ISBN 978-952-5726-00-8 (Print), 978-952-5726-01-5 (CD-ROM)
Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)
Nanchang, P. R. China, May 22-24, 2009, pp. 257-260

A Router-based Technique to Detect and Defend against Low-rate Denial of Service

Zhu Lina [1], Zhu Dongzhao [2]
[1] Computer science department, Guangdong Police Officer College, Guangzhou ,China
Email: zhuln020@yahoo.com.cn
[2] Mobile Corporation of Heilongjiang Province, Harbin ,China
Email: zhudongzhao@hl.chinamobile.com

Abstract—**With the successful use of router technique, we consider to give routers additional function to defect and defend against LDOS. LDOS is a kind of miniature network attack which can affect TCP flows to zero or very low transmission bandwidth, just because it takes advantage of retransmission timeout of TCP. This sort of attack is difficult to identify due to its good cryptcity. We appiciate the distributed detection mechanism, and we add a new fast detection function on it . We can accurately and fast find and locate the LDOS with it. Otherwise, we always try to remove the attack without complicated arithmetic or losing legal data. At the end of this paper, we will show the new way can break up the attack burst into parts.**

***Index Terms*—Network security; Low-rate; Denial of service ; retransmit-overtime**

I. Introduction

Nowadays DDOS（Distributed Denial of Service）has been a main threat to network applications including web HTTP access, e-commerce, and file transfers etc. Many agent machines were connected to attack an aimed victim. The DDOS attack is fierce, strong destructiveness and difficult to defend. In recent years many effective defense means have been bring forwarded.

A new kind of DoS attack was put forward which was called Low-rate Denial of Service or Shrew Attack. It can efficiently attack target victims without substantial attack flows. LDOS is more complicated than DDOS. It takes advantage of the safety loophole existing in choking control of TCP protocol. The LDOS is different from traditional Flood DDOS. It is essentially a periodic short burst or shot attack flow pulse. Its period, pulse last-time and pulse amplitude must be changed according to the case. LDOS exploits the homogeneity of the minimum retransmission timeout(RTO) of TCP flows and forces all affected TCP flows to back off and enter the retransmission timeout state, and try to resent a new packet after a period of RTO. Repetitional attacks make flows reduce their congestion window, so the flows become packet flows of low-rate transmission. Comparing with DDOS, LDOS has a worse attack action but a better crypticity especially in a distrubuted network. It is difficult to find out LDOS by detecting data flow quantity. The characteristics of Ldos is that all attack agents and attack flows are scattered in the distrubuted agents, so this kind of attack is more difficult to be detected.

Ⅱ. Description of Low-rate Attacks

A. Mathematical Model of Low-rate Attack

Given that the throughput capacity of a router is C bit/s, the value of R is near to C. After normalized with the max throughput capatity C of router, value range of R is (0,1). The mean rate of period square-wave is RL/T. Because the value of RL/T is low, so this kind of attack is called Low-rate attack. Just because LDOS can send appropriate pachets to make queue buffers full in the time length L of pulse peak, any other TCP flow packets will be discarded by the router. The worse is that because the value of RTO is predefined and fixed, LDOS attack can easily adjust its period of attack to make TCP flow into retransmission timeout. Supposed that there are K TCP flows affected by TCP attack, RTTi is round trip time from agent i to target victim. So the length of pulse must meet the following requirements :

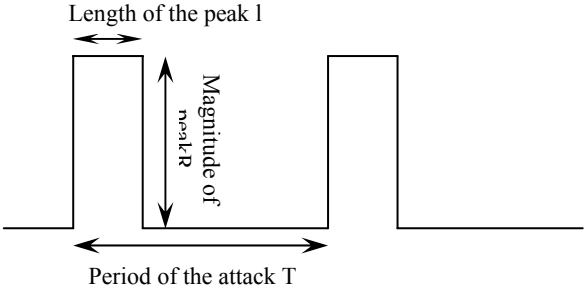


Figure 1. Period features of LDOS square-wave

$$L \geq MAX\{RTTi\}, I = 1, 2, 3 \ldots\ldots k \quad (1)$$

In order to avoid detection, the value of L mustn't be near to the period T but meet (2):

$$MAX\{RTTi\} \leq L \leq \beta 1T, \beta 1 \leq 0.25 \quad (2)$$

The attack flows from agents will become huge pulses. The regular TCP flow senders can calcalate their RTO through (3).

