Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A PREVENTION MODEL AGAINST SIP FLOODING ATTACKS

[1]XUEHUA YANG, [2]HONGBIN LI

1College of Educational Technology, Shenyang Normal University, Shenyang 110034, Liaoning, China

[2]Shenyang Institute of Computing Technology Chinese Academy of Science, Shenyang 110168, Liaoning, China

ABSTRACT

Through deeply analyzing on the principle, mode, character of SIP DoS and the flooding attacks faced by SIP network, the prevention model to combine a dynamic threshold adjustment with real-time dynamic prevention for SIP flooding attacks was proposed. This model included logically chi-square traffic judgement model, cumulative statistics model and IP prevention model, among which chi-square traffic judgement module and cumulative statistics module were combined to dynamically adjust the threshold and detect SIP flooding attacks, and IP defense model dynamic prevented IP-based SIP flooding attacks. The experimental result shows that the model can effectively detect and prevent the SIP flooding attacks, and reduce the probability of SIP proxy server or IMS server been attacked when the SIP network is on the abnormity.

Keywords: *Session Initiation Protocol, Flooding Attacks, Chi-Square Traffic, Cumulative Statistics, Threshold Dynamic Adjustment*

1 INTRODUCTION

With the IMS technology[1] and IMS product maturing, major carriers at home and abroad have begun to deploy IMS/SIP system, and some carriers are doing the relevant tests. Because of its ease of use, SIP protocol has become the core protocol of VoIP, IMS and IPTV. At the same time, NGN architecture defined by ETSI and ITU-T also adopt the SIP protocol. SIP is mainly used to resolve the signaling control of IP network, and process the session management, call establishment, modification and termination of multimedia sessions[2]. Relative to the PSTN network, SIP protocol works in the open IP network, it not only suffers from the challenge from traditional network attacks, but also it deals with SIP-specific attacks[3]. NIST takes DoS attacks as a serious security threat to VoIP network architecture[4]. In the analysis of security threat in converged network, DoS attacks have become a most important security problem. Sprint, American telecommunications company, claimed that detection technology against the common type of DoS attacks can't solve the SIP-based VoIP attacks, they recommended SBC as the first line of DoS detection and prevention.

Flooding attacks including single-source flooding attacks and distributed flooding attacks, have become the main form of SIP service attacks in recently study on SIP DoS attacks. Iancu et al. proposed a DoS flooding attacks mitigation method of host-based packet rate limiting, which calculated the SIP request messages numbers of each source IP in a predefined time period, when the number of SIP messages reaches the maximum threshold settings by this system, the messages will be discarded[5]. Reynolds et al. proposed a detection mechanism which used the CUSUM algorithm to detect SIP-based single-source flooding attacks, which need set the threshold to generate the correct alarming information [6]. Rebahi et al. proposed a CUSUM algorithm based on change point detection method to solve the detection of multi-source flooding attacks, but it couldn't solve the dynamic thresholds settings and defense problem[7, 8]. Sengar et al. proposed a flooding attacks detection method that based on Hellinger distance calculation algorithm, and this threshold could be dynamically adjusted, but it did not provide an method of reducing flooding attacks[9]. Chen and Ehlert et al. proposed a SIP state machine-based flooding attacks detection and defense mechanisms which could deal with multi-source flooding attacks. But the reduced mechanism was relate to the threshold of flooding attacks set by this system, and it needed maintain status information and the system resource consumption would been increased dramatically [10,11]. Bouzida proposed an intrusion detection model based on decision tree. Training data sets for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

decision tree had a great influence on these results, and training and learning process required lots of system resources[12]. Fang-Yie Leu et al. proposed a chi-square statistics method of detecting DoS and DDoS attacks in which the alarm threshold could not be dynamically adjusted, and meet the complex network environment[13]. Wenhai Li et al. proposed a CUSUM algorithm based on the change-point detection method of detecting DoS attacks, but the static threshold was set directly and affected the detection accuracy in this algorithm[14].

From the above analysis, we can see the detection and defense research on the SIP flooding attacks is mainly in the theoretical orientations, so it can not really been really used, and the simplest detection technique is to set a static threshold value(eg, snort). Although this static threshold method is easy to implement, there is the threshold selection problem for the existence of specific network environment. For the state machine model, it need maintain the SIP transaction status, consume system resources, and detect slowly. For pattern classification techniques (Bayesian, decision tree, SVM), the training model is essential for the detection system, so the adequacy of the training model has become a problem of pattern classification techniques. It has a significant impact on the test results for the detection means using statistical features, the selection of statistical feature and relevant parameters, and it also needs some specialized field knowledge. Most of the system has a poor real-time problem for defense system. If this system has a large detection delay, it will lead to poor availability of defense system, can not real-time defense SIP attacks. Considered with a view to their practical application, according to the chi-square traffic, cumulative statistics, SIP sessions and SIP network features a SIP flooding attacks prevention model is proposed, which combine dynamic threshold adjustment with real-time dynamic defense to improve system's capacity against SIP flooding attacks, and designs some appropriate experiments to validate this defensive model. Experimental results show that the SIP defense model based on the chi-square cumulative statistics and calculation can greatly improve the defense capability of SIP/IMS system against the SIP flooding attacks, especially the single-source flooding attacks.

2 RELATED KNOWLEDGE

2.1 The Principle of Sip DOS Attacks

To divide from the principle of SIP attacks, SIP DoS attacks can be divided into two categories: one is SIP logic attack, including SIP malformed messages attacks, SIP signaling attacks and SIP messages tampering, the other is SIP flooding attacks, including single-source flooding attacks and distributed flooding attacks. SIP logic attack direct at defects of SIP server or interactions of SIP protocol, signaling through interaction with the SIP server to complete the attack on the target server. Flooding attacks is that the attacker sends a large number of SIP requests to the SIP server in a short time to run out of its computing power, memory or bandwidth resources so that the server can't provide the service for legitimate clients.

2.2 The Manner of SIP DOS Attacks

For SIP flooding attacks, attackers mainly sends a large number of INVITE, REGISTER and other messages to the SIP server that need been summary authenticated so that it can been challenged, and the attacked server makes a large number of MD5 calculations when it generates nonce value to consume the server's processing power, so that the server's the burden on the server is added through the retransmission to challenge information. For the INVITE flooding attacks, the attackers send these response messages to the server in three ways: 1) the attackers only send a large number of INVITE messages and do not been respond, and it is very difficult to track the attack for the attackers forging the source IP; 2) the attackers send a large number of INVITE and ACK messages, so that it will result in the more waiting time longer, and consume the more memory resources; 3) the attackers send a large number of INVITE, ACK, and false identity messages, and it requires complex MD5 calculations for the wrong authentication information to consume server's computing resources.

2.3 SIP session establishment flow

As shown in Figure 1, A typical SIP session process is depict between UAC-alice and UAS-bob. Alice and bob establish this session through INVITE, 200 OK, ACK three-handshake, and they use the SDP message in SIP message body to consult session parameters, and transmit media data through these parameters at the end of the session. UA terminates the current session by a BYE message. However, for SIP flooding attacks, they do not establish SIP sessions, generally above the dotted line in Figure 1. In order to ensure the process speed and effectiveness of SIP flooding attacks, SIP flooding attacks occurred mainly in the first three steps of SIP sessions, but there are lots of DoS attacks forging the fourth packets in order to conceal and achieve better effectiveness.

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

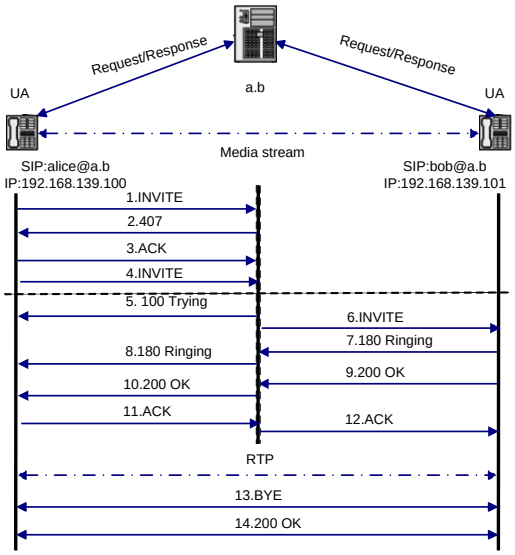

Figure 1: SIP Session Flow

2.4 Chi-Square Statistics

Through analyzing on the SIP session establishment process in section 2.3, the distribution of the number of SIP messages shows a stable distribution under normal circumstances[7]. These messages include INVITE, ACK, 200 OK; REGISTER, 200 OK and OPTION, 200 OK. This paper gives a scenario in SIP flooding attacks that the attackers can not complete the session establishment process, leading to abnormal distribution of SIP messages in section 2.2. Therefore, SIP flooding attacks can be detected through changes in the distribution of SIP messages. The paper use chi-square statistic method to measure the distribution similarity of SIP messages based on sliding time window, the chi-square statistic is calculated as Formula (1). Where k is 3, 2, 2, ni represents the message msgi proportion in current time window, ni' represents msgi proportion in previous time window, which msgi is INVITE, ACK, 200; REGISTER, 200 OK and OPTIONS, 200 OK.

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - n_i')^2}{n_i'} \qquad (1)$$

The message number in normal SIP session is shown in Figure 2. It can be seen from the figure 2 that the percentage of SIP messages will fluctuate because of network data packet loss, but it basically remains the same percentage. So the value of chi-square statistic should be close to zero.

