Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks

Suratose Tritilanunt, Suphannee Sivakorn, Choochern Juengjincharoen, Ausanee Siripornpisan
Computer Engineering Department, Faculty of Engineