DDoS Attack Defense Architecture Using Active Network Technology*

Choong Seon Hong[1], Yoshiaki Kasahara[2], and Dea Hwan Lee[1]

[1] School of Electronics and Information, Kyung Hee University
1 Seocheon Giheung Yongin, Gyeoggi 449-701 KOREA
cshong@khu.ac.kr,blackl@networking.khu.ac.kr
[2] Computing and Communications Center, Kyushu University
Hakozaki 6-10-1, Higashi-ku, Fukuoka, 812-8581 JAPAN
kasahara@nc.kyushu-u.ac.jp

Abstract. To solve the congestion problem, network nodes at near the zombies need to filter the attack traffic. But the amounts of attack packets are small at upstream node and it is hard to detect an occurrence of an attack. In this case, the network node near the protected site should perform attack detection. Our proposed system uses active network technology and allowing detecting attack at active router near protected server. This detecting process uses dynamic, adaptive detecting algorithm. Elementary classification will reduce network congestion and adaptive classification will reduce error detecting rate. Signatures which are created by these two classifications are transferred to other active routers. And then they perform filtering process based on signatures.

1 Introduction

Nowadays, Internet becomes storehouse of information that can distribute information fast and easily. But, internet is a collection of networks that can not be trusted. So it is hard to control information. Therefore, network security became serious problem that protects internal resource against internet. Recently, a number of major commercial webs were attacked, rendering useless for a period of time by DDoS attacks. And also, in January 2003 internet was paralyzed because of the traffic increase caused by SQL slammer. Since then, DDoS attacks have become one of most annoying security problems for companies using internet. Currently, various security tools to defend against DDoS attack exist. Among these, we can use NIDS to detect flooding attacks. They have been developed to detect abnormal traffic and to notify system administrators or firewall systems of attacks. In most NIDS, the notification includes the time of detection, targets under attack and the attack signatures. But in this system certain problems exist without proper countermeasure. Because, it takes time to analyze network problem, even if administrator receive alert message. To defend against flooding attacks, packet filtering at gateway routers between user's networks and

* This work was supported by University IT research center of MIC.

A. Laganà et al. (Eds.): ICCSA 2004, LNCS 3043, pp. 915–923, 2004.

ISP's networks can prevent attack packets from flowing into site. However, these solutions have three drawbacks.

1. The access link between backbone network and the gateway router may be congested.
2. The bandwidth of the backbone network may be consumed.
3. Packets from legitimate users may be discarded mistakenly.

To solve these problems, detecting position has to be determined as protected site. And effective algorithm is needed, and also, created signatures are transferred to upstream node, filtering process has to be performed based on these signatures. To satisfy these conditions, active network technology that gives programmability to node is needed. The rest of this paper is organized as following. We will talk about related works in section 2. And we will propose DDoS attack defense architecture using active network technology in section 3. Testing results of detecting algorithm are presented in section 4. Finally, we give some concluding remarks.

2 Related Work

2.1 Defense Methods of DDoS Attack

There are three line of research about DDoS attack defense; attack prevention and preemption, attack detection and filtering, and attack source traceback and identification. The first line of defense is obviously to prevent DDoS attacks. With this method, hosts may be securely protected from master and agent. There are indeed known signatures and scanning procedures to detect them.[1] Attack source traceback and identification is to identify the actual source of packet sent across network without replying on the source information in the packet.[2][3] The third approach is attack detection and filtering. DDoS attack detection is responsible for identifying DDoS attacks, and filtering is responsible for classifying those packets and then dropping them.[4][5] The performance of research depends on FPR(False positive ratio) and FNR(False negative ratio). FPR is given by the number of packets classified as attack packets that are confirmed to be normal. FNR is the opposite case. The effectiveness of packet filtering, on the other hand, refers to the level of normal service that can be maintained by the victim during a DDoS attack by filtering. The detection process use the victim's identities, such as IP address and port number, as the signature of the attack packets. As a result, packet filtering usually drops attack packets as well as normal packets because both match the signatures. Effectiveness about this problem can be measured by NPSR(Normal Packet Survival Ratio), which gives the percentage of normal packets that can be transferred to the victim. Among these methods[6], attack prevention and preemption have to recognize how DDoS attack is performed and detect feature of attack by predefined signatures. So if attack tools are developed, new signatures that detect the pattern of attack is defined. Current IP traceback solutions are not always

able to trace packets' origins. Moreover, if the attack sources can be successfully traced, stopping them from sending attack packets is another very difficult task. Among attack detection and filtering, UIPF and RPF can achieve zero FPR and zero FNR if all attack packets use spoofed addresses. But its deployment difficulty is obviously the highest among them. And packet filtering in LAD is very ineffective in the midst of a sufficiently large-scale attack. However, this approach is most deployable. Finally, DAD's effectiveness in detecting attacks and filtering attack packets depends on the performance of the distributed detection algorithms. But it poses a higher computation requirement.

