, because the TCP traffic waves hugely and the ACK traffic fluctuates acutely, μ_3 is small but σ_3 sharply rises. Therefore, the average and the variance of the ACK traffic in three scenes meet $\mu_1 > \mu_3 > \mu_2 \approx 0$, and $\sigma_3 > \sigma_1 > \sigma_2$.

In order to distinguish these three scenes, the Coefficient of Variation (CV) is introduced as follows.

$$CV = \frac{\sigma}{\mu} \qquad (4)$$

Then, the $CV_i (i=1,2,3)$ denote the coefficient of variation of these three scenes. As $\mu_1 > \mu_3 > \mu_2 \approx 0$, and $\sigma_3 > \sigma_1 > \sigma_2$, then the coefficient of variation of three scenes meet $CV_3 >> CV_1$ and $CV_3 >> CV_2$.

Therefore, the LDoS attacks can be preliminarily detect by measuring the coefficient of variation. The advantage lies that this method can filter the normal traffic very rapidly for its low cost and the false-negative rate is low. But the false-positive rate may be high because there are some misjudgments in certain cases. In order to reduce the false-positive rate, the other abnormal characteristics caused by the LDoS attacks should be made a further study.

C. The Abnormal Distribution Of ACK Traffic

A large number of experiments have proved that, according to the central limit theorem the Gaussian distribution can describe most of the real network data traffic distribution [9]. So we use the Gaussian distribution to express the ACK traffic Probability Distribution Function (PDF) of the three different scenes, such as $\Phi_1(x,\mu_1,\sigma_1)$, $\Phi_2(x,\mu_2,\sigma_2)$ and $\Phi_3(x,\mu_3,\sigma_3)$. For those three function Φ_i $(i=1,2,3)$, $x=\mu_i$ $(i=1,2,3)$ is the symmetry axis. In order to compare the distribution of the 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 2.

Fig. 2 shows that there are some differences of the distribution of the functions Φ_1, Φ_2 and Φ_3 after normalized. The differences manifest that there is such an interval, which the probability of which Φ_1 and Φ_2 are outside of this interval is much lower (<1%), but the probability of which Φ_3 is outside of this interval is much higher (>>1%). The probability of outside this interval has the greater "deviation" between function Φ_3 with function Φ_1 and Φ_2. This deviation is the abnormal distribution 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), defined as $CI=[\mu_i - h,\ \mu_i + h]$, where h is called the control factor which determines the size of the CI. The range of CI is associates with μ_i and h. μ_i is the average ACK traffic of the network traffic data which to be tested (called testing data), and h is closely related to the variance of the ACK traffic which we have got the network traffic date without any attack in advance (called training data). A reasonable CI is effective to analyze the abnormal distribution because it decides the discrimination of the abnormal distribution.

According to the analysis above, in the Scene 3, because the LDoS attacks have convulsed the ACK traffic, there would have the two abnormal characteristics as follows: the sharp rise of the coefficient of variation and a significant deviation of the distribution. To the testing data, we can firstly observe the coefficient of variation. If there was the sharp rise of the coefficient of variation, the LDoS attacks may exist and we would continue to measure the distribution of ACK traffic to confirm the LDoS attacks. Otherwise, if there was not the sharp rise of the coefficient of variation the traffic must be normal and without the LDoS attacks.

III. Detection Method

A. Measure the Abnormal Traffic

In order to analyze the abnormal ACK traffic samples, the concept of the Testing Window is defined as follows.

Definition 1: A certain number of consecutive the sample values of the ACK traffic compose a Testing Window (TW).

Where, the length of the sampling time corresponding to a TW denotes $Time_{TW}$.

In the i-th testing window TW_i, the average μ_i and the variance σ_i^2 can be calculated, and then the coefficient of variation CV_i can be calculated as (4). The mapping point in the two-dimensional coordinate system of the group $<i, CV_i>$ is named the coefficient of variation point (CVP), denotes $CVP_i(i, CV_i)$. According to the analysis above, the coefficient of variation of three scenes meet $CV_3 >> CV_1$ and $CV_3 >> CV_2$. Thus there is exist a specified constant Λ_{CV}, making CV_1,CV_2 and CV_3 meet $CV_1 < \Lambda_{CV}$, $CV_2 < \Lambda_{CV}$, and $CV_3 > \Lambda_{CV}$. Then the definition 2 is introduced as follows.

Definition 2: in the TW_i, if $CVP_i(i, CV_i)$ meet $CV_i > \Lambda_{CV}$, then the CV_i called the abnormal CV and the CVP_i is called the abnormal CVP, otherwise the normal CV and normal CVP.

The TW and the CVP of ACK traffic are shown in figure 3. Fig. 3 shows that CV_8, CV_{15}, CV_{16}, CV_{17},and CV_{18} meet $CV > \Lambda_{CV}$, then these CVPs are abnormal CVP. As the fact that the LDoS attacks led the sharp rise of CV, then the LDoS attacks may exist in the TW_8, TW_{15}, TW_{16}, TW_{17} and TW_{18}.

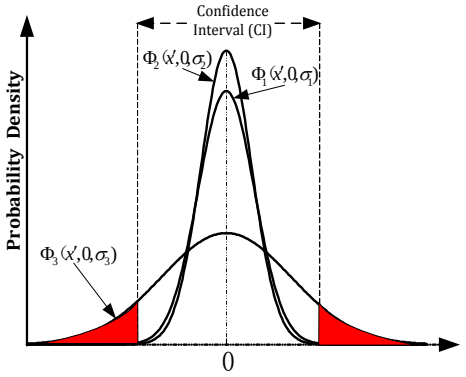

Figure 2. The Normalized PDF of ACK Traffic

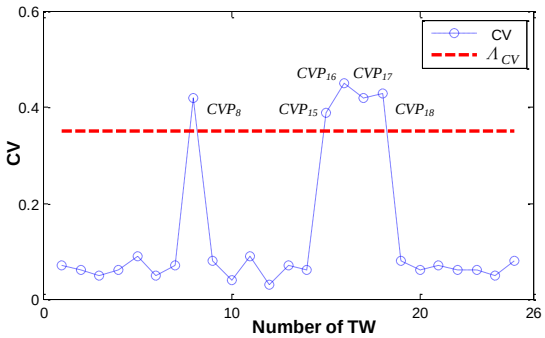

Figure 3. The TW and the CVP of ACK traffic

According to the characteristics of CV for ACK traffic in the three scenes, the judgment criterion is proposed as follows.

Judgment Criterion 1 (JC1): In the i-th testing window TW_i, if $CV_i > \Lambda_{CV}$, then the LDoS attacks may exist in TW_i. Where Λ_{CV} is a specified constant which can be calculated from training data.

Then if JC1 is meeting in TW_i, the LDoS attacks may exist in this TW, thus the other characteristics of distribution need to measure and analyze. While the accidental error would have a negative effect when the distribution of ACK traffic is measured and analyzed. In order to eliminate this negative effect, the AEWMA (Adaptive Exponentially Weighted Moving Average algorithm) algorithm is employed to smooth the accidental error.

B. The AEWMA Algorithm

The AEWMA algorithm is a kind of improved EWMA algorithm. The fundamental principle of the EWMA algorithm is that the more recent of the sample values, the more information and the more weight. Its statistical value is a weighted linear combination of the sample values. The improvement lies that, the AEWMA algorithm which is compared with the EWMA algorithm, uses the weighted nonlinear combination for the sample values. By using a nonlinear weight function the AEWMA algorithm can retain the exception mutation and smooth the accidental error of the sample. So the AEWMA algorithm is adaptable. The arithmetic [10] is shown in (5).

$$\begin{cases} S_0 = \dfrac{1}{n}\sum_{i=1}^{n} X_i & (n \in N^+) \\ S_i = S_{i-1} + \phi(e_i) \end{cases} \tag{5}$$

X_i is the i-th sample values, S_i is the i-th AEWMA statistical value. $\phi(e)$ is a nonlinear weight function called the Score function, which can keep the larger mutation and eliminate the small noise of objects. $e_i = X_i - S_{i-1}$, describe the degree of change between the sample value and the AEWMA statistical value, the Score function $\phi(e)$ is shown in (6).

$$\phi(e) = \begin{cases} e\{1-(1-\lambda)[1-(e/k)^2]^2\} & (|e| \le k) \\ e & (|e| > k) \end{cases} \tag{6}$$

λ and k are parameters of the Score function $\phi(e)$. $\phi(e)$ is a piecewise function so that it can preserve the larger e and smooth the smaller e. The smooth factor λ decide the smoothing ability of AEWMA, and the factor k is the threshold value of the piecewise function. λ and k determine the distribution of the AEWMA statistical values for the ACK traffic.

