PPF Model with CTNT to Defend Web Server from DDoS Attack*

Jungtaek Seo¹, Cheolho Lee¹, Jungtae Kim²,
Taeshik Shon³, and Jongsub Moon³

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) model to defend the Web server against Distributed Denial-of-Service (DDoS) attacks. To distinguish abnormal traffics from normal ones, we used Concentration Tendency of Network Traffic (CTNT). The CTNT mechanism computes the ratio of a specific type of packets among the total amount of network packet, and detects abnormal traffic if and only if the computed ratio exceeds the ratio in normal situation. If the CTNT mechanism detects DDoS attacks, the proposed model probabilistically filters the packets related to these. The simulation results demonstrate it is useful to early detect DDoS attacks. Furthermore, it is effective to protect the Web servers from DDoS attacks.

1 Introduction

These days, many businesses are performed in an opened e-Society named as the Internet, especially Web environments. However, those kinds of environments are very vulnerable to Distributed Denial-of-Service (DDoS) attacks [1], [2]. In February 2000, several high profile sites including Yahoo, Amazon, and eBay were brought down for hours by DDoS attacks. As we can see the incident, most of Web servers are exposed to DDoS attacks.

In order to cope with the threat, there have been many researches on the defense mechanisms including the mechanisms based on real-time traffic analysis technique [3], [4], [5], [6], [7], [8]. However, the previous mechanisms have some drawbacks such as overhead for managing IP address and lack of commonness. In this paper, we discuss these shortcomings of previous works in detail and propose Probabilistic Packet Filtering (PPF) model to solve the flaws.

The proposed model distinguishes abnormal traffics from normal ones based on Concentration Tendency of Network Traffic (CTNT). The CTNT monitors the ratio

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

of a specific type of packets among the total amount of network packet. The ratio is divided into 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. If the proposed model detects DDoS attack using the CTNT mechanism, it probabilistically filters suspicious packets to protect the Web server against the DDoS attacks. Performance simulation of the proposed model on synthetic topologies shows that the proposed model is useful to early detect DDoS attacks and it is effective to protect Web servers against DDoS attacks

This paper is organized as follows. In section 2, we analyze other researches to detect and defend DDoS attacks. Section 3 shows the differences between Web service traffic and DDoS attack traffic at the point of CTNT's view. This is followed by the detailed describing the proposed model in section 4. The experimental results of filtering suspected packets are shown in section 5. We summarize our research and mention future work in section 6.

2 Analysis on the Previous Works

An efficient management of network traffic helps reducing the damage caused by DDoS attacks. Accordingly, a lot of current researches are focusing on managing network traffic to defend DDoS attacks [5], [7]. Kargl. divides network bandwidth into several queues which have different network bandwidth using Class Based Queuing (CBQ) techniques, then classify network packets and make them flow through the classified queue in each [5]. For instance, if normal network traffic flows through a high bandwidth queue and DDoS attack traffic flows through a queue of low bandwidth, flooding packets of the DDoS attacks can be reduced. However, this defending scheme needs IP address management because classifying packet is done by watching the IP address. Thus, this defending scheme needs unreasonable overhead. Ricciuli. randomly drops a SYN flooding packet to insert a new SYN packet [7]. However, this method is useful to defend only SYN flooding attacks. Table 1 shows the analysis of related works.

Table 1. Analysis of related work

	Kargl	Ricciuli	Gil and Poletto	Wang	Kulkarni
Detection	Spoofed IP addresses	Heuristic	Disproportion between "from-rate" and "to-rate"	Difference between SYN and FIN in TCP traffic	Kolmogorov complexity metrics
Defending	CBQ	Random Drop	Not supported	Not supported	Not supported
Advantages	Strong defense	Simple and effective	Applicable to backbone routers	Early Detection, Applicable to any location	Detect any type of DDoS attacks
Disadvantages	Overhead for managing IP addresses	Only for SYN flooding attacks	Only for non-spoofed IP addresses	Only for SYN flooding attacks	Overhead for managing the metrics

