A Real-time Detection Method of LDoS Based on Shewhart Control Chart Detection Theory

Kai Chen, Huiyu Liu
School of Computer Sci. & Tech.
Huazhong Univ. of Sci. & Tech.
Wuhan, China
kchen@mail.hust.edu.cn

Xiaosu Chen
School of Computer Sci. & Tech.
Huazhong Univ. of Sci. & Tech.
Wuhan, China
x_s_chen@mail.hust.edu.cn

***Abstract*—The low-rate denial of service (LDoS) attack is a new threat to Internet security. Due to its low rate and high concealment characteristics, LDoS attack is difficult to be detected through the analysis of attack flow directly. Most present methods primarily analysis network traffic or feature of LDoS flows to determine LDoS, but they cannot get the satisfactory outcome. From the phenomenon that TCP flow exhibits special different characteristics under LDoS attack and with the superiority of Shewhart Control Chart in outlier detection, this paper proposes a real-time LDoS attack detection method based on Shewhart Control Chart theory, and devises detection criterions based on abundant experiments. This detection method can detect LDoS attack accurately and effectively.**

Keywords- Low-rate denial of service, Shewhart Control Chart, detection criterions

I. INTRODUCTION

DoS (denial of service) attack is one of the main threats to Internet security. DoS attack usually behaves as distributed denial of service (DDoS). In 2003 Kuzmanovic and Knightly proposed a kind of DoS attack called Shrew at Rice University, and pointed out that just sending a short pulse periodically may cause TCP flow to decline seriously [1]. Afterwards Luo et al proposed another kind of DoS named LDoS (low-rate denial of service) [2] upon the basis of thorough research on the Shrew attack. In 2005, the LDoS attack was found on the Internet2 Abilene backbone network, so LDoS attack became the reality [3].

LDoS attack aims at self-adaptive mechanisms of network, such as the Congestion Control Mechanism of the TCP protocol and Active Queue Management (AQM) mechanism on routers. Periodically, in a specific short time-gap, LDoS attacker sends a massive burst attack data packet to cause the normal TCP data packet to be lost, and then induces TCP flow to "congestion avoidance" repeated, so as to reduce the TCP throughput. The feature of which LDoS intermittent attack makes the average rate of attack flow relatively low, is difficult to identify attack flow in the normal data flow, increases attack efficiency of LDoS significantly, and avoids detection and defense more effective than DDoS. Therefore, most DDoS detection methods impossibly work on it.

Currently, many methods are used to detect LDoS, such as spectral diversity[3], Wavelet Analysis[4], DTW detection[5], HAWK detection[6], Vanguard detection[7] and so on. These methods primarily analysis network traffic or feature of LDoS flow to determine LDoS, but some insufficient exist in them, such as a high false positive rate, a large amount of computation and storage space, weak timeliness.

LDoS attack data flow is difficult to be directly detected and analyzed, due to its low rate and high concealment characteristics. From the phenomenon that TCP flow will display exceptionally under LDoS attack and with the superiority of Shewhart Control Chart in outlier detection, this paper proposes a real-time LDoS attack detection method based on Shewhart Control Chart theory.

II. RELATED WORK

A. LDoS attack PRINCIPL

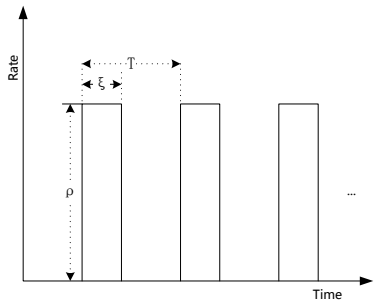

Figure 1. Diagram of LDoS attack

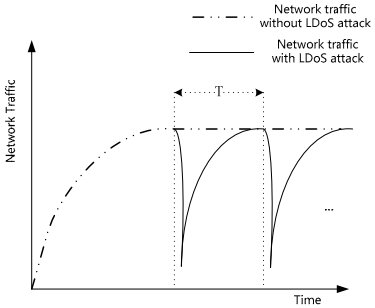

Figure 2. Effect of LDoS attack on network traffic

The current network adaptive congestion control mechanism is that for relieving the congestion state when

congestion occurs in the network, the "congestion avoidance" strategy is adopted to reduce the network traffic, after that the "congestion recovery" strategy is executed to make the network traffic gradually increase to a reasonable load status. It is the primary way to enhance reliability and stability of network. However, the mechanism causes network traffic far lower than usual and results the network throughput decline sharply. The LDoS attacker exactly makes used of this "flaw" of the congestion control mechanism.