C. Measure the Abnormal Distribution

By using the AEWMA algorithm the accidental error can be smoothed and the exceptional mutation can be retained, then the abnormal distribution of ACK traffic caused by the LDoS attacks can be exactly measured. When the LDoS attacks exist, the distribution of the ACK traffic will deviate, we use the specified CI to measure the dispersion degree and the oscillation frequency. So the LDoS attacks can be detected by analyzing and contrasting the dispersion degree and the oscillation frequency of ACK traffic's distribution.

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 $< i, S_i^{ACK} >$ is named the AEWMA statistical point (i, S_i^{ACK}). Then the definition 3 and definition 4 are introduced as follows.

Definition 3: As the AEWMA statistical point (i, S_i^{ACK}) in a TW, If $S_i^{ACK} \in CI$, the AEWMA statistical point is called the Normal Point (NP), otherwise, called the Abnormal Point (AP).

Definition 4: A congregation which is composed of a set of consecutive AP is called an Abnormal Chain (AC).

Obviously, each AC contains at least an AP.

The concept of AP and NP denotes the relative position between the AEWMA statistical point and CI, and then the number of AP denotes the dispersion degree of ACK traffic's distribution. Moreover, each AC can denote one oscillation beyond the CI, and then the number of AC can denote the oscillation frequency of ACK traffic's distribution. In order to analyze and contrast the dispersion degree and the oscillation frequency of ACK traffic's distribution in the TW, definition 5 is introduced as follows.

Definition 5: In a TW, the ratio of the number of AP to the number of all AEWMA statistical points is called RAP. The frequency of AC to the number of all AEWMA statistical points in this TW is called FAC.

RAP can denote the dispersion degree of ACK traffic's distribution, and FAC can denote the oscillation frequency of ACK traffic's distribution. Thus the ACK traffic's distribution can be exactly measured.

In the Scene 1, the ACK traffic is stable and S^{ACK} is normal distribution, namely few S^{ACK}s are outside CI. So NP is more and AP is less. Therefore RAP and FAC are both small. In the Scene 2, DDoS attacks cause the network continued congestion, and the traffic is almost zero the same as the S^{ACK}. So RAP and FAC approach to zero. In the Scene 3, LDoS attacks cause the ACK traffic more volatile and the S^{ACK} anomalistic, the dispersion degree and the oscillation frequency increase quickly, so AP is more and RAP is larger, at the same time AC and FAC are larger too.

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

Judgment criterion 2 (JC2): In a TW, if $RAP > \Lambda_{AP}$ and $FAC > \Lambda_{AC}$, then the LDoS attacks may exist. Where Λ_{AP} and Λ_{AC} are the specified constants which can be calculated from training data.

According to the analysis above, if in a TW, JC1 and JC2 are both meeting, the LDoS attacks can be confirmed.

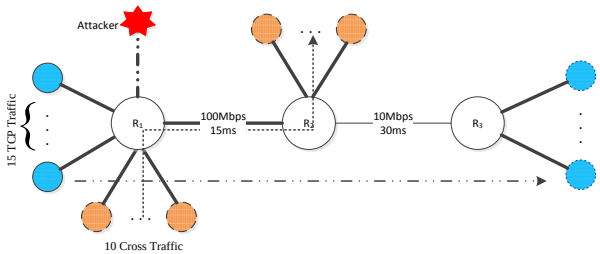

Figure 4. The network topology for NS2 Experiments

IV. EXPERIMENTS

A. Experiment 1

In order to detect the feasibility and accuracy of the AEWMA algorithm, we build the experiment system