2.2 Statistical Detecting Algorithm

DDoS attacks are difficult to distinguish from legitimate traffic, and packet rates from individual flood sources are low enough to escape notice by local administrator. It is efficient that use statistical approach to detect this. Entropy computation or Chi-Squire test is used as statistical detecting algorithm.[7] Entropy computation provides a mechanism for detecting changes in the randomness. It detects the change of entropy average as follows

$$H = -\sum_{i=1}^{n} pilogpi$$

In the above equation, pi is probability of choice of n independent symbols. Pearson's chi-square test is used for distribution comparison in cases where the measurements involved are discrete values. It can compute degree of distribution about expected value and detect anomaly attribute of traffic. The shows formula of chi-square test is follows.

$$x^2 = \sum_{i=1}^{B} \frac{(Ni - ni)^2}{ni}$$

In the above equation as follows, B is the number of available binning value that is the expected number of packets in a sample having each possible value. And Ni is the number of packets whose value falls in the ith bin and ni is the expected number of packets in the ith bin under the typical distribution.

3 Proposed Defending Architecture

In this section, we are going to talk about proposed DDoS defense system. Proposed system detects attack at AR near protected site using active network technology and transmits signature that created at detecting process to other AR and performs filtering process based on these signatures. And we will propose dynamic and adaptive detecting algorithm that can detect attack with accuracy. Finally, we will propose architecture of AR that includes these modules (Fig. 1).

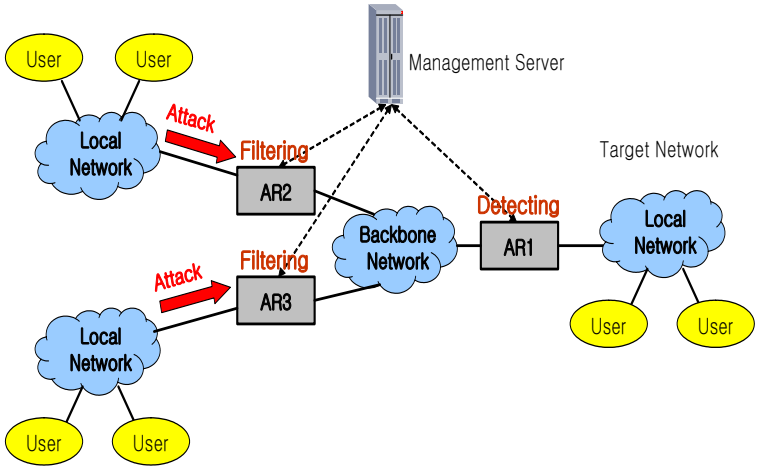

Fig. 1. Overview of Active Network Security System

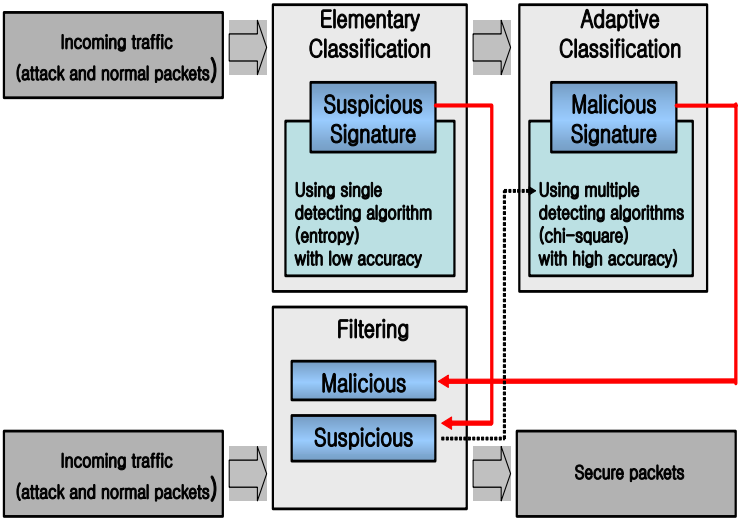

Fig. 2. Process of Signature Creation

3.1 Detecting Algorithm

Figure 2 shows the process of signature creation. There are two classification processes; Elementary classification and adaptive classification. Elementary Classification monitor packet that pass ARs. And it computes entropy of packet attributes and updates average of entropy value. If current entropy value exceeds

some average degree (threshold value), it creates suspicious signature using single entropy computation with low accuracy. In another word, this classification is achieved widely about attack packet (low threshold value). This process will reduce network congestion. Next, Adaptive Classification is performed to reduce ratio of normal packets that detect false. It analyzes packet attribute that belongs to suspicious signature during some period using multiple chi-square test with high accuracy and create malicious signature. Its threshold value is set high to analyze with high accuracy.