Detecting the DDoS attacks is an essential step to defend DDoS attacks. Thus, there have been many researches to detect the DDoS attacks [4], [6], [8]. When DDoS attacks occur, there is a big mismatch between the packet flows “to-rate” toward the victim and “from-rate” from the victim. Gil and Poletto propose the method that examines the disproportion between “to-rate” and “from-rate” in order to detect DDoS attacks [3]. However, it is not applicable to detect attacks using IP spoofing. Kulkarni et al. presented DDoS detection method based on randomness of IP spoofing [6]. Many DDoS attackers use IP spoofing to hide their real IP addresses and locations. Additionally, the spoofed IP addresses are generated randomly. The characteristic of randomness may reveal the occurrence of DDoS attacks. Kulkarni’s method uses Komogorov complexity metrics to find randomness of source IP addresses in network packet headers [9]. However it does not prohibit the DDoS attacks that do not use randomly generated address. Wang et al. proposed the method that detects DDoS attack based on the protocol behavior of SYN-FIN(RST) pairs [8]. In the normal situation, the ratio of *SYN* and *FIN* is balanced because of the characteristic of the TCP 3-Way handshake. However, the ratio of SYN packet increases drastically during the SYN flooding attack. By monitoring sudden change of the ratio of *SYN* and *FIN*, the method detects SYN flooding attacks. However it is only applicable to SYN flooding attacks.

3 Web Service Traffic Analysis

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. In this section, we show the differences between normal web traffic and attack traffic. To analyze web traffic, we use the CTNT method that proposed in the earlier study [10], [11]. Details of the CTNT and the differences of normal traffic and attack traffic are explained in section 3.1 and 3.2.

3.1 Concentration Tendency of Network Traffic

CTNT (Concentration Tendency of Network Traffic) is defined as a phenomenon that network traffics are mainly composed of one or more specific types of network packets. For instance, almost all TCP packets have ACK flags in their headers during their connection sessions. Since the Internet has dominant network services such as WWW, E-mail, FTP etc, which are dependent on specific network protocols, CTNT can be found on not only endpoint clients and servers but also core backbone networks [12].

To analyze web traffic, we use the CTNT method that proposed in the earlier study [10], [11]. 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).

$$R_{td}[F i | o] = \frac{\sum \text{flag}(F) \text{ in a TCP header}}{\sum \text{TCP packets}} \quad (1)$$

$$R_{td}[[TCP|UDP|ICMP]i | o] = \frac{\sum [TCP|UDP|ICMP] \text{ packets}}{\sum IP \text{ packets}} \quad (2)$$

3.2 Network Traffic Analysis

In this section, we analyze normal Web traffic and DDoS attack traffic using the CTNT and show differences between them. The network traffic analyzer is made using *libpcap* to capture the network traffic. The analyzer captures network traffic and calculates TCP flag rates and protocol rates in a manner of the CTNT.

3.2.1 Normal Web Service Traffic

This section shows the characteristics of normal Web service traffic without any DDoS attacks. We used *SPECweb99* to generate normal web service traffic. This tool sends HTTP requests to the Web server and receives HTTP replies from the Web server like the real Web browsers do.

Fig. 1 shows the experimental results of *SPECweb99*. We changed Simultaneous Connections (SC) to 5, 10, 50, 100, and 150, and Requests per Connection (R/C) to 1, 2, 5, and 10. As a result, the experiments show that Web service traffic has a

Fig. 1. Web service traffic (average value) using *SPECweb99*

Table 2. The averages and the standard deviations of occurrence rates of packets

In	$R[Si]$	$R[Fi]$	$R[Ri]$	$R[Ai]$	$R[Pi]$	$R[Mi]$	$R[Ui]$	$R[TCPi]$	$R[UDPi]$	$R[ICMPi]$
Avg.	0.17	0.00	0.16	0.67	0.16	0.00	0.00	1.00	0.00	0.00
StdDev	0.01	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00
Out	$R[So]$	$R[Fo]$	$R[Ro]$	$R[Ao]$	$R[Po]$	$R[No]$	$R[Uo]$	$R[TCPo]$	$R[UDPo]$	$R[ICMPo]$
Avg.	0.20	0.20	0.00	1.00	0.60	0.00	0.00	1.00	0.00	0.00
StdDev	0.01	0.01	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00

constant pattern with regardless of *SC* and *R/C*. The resulting rate of *SYN* and *FIN* is almost identical. The other distinguishing result is that the rate of *ACK* is very high. It's because HTTP is based on TCP which is a connection-oriented protocol. These results show that network traffic of normal Web services has a specific pattern. Table 2 shows the specific pattern of the Web service traffic.