G is interval scale (it isn't more than 100ms), SRTT is smoothed round-trip time, RTTVAR is round trip time ariation. The iterative formulas of RTTVAR and SRTT are (5) (6). The parameter T must meet (4). R is initial value of RTT, R/2 is initial value of SRTT, $\alpha=1/8$, $\beta=1/4$.

$$RTO=\max(\text{minRTO}, SRTT+\max(G, 4RTTVAR)) \quad (3)$$

$$\text{minRTO} < T \le \text{minRTO} + 2\max\{ RTTi \}, \quad (I = 1, 2 \ldots\ldots k) \tag{4}$$

$$RTTVAR = (1-\beta)RTTVAR + \beta|SRTT - R| \tag{5}$$

$$SRTT = (1-\alpha)*SRTT + \alpha R \tag{6}$$

Ⅲ. Distributed Detection System of Based on Router Technique

A. The Architecture of Detection System Based on Router Technology

We decide to adopt the distributed detection architecture based on router technology put forward by H.sun[3], and do some reasonable improvement to make it more safety and steady.

B. General Design for Fast Detection System

In order to detect LDOS attack, we should compare the features of input flow with the features of LDOS attack flow. The detecting steps are following: Input flow go through fast filter: background flow can be filtered from input flow, the output valve f(x) is a discrete function.The discrete function f(x) is sent into the detecter, f(x) will be compared with features of LDOS attack flow.

The advantages of our fast detction system are following: 1. flows needn't be saved 2. less calculation is needed 3. realtime LDOS attack can be detected.

C. The Design of Fast Filter

Our original intention is to design a kind of fast and simple singnal filter. It must have the following functions : 1. It must can separate LDOS attack flow from legal flow. 2 It must be easy and fast to do. 3. It must be realtime filter. The function of the filter is Fig.2:

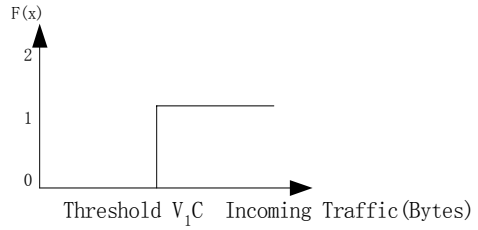


Figure 2. The function f(x)of the filter

C: throughput capacity of router. V1 is adjustable parameter. $0.5 \leqslant V1 \leqslant 0.8$

D. The Design of Detector

1) The feature functions of realtime flow L(t)、M(t)

In order to detect whether the features of f(t) are similar with the features of LDOS attack pulse, we must get the parameters: length of pulse L(t), Interval of pulse M(t). So we do discrete convolution between signals f(t)、1- f(t) and step pulse signal U(t).

$$L(t) = f(t)*U(t) \tag{7}$$

$$M(t) = [1-f(t)] * U(t) \tag{8}$$

2) The steps of detection

According to features of attack flow described in above, we design the following detection steps:

The detection is real time. "Flag" is a label variable of the result of detection. The initial value of it is "True" .In order to determine weather there is an attack pulse, we must detect two variables. Weather the Length of pulse is satisfied with (2). Weather Period of attack (L+M) is less than RTO. If one of the two results is "false", this pulse is not attack pulse, and reset the counter of attack pulse zero. If both of the two results are "true", this pulse is an attack pulse. And the counter of attack pulse will be increased by one. When the counter of attack pulse C equales the minimum value of attack pulse number V5, the system will alert that a LDOS attck happens and reset the counter C.