At the beginning of attack period T, LDoS attacker sends a data pulse of intensity ρ to make the target network congestion. After ξ time, LDoS attacker stops until the next attack cycle to send an attack pulse again. This action leads to the victim applying congestion control mechanism repeatedly, to cause the average of network traffic to reduce significantly. Figure 1 shows the method of LDoS; Figure 2 illustrates the influence on network traffic under LDoS attack.

Network traffic can recover slowly under LDoS attack, and then at the most time LDoS attack does not cause to refuse to serve completely, so it is inferior in effect to the DDoS. However, the LDoS attack exploits the "flaw" of the adaptive congestion control mechanism, and the intermittent attack allows the average of attack flow traffic to be low. Therefore, it has high concealment and is difficult to be detected directly.

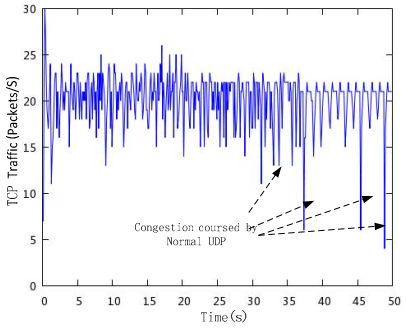

Figure 3. TCP traffic in “Normal network”

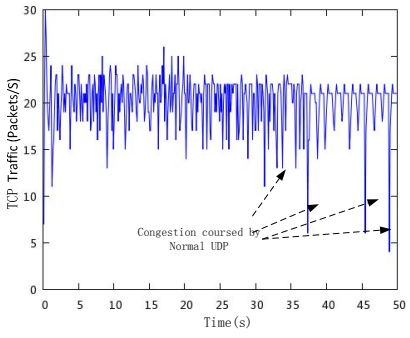

Figure 4. TCP traffic in network under LDoS attack

Aimed at difference congestion control mechanisms, LDoS may be divided into two categories, directing at TCP Congestion Control mechanism and directing at Router Active Queue Management mechanism. The MCI statistic shows that 95% of the total byte number on the Internet and 90% of the total data packet number on the Internet use the TCP protocol to transmit. Those two kinds of LDoS affect network TCP traffic equally. Therefore, this paper will detect LDoS by observing TCP traffic. Figure 3 shows the TCP traffic when the network is "normally"; Figure 4 shows the TCP traffic when the network is under LDoS attack.

It can be seen from Figure 3 that in the network without any attack, the fluctuation of TCP traffic is within a certain range, and because of congestion TCP traffic reduces at 30s, 37s, 45s and 49s, then rebound. We call network is in "stable state" and refer to the TCP traffic as "normal TCP flow" at this time.

In the network under LDoS attack, because the attack pulse generates periodically, TCP traffic fluctuates violently in the attack period, and average TCP traffic is far lower than normal. This phenomenon is shown in Figure 4. We call network at “the non-steady state” at this time and call the TCP traffic "abnormal TCP traffic".

From the above of analysis, we can discover that there is an obvious difference between normal TCP traffic and abnormal TCP traffic. Therefore, according to this characteristic and based on Shewhart Control Chart detection theory, this paper proposes a LDoS detection method by detecting abnormal TCP traffic.

B. Shewhart Control Chart

The Shewhart Control Chart was created by Dr. Shewhart in 1924. At first it was used in production management and then spread to other fields.

