Research on the Detection of denial service attack based on the correlation of changing points

Li Xiyong [1,a]

Computing Department ,Ping Xiang University, JiangXi,China

[a]lixiyong@126.com

*Li Xiyong

Keywords: CUSUM, Attack detection, Correlation algorithm, Denial of service.

Abstract. The attack detection method of the coherency based on changing point by of multiple message types variables computed CUSUM accumulated value, and according to the changeable correlation analysis, set a reasonable threshold for many types of flooding attack detection, through the experiment on the performance index of the anomaly detection system in the evaluation. In this paper, the attack detection method based on the correlation of the changing point is proposed by calculating the CUSUM cumulative value of the plurality of message type variables, and correlation analysis based on the changing point to set a reasonable threshold to detect multiple types of flooding attacks and to evaluate the anomaly detection system performance.

Introduction

With the widely spread use of the changing point detection algorithm in speech processing, image processing, biological signal automatic analysis, digital signal transmission system, security system detection and other fields, more and more researchers put the changing point theory into the use of the security system. The idea of changing point theory is to describe a statistical model of the information system first, then a sudden change of the model caused by the attack and error, which occurs at the time of the unknown. There are two kinds of methods for detection of point mutations, including batch detection of fixed size (batch detection) and sequence variable (sequential change - point detection). Due to the time sensitivity of the VoIP system, the sequence of change point detection method is mainly used. When it happens, the model can be rapidly detected while the false alarm rate is maintained at a given level. There are two kinds of sequence point change algorithm, CUSUM (sum cumulative) detection and Shiryaev-Pollak detection process. Because of its robustness, low cost and easy implementation, the CUSUM algorithm is widely used in intrusion detection. CUSUM algorithm is also used in the detection process in this paper.

The fast sequence changing point method includes two performance indexes: optimization and equalization, that is, the average detection delay and false alarm rate. In changing point detection algorithm, the false alarm rate is determined to solve the optimization problem so that the average detection delay is minimized. There are two traditional methods to solve optimal equilibrium problems---the minimax method and the worst case delay.

Since the complete call setup is realized by a three-way handshake, therefore variables (SYN, FIN) and (INVITE, 200OK) news only take dialogue process into account instead of the task to establish a process. The INVITE task is completed till the ACK message is received. Hence ACK message must be considered.

The common parameter distribution can not describe the changing law of the SIP message flow. The performance metric must be comprehensively consideration from every aspect. We must fully protect the VoIP network from the proxy server, user agent, and registered proxy server on DOS flooding attack.

Improved detection algorithm

Traditional change point algorithm

Changing point technology is realized by CUSUM technology. Traditional change point technology is described as follows:

At fixed time interval t2, t1,..., the TN detection system of the observation sequence is N1, N2,... , Nn. Attack activity at the time point of TK will be caused by the change of the statistical data of the flow parameters. Assuming that the average value of the change point is μk, and the average value is $\overline{X_K}$. The CUSUM value Sk is shown in the formula (1):

$$S_K = \max\{0, S_{K-1} + N_K - \mu_K - \alpha \cdot \overline{X_K}\} \quad (1)$$

Nk is adjustable parameter, the value is between (0, 1), and the Xk is the upper bound of the value. The choice of a parameter affects the performance of the algorithm; the false alarm rate is increased if it's too big or too small. A value can be set to a constant by experiment and can be calculated by formula (2).

$$0 \le \alpha < 1 - \frac{\mu_k + h_k / T}{\overline{X_K}} \quad (2)$$

hk is the detection threshold at the time tk, and T represents the maximum time to detect the change.

The average number of TK packets in time is estimated by EWMA. As shown in formula (3).

$$\overline{X}_K = (1-\beta)\cdot \overline{X}_{K-1} + \beta \cdot N_K \quad (3)$$

Here 1< beta <1 is a smoothing factor, giving more weight to the current observation value. The comparison between Sk and CUSUM is to detect the change of H value. If the value of tk is greater or equal to the value of H in time Sk, it indicates that the parameter property has changed.