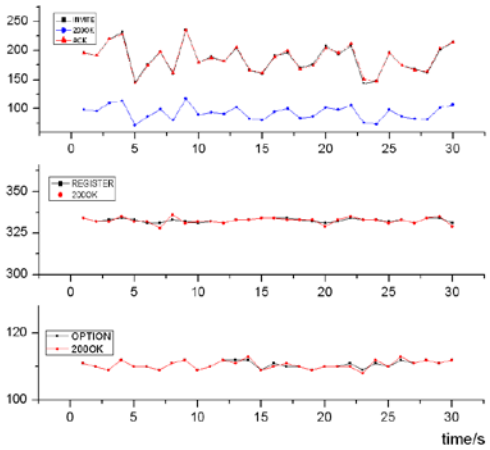

Figure 2: Messages Number In Normal Session

As the chi-square statistic has some small changes and low sensitivity, especially when there are a big concurrent number in the case of system, the chi-square statistic is the same when low-flow attacks occur, and it will cause serious omission. In order to improve system sensitivity and detection accuracy, the deformation chi-square statistics is used while allowing the adjustment of the threshold. The deformation chi-square statistic is calculated as Formula 2. Where k is 3,2,2, ni represents the message msgi proportion in current time window, ni' represents msgi proportion in previous time window, which msgi is INVITE, ACK, 200; REGISTER, 200 OK and OPTIONS, 200 OK.

$$\chi^2 = \sum_{i=1}^{k} \frac{|n_i - n_i'|}{n_i'} \qquad (2)$$

There are a big concurrent number In the case of the system. Changes of chi-square statistic caused by low-flow attacks is small, if the threshold is over the general setting value it will be omitted. In order to avoid the omission of low-flow attack, the number of messages per second to detect the attacks is required more than 100 in the system, for which concurrency-related threshold value is set, the threshold limiting is calculated as Formula (3). Where k is 3,2,2, nc is the proportion of msgi in ideal case that the concurrent occurrence is C and the number of messages per second is 100 when attacked, ni is the proportion of msgi in an ideal case, which msgi is INVITE, ACK, 200 OK; REGISTER, 200 OK and OPTIONS, 200 OK. In order to reduce the times of the threshold calculated, the concurrent value C is made bigger than the concurrent number and is smallest integer multiple of 100.

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$T_{\max} = \sum_{i=1}^{k} \frac{|n_c - n_i|}{n_i} \quad (3)$$

3 PREVENTION MODEL

SIP flooding attacks prevention model is mainly designed for flooding attacks in SIP network, especially for single-source flooding attacks. The purpose is to improve the system ability against SIP flooding attacks, to prevent been submerged by single-source flooding attacks under high concurrency. In this model, a threshold Talarm is set, which expresses chi-square statistic threshold alarm value for SIP messages. The chi-square statistic threshold alarm value will be dynamically adjusted based on cumulative statistics model, and defense model is shown in Figure 3.

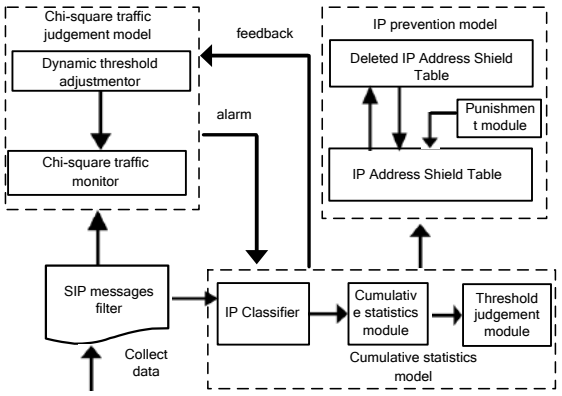

Figure 3: SIP Dos Attacks Prevention Model

3.1 Working Process

Defense model works as follows:

1. Capturing SIP data from network card by using PF_RING [2], and extracting some key data (call-id, message type, the first VIA and source IP address), then giving it to chi-square traffic judgement model and cumulative statistics model for parallel processing;

2. Chi-square traffic monitor processes the collected SIP feature data further to get the data to calculate the value of chi-square statistic, and uses these data to calculate chi-square statistic value;

3. Chi-square traffic monitor inspects whether the chi-square statistic exceeds the threshold value. The threshold Talarm is set relatively small when the system is initialized, and the default value is 0.001;

4. Cumulative statistics model receives SIP feature data from SIP messages filter, then it adds up three types of messages INVITE, REGISTE and OPTIONS at unit time at the beginning according to classified IP address, counts cumulative number of IP addresses, and takes this value as the number of concurrent users at unit time. At last latest statistical results is compared. If the compared value is 100 greater than last value, the concurrent information is fed back to the chi-square traffic judgment model;

5. If alarming, the cumulative statistics model is notified, and the threshold judgment module of cumulative statistics model determines the cumulative results of cumulative statistics module. If all the statistics results are not greater than 10, there is no invasion of the results which will be fed back to the chi-square traffic judgment model; If some statistics results are greater than 10, the user of this IP is attacker, step 8 is performed, and the chi-square traffic judgment model is fed back that there is a invade happened;

6. Threshold dynamic adjustmentor makes different adjustments according to the feedback information given by step 5. If there is no invade information, it will automatically increase the threshold to 4 times of initial value. Otherwise it will lower this threshold 2 times of initial value. If the system had ever been adjusted from high value to low value, it does not been increased to four times, increase the value of 1 times of initial value which is the optimal value;

7. Threshold dynamic adjustmentor uses the Formula 3 to calculate the upper threshold according to the feedback concurrent information at step 4 and compares with the current threshold. If the current threshold is greater than the upper threshold, the upper threshold is taken as current threshold, and the threshold value is re-adjusted;

8. IP defense model checks whether the forbidden IP is in current IP address mask table based on tests results of step 4. If the forbidden IP is in it, prohibition time will extend to 2 times of prohibition time for this record; Otherwise it will check whether recently deleted IP address mask table has the forbidden IP address. If there is this IP, this record will be re-added to the current IP address shield table, while the prohibition time extended to 2 times of prohibition time of this record. The IP address in recently deleted IP address shield table will remain 24 hours according to added time, and it will be automatically deleted from the temporary table 24 hours later.

3.2 System Module

3.2.1 SIP messages filter

This module firstly collects SIP data from NIC and gives them to parse module for processing; Achieving bypass data acquisition by using

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PF_RING technology, the kernel layer implements by adding SIP packet filtering plug-in, and discards the non-SIP data directly in the kernel layer. It is responsible for processing SIP traffic in SIP network, extracting the feature of SIP message preliminary and storing, supplying data for the chi-square traffic judgment model and cumulative statistics mode. The SIP feature data includes SIP messages timestamp, source IP address, the first via, SIP messages type and call-id.

3.2.2 Chi-square traffic judgement model

This model consists of chi-square traffic monitor and threshold dynamic adjustmentor. Chi-square traffic monitor processes the SIP feature data further to get the data for calculating the value of chi-square statistic. This model uses processed data to calculate the chi-square statistic, and determines whether an exception occurs. Threshold dynamic adjustmentor is responsible for adjusting the threshold of alarm dynamically based on the results fed back by cumulative statistics model.

3.2.3 Cumulative Statistics Model

This model consists of IP address classifier, cumulative statistics module and threshold judgment module. IP address classifier mainly charge of the classification of the IP address for SIP feature data; Cumulative statistics module calculates the total number of INVITE, REGISTER and OPTIONS messages of classification IP addresses in the specified time, cumulative number of IP addresses in the specified time, and it take this value as the number of concurrent users in the specified time. Threshold judgment module is responsible for comparing statistical results and the setting threshold, feeding the results to chi-square traffic monitor module, and notifying the ban IP address to IP defense model.

3.2.4 IP defense model

This model is mainly responsible for adding the SIP firewall rules including current IP address shield table, recently deleted IP address shield table and punishment module. These features are described in table 1, IP Addresses means the source IP address pairs of SIP messages, Tnum means the prohibited time. Punishment module is responsible for punishment of the prohibited time in SIP firewall rules. If this address is in serial time, it gives double punishment to the prohibited time of this IP address (prohibited time*2).

TABLE I : SIP Firewall Rules

IP Addresses	T_{num}(s/unit)
202.96.64.12，192.168.139.80	10

The above strategy has a problem that there are many sessions in IMS server or SIP server at the same time, this may be seen the normal communication in SIP proxy server as a DoS attacker, then it may result in false judgment. To solve this problem, a trusted host list is added, these addresses of the trusted IMS server or SIP server are added to the trusted host list. Hash table is used to improve the execution efficiency.

4 IMPLEMENTING OF KEY TECHNOLOGY

4.1 Storage Structure Of IP Address Pairs

As its possible that there are thousands of sessions coming from different IP at the same time, these IP information need to be stored before statistics, a hash table IP_Detect is built, which is used to store all IP addresses information. The structure of IP_Detect is shown in figure 4.

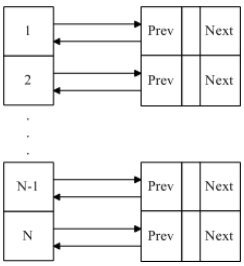

Figure 4: IP_Detect structure

Storage structure of fsm_t is defined as follows:

```
typedef IP_fsm{
    char * private_ip; // private IP address
    char * public_ip;  // public IP address
    int md_ip_md;      // the hash value
    ……
    struct fsm_t *prev;  //previous IP hash
    struct fsm_t *next;  //next IP hash value
}fsm_t;
```

4.2 Algorithm

Traffic anomalies need be detected in implementation of the model, so traffic anomaly detection algorithm and IP_Detect table establish algorithm are used; Otherwise dynamic adjustment of the threshold and punishment for the prohibited time of IP address also need be used, so the dynamic threshold adjustment algorithm and the time penalty algorithm are introduced as follows.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2.1 Traffic anomaly detection algorithm

Using χ^2 to measure the stability of SIP messages distribution, using the SIP message's distribution of adjacent sliding time window to calculate the χ^2, the algorithm is described as follows:

1. Calculating the distribution of SIP messages (INVITE, ACK, 200 OK; REGISTER, 200 OK; OPTIONS, 200 OK) in current window separately;
2. Sliding the time window and recalculating the distribution of SIP message in current time window;
3. Using the distribution of SIP messages calculated in step 1 and 2 to calculate χ^2 according to formula 2;
4. Determining whether χ^2 is bigger than the set threshold. If it is bigger than before, it is sent to cumulative statistics model for processing;
5. Repeating steps 1 to 4.

4.2.2 IP_Detect table establish algorithm

IPDTEA(IP detect table establish arithmetic) table creation algorithm is described as follows:

```
Function NodeAdd(msg){
        IP = GetSipIP (msg); // Intercepted ip
        h = Hash(IP1,IP2);  //Get the hash value
        if FsmMatch(h) < > NULL
        {
                return 1;
        }
        else
        {
                node= NodeCreate(h,msg);
                NodeInsert(node);
        }
        return 0;
}
```

4.2.3 Dynamic threshold adjustment algorithm

Dynamic threshold adjustmentor does different adjustment according to feedback results, and adjustment algorithm is described in figure 5.

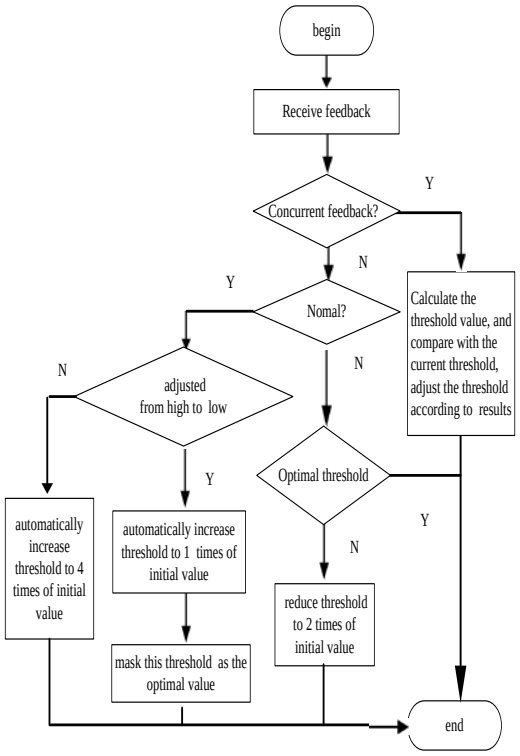

Figure 5: Dynamic Threshold Adjustment Algorithm

4.2.4 Time penalty algorithm

Time penalty algorithm is used to adjust the IP address shield time in IP address shield table and time penalty algorithm process is shown in Figure 6.

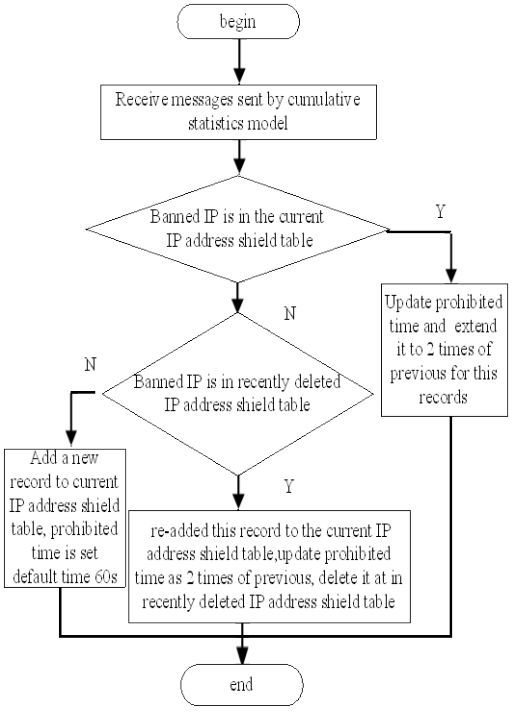

Figure 6: Time Penalty Algorithm

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5 EXPERIMENT AND ANALYSIS

5.1 Experimental Environment

The experiment was built by three experimental hosts, OPENSIPS software is installed in one host and it works as the server host; Prototype system of defense system is installed in one host, and it works as bastion host which run in the front-end of server; One host works as messages generate host which run the SIP message generate tool SIPp and send SIP messages to the server host. In this experiment, the system maximum processing capacity is set as 1000, and set time window as 1s. As the three types of messages (INVITE, REGISTER and OPTIONS) have similar process method, and process and statistics respectively, the paper only simulates the processing of INVITE message.

