WUJNS
Wuhan University Journal of Natural Sciences

Vol.11 No.6 2006 1823-1826

Article ID:1007-1202(2006)06-1823-04

DDoS Defense Algorithm Based on Multi-Segment Timeout Technology

□ DU Ruizhong, YANG Xiaohui, MA Xiaoxue, HE Xinfeng

Institute of Network Technology, Hebei University, Baoding 071002, Hebei, China

Abstract: Through the analysis to the DDoS(distributed denial of service) attack, it will conclude that at different time segments, the arrive rate of normal SYN (Synchronization) package are similar, while the abnormal packages are different with the normal ones. Toward this situation a DDoS defense algorithm based on multi-segment timeout technology is presented, more than one timeout segment are set to control the net flow. Experiment results show that in the case of little flow, multi-segment timeout has the ability dynamic defense, so the system performance is improved and the system has high response rate.

Key words: DDoS(distributed denial of service); multi-segments timeout; dynamic defense; net flow analysis

CLC number: TP 393

Received date: 2006-05-20

Foundation item: Supported by the Natural Science Foundation of Hebei Province (F2004000133)

Biography: DU Ruizhong (1975-), male, Lecturer, research direction: distributed computing and information security. E-mail: drzh@mail.hbu.edu.cn

0 Introduction

Along with the development and prevalence of Internet, network has more and more close relation with us; On the other hand it brings us many problems. Among these problems security problems is the chief problem and the attacks of DoS(Denial of Service) and DDoS(distributed DoS)) are the first threaten against network security[1,2].

The DDoS defense techniques have their respective characteristics, but there are also different defects in them. The Rate Limiting Filter[3] can effectively reduce the bandwidth which some type of data package take and defense against the Flood attack which is made by the attacker using this type of data package; but this filter take a obvious effect only if it is set closed to the position of the source of attacker, and many natural data package are discarded. Ingress Filter[4] can track the attacker using preventive manage filter, on the other hand, this method must sacrifice the effective throughput of router in order to provide considerable compute resource in routers to check whether all the outputs are natural. Out of Band Tracing [5] is redounded to confirm the resource of the Flood attack, on the other side, it may increase the flow of the information. Because of restricts of falsification IP, multi-lever router and the multi-lever agent, it is difficult for IP Trace to find the resource of the attacker. Firewall[6] can shut down a specific flow associated with an attack, but like routers, they can't perform anti-spoofing. In present, there are other research on DDoS defense, such as package filter, package earmark techniques and Traffic Statistics, but these methods have some more detects, and can't resolve the DDoS attack[7-9].

According to analysis of hierarchical, multidirectional system of DDoS, we can find that it's hard to keep away, hard to pursue just because of its natural, single action and normal, legal attack channel. Furthermore attacker often uses some familiar protocol (TCP-Transmission Control Protocol, UDP-User Datagram Protocol etc), it's difficult to distinguish vicious request from normal link request. The attack of DoS boil down to that server has to deal with more data over natural limit. Thus the basis of detect and defense of DDoS's attack is that, timely detect the flow state of bit, distinguish the characteristic of normal and abnormal form bottom[10]. So toward this kind of attack action, the most fundamental approach is to adopt direct method-flux control method to suppress DDoS's attack.

A dynamic DDoS defense algorithm based on multi-segment timeout technologies is presented to withstand DDoS attack while do not depress the system performance in the case of attack flow is not large.

1 Analysis of DDoS Algorithm Based on Multi-Segment Timeout

1.1 Definitions about DDoS Attack

Definition 1 Package death rate F: The package amount of quit the buffer queue to the mount of all packages stay in the queue.

Definition 2 Package arrive rate A: How many packages that insert into the host computer buffer queue in a unit time.

Definition 3 Attack rate E: The flow of attack brings to the flow of primary flow in the net.

Definition 4 Package life D: How long the package stay in the buffer queue.

Definition 5 Package response rate G: The amount of normal packages responded by system to the amount of all normal packages in the buffer queue.

Definition 6 All buffer resource M_0: The length of the buffer queue that allocated by the system.

1.2 Check Algorithm of Net Flow

In order to differentiate the normal flow and the abnormal flow, statistic method is adoped to analyze the statistic behavior of net flow. Using statistic method we can calculate the average value and variance of normal package and abnormal package, we also can obtain the distribution function $F(x)$:

$$F(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\,\sigma}\exp\left[\frac{-(y-\zeta)^2}{2\sigma^2}\right]\mathrm{d}y \qquad (1)$$

$G(x)$ denotes the distribution of net flow:

$$G(x) = \frac{F(x)-F(0)}{1-F(0)} \qquad (2)$$

Many experiment results show that at different time segments all $G(x)$ of the arrive rate of normal SYN (Synchronization) package are similar, while the abnormal packages are different with the normal ones.