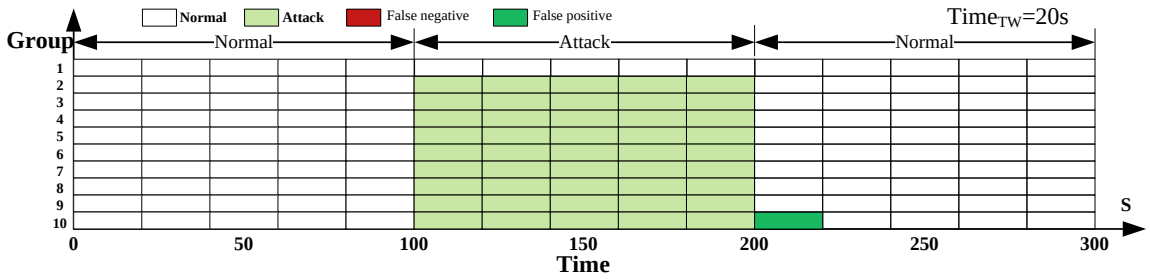

Figure 5. The detection results of experiment 1

based on NS2 simulator platform. The network topology is shown in figure 4, where R1, R2 and R3 are routers, and the link between R2 and R3 is the bottleneck link whose bandwidth is 10Mbps and delay is 30ms. All other links are 100Mbps bandwidth and 15ms delay. The network contains 25 TCP connections, in which 10 TCP connections is regarded as the background traffic [7]. All TCP connections use the New Reno congestion control algorithm, and the minimum timeout is 1.0s. 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 0s to 300s and the background TCP traffic last from 0s to 300s, the LDoS or the DDoS attacks last from 100s to 200s. We design 10 group experiments 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 (20M attack pulse) is used to validate the accuracy of the Scene 2. From experiments group 3 to experiments group 10 are used to test the accuracy of the Scene 3, and the parameters of LDoS attacks (T_{attack}, t_{attack}, R_{attack}) are set as follows: (1.2s, 0.05s, 20Mbps), (1.2s, 0.1s, 20Mbps), (1.2s, 0.3s, 20Mbps), (1.2s, 0.1s, 30Mbps), (1.2s, 0.4s, 30Mbps), (2.0s, 0.1s, 30Mbps), (2.0s, 0.4s, 20Mbps), (5.0s, 2.0s, 20Mbps), We have got prior 20 groups training data for this network topology, each group training data lasts 3600s and doesn't contain any attacks. The sampling time is 0.05s and $Time_{TW} = 20\ s$. Based on the training data, the available parameters of AEWMA algorithm as follows: $(\lambda, k) = (0.2,\ 3.6)$, $h = 3.6$, $\Lambda_{CV} = 0.16$, $\Lambda_{AP} = 5.2\%$, $\Lambda_{AC} = 3.1\%$.

The detection results are shown in figure 5. Fig. 5 shows that this detection method is accurate for the Scene 1 and the Scene 2 and has not produced the false-negative, although the experiment group 10 appears false-positive. The false-negative and false-positive generate at the time when the LDoS attacks have been just beginning or finished. In the TW_{11} of experiment group 10 after the LDoS attacks have been just finished, the t_{attack} is large and the network self-healing process is slow, then the false-positive appears. Experiment results show that false-positive rate is only 2%, so this proposed method has a high accuracy rate.

B. Experiment 2

The experiment 2 evaluates the misjudgment without any attacks. 21 datasets randomly from LBNL (Lawrence Berkeley National Laboratory) Datasets [11] and 24 datasets randomly from MAWI (Measurement and Analysis on the WIDE Internet) Datasets [12] are chosen as the test datasets.

Set $Time_{TW}$=100s , Δt=0.1s , employ separately the data at first 600s of LBNL Datasets and 300s of MAWI Datasets as the training data, then we get the relevant parameters from the training data as shown in Table I.

We get 756 TWs from LBNL Datasets and 217 TWs from MAWI Datasets as the testing data. The detection results of LBNL Datasets by using this proposed method and the EWMA method are shown in figure 6. The detection results of MAWI Datasets by using this proposed method and the EWMA method are shown in figure 7.

TABLE I. THE PARAMETERS OF DETECTION METHOD

Datasets	Parameters				
	(λ, k)	h	Λ_{CV}	Λ_{AP}	Λ_{AC}
LBNL	(0.2, 100.2)	100.2	0.32	10.9%	2.7%
MAWI	(0.2, 87.3)	87.3	0.39	8.2%	4.3%

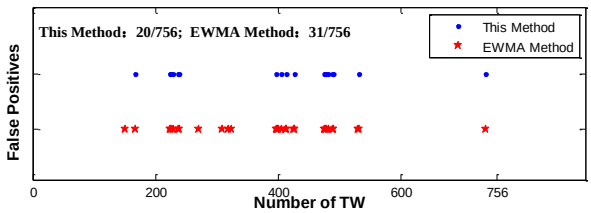

Figure 6. The detection results of LBNL Datasets

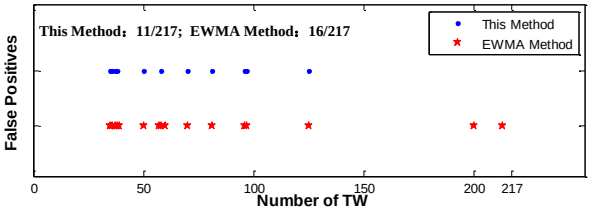

Figure 7. The detection results of MAWI Datasets

By using this proposed method, 20 misjudged TWs for LBNL Datasets and 11 misjudged TWs for MAWI Datasets are produced. So, the false-positive rate of LBNL Datasets is 2.6% and the false-positive rate of

MAWI Datasets is 5.1%. By using the EMWA algorithm, 31 misjudged TWs for LBNL Datasets and 16 misjudged TWs for MAWI Datasets are produced. So, the false-positive rate of LBNL Datasets is 4.1% and the false-positive rate of MAWI Datasets is 7.4%. The detection results of this proposed method and EWMA method are shown in Table II. In this experiment for LBNL Datasets and MAWI Datasets, the results show that the false-positive rate of this proposed method is lower than that of the EWMA method.

TABLE II. THE DETECTION RESULT OF THIS METHOD AND EWMA METHOD

Datasets	False-Positive Rate	
	This method	EWMA method
LBNL	2.6%	4.1%
MAWI	5.1%	7.4%

V. CONCLUSIONS

According to the abnormal characteristics of the ACK traffic caused by LDoS attacks, firstly, the abnormal traffic and abnormal distribution of ACK traffic are summarized. Secondly, the concept of coefficient of variation is used to measure the abnormal traffic, and then the concept of abnormal point and abnormal chain are used simultaneously to measure the abnormal distribution from the dispersion degree and the oscillation frequency. Thirdly, the judgment criteria are developed. Therefore, a new LDoS attacks detection method based on coefficient of variation and AEWMA algorithm is proposed. Two sets of Experiments have proved that this LDoS attacks detection method is effective. In the future work, we will extend the judgment criteria to improve the detection accuracy in the further study of the test parameters.

REFERENCES

[1] A. Kuzmanovic, and E.W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM'03)*, ACM: Karlsruhe, Germany. 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, 2004.

[3] M. Guirguis, et al, "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. Xiapu, 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 (NDSS'05)*, pp. 2-5, 2005.

[5] 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 (ICNP'04)*, pp. 196-205, 2004.

[6] Y.K. Kwok, et al., "HAWK: Halting Anomalies with Weighted Choking to Rescue Well-Behaved TCP Sessions from Shrew DDoS Attacks," in *Networking and Mobile Computing, 2005, Springer Berlin / Heidelberg*. pp. 423-432, 2005.

[7] L. Xiapu, 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.

[8] K. Chen, H.Y. LIU, and X.S. Chen, "Detecting LDoS Attacks based on Abnormal Network Traffic," *KSII Transactions on Internet and Information Systems (TIIS)*, 6(7): pp. 1831-1853, 2012.

[9] P. Abry, and D. Veitch, "Wavelet analysis of long-range-dependent traffic," *IEEE Transactions on Information Theory*, 44(1): pp. 2-15, 1998.

[10] G. Capizzi, and G. Masarotto, "An adaptive exponentially weighted moving average control chart," *Technometrics*, pp. 199-207, 2003.

[11] Lawrence Berkeley National Laboratory (LBNL) and ICSI. LBNL's internal enterprise traffic. http://www.icir.org/enterprise-tracing

[12] G. W. MAWI. Packet traces from WIDE backbone. http://tracer.csl.sony.co.jp/mawi

Dan Tang received his M.S. degree in Huazhong University of Science and Technology (HUST) in June 2006. Currently he is a PhD candidate in HUST. His research interests include the areas of computer network security, computer information security, and architecture of future Internet.

Kai Chen received his Ph.D. degree in Huazhong University of Science and Technology in 2012. His current research interests include computer network application, computer network security and computer network protocol analysis.

Xiaosu Chen is a professor of Huazhong University of Science and Technology. His research interests include computer network application, computer network security, computer network protocol analysis, and image recognition.

Huiyu Liu is a lecturer of School of CS at HUST. In 2011, He received the Ph.D. degree in Systems Architecture from HUST. His research interests include network security, cloud computing and semantic network.

Xinhua Li Currently he is pursuing the PhD. degree in HUST. His current research interests include image recognition, computer network security and network protocol analysis.