It generally can accept that "data" is produced in some kind of "process”, for example, the characteristics of product form in production process, and network traffic generate in the process of network transmission. Shewhart believes that the "data" has two objective laws: First, the fluctuation, that is, the data is not always consistent in a process; second, the distribution, namely that the data accords to a certain rule such as distributing in a value. The fluctuation of the data has two components: the first component is the random component from inner of a process (called the random fluctuation); the second component is the discontinuity fluctuation caused by the external analyzable reasons (called abnormal fluctuation). And the reasons that cause two fluctuation components are called "random factor" and "abnormal factor" respectively. If "data" is affected only by the random factor, its distribution approximate to normal distribution. If "data" is affected by the abnormal factor simultaneously, then the data deviates from the normal distribution.

According to the statistical principle, statistical value θ of the data fluctuates within a certain range, so a region can be chosen to cause that the possibility of θ being out of the region is a tiny value α . This region is called "the confidence interval". Based on Significance Testing principle, Small Probability Event will not happen generally. Conversely, if it happens, it means that the situation has variations, namely existing "abnormal fluctuation" in a process.

Shewhart takes the region [$\mu_\theta - 3\sigma_\theta$, $\mu_\theta + 3\sigma_\theta$] as the confidence interval, and calls $\mu_\theta + 3\sigma_\theta$ the Upper Control Limit(UCL), calls $\mu_\theta - 3\sigma_\theta$ the Lower Control Limit(LCL),and calls μ_θ the Center Line(CL). μ_θ is the mean of θ, σ_θ is the standard deviation of θ, and θ can be obtained by sampling. Shewhart provides many kinds of models to analysis "Process", and this paper only concerns the $\overline{X}$ chart. The basic structure of $\overline{X}$ chart is shown in Figure 5.

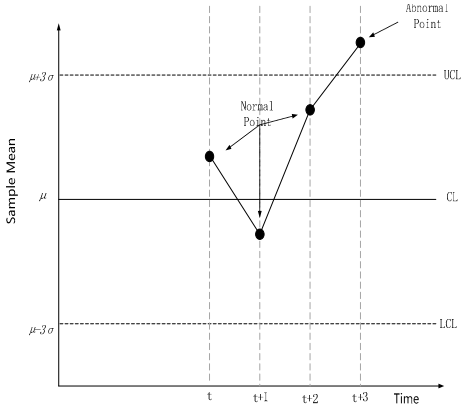

Figure 5. the structure of $\overline{X}$ chart and two kinds of Sample Point

III. LDoS Attack Detection

A. Definitions and Formulas

Let the normal TCP traffic data to be s (t) and abnormal TCP traffic data to be d (t). Under LDoS attack principle, s (t) obeys the normal distribution and has a great difference with d (t). We express TCP flow data at the time t with function f(t), and give a detection period [T，T+T0] in which T0 is the length of the period. If there is only normal TCP traffic in a network, then f (t) is fixed by s (t). According to the normal distribution, the probability of f (t) in confidence interval [μ -3σ , μ +3σ] d the curve of f (t) generally appears as a fluctuations curve fluctuationonfidence interval. μ is the mean value of f (t) and σ was the standard deviation of f (t). Conversely, if curve of f (t) "crthe curve onfidence interval, then in the detection period, f (t) possibly is affected by d (t), that is, the network may suffer the LDoS attack in certain time.

For parameters μ and σ , We get their estimation value $\hat{\mu}$ and $\hat{\sigma}$ through real-time sampling of TCP traffic. First to gain the TCP traffic in real time with the period T0, then to get samples by appropriately continuous sampling of the TCP traffic, and each sample contains a specified number (sample size) of observed values. $\hat{\mu}$ can be obtained by formula (1), and $\overline{X}$ is the sample mean of sample i, and $\overline{\overline{X}}$ is the average of all samples mean, and L is the sample number. $\hat{\sigma}$ is the estimation of σ which can be gotten from formula (2), and $\overline{R}$ is the average of all sample range R, and d_2 is a constant associated with the sample size n.

$$\hat{\mu} = \overline{\overline{X}} = (\overline{X_1} + \overline{X_2} + \ldots + \overline{X_L})/L \quad (1)$$

$$\hat{\sigma} = \overline{R} / d_2 \quad (2)$$

Based $\hat{\mu}$ and $\hat{\sigma}$, confidence interval can be calculated by the formula (3)~(5).