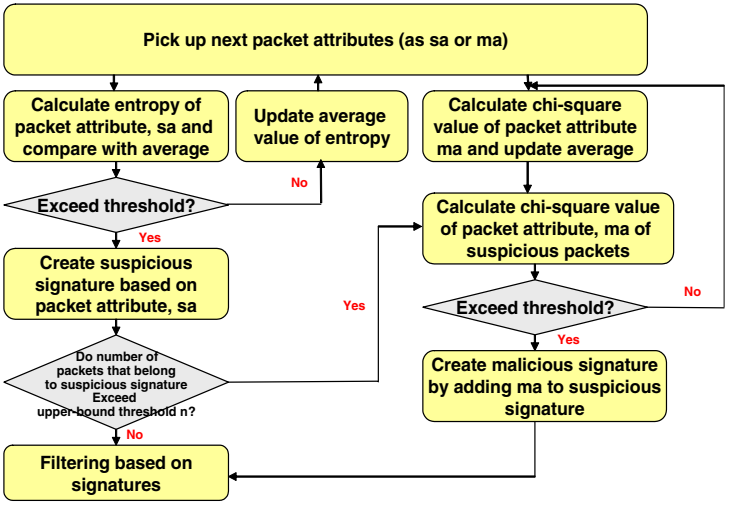

Fig. 3. Flowchart of Signature Creation

Table 1. Example of Suspicious Signature

Entropy Average	Current Entropy Value	Suspicious Signature
7(threshold 8)	8.7	Src=201.170.123.6

Figure 3 is the flowchart of signature creation. First each AR collects packet attributes (sa, ma) in monitoring tool for signature creation. It calculates entropy of packet attributes sa and compares the result with average value. If difference of average value exceeds threshold, AR creates suspicious signature as sa. Otherwise, AR updates entropy the average value of entropy. If the number of suspicious packets is larger than certain value, it should be malicious packet. So these packets are adaptive classified. In Adaptive Classification, the attributes (ma) of packet that belong to suspicious signature are performed chi-square test. If this value exceed threshold, it creates malicious signature by adding sa

to ma. Otherwise, AR also updates average. Table 1 shows example of creating of suspicious signature in elementary classification when it analyzes about source address. If entropy average is 7 and threshold is 8 and current entropy is 8.7, then detecting module creates signature based on source address. Table 2 is an example of malicious signature creation. If suspicious signature is the same as that of table 1 and the difference between current chi-square value of packet length and average exceed threshold, Elementary Classification create malicious signature by adding sa(source address : 201.170.123.6) with ma(packet length : 1-64byte).

Table 2. Example of Malicious Signature

Chi-Square Average	Current Chi-Square Value	Malicious Signature
1200(threshold 1300)	2000	Scr=201.170.123.6 leng=1-64byte

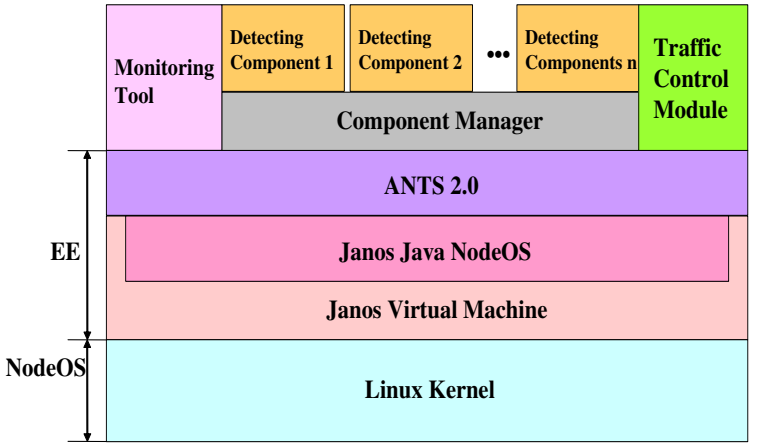

Fig. 4. Architecture of Active Router

3.2 System Architecture

For easy updating, detecting algorithm executes in AR as components. Figure 4 is the proposed architecture of active router. In figure 4, component manager receives instruction of management server and perform component management as threshold value setting, transmitting control message and signatures and computing average value. Each detecting components perform entropy computation and chi-square test. We used Janos and ANTS2.0 as an EE (Execution Environment), and Linux kernel as an NodeOS.