The value of the changing point tk is shown in the formula (4):

$$h_K^{start} = \sigma_{K-1}, h_K^{end} = 0.25 \cdot h_K^{start} \quad (4)$$

When h_K^{start} , h_K^{end} , is the threshold for the beginning and end of the change point in time tk, and σ_{K-1} is the time window tk, data element standard is deviated. The warning is cancelled till τ reaches a specific number by reducing the false alarm rate or the additional combination of counter τ and h_K^{end} .

As shown in formula (5).

Alarm=if(Sk≤ h_K^{end} AND τ≥2，end，to continue) (5)

Improved algorithm for changing point

In the paper, the changing point detection uses changing point and analyzes the correlation among the changing points due to the Dos attack mentioned above with a variety of messages flooding types such as INVITE，Register，Option, which is different from the single variable changing point detection method. The improved CUSUM is based on the online changing point detection by accounting a number of statistical variables values according to the mutation statistics in the time sequence.

Experimental analysis and model verification

There are three experimental cases. The first is only when the normal call data flow without the DoS attack or network congestion. The second is that INVITE attacks the Asterisk server at different ratios. The third includes the normal call date flow and the INVITE flooding.

INVITE, BYE, 200OK, ACK, Register, Option messages are collected in each time period. Here is the conclusion:50% of the phone lasts about 1 minute; 10% of the phone's duration is longer than 10

minutes or even longer. In order to achieve higher detection, the size of the sampling window is set as second. Then, the threshold of each message flow and the detection time are not the same. Compared with the traditional changing point, the detection time is reduced, but the false alarm rate is increased. The parameter =0.98 is set up here, and if the parameter is less than 1, then the value of CUSUM is reduced, and the detection time is increased accordingly. the change of the correlation analysis is increased and the change of false alarm rate is also observed.

Normal CUSUM flow

Figure 1, 2, 3, 4 described the NINVITE-BYE parameters, NACK-200OK parameters, NINVITE-ACK parameters, CUSUM values of NRegister parameters in normal condition. The values of the model are negative, and the fluctuation of [-1.8 and 0] in the interval.