$$\mu \approx \overline{\overline{X}} \quad (3)$$

$$\mu + 3\sigma \approx \overline{\overline{X}} + \frac{3}{d_2}\overline{R} = \overline{\overline{X}} + A_2\overline{R} \quad (4)$$

$$\mu - 3\sigma \approx \overline{\overline{X}} - \frac{3}{d_2}\overline{R} = \overline{\overline{X}} - A_2\overline{R} \quad (5)$$

$A_2 = \frac{3}{d_2}$ is a constant associated with the sample size n, and is called the reliability coefficient.

According to the data of sample, the estimate of f(t) at the time ti can be expressed as:

$<\overline{X_1}$, t1>…$<\overline{X_i}$, ti>…$<\overline{X_L}$, tL> , ti∈[T，T+T0] 1≤i≤L

We call the 2-Tuple Pi=<$\overline{X_i}$,ti> the Sample Point (SP), then a SP sequence in the order of the parameter t is generated in each detection period. According to sample point distribution and the definition of UCL and LCL in Shewhart Control Chart, SP can be divided into two categories defined as follows.

Definition 1 Normal Point(NP) the SP Pi=<$\overline{x_i}$, t_i > is called "Normal Point" if LCL＜$\overline{x_i}$ ＜UCL

Definition 2 Abnormal Point(AP) the SP Pi=<$\overline{x_i}$, t_i > is called "Abnormal Point" if $\overline{x_i}$ ≥UCL or $\overline{x_i}$ ≤LCL

The two types SP is drawn in the chair with their parameters as coordinates, as shown in Figure 5.

The confidence interval which set by Shewhart, namely the so-called 3σ way, means that the confidence level is 99.73%. That is to say, that when the network is in "stable state" the probability of SP falling into the confidence interval is nearly 99.73%. The probability of SP outside confidence interval($\overline{X} > \mu + 3\sigma$ or $\overline{X} < \mu - 3\sigma$) is 0.27%/2=0.135%≈1‰,is a "small probability" . According to Shewhart Control Chart theory, if the network is at "steady state", then we may regard all SP as NP; Otherwise, if AP appears, we may judge that network is at "non-steady state", and may exist abnormal TCP flow. Therefore, by detecting abnormal points, we can find out the abnormal TCP flow in detection period.

To ensure the validity and accuracy of detection, sufficient sample is required by Shewhart Control Chart, so many SP may produce in a detection period. In order to

improve the detection accuracy, according to the viewpoint of local information related, this paper introduces the Detection Window.

Definition 3 Detection Window (DW) The window which takes SP as the basic units and slides on SP sequence following certain rules, is called Detection Window.

Set size of DW to w, then when DW slides, the window maintains a group of continuous SP $\{<\overline{X_i}, ti>\ldots<\overline{X_{i+w}}, ti+w>\}$. Considering the simplicity of detection, we define DW sliding step length as w, then in a detection period DW can slide $\lceil T_0/w \rceil$ times. DW converts the analysis of all SP in a detection period to the analysis of a series of local continual SP.

However, only based on AP existing to judge LDoS is an inadequacy, and may result mistaken sanctions and missed sanctions under at least following three situations.

(1)Even only normal TCP traffic existing in a detection period, there is still 0.27% probability of AP;

(2)While abnormal TCP traffic exists simultaneously in a detection period, the SP corresponding to abnormal TCP flow may not be AP totally;

(3)Abnormal TCP flow may not necessarily be caused by LDoS attack.

To solve the mistaken sanctions and missed sanctions led by above three situations, criterions of LDoS attack detection should be framed. The detection process is as follows: basing on the criterions to analyze the SP of TCP traffic in a detection period, so to discover abnormal TCP traffic, and further to determine whether the abnormal TCP traffic cause by LDoS attack. This process can be divided into two stages, Judging Steady State stage (fast detect) and Judging No-Steady State stage (discovery and analysis exception). The criterions in two stages may be called "Determining Normal Criterions" and "Determining Abnormal Criterions" respectively.