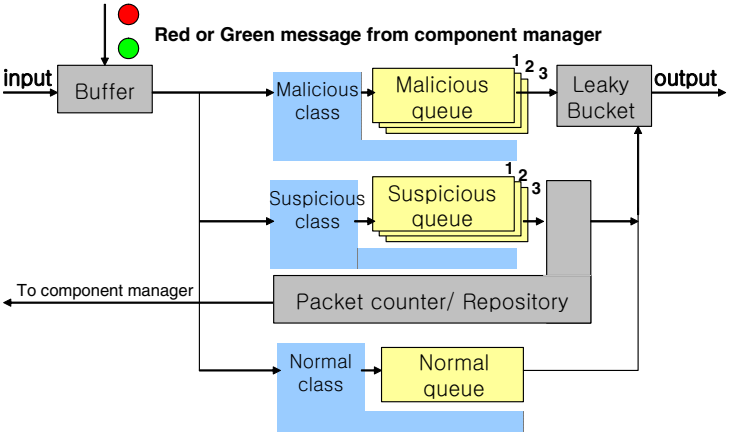

Fig. 5. Traffic Control Module

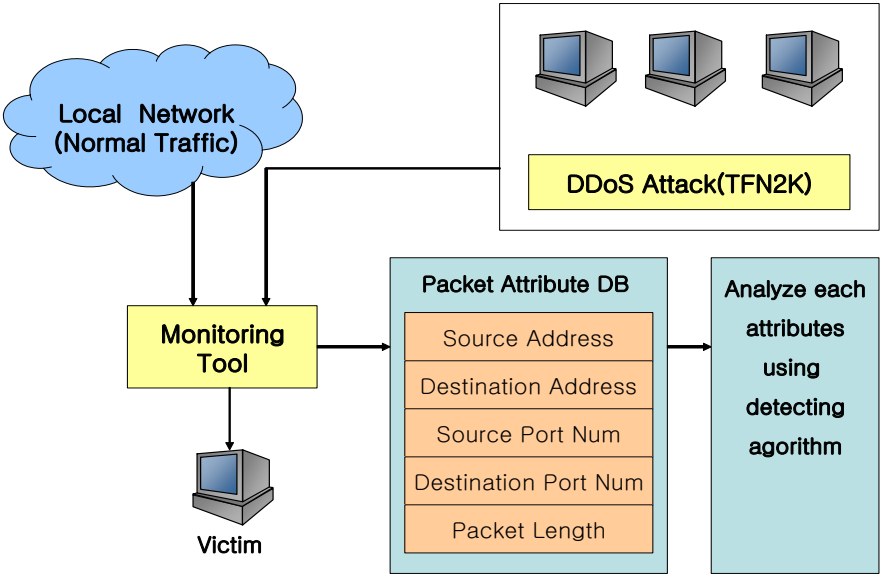

Fig. 6. Test Environment

Figure 5 shows the traffic control module. If attack is detected, component manager send red message to traffic control module, and then it deposits packets passed to module. Next component manager sends green message after creating each class of receiving signatures in component module. If traffic module receives this message, each class gets packets to queue that belong to signature. According to available packets that deposited in queue are passed in the following order that (1) normal (2) suspicious (3) malicious. Suspicious classification