5.2 Threshold Adjustment Experiments

Message generator can generate INVITE messages of different concurrency and different packet loss rate to simulate the chi-square value and threshold changes in different network environment. In this experiment, the number of calls per second and packet loss rate curves are shown in figure 7, chi-square statistic and threshold curve are shown in figure 8.

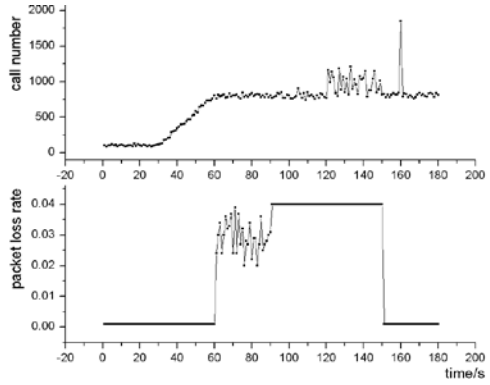

Figure 7: Call Number And Packet Loss Rate

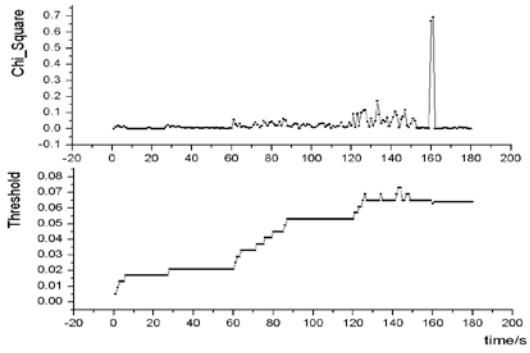

Figure 8: Chi-Square And Threshold

It can be seen from the above figure 7-8: the number of messages per second is around 100 in 0 ~ 30s, packet loss rate is 0.1%, and simulate packet low-loss and low-concurrency case. Chi-square statistic tends to 0, as the initial threshold value is very small, the threshold value rise for some time and achieve the stabilization; Loss rate steady at 0.1% in 30 ~ 60s, the number of messages per second rising steadily from 100 to 800, and simulate the concurrent number increasing and packet low-loss case. Chi-square statistic is very small and remain stable, because the chi-square statistic is less than the current threshold, and the threshold remains unchanged; The number of messages per second stable at around 800 in 60 ~ 90s, packet loss rate shock from 2% to 4%, and simulate packet loss rate instability under high concurrent number. Chi-square statistic increases and has great shock, the threshold increases corresponding; The number of messages per second is stable at around 800 in 90 ~ 120s, packet loss rate steady at 4%, and simulate high packet loss and packet loss rate is stable under high concurrent number case. Chi-square statistics is lower than packet loss rate instability case, and the threshold remains unchanged; In 120 ~ 150s the packet loss rate steady at 4%, the number of messages per second shocks from 800 to 1200, and simulate high concurrent number and high packet loss and deal with unexpected traffic exceeds capacity of the system case. Since exceeding capacity of the system result to packet loss, chi-square statistic increases significantly, and the threshold growth steady at beginning, in the 126s as the threshold value which exceeds the upper threshold, take the threshold limit as the current threshold. Since the threshold upper limit changes with concurrent number changes, the threshold makes appropriate adjustments; The number of messages per second is stable around 800 n 150 ~ 180s, packet loss rate remains stable at 0.1%, and simulate low packet loss rate under high concurrent num case. The chi-square statistic is very small before 160s, the threshold remains unchanged. At 160s there are flooding attacks with the number of messages per second is 1000, the chi-square statistics increases largely, cumulative statistics module fed back the attack, the threshold value decreases 2 times of initial value. The attacking IP was shielded at 161s, because chi-square statistic is still significant when it turn from attacking to normal. The last threshold is adjusted from high to low, and this threshold value increases to 1 times of initial value. The chi-square statistic and threshold remains stable after 161s.

Journal of Theoretical and Applied Information Technology
15th November 2012. Vol. 45 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5.3 Detection Rate Experiment

In the network environment there are about 0.1% packet loss rate and different concurrent number, the message generated host simulates about 200 different IP and makes different intensity of attacks to server under different concurrent number each time to test detection rate. Conducted experiments six times totally, the concurrent number and attacks of messages per second of each experiment are shown in table II, the experimental results are shown in figure 9.