B. Determining Normal Criterions

Judging Steady State Stage give the coarse-grained analysis of SP in a detection period, thus to quickly determine whether the network is in "steady state". The criterions in this stage are defined as follows.

Determining Normal Criterion 1 If all SP in a detection period are judged as NP, it determines that network is in "steady state" in the period.

Determining Normal Criterion 2 If all AP in detection period are caused by "the non-attack origin", it determines that network is in "steady state" in the period.

"The non-attack origin" so-called in determining normal criterion 2 mainly contains the following several kinds of common conditions (not ruling out other conditions).

(1)In a detection period, it may burst a great number of TCP connections to lead to short congestion;

(2)In a detection period, the change of status of the network link may cause the TCP traffic varied in a short-term;

(3)Network congestion in a detection period may also be caused by a burst of massive normal UDP data.

The following rules can be used to judge the above-mentioned conditions.

(1)If in the progressive sliding of DW, the number of AP in DW is always less than α which prior given, these AP may result from “the non-attack origin”;

(2) If in the progressive sliding of DW, every SP in DW is AP, and in next existent DW the first continuous β SP are NP, then all SP in this DW may result from "the non-attack origin", β is a constant given beforehand.

α and β in above rules relate to the detection accuracy, and are called parameters of Judging Steady State.

If not to determine network in "steady state", it indicates that network suffer one or more types of attacks in the detection period. Because the concern of this paper is LDoS, so we need to formulate the judgment criterions of LDoS detection to discover that network is abnormal. Such criterion is called "Determining Abnormal Criterions"

C. Determining Abnormal Criterions

If not able to determine network in "steady state" at Judging Steady State stage, then it is into Judging No-Steady State stage.

The determining abnormal criterions are defined on this: LDoS attack cause TCP traffic to fluctuate continuously, then corresponding SP will continuously distribute inside or outside of the confidence interval, therefore, it generates isolated AP (around the SP all be NP) or a group of continual AP. We refer to this phenomenon as LDoS Attack Phenomenon, and label the isolated AP or the group of continual AP as Abnormal point Group (AG).

A large number of experiments indicate that other types attack will not produce LDoS Attack Phenomenon, so the phenomenon can be used to distinguish between LDoS attack and other type attack. Based on this we define Determining Abnormal Criterions.

Determining Abnormal Criterion If the number of AG in DW is not less than δ at γ times during the DW sliding in a detection period, then it can judge LDoS attack may occur in the period. γ and δ are constants given in advance.

γ and δ are called determining abnormal parameters, and γ can be set according to this rule: initial γ=1, if suspected LDoS attack in the previous detection period, then set $\gamma=\lceil T_0/w \rceil$-1, else γ=1.

However, according to the detection result in only one detection period cannot determine whether the LDoS attack occurs. Under LDoS principle, LDoS attacker should attack sustainably so as to affect TCP streams enough to achieve the purpose of attack. So at least in the continual two detection period LDoS attack is detected, we can suspect that LDoS attack occurs in the network.

IV. SIMULATION EXPERIMENT AND RESULT ANALYSIS

A. Experiment Environment

Simulation experiment is carried on using NS2 (Network Simulator 2). The network topology of experiment is shown in Figure 6, including four TCP Senders, one UDP Senders, one Server (TCP and UDP Receiver) and two Routers.

Propagation Delay of each link is 10ms. The band of the link between Senders and Router A is 15Mb/s, the bank of the link between Server and Router B was 30Mb/s, the link between Router A and Router B is the bottleneck and the band of it is 1.5Mb/s, TCP Sender used Reno congestion control algorithm, the queue management of all router is RED.