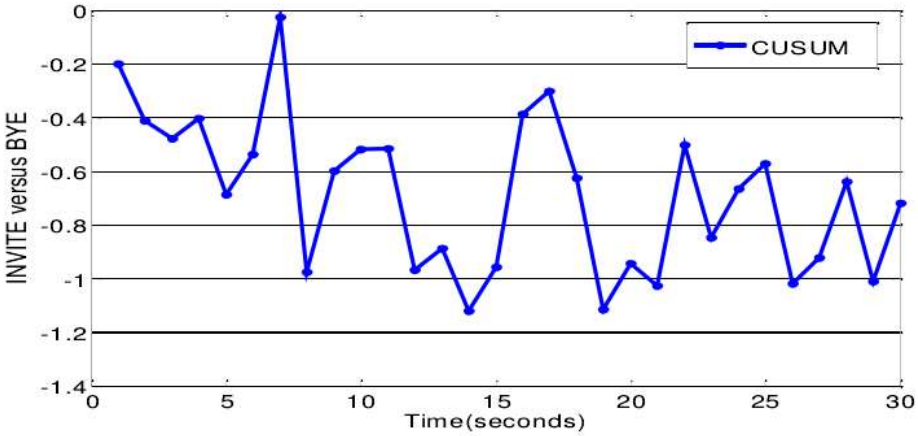

Figure 1 CUSUM values of the $N_{INVITE\text{-}BYE}$ parameter in normal scenes

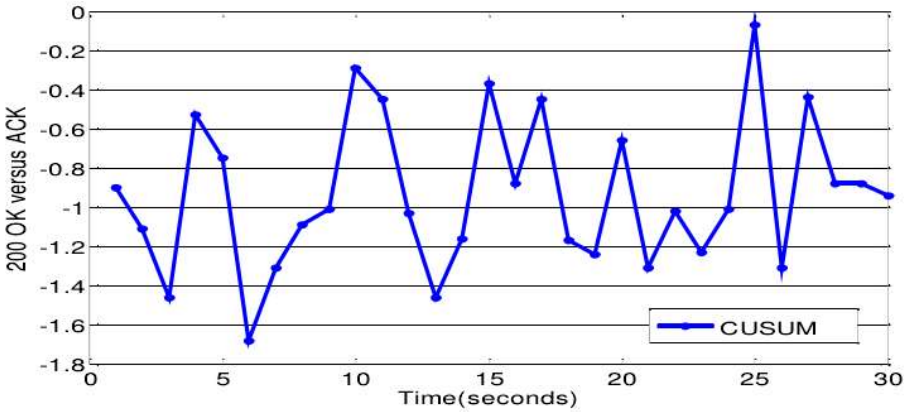

Figure 2 CUSUM values of the $N_{ACK\text{-}200OK}$ parameter in normal scenes

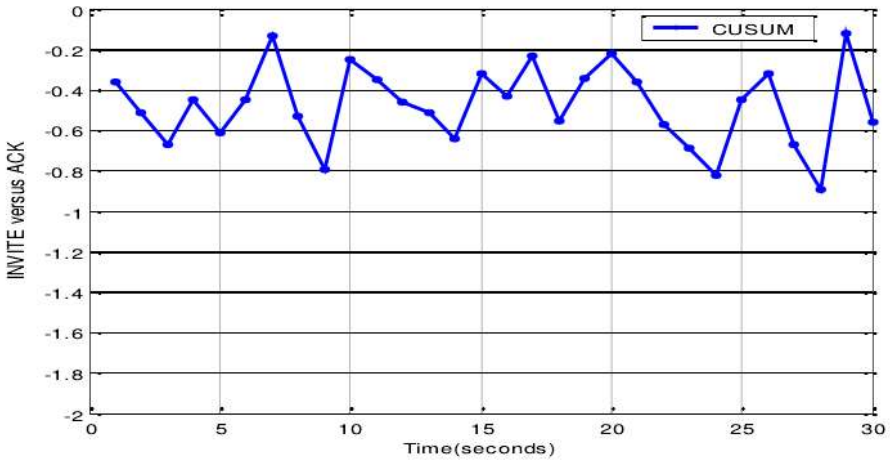

Figure 3 CUSUM values of the $N_{INVITE-ACK}$ parameter in normal scenes

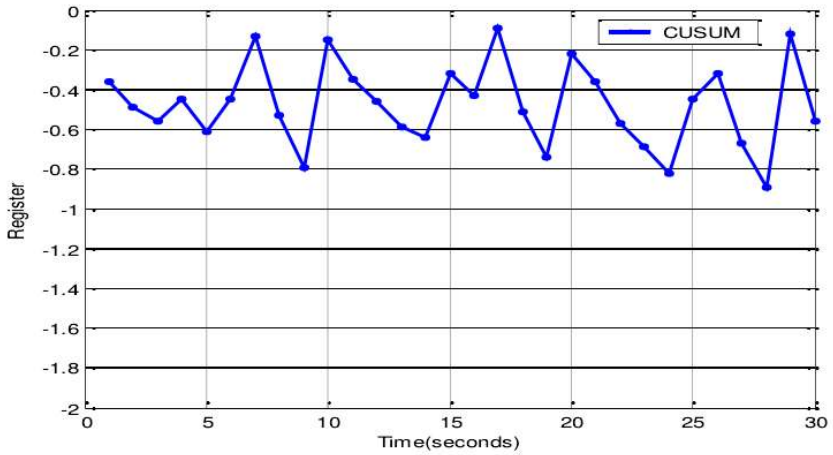

Figure 4 CUSUM values of the $N_{Register}$ parameter in normal scenes

CUSUM value and threshold value of mixed flow

In the case of mixed data flow, the flow of SIPp is used as normal current, and FLOOD INVITE is mixed with 500 INVITE requests per second. Simulate normal traffic and attack traffic for 30 seconds. Setting reasonable thresholds can be very important for the detection rate of flood attack in a very short time. Figure 5 depicts the CUSUM and the threshold of the