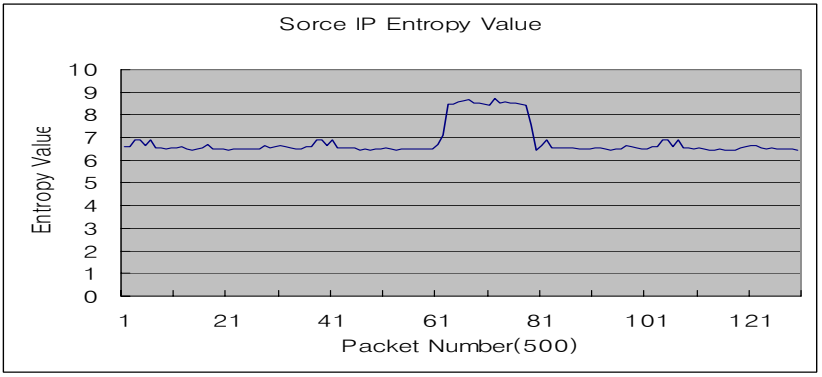

Fig. 7. IP Entropy Value

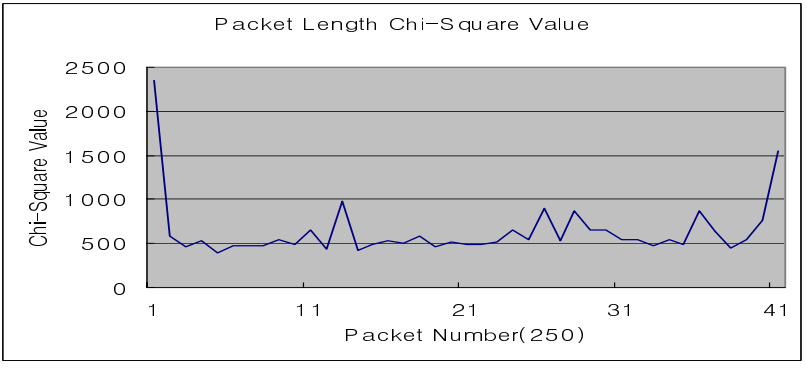

Fig. 8. Packet Length Chi-Square Value

deposit attributes of packets in repository and count number of them belonging to suspicious signature. If the number of packets exceeds threshold, control module transits packet attributions to component manager and these are analyzed in the component that performs adaptive classification.

4 Detecting Algorithm Test

We use TFN2K as attack tool and collect packet attribution using monitoring tool that based on libcap in test environment shown in Figure 6. This monitoring tool is designed so that can deposit source/destination address, source/destination port number and packet length to repository. And we analyze this data using detecting algorithm.

Figure 7 is the result that compute entropy of source address correspond to elementary classification. X axis is entropy value and Y axis is number of packets (500 packets per 1). If sampling size of the packet is bigger, accuracy is

higher but computation spends more time. If sampling size is smaller, accuracy is lower but computation performs faster. In this case, we compute entropy per 500 packets. In figure 7, we detect 10,000 packets that use TFN2K. (part of 61-81) It will detect DDoS attack when we set threshold as 8.5. But normal packet is detected as attack packet by elementary classification. The subsequent illustrate the result of adaptive classification that reduces the ratio of normal packets. Figure 8 is the result of analyzing packet length belonging to suspicious signature. We decrease sampling size of packet to reduce FPR. In this result, we detect 3 points that exceed 1000. It should be normal packets that falsely detected. Because we perform chi-square test about attributes of packet that classify DDoS attack packet, if the chi-square value is high, it will be normal packet.

5 Conclusion

In this paper, we discussed problems of previous research about defense of DDoS attack and proposed the architecture to solve those problems. In our algorithm, elementary classification solves network congestion problem and adaptive classification reduces error detection ratio. Test results using TFN2K show the proposed architecture can detect DDoS attacks. Especially, we confirmed that elementary classification mechanism can detect the source addresses for DDoS attacks. Also, adaptive classification mechanism can correct normal packets that detected as malicious packets. However, according to network states and use of attack tools, the useful attributes of packets can be differentiated. So, the proposed architectures need to be tested in various environments. If the created signature is disclosed to attackers, it could be abused. Therefore, we need to have a mechanism to confidentially keep it. For the purpose of interacting among the active routers, management server needs to consider its detailed enhancement.

References

1. S.Gibson, "The Strange Tale of the Denial of Service Attacks Against GRC.COM" http://grc.com/dos/grcdos.htm, 2002
2. A. Snoeren et al., "Hash-Based IP Traceback," Proc.ACM SIGCOMM, Aug. 2000
3. S. Savage et al., "Practical Network Support for IP Traceback," Proc.ACM SIGCOMM, Aug. 2000
4. P. Ferguson and D. Senie, "Network Igress Filtering : Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC 2827, May 2000
5. P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," Proc. Net. andMar. 1998
6. Rocky K.C Chang, "Defending against Flooding-Based Distributed Denial-of-Service A Tutorial," IEEE Communications Magazine 2002
7. Feinstein L., Schnackenberg D, Balupari R., Kindred D., "Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition(DISCEX 2003), April 22-24, 2003