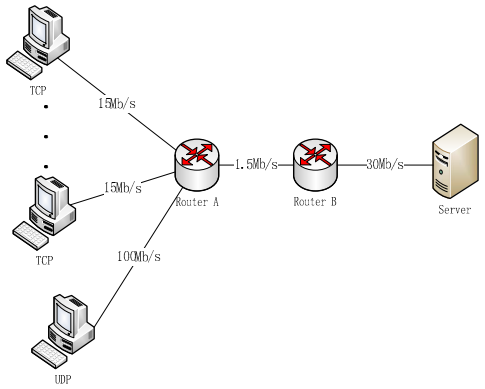

Figure 6. network topology of experiment

The duration of the simulation experiment is 80s; the first TCP flow starts at 0s and stops at 80s; the other TCP flows start randomly and continue 20s. TCP packet size is 1040 bytes, as shown in Table 1.

TABLE I. TCP FLOW PARAMETERS IN THE SIMULATION EXPERIMENT

Data Flow Type	Start Time(s)	Stop Time(s)	Continues (s)	packet size (Byte)
TCP0	*0.00*	*80.00*	*50*	*1040*
TCP1	*0.00*	*40.00*	*40*	*1040*
TCP2	*44.47*	*84.47*	*40*	*1040*
TCP3	*1.14*	*41.14*	*40*	*1040*

Because the timeout-based retransmission asynchronous Shrew attack is the most easily and common LDoS attack mode, so UDP Sender simulates Shrew attack in simulation experiment. UDP attack data flow parameters set as follows: attack period T is 1.4s, the rate of attack pulse burst data is 15Mb/s, attack start time is at 30s, total attack time is 50s.

B. Related parameters setting

First to determine the parameters of sampling, include detection period length m and sampling interval λ and sample size n and reliability coefficient. Due to TCP packet size fixed, for simplifying the analysis, this paper uses the number of TCP packets as the TCP traffic. Let m=40s to divide simulation time into two detection period. From the relevant definitions to know that detection accuracy related the sample interval λ and sample size n and reliability coefficient, so we studied the influence of different values combination of λ and n and A_2 on the experimental result. According to the analysis above of each parameter, λ investigated 10ms, 30ms, 50ms, 100ms, 150ms and 200ms; n investigated 3, 5, 7, and 9; A_2 investigated 3, 4, 5 and 6. Through repeatedly comparative experiment, the parameters final determine as Table 2 shown.

TABLE II. SETTING OF PARAMETERS M, Λ, N AND A_2

Name of parameter	Value
Detection Period *m*	40s
Sampling Interval *λ*	50ms
Sample Size *n*	5
Reliability Coefficient A_2	3

Second to set the LDoS attack detection related parameters, including DW size w, judging steady state parameters α and β, judging non-steady state parameters γ and δ.

According to the values of m, λ and n in Table 2, the number of SP is m/(λ*n)=160. According to the definition of DW, DW should slide at least once in a detection period to cause DW meaningfully. Then let DW size w to 40(number of SP) in this experiment. Therefore DW can slide 4 times in the detection period.

TABLE III. SETTING OF PARAMETERS A, B, Γ AND Δ

Name of parameter	Value
α	4
β	6
γ	≥1
δ	6

From the definition of each rule, we may find out that the settings of α, β, γ and δ affect the rate of mistaken sanctions and missed sanctions. To these four parameters, we try each integer between 1 and 20, and assign by contrast to balance mistaken sanctions and missed sanction. The values of them are shown in Table 3.

C. experiment process and result analysis

We take the TCP traffic from Router A to TCP Senders as sampling object in experiment and divide the examination into two detection periods.

In the first detection period, we obtain 160 continuous samples, and each sample contains 5 observed values, as shown in Table 4. In Table 4,"No" is the number of samples, " Time" is the time of samples producing,"X1" to "X5" are the 5 observed values of each sample, $\overline{X}$ is the sample mean, R is the sample range.