3.2.2 DDoS Attack Traffic

In this section, we discuss the changes of network traffic when a Web server is attacked by various DDoS attacks. Fig. 2 shows the change of network traffic when a SYN flooding attacks occur. We generate Web service traffic during 72 seconds after 10th second from start the simulation, and a SYN flooding attack was generated during 40 seconds after 17th second from start the generation of the Web service traffic. As shown in Fig. 2-(a), the rates of *SYN* and *URG* increased to almost 1.0 and the rates of other flags, especially *ACK* rate, decreased to almost 0.0 during SYN flooding attacks.

Fig. 2. SYN flooding attacks against the Web server. Under SYN flooding attacks, the rates of SYN and ACK of inbound traffic change significantly.

Fig. 3. UDP flooding attacks against the Web server. During UDP flooding attacks, changes are made in only inbound protocol rates.

Fig.3 presents the changes under UDP flooding attacks. UDP flooding attack occurs from 18th to the 60th second. During the attack, the rate of *UDP* drastically increases almost from 0.0 to 1.0 and TCP drastically decrease almost from 1.0 to 0.0 in Fig.3-(b). However, there is no significant change in the others.

We examined the changes of network traffic characteristics under typical DDoS attacks (SYN, UDP, ICMP flooding attacks), and found significant differences between normal Web service traffic and DDoS attack traffic as mentioned in this section. We believe that we can early detect and defend DDoS attacks by using these differences and changes of network traffic. Detail of the detection and defense mechanism are explained in section 4.

4 The Proposed Probabilistic Packet Filtering Model

As shown in the previous section, the rate of specific type of packet exceeds that of normal situation during an attack situation. Thus, if we always maintain the rate of normal situation, we can mitigate the effect of the DDoS attacks.

The proposed Probabilistic Packet Filtering (PPF) model is similar to the Random Early Detection (RED), which is one of active queue management models and used for the purpose of congestion avoidance on network router equipments [13], [14]. The RED doesn't drop the packets when an average queue size is smaller than *Minimum Threshold*, drops the packets with the probability varying from 0.0 to *Maximum Probability* when an average queue size is greater than *Minimum Threshold* and smaller than *Maximum Threshold*, and drops all the packets if the average queue size is greater than *Maximum Threshold* [14].

The RED algorithm behaves according to the queue size of entire packets and 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). The rate of specific type of packet is excessively higher than that of normal situation during DDoS attacks. Thus, the proposed model effectively distinguishes attack packet from normal packet using TCP flag rate and Protocol rate, and drops attack packet without dropping of legitimated packet.

Fig. 4-(a) describes the PPF model proposed in this paper. Let the currently analyzed network traffic rate by the CTNT 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*). In this case, the rates of normal web traffic are the values in the Table 2 of section 3.2.1. 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. Floyd et al. recommend a quite small w_q to prevent the algorithm reacting to short bursts of congestion [14]. However, the proposed algorithm adopts big w_q (e.g., 0.5) since bursts of traffic are very serious threat during DDoS attack.

Fig. 4. 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 $P_H[Xi]$

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

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

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

where m is the amount of time CTNT 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., $R[Ui]$ in Fig. 4-(b)), 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., $R[Si]$ in Fig. 4-(b)), 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 (e.g., $R[Fj]$ and $R[Aj]$ in Fig. 4-(b)). The probability depends on the factor; the closer AR to P_H , the higher the 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.

$$E - 1.96 \times SD \leq R \leq E + 1.96 \times SD \tag{5}$$
$$P_L \leq R \leq P_H$$

$$P_d = \frac{AR - P_L}{P_H - P_L} \tag{6}$$

In the Table 2, for example, the average and the standard deviation of $R[Si]$ are 0.17 and 0.01, respectively. Then, we have confidence interval from 0.15(= $P_L[Si]$) to 0.19(= $P_H[Si]$) at a 95% of confidence level. If we assuming that $AR1[Si]$ (0.40), $AR2[Si]$ (0.18), $AR3[Si]$ (0.16), and $AR4[Si]$ (0.10), $AR1[Si]$ must be dropped because it exceeds $P_H[Si]$, and $AR4[Si]$ should be accepted because it is lower than $P_L[Si]$. On the other hand, $AR2[Si]$ and $AR3[Si]$ may be dropped or accepted according to the calculated probabilities 75% and 25%, respectively. Thus, as AR is close to P_H , the more packets are discarded.