NINVITE-BYE parameter in a mixed scene. Threshold 7.2, the detection time is close to 9 seconds. Figure 6 shows the CUSUM and the threshold of the NACK-200OK parameter of the mixed scene, the threshold 6.2, the detection time is close to 7.5 seconds. Figure 7 shows the CUSUM and the threshold of the NINVITE-ACK parameter of the mixed scene, the threshold 6.9, the detection time is close to 8.2 seconds. Figure 8 shows the CUSUM and the threshold of the NRegister parameter of the mixed scene, the threshold 6.3, the detection time is close to 8 seconds. From the experiment, the higher the threshold, the longer the detection time.

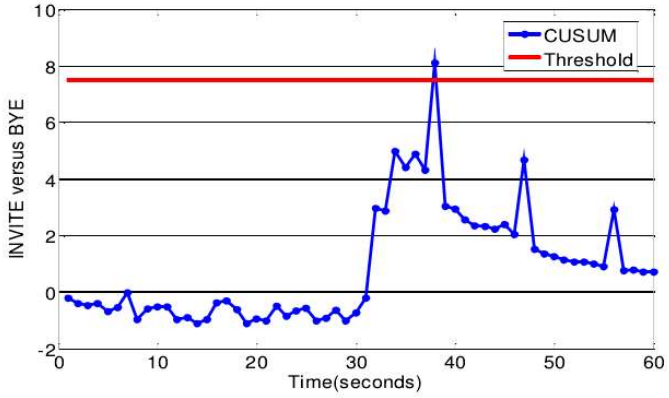

Figure 5 CUSUM values and thresholds of $N_{INVITE-BYE}$ parameters in a mixed scenario

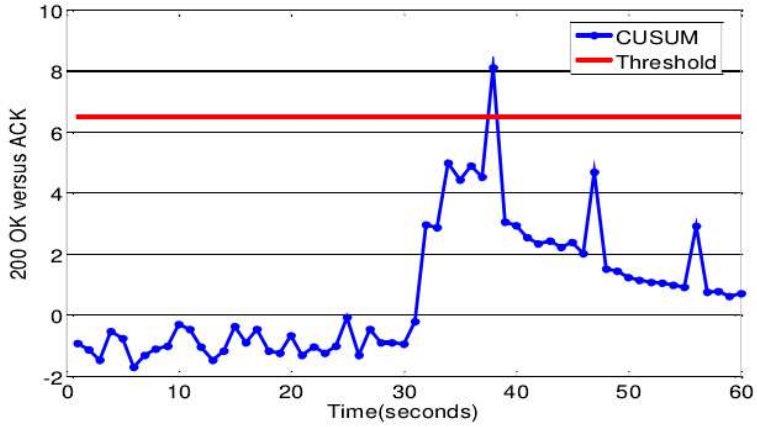

Figure 6 CUSUM values and thresholds of $N_{ACK-200OK}$ parameters in a mixed scenario