TABLE IV. THE SAMPLES OF THE FIRST DETECTION PERIOD

No	Time	X1	X2	X3	X4	X5	$\overline{X}$	R
1	0.25	2	4	4	4	16	6	14
2	0.5	12	18	14	10	12	13.2	8
3	0.75	9	9	9	3	2	6.4	7
…	…	…	…	…	…	…	…	…
120	30	8	5	10	11	6	8	6
121	30.25	8	6	0	0	1	3	8

122	30.5	2	4	2	2	6	3.2	4
123	30.75	7	3	7	7	7	6.2	4
…	…	…	…	…	…	…	…	…
158	39.5	9	10	8	5	7	7.8	5
159	39.75	7	5	6	7	7	6.4	2
160	40	5	5	2	0	0	2.4	5

According to the data in the Table 4 and formulas in section 3.1 to calculate the parameters of the chart, we get $\overline{R} = \sum_{i=1}^{m} R_i$ /m=4.1687, $\overline{\overline{x}}$ =8.0062,CL=8.0062 , LCL=5.6008，UCL=10.4116.

In the detection period, it constitutes 160 SP. At first to determine all SP by determining normal criterions, but beyond the AP caused by "the non-attack origin", it still exists AP caused by some kinds of attack, as shown in Figure 7. So it can judge that there possibly exist abnormal TCP traffic in the network, and need further detection by determining abnormal criterions.

When DW slips to 30s ~ 40s, there are 20 AP in it. These AP compose 8 AG. According to determining abnormal criterions, it can judge that LDoS attack may occur in the detection period.

The samples obtained at the second detection period are shown in Table 5, and the fields in Table 5 are same as Table 4.

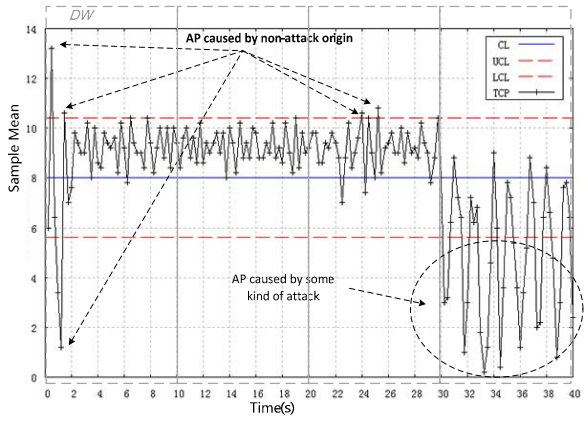

Figure 7. $\overline{X}$ Chart the first detection period

TABLE V. THE SAMPLES OF THE SECOND DETECTION PERIOD

No	Time	X1	X2	X3	X4	X5	$\overline{X}$	R
1	40.2	0	2	0	0	0	0.4	2
2	40.45	0	0	0	0	2	0.4	2
3	40.7	2	4	2	7	4	3.8	5
…	…	…	…	…	…	…	…	…
41	50.2	0	0	1	0	2	0.6	2
42	50.45	2	3	0	4	5	2.8	5
…	…	…	…	…	…	…	…	…
81	60.2	5	3	3	8	6	5	5
82	60.45	3	6	8	6	7	6	5
…	…	…	…	…	…	…	…	…
121	70.2	5	3	3	5	3	3.8	2
122	70.45	2	3	6	5	3	3.8	4
…	…	…	…	…	…	…	…	…
159	79.7	1	5	5	3	7	4.2	6
160	79.95	9	5	8	9	7	7.6	4

According to the data in the Table 5 and formulas in section 3.1 to calculate the parameters of chart, we get $\overline{R} = \sum_{i=1}^{m} R_i$ /m= 4.0437， $\overline{\overline{x}}$ = 3.6225，CL= 3.6225，LCL= 1.2892，UCL= 5.9557.

According to the data in Table 5, it produces 160 SP in the detection period. Based on the DW sliding rule, DW slides 4 times in the detection period. When the DW is sliding, we find that all AP may be caused by attack through analysis of SP in DW. In each time DW slides, the number of AG in DW is 8, 8, 9 and 9 respectively, as shown in Figure 8. In accordance with determining abnormal criterions, there is LDoS attack phenomenon at every time slot DW corresponding, so LDoS attack may occur in this detection period.

Based on the above detection result, it judges that LDoS attack may occur in the consecutive detection period; therefore, we can suspect the network is under LDoS attack and the LDoS starts at about 30s and continues to 80s. The detection result is relatively accurate.

We set Reliability Coefficient A_2=3, that is to say, level of significance of normal distribution is 3‰, it means that the rate of misjudgment is only 3‰ in "stable state" network. This paper use step by step detection mode and apply DW for local detection, so that further reduce the rate of mistaken sanctions. The characteristic of LDoS makes the LDoS attack get an enough effect, unless it continues long time. So this paper samples continuously, and analyses and determines in each detection period, so it gets a lower rate of missed sanctions.

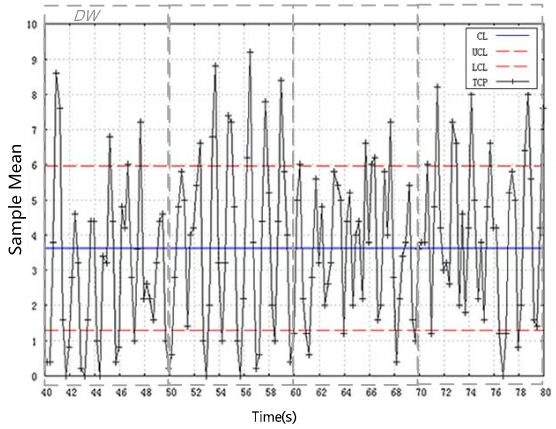

Figure 8. $\overline{X}$ Chart the second detection period

V. SUMMARIES

This paper proposes a LDoS attack detection method based on Shewhart Control Chart theory. Considering the concealment of the LDoS attack, this method does not detect the LDoS attack data, so it is different with present majority methods which directly detect network traffic or LDoS attack traffic. Instead, this paper detects LDoS attack indirectly through the observation of TCP traffic, less calculation, high efficiency and good scalability, and defines a series of detection rules to increase the accuracy of detection. Meanwhile, this method takes sample in real time, and delays only one detection period for analysis, so it has good real-time performance.

After repeat experiments, it proves that this method can detect LDoS attack in time and effectively, without protocol modification and training data and it has the characteristics of less calculation, high velocity, high efficiency, low error rate, simple and easy to implement. It can deploy in any key nodes of the network, and can take bypass monitoring method, so that need not to modify the network architecture, will not affect the performance of the network and get high real-time performance.

However, the actual network current capacity is changeable and complex, and the Shewhart Control Chart theory does not use historical data fully, so just one way to detection and prevention does not really work, and it is better to combine a variety of means to deal with LDoS. Therefore, the future work is to further optimize detection rules and algorithms, and combine with other methods to cooperate detection.

REFERENCES

[1] Kuzmanovic A; Knightly E W. Low-rate TCP-targeted denial of service attacks: the shrew vs the mice and elephants. In: Proceedings of the ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Karlsruhe, Germany, August 2003

[2] Luo X Chang, R K C. On a new class of pulsing denial-of-service attacks and the defense. In: Proceedings of the 12th Annual Network and Distributed System Security Symposium, San Diego, California, USA, February 2005

[3] Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis [J].Journal Journal of Parallel and Distributed Computing, 2006,66(9)

[4] Xiapu Luo, Rocky K. C. Chang. On a new class of pulsing DoS attacks and the defense [A]. In Proc. Network and Distributed System Security Symp (NDSS) [C], California, USA, February 2005

[5] Sun H, Lui J C S, Yau D K Y. Distributed mechanism in detecting and defending against the low-rate TCP attack. Computer Networks [A]: The International Journal of Computer and Telecommunications Networking[C]. 2006, 50(13): 2312-2330.

[6] YU-Kwong Kwok, R T, Yu Chen, et a1.HAWK:halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks [C].In ICCNMC 2005,Germany,2005.

[7] Xiaopu Luo, Edmond W.W. Chan, Rocky K.C. Chang. Vanguard: A new detection scheme for a class of TCP-targeted denial-of-service attacks [A]. Proceeding of the 10th IEEE/IFIP Network Operations and Management Symposium[C], Cannada, 2006.

Published by Atlantis Press, Paris, France.