Ⅳ. Low-rate Attack Defense Mechanism

A. Defuse Risks

Because the attack flows sent by LDOS attackers are all legal data packets. We can't distinguish the legal packets from malicious packets. Otherwise, some of instantaneous LDOS attack flows are formed by legal data flow coincidently. Any filtering algorithm or choking algorithm will make flow packets lose more or less. The most difference between LDOS and DDOS is that the general flow of LDOS isn't very large, it's nothing but a periodic burst. So iti's reasonable and workable to change the traditional flow choking into flow sharing. This defusing risks has two advantages: 1.no legal packets is lost; 2. It's easy to work and don't need complicated algorithm.

$$Bi = (Ai>V1?\ Ai:Ai/L) + (Ai-L>V1?\ Ai-L:Ai-L/L)$$
$$L=10,11\cdots\cdots 15 \tag{9}$$

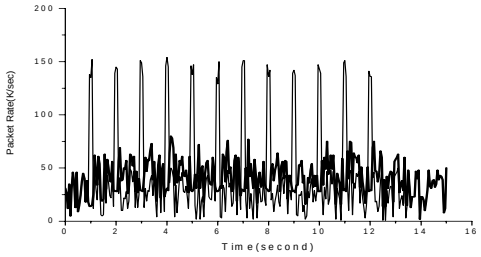
Where Ai are packet rate under LDOS attacks at time i, Bi are packet rate after LDOS attacks are defused at time i , L is the number of defusing pulses. The truth table of expression 9 is shown in Table 1.

TABLE I. THE TRUTH TABLE OF EXPRESSION 9

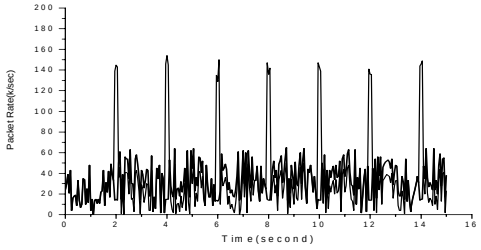
Ai>V1	Ai-L>V1	Bi
T	T	Ai + Ai-L
T	F	Ai + Ai-L/L
F	T	Ai/L + Ai-L
F	F	Ai/L + Ai-L/L

There are two cases shown in Fig.3. Period of the attack T < the number of defusing pulses L in Fig. 3 <a>, Period of the attack T > the number of defusing pulses L in Fig.3 <b>.

After risks defusing, routers maybe work more busily, but won't break down just because of temporary overwork.



<a>



<b>

Figure 3. (a) Period of the attack T < the number of defusing pulses L (b) Period of the attack T > the number of defusing pulses L

Ⅴ. Simulation Results and Discussion

Let us use the following four attack flows[3] to detect the robustness and accuracy of our detection system.

SPSB (strictly periodic square burst): In Fig.4, the black line shows SPSB LDOS attck packet rate, and the bold line shows the packet rate which has been defused.

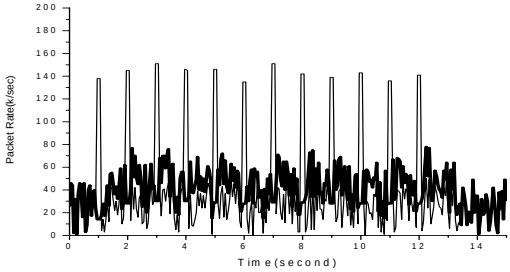


Figure 4. SPSB LDOS attack

RPSB (random periodic square burst): In Fig.5, the black line shows RPSB LDOS attck packet rate, and the bold line shows the packet rate which has been defused.

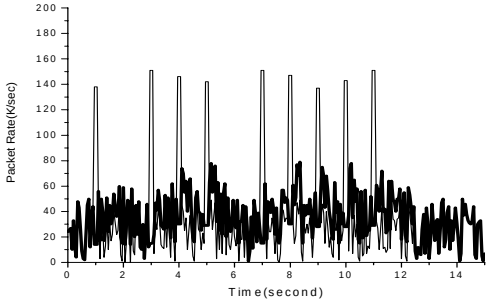


Figure 5. RPSB LDOS attack

SPGB (strictly periodic general burst): In Fig.6, the black line shows SPGB LDOS attck packet rate, and the bold line shows the packet rate which has been defused.