5 Experimental Results

In order to evaluate the effectiveness of the proposed model, we construct simulation network and build attack model against the Web server using DDoS attack tools such as *TFN2K*. Detail of experimental environments and results are explained in the next two sections.

5.1 Experimental Environment

Fig.5 shows the network configuration to evaluate our DDoS defending mechanism in a simulated environment. The locations of web clients and DDoS attackers are randomly selected.

Fig. 5. Experimental Environment

Web clients send HTTP requests to and receive HTTP documents from the Web server using *SPECweb99*. While the normal Web traffic flows between Web clients and Web server, DDoS attackers generating flooding traffic against the Web server using *TFN2K*. *TFN2K* has all characteristics of other DDoS tools. We used Linux based *Apache* for the Web server.

The DDoS protector captures the network traffic both inbound and outbound one, analyzes them using the CTNT, determines drop probability of each packet, and finally forwards or drops the network packets. It works on the Linux 2.4.18 and uses *libpcap* to capture the network traffic and raw socket to forward the packets.

5.2 Experimental Results

Table 3 shows the experimental results of the proposed DDoS defense model. The normal Web service traffic flows during 60 seconds and the attacks using *TFN2K* are done between 20th second and 40th second.

As we can see in Table 3, the proposed defense mechanism shows very high performance in defending DDoS attacks. In the experiment, most of DDoS attack packets are dropped by PPF model with extremely low false positives; in 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 as shown in section 3. Moreover, in the normal situation, 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. On the other hand, in SYN flooding attacks, there is 0.57% false-positive rate since some legitimated SYN packets are generated while average $R[S_i]$ is higher than standard $R[S_i]$. Nevertheless, almost all the attacking packets are dropped by our defending mechanism.

Table. 3. Performance of our defense mechanism. Our packet dropping mechanism helps reduce the damage of DDoS attacks.

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%

6 Conclusion and the Future Work

In this paper, we analyze Web traffic using CTNT mechanism and 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 invalid packets based on 95% confidence level in accordance with an appropriate thresh hold. Our proposed model filters the suspected packets after detecting DDoS attacks via CTNT presented in the earlier study. Experimental results show very excellent results. Most of attacking packets are blocked by the proposed defending mechanism. Overall performances of our mechanism were 96.87%, 100%, and 100% on SYN, UDP, and ICMP flooding attack in each. Moreover, false-positive rate was only 0.57%. Therefore, we think our reasonable experiment results would be useful in Internet environments to defeat DDoS attacks.

In future work, we will try to evaluate our proposed model in more various situations and apply our proposed model for other specific targets such as a variety of application servers and Internet worms, especially high speed propagating 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. Kulkarni, A.B., Bush, S.F., and Evans, S.C.: Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics. Technical report 2001CRD176, GE Research and Development Center, (2001).
7. Ricciuli, L., Lincoln, P., and Kakkar, P.: TCP SYN Flooding Defense, Communication Networks and Distributed Systems Modeling and Simulation, (2000).
8. Wang, H., Zhang, D., and Shin, K.G.: Detecting SYN Flooding Attacks, In Proceedings of IEEE INFOCOM – The Conference on Computer Communications, vol. 21, no. 1, (2002) 1530-1539.
9. Li, M., and Vitanyi, P.: An Introduction to Kolmogorov Complexity and Its Applications, Springer-Verlag, Section 7.6, (1997) 506-509.
10. 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.
11. 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.
12. Paxson, V.: Growth Trends in Wide-Area TCP Connections, IEEE Network, vol. 8, (1994) 8-17.
13. Braden, B., et al.: Recommendations on Queue Management and Congestion Avoidance in the Internet, RFC 2309, (1998).
14. 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.