TABLE II: Concurrent Number And Attacks Messages Per Second

No	concurrent num	attacks messages/second
1	100	100
2	100	1000
3	100	50
4	900	100
5	900	1000
6	900	50

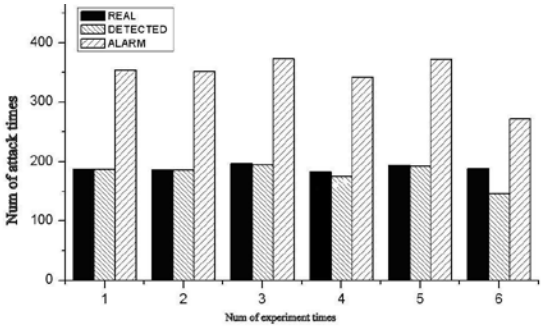

Figure 9: Attack Number And Detected Number

It can be seen from figure 9 that the system has a high detection rate to the attack that messages per second is higher than 100. For the attacker that messages per second less than 100, there is high detection rate still under the low concurrent number. While under high concurrent number as messages per second is very small compared to concurrent number, the influence to chi-square statistic is very small when the attack occurred, which resulted in that chi-square statistic is below the threshold, and cause certain amount of omission. And because the percentage of different messages has big changes between the attack occurred and the system shield attack IP, chi-square statistic will significantly been increased, so the alarm times is about 2 times of actual attacks times.

5.4 Delay Simulation

As the chi-square statistics only need to wait for message type parsing completed to finish statistics, and CUSUM algorithm need to search and match the existing IP after waiting for the IP address parsed. The system and the CUSUM algorithm delay will be influenced by the number of messages, the distribution of SIP messages IP address and messages parsing speed and many other factors. The delay in the actual test can not fully reflect performance comparison of system algorithms and CUSUM algorithm. Therefore, we only simulate the system algorithm delay and the CUSUM algorithm delay in an ideal case. We assume that time for each message to CUSUM processing and chi-square statistics is constant in the simulation, we use the average of CUSUM processing time and chi-square statistical processing time in the actual system as the constant value. We study the relationship between CUSUM algorithm/system algorithm delay the number of messages per second under different attack percentage, the experimental results are shown in figure 10 and figure 11. It can be seen from the figure that the system delay is far lower than the CUSUM algorithm delay without attacks. There is mainly reason that the system only need chi-square statistics and need not wait CUSUM modules completion when no attack occurs, the processing time significantly is lower than the CUSUM algorithm; As attack percentage increasing, the system algorithm delay gradually approaching the CUSUM algorithm delay. The system algorithm delay and the CUSUM algorithm delay is same in 50% attack percentage case, which is that along with attack percentage increasing, the times of chi-square statistics exceeds the threshold increase, so system need to wait CUSUM calculations completed, resulting system delay approach to the CUSUM algorithm. In 50% attack percentage case, almost every chi-square statistic exceeds the threshold and need to wait for CUSUM calculation completed, therefore the delay has been consistent to the CUSUM algorithm delay. In 10% and 30% attack percentage case, the system delay starts to grow slowly, the growth rate is significantly larger after the number of messages per second is greater than 900. The reason is that when the number of messages is greater than 900, there were thresholds larger than then threshold limit due to the system concurrent number is very large. In order to reduce the false alarm rate taken a smaller threshold limit as the threshold that lead to frequent occurrence of the chi-square statistics is larger than the threshold, the system need to wait CUSUM calculation completed and delay increased greatly.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

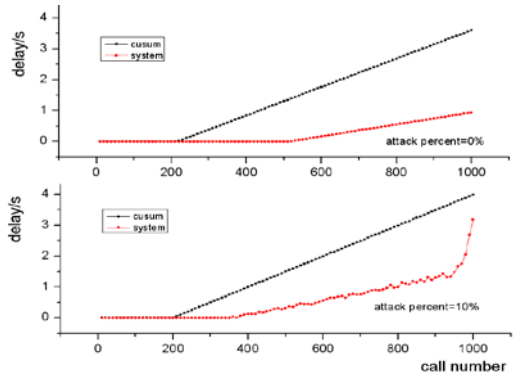

Figure 10: Delay Of CUSUM Algorithm And System Algorithm (0% And 10% Attack Percent)

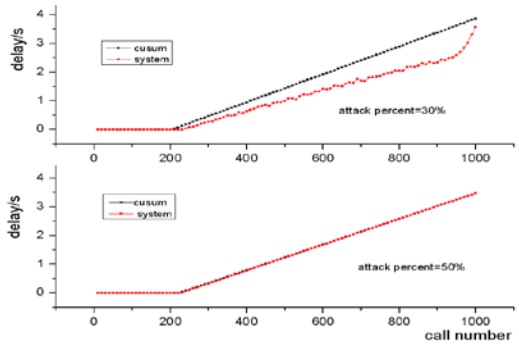

Figure 11: Delay Of CUSUM Algorithm And System Algorithm (30% And 50% Attack Percent)

5.5 Performance Analysis

When concurrent number is very large, the attack that number of messages per second is small, and it will be omitted as its influence to chi-square statistic is too small. But the system can always detect single-source attack that number of messages per second is larger than 100 because of the role of the upper threshold limit. In actual test, there are few attacks that messages per second is less than 100 except that the originate stage of slow start attack, and even the low-intensity attacks are omitted it will not have a huge influence to server.