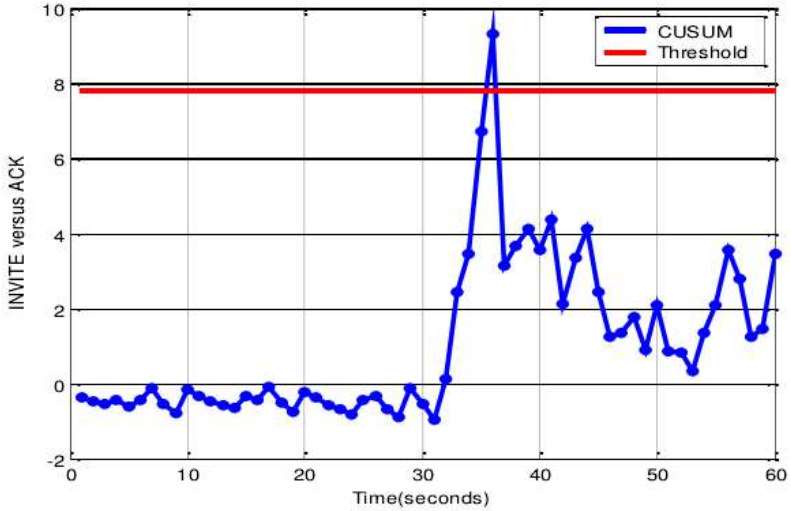

Figure 7 CUSUM values and thresholds of $N_{INVITE-ACK}$ parameters in a mixed scenario

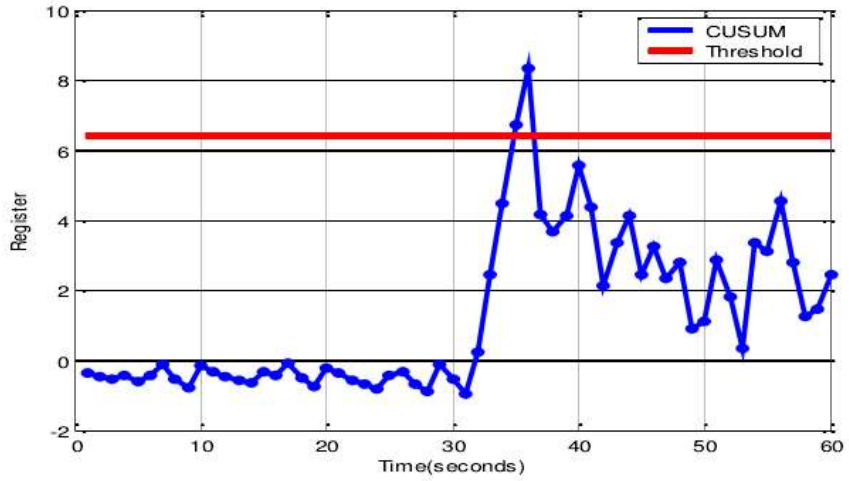

Figure 8 CUSUM values and thresholds of $N_{Register}$ parameters in a mixed scenario

Conclusions

The correlation of attack detection method based on changing point is proposed by multiple messages types variables computed CUSUM accumulated value and with the relevant analysis of the changing point to set a reasonable threshold for many types of flooding attack detection. This model can not only detect INVITE, Register flooding attack, but also can detect Optional flooding attacks in theory.

On the anomaly detection system, performance is evaluated by experiments. The evaluation results show that the detection mechanism has high detection rate, low bit error rate and produces no adverse effect on the quality of VoIP service so that it can meet the requirements of users who are satisfied with the quality of service.

References

[1] Wang H, Zhang D, Shin K G. Detecting SYN flooding attacks.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2002[C].IEEE, 2012, 3: 1530-1539.

[2] Rebahi Y, Sisalem D. Change-point detection for voice over ip denial of service attacks.In Proceedings of Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference[C]. VDE, 2007: 1-7.

[3] Pollak M. Optimal detection of a change in distribution [J]. The Annals of Statistics, 2009: 206-227.

[4] Siris V A, Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks.The proceedings of Global Telecommunications Conference, GLOBECOM'04[C],IEEE, 2008, 4: 2050-2054.

[5] Chang R K C. Defending against flooding-based distributed denial-of-service attacks: A tutorial [J]. Communications Magazine, IEEE, 2010, 40(10): 42-51.

[6] Sun C, Fan J, Liu B. An robust scheme to detect SYN flooding attacks. he proceedings of Second International Conference on Communications and Networking in China, CHINACOM'07. IEEE, 2007: 397-401.

[7] Ohsita Y, Shingo A T A, Murata M. Detecting distributed Denial-of-Service attacks by analyzing TCP SYN packets statistically[J]. IEICE transactions on communications, 2009, 89(10): 2868-2877.