We use P to describe the difference between the model of the real flow in the net and the model of the normal flow: if we detect the SYN arrive rate at a period of time and divide the rate into n parts average. So P can be denoted:

$$P = \frac{\sum_{i=1}^{n}(G(r_i)-i/n)^2}{n} \qquad (3)$$

r_i denotes the value of the arrive rate in the ith part, so P reflects the size of the attack intension.

1.3 Definition of Attacking Model

At the beginning time t_0, there are some normal connection to the host be attacked, they occupy a length of buffer queue M, they have an average lifetime D. From the time t_1 attack happens, and the attack rate is from 0 : 1 high to n : 1, and this value will keep a period of time. The attack packages occupy a length of buffer queue M', their average lifetime is D'. Generally, after the attack happens M_0 is exhaust.

1.4 Analysis of Multi-Segment Timeout Algorithm

Assume of DDoS attack:

① The arrive rate is changeless at a period of time. The drop speed of the packages is average, and the drop chance is average.

② The package death rate and the length of the package queue have the relation of direct ration.

③ To SYN packages, if they can enter the buffer, every one occupies a length of 1.

Based on the model and assumes mentioned above, we can obtain the relation among every variable.

The relation among the length of the queue that received normal packages M, the arrive rate of SYN packages A and the death rate of normal SYN packages F is shown as follow:

$$\Delta M = (A-F)\Delta T \qquad (4)$$

T is the time, ΔT is the time increment, ΔM is the change of M during ΔT.

If the queue is long enough, after a period of time the length will be a fixed value, the death rate of the normal packages should equal to the arrive rate of normal packages and the abnormal ones. Now the death rate of normal packages is BM while the abnormal packages is $B'M(B,B'$ are proportion coefficient), the arrive rate of abnormal packages is A'.

$$M = AD, M' = A'D', B = 1/D, B' = 1/D'$$

Let $\Delta T \rightarrow 0$, put every coefficient into the first formula and integral:

$$A - BM = C_1/\exp(BT), M + M' < M_0 \quad (5)$$

$$A - B'M' = C_2/\exp(B'T), M + M' < M_0 \quad (6)$$

C_1 and C_2 are integral constant. At the beginning of the connection set up, there is resource existing, the change of M and M' is follow the formula (5) and (6). When the queue full, because some packages will be dropped create rate is not equal to arrive rate. So the following formula is obtained:

$$\Delta M = [L(BM + B'M') - L'(BM + B'M')]\Delta T$$

Let $\Delta T \rightarrow 0$, integral the above formula, we can obtain the following one:

$$\frac{C_3}{e^{T(L'B - LB')}} = [LB'M_0 - (L'B + LB')M]$$

$$(\text{when } M + M' = M_0) \quad (7)$$

In all arrived packages L is the proportion of normal packages while L' is the proportion of abnormal packages, C_3 is integral constant.

The seventh formula denotes the relation among M', M and T when the above assumes are true and the model is true. Let $T \rightarrow +\infty$, we have:

$$\frac{M'}{M} = \frac{D'}{D} \cdot \frac{L'}{L} \quad (8)$$

The eighth formula denotes that after attacks happen when the queue length of normal packages and abnormal packages do not change, the relation among resource consume rate $H = M'/M$, attack rate $E = L'/L$ and life time rate D'/D. The response rate G is

$$G = \frac{\frac{M}{D}T}{AT} = \frac{M}{AD} = \frac{M + M'}{AD(H + 1)} \quad (9)$$

When the system resource exhaust, that is the buffer is full, G is:

$$G = \frac{M_0}{AD(H + 1)} \quad (10)$$

2 Performance Evaluation

In TCP/IP protocol, during the process of setting connection, in Linux the timeout of re-send is 180 s while in Windows 2000 server it is 40 s.

Emulational experiment, according to formula (9) and (10) we can calculate the effect that multi-segment timeout can defend DDoS attack. System parameter:

① In normal situation, 100% of the connection delay is less than 180 s, 80% percent of the connection delay is less than 40 s, and 10% of the connection is less than 10 s.

② The most length of connection queue is ($M_0 = 1024$), if the queue is full the packages arrived later will be dropped.

③ We set the connection life time D=51.2s, when there are no attacks, the queue is in a half-full state, that is ($M = M_0/2$).