When the chi-square statistics module does not generate an alarm system, it need not wait CUSUM calculation completed to save a lot of processing time. Particularly when no attack occurs, this system only executes chi-square statistics, and delay greatly reduced compared to CUSUM algorithm. In practical applications, as most of the time the SIP network is in no attack state, the system average processing delay is much lower than this system that is using the CUSUM algorithm.

6 CONCLUSION

Using chi-square traffic monitor to detect abnormal SIP traffic and to alarm, it will not activate the threshold judgment module in cumulative statistics model when SIP messages are not abnormal. The system parallel calculate the chi-square statistic of SIP message's distribution, simply and cumulative statistics three types of SIP request messages, so the processing speed is very fast. For the abnormal traffic case, Cumulative statistics model accumulates and analyzes IP-based SIP requests to determine whether there is an attack happened. If it is attacking, the attacker's IP address and SIP messages are given. In addition, the system testing process only needs to maintain the numbers of SIP messages of different IP addresses, and require low system resource, and will not become the targets for attackers. Experimental result shows that this model can effectively reduce system detection delay and improve the SIP network high availability.

REFRENCES:

[1] 3GPP TS 23.228. "IP Multimedia Subsystem (IMS)". Stage2, Rel.7, V7.7.0. March 2007.

[2] J. Rosenberg, H. Schulzrinne, G. Camarillo, et al. "Session Initiation Protocol", 2002, RFC 3261.

[3] D. Geneiatakis, G. Kambourakis, T. Dauiuklas, et al.,2qwsd "SIP security mechanisms: A state-of-the-art review". In: Proceedings of 5th international network conference (INC 2005). New York: ACM press, 2005, pp. 147-155.

[4]R. Kuhn, T. J. Walsh, S. Fries. "Security Considerations for Voice OverIP Systems – Recommendations of the National Institute of Standards and Technology". Technical Report SP 800-58, National Institute of Standards and Technology, USA, January 2005, pp. 26-40.

[5]B. Iancu. "SER PIKE Excessive Traffic Monitoring Module 2003". http://www.iptel.org/ser/doc/modules/pike.

[6] B. Reynolds, D. Ghosal. "Secure IP Telephony using Multi-layered Protection". In 10th Annual Network and Distributed System Security Symposium, San Diego, USA, February 2003, pp. 151-158.

[7] Y. Rebahi. "Change-Point Detection for Voice over IP Denial of Service Attacks". Proceedings of Communication in Distributed Systems.IEEE Press, February 2007, pp. 1 - 7.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[8] Y. Rebahi, M. Sher, T. Magedanz. "Detecting Flooding Attacks Against IP Multimedia Subsystem (IMS) Networks". In the 6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-08), Doha, Qatar, March 2008, pp. 848-851.

[9] S. Hemant, N. WANG, W. Duminda, et al. "Detecting VoIP floods using the hellinger distance". IEEE Transactions on Parallel and Dis-tributed Systems, Vol. 19, No. 10, 2008, pp. 794-805.

[10]E. Chen, "Detecting Dos Attacks on Sip Systems", Proc. IEEE FirstWorkshop VoIP Management and Security (VoIP MaSe '06), Apr. 2006, pp. 51-56.

[11]S. Ehlert, Y. Rebahi, et al. "Intrusion Detection System for Denial-of-Service flooding attacks in SIP communication network", International Journal of Security and Networks, Vol. 4, No.3, 2009, pp. 189-200.

[12] Y. Bouzida, C. Mangin. "A Framework for Detecting Anomalies in VoIP Networks". In Third International Conference on Availability, Reliability and Security (ARES 08), March 2008, pp. 622-632.

[13] Fang-Yie Leu, Chia-Chi Pai. "Detecting DoS and DDoS Attacks using Chi-Square". In the fifth International Conference on Information Assurance and Security(IAS'09), February 2009, pp. 255-258.

[14] Wenhai Li, Wei Guo, Xiaolei Luo, et al. "On Sliding Window Based Change Point Detection for Hybrid SIP DoS attack". In Proceedings of APSCC, January 2010, pp. 425-432.