Probabilistic Packet Filtering Model to Protect Web Server from DDoS Attacks*

Jung-Taek Seo[1], Cheol-Ho Lee[1] , Jungtae Kim[2],
Taeshik Shon[3] , and Jongsub Moon[3]

[1]National Security Research Institute
KT 463-1, Jeonmin-dong, Yuseong-gu, Daejeon, 305-811, Republic of Korea
{seojt, chlee}@etri.re.kr
[2] Graduate School of Information and Communication, Ajou University, Republic of Korea
coolpeace@ajou.ac.kr
[3] CIST, KOREA University
1-Ga, Anam-dong, Sungbuk-Gu, Seoul, Republic of Korea
{743zh2k, jsmoon}@korea.ac.kr

Abstract. We present a probabilistic packet filtering (PPF) mechanism to defend the Web server against Distributed Denial-of-Service (DDoS) attacks. To distinguish abnormal traffics from normal ones, we use Traffic Rate Analysis (TRA). If the TRA mechanism detects DDoS attacks, the proposed model probabilistically filters the packets related to the attacks. The simulation results demonstrate that it is useful to early detect DDoS attacks and effective to protect the Web servers from DDoS attacks.

1 Introduction

These days, Web environments are very vulnerable Distributed Denial-of-Service (DDoS) attacks [1], [2]. In order to cope with the threat, there have been many researches on the defense mechanisms including several approaches based on real-time traffic analysis technique [3], [4], [5]. However, the previous mechanisms have some drawbacks such as overhead for managing IP address and lack of commonness. In this paper, we propose Probabilistic Packet Filtering (PPF) model to deal successfully with the flaws of the previous works. The proposed model distinguishes abnormal traffics from normal ones using Traffic Rate Analysis (TRA) method [6], [7]. When it detects DDoS attack, it probabilistically filters suspicious packets. Experiment results shows that the proposed model is useful to early detect DDoS attacks and it is effective to protect Web servers against DDoS.

* This work was supported by the Ministry of Information Communication, Korea, under the Information Technology Research Center Support Program supervised by the IITA.

2 The Proposed Probabilistic Packet Filtering Model

In a normal situation, network traffic rate has specific characteristics. For instance, SYN and FIN are in the ratio of 1:1 and TCP and UDP traffic are in the ratio of 9:1. However, in an abnormal situation (e.g., SYN flooding, UDP flooding), these ratios are broken. Using this fact, the proposed model distinguishes a normal situation and abnormal situation, and drop attack packet probabilistically.

To analyze web traffic, we use the TRA method that proposed in the earlier study [6], [7]. It examines the occurrence rate of a specific type of packets within the stream of monitored network traffic, and computes TCP flag rate and Protocol rate. The TCP flag rate means the ratio of the number of a specific TCP flag to the total number of TCP packets. The protocol rate means the ratio of specific protocol (e.g. TCP, UDP, and ICMP) packets to total amount of IP protocol packets. TCP flag rate and protocol rate is defined in the equation (1) and (2), respectively. In the equation, '*td*' is the time interval used to calculate the value. The direction of network traffic is expressed as '*i*' (inbound) and '*o*' (outbound).

$$R_{td}[F\,i \mid o] = \frac{\sum flag\,(F)\ in\ a\,TCP\ \ header}{\sum TCP\ \ \ packets} \tag{1}$$

$$R_{td}[[TCP|UDP|ICMP]i \mid o] = \frac{\sum [TCP|UDP|ICMP]packets}{\sum IP\ \ \ packets} \tag{2}$$

Packet filtering mechanism of the proposed model is similar to the Random Early Detection (RED) algorithm [8]. The RED algorithm behaves according to the queue size of entire packets. Thus, it doesn't discriminate attack packet from normal packet. Thus, most legitimate packet is dropped with attack packet during DDoS attack. On the other hand, the proposed model acts according to the occurrence rate of a specific type of packets (i.e., TCP flag rate and Protocol rate of TRA method).

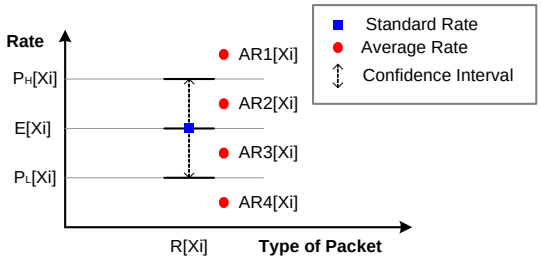

Fig. 1. Proposed PPF model; if the average occurrence rate of a type of packet *X* is *E*[*Xi*] in normal environment, we have confidence interval from $P_L[Xi]$ to $P_H[Xi]$.