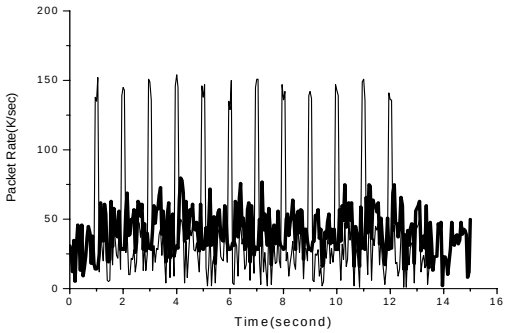


Figure 6. SPGB LDOS attack

RPGB (random periodic general burst): In Fig.7, the black line shows RPGB LDOS attck packet rate, and the red line shows the packet rate which has been defused.

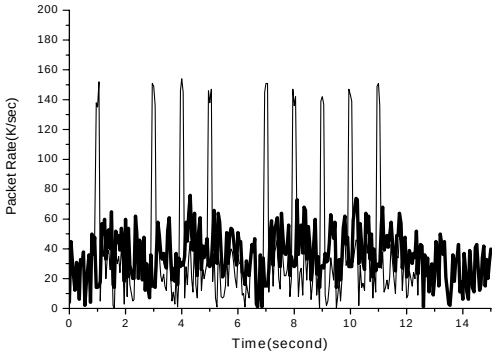


Figure 7. RPGB LDOS attack

Ⅵ. Conclusion

LDOS was first put forward in 2003, the deep reserch about LDOS attack is absent. In this work we present the following: reserch on attack model and principle of LDOS can help us know the features of the attack and provide a basis for further reserch. The aim of our detection measure is to detect and defense LDOS in time with calculation resource as little as possible. According the feature of attack flow without large flow rate and high flow speed, we put forward the risks defusing without any algorithm. The reserch on LDOS begins just now, so it must become a new hot spot and keystone in the future.

References

[1] Kuzmanovic.E.Knightly,Low-rate TCP-targeted denial of service attacks(The Shrew vs.the Mice and Elephants),in :ACM SIGCOMM 2003 pp75-86

[2] Richard Stevens W.TCP/IP locale volume 1 : protocol, China Machine PRESS (CMP), 2000.4 P226-234

[3] Haibin Sun, John C.S , David K.Y.Yau Distributed mechanisam in detecting and defending against the low_rate TCP attack , in:computer Networks 50(2006)2312-2330

[4] R.allen, D.Mills, Signal analysis:Time,Frequency,Scale and Structure,Wiley, New York,2004

[5] X..Luo,R.Chang, Performance analysis of TCP/AQM under denial-of-service attacks ,in:Proceedings of IEEE MASCTS,Atlanta.GA,September 2005.

[6] S.Specht,R.Lee,Distributed denial of service: taxonomies of attacks, tools and countermeasures, in:Proceedings of 2004PDCS,San Francisco,CA,15-17 Sepember,2004.

[7] Y.xu, R.Guerin,On the robustness of router-based denial-of-service(DOS)defense systems,ACM Computer Communications Review 35(3)(2005)47-60

[8] R.Chertov, S.Fahmy, N.Shroff, Emulation versus simulation:a case study of TCP-targeted denial of service attacks, in:TridentCom 2006,2006,pp.316-325.

[9] R.Beverly, S.Bauer, The Spoofer project inferring the extent of source address filtering on the Internet, in:USENIX SRUTI'05,2005,pp.53-59

[10] J.Mirkovic, P.reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review 34(2)(2004)39-54

[11] A.Shevtekar, N.Ansari, A router-based technique to mitigate reduction …,Comput.Netw.(2007),doi:10,1016/j.comnet.2007.11.015

[12] William L, Oellermann Jr. Architecting Web Services.Apress,2001,10

[13] A.shevtekar, K.anantharam, N.Ansari, Low rate TCP denial-of-service attack detection at edge router,IEEE Communication Letters 9(4)(2005)363-365

[14] X.Luo,R.K.C.Chang,On a new class of pulsing denial-of-service attacks and the defense, in:NDSS 2005,2005.

[15] G.Yang, M.Gerla, M.Y.Sannadidi,Tandomization :defense against low-rate TCP-targeted denial-of-service attacks, in:IEEE Symposium on computers and Communications,2004,pp.345-350.

[16] Y.Chen,K.Hwang,Collaborative detection and filtering of Shrew DdoS sttacks using spectral analysis.Journal of Parallel and distributed Computing,Special Issue on Security in Grids and Distributed Systems 66(9)(2006).