④ The normal net flow is 10 SYN packages per second ($A = 10$), the configuration of multi-segment timeout is: a quarter of buffer queue is long timeout (180 s), a half of buffer queue is middle timeout (40 s), a quarter of buffer queue is short timeout (10 s). If the system received the data packages, it put the packages into long timeout queue first.

After the DDoS attacks happen, with the attack packages increasing the system resource occupied by normal packages is reduce, response rate descends, consume rate ascend, after a period of time these values will be fixed.

In order to evaluate the effect of the algorithm, we will discuss the performance value of the system in four kinds of situation in the case of different attack rate when the system is balance.

When the time of timeout is shorter, some normal connection is not responded so when we calculate the consume rate they will be considered to be the attack flow. If the fall is quickly than the climbing of lifetime rate, shorting the timeout will depress the system efficiency. We can analyze it quantificationally from formula (8). The result is shown in Table 1.

The above table shows that at the case of the attack rate are not large (less than 2 : 1), multi-segment timeout can improve the system performance. At long multi-segment timeout the system resource is consumed badly, while at short multi-segment timeout it has a high using rate, so the multi-segment timeout module has a high response rate.

There is a problem we should pay attention, when the attack rate is large the response rate is too low though multi-segment timeout can enhance response rate,

Table 1 The consume of system resource under SYN flood attack

Attack rate	Normal timeout		Every multi-segment timeout			Multi-Segment timeout (average)	
	Consume rate	Response rate	Consume rate(long)	Consume rate(middle)	Consume rate(short)	Consume rate	Response rate
1∶1	3.51	0.440	3.51	1.17	0.78	1.47	0.697
2∶1	7.03	0.249	7.03	2.15	1.27	2.34	0.596
10∶1	35.10	0.055	35.10	9.95	5.16	15.04	0.126
100∶1	351.00	0.005	351.00	97.63	49.04	148.80	0.013

in fact system can response the connection in this case. This problem shows that using multi-segment timeout technologies, when the attack flow is low the system can defend DDoS attack well. But when the attack flow is high the system performance falls quickly, so multi technologies and multiplayer defense should be adopt, only in this way the system the system has the ability of defend DDoS attacks.

3 Conclusion

A DDoS defense algorithm based on multi-segment timeout is introduction in this paper; the analysis result shows that when the flow of net attacks is not large, the multi-segment timeout has fine ability of against DDoS. If the setup of multi-segment timeout is in reason, this algorithm can defend the DDoS attack while not reduce the system performance.

References

[1] Li Dequan, Su Purui, Feng Dengguo. Notes on Packet Marking for IP Traceback [J]. *Journal of Software*, 2004, **15**(2):250-258(Ch).

[2] He Hui, Zhang Hongli, Zhang Weizhe, *et al*. A DDoS Intrusion Detection Method Based on Likeness[J]. *Journal of China Institute of Communications*, 2004, **25**(7): 176-184 (Ch).

[3] Jiang Weihua, Shi Xingjian, Du Jun. An Algorithm for Recognizing Denial of Service (DoS) Attack [J]. *Journal of Northwestern Polytechnical University*, 2003, **21**(4): 398-401 (Ch).

[4] Wang Xinsheng, Wang Xuwei. Realtime and Dynamic Security Model Against Denial of Service Intrusion [J]. *Computer Engineering*, 2002,**28**(3):126-127 (Ch).

[5] Xiong Y, Liu S, Sun P. On the Defense of the Distributed Denial of Service Attacks: An On-Off Feedback Control Approach[C]// *Systems, Man and Cybernetics, Part A, IEEE Transactions on Communications*, 2001,**31**(4):282-293.

[6] Yao Xiaoyu, Gu Guanqun. An Active Network Based Intrusion Response System [J]. *Computer Engineering and Applications*, 2002,**38**(6):130-133 (Ch).

[7] Doeppner T W, Nklein P N, Koyfman A, *et al*. Using Router Stamping to Identify the Source of IP Packets[C]// *Proceedings of the 7th ACM Conference on Computer and Communications Security*. Athens, Greece, Nov, 2000: 184-189.

[8] Li Jinming, Wang Ruchuan. Study of a New Packet Marking Scheme for DDoS Attack Source Traceback [J]. *Journal on Communication*, 2005,**26**(11):18-23(Ch).

[9] Zhuang Xiaobin, Lu Kangjun, Wang Li, *et al*. A Detecting Method of DDoS Attacks Based on Traffic Statistics [J]. *Computer Engineering*, 2004,**30**(22):127-130(Ch).

[10] Hu Xiaoxin, Wang Ying, Luo Xubin. A Scheme to Prevent DDoS Attacks[J]. *Computer Engineering and Applications*. 2004,**40**(12):160-163 (Ch).

□