Fig. 1 describes the PPF model proposed in this paper. Let the currently analyzed network traffic rate by the TRA as Current Rate (*CR*), average traffic rate from the initial time to the current time as Average Rate (*AR*), and network traffic rate of

normal traffic as Standard Rate (*SR*). Current *AR* is calculated using an exponentially weighted average of previous *CR* values. If the previous *CR* values are non zero, current *AR* is defined by equation (3). Otherwise, current *AR* is defined by equation (4). The weight, w_q, determines how rapidly *AR* changes in response to changes in actual current rate. Flyod et al. recommend a quite small w_q to prevent the algorithm from reacting to short bursts of congestion [8]. However, the proposed algorithm adopts large w_q (e.g., 0.5) since bursts of traffic are very serious threat during DDoS attack.

$$AR_{cur} = (1 - w_q) \times AR_{prev} + CR \times w_q \quad (3)$$

where AR_{cur} is Current Average Rate and AR_{prev} is Previous Average Rate

$$AR_{cur} = (1 - w_q)^m \times AR_{prev} \quad (4)$$

where m is the amount of time that is TRA value was zero

In the proposed model, if average rate of a specific type of packet *AR* is less than lower bound of confidence interval P_L (e.g., AR_4), the incoming packet is serviced. On the other hand, if *AR* is greater than or equal to upper bound of confidence interval P_H (e.g., *AR1*), the incoming packet is automatically discarded. Between P_L and P_H is denoted by the critical region. In this region, PPF assigns a probability of discard to an incoming packet that defends on the factor; the closer *AR* to P_H, the higher probability of discarding. The confidence interval (P_L to P_H) and the probability of discard (P_d) are defined by equation (5) and (6), respectively. In the equation (5), the proposed mechanism used 95% confidence level according to our preliminary test results.

$$E - 1.96 \times SD \le R \le E + 1.96 \times SD \quad P_L \le R \le P_H \quad (5)$$

$$P_d = \frac{AR - P_L}{P_H - P_L} \quad (6)$$

3 Experimental Results

In order to evaluate the effectiveness of the proposed model, we construct synthetic network and build attack model against the Web server using DDoS attack tools such as *TFN2K*. In the experiments, the normal Web service traffic flows during 60 seconds and the attacks using *TFN2K* are done between 20th second and 40th second.

Table 1 shows the experimental results of the proposed DDoS defense model. In the experiment, most of DDoS attack packets are dropped by PPF model with extremely low false positives. The most of attack cases the false positive rate is zero except for the case of SYN flooding attack. During the DDoS attacks, the *AR* values excessively exceed the traffic rate of the normal situation. Moreover, UDP packet rate and ICMP packet rate are almost zero. It means that the normal web traffic is scarcely dropped since it rarely contains these packets. There is 0.57% false-positive rate since some legitimated SYN packets are generated while average *R*[*Si*] is higher than

standard $R[Si]$ in SYN flooding attacks. Nevertheless, almost all the attacking packets are dropped by our defending mechanism.

Table. 1 Performance of the proposed defense mechanism.

Packet / Attack	Received Packets		Dropped Packets		Drop Rate (%)		Overall
	normal	attack	normal	attack	normal	attack	
No attack	9,187	0	0	0	0%	0%	100%
SYN flooding	9,028	76,698	52	74,740	0.57%	97.45%	96.87%
UDP flooding	8,302	142,436	0	142,436	0%	100%	100%
ICMP flooding	8,545	63,674	0	63,674	0%	100%	100%

4 Conclusion and the Future Work

In this paper, we propose the Probabilistic Packet Filtering (PPF) model to protect Web servers from DDoS attacks. Our PPF model has not only an idea of RED mechanism to Internet traffic control, but also a mechanism to drop suspicious packets based on 95% confidence level in accordance with an appropriate threshold. In the experiment, most of attacking packets are blocked by the proposed defending mechanism. In the future work, we will try to evaluate the proposed model in more various situations, and we apply the proposed model to other specific targets such as a variety of application servers and Internet worms.

References

1. Garber, L.: Denial-of-Service Attacks Rip the Internet, IEEE Computer, vol. 33(4), (2000) 12-17.
2. Houle, J.K., and Weaver, M.G.: Trends in Denial of Service Attack Technology, CERT Coordination Center, (2001).
3. Gil, T.M, and Poletto, M.: MULTOPS: a data-structure for bandwidth attack detection, In Proceedings of the 10th USENIX Security Symposium, (2001) 23-38.
4. Householder, A., Manion, A., Pesante. L., and Weaver. M.G.: Managing the Threat of Denial-of-Service Attacks, CERT Coordination Center, (2001).
5. Kargl, F., Maier, J., and Weber, M.: Protecting Web Servers from Distributed Denial of Service Attacks, In Proceedings of the 10th International Conference on World Wide Web, (2001) 514-524.
6. Lee, C., Choi, K., Jung, G., and Noh, S.: Characterizing DDoS Attacks with Traffic Rate Analysis, In Proceedings of IADIS International Conference on e-Society 2003, vol. 1, (2003) 81-88.
7. Seo, J., Lee, C., and Moon, J.: Defending DDoS Attacks Using Network Traffic Analysis and Probabilistic Packet Drop, In Proceedings of the Third International Conference on Grid and Cooperative Computing, (2004) 390-397.
8. Floyd, S., and Jacobson, V.: Random Early Detection (RED) gateway for Congestion Avoidance, IEEE/ACM Transactions on Networking, vol. 1, no. 4, (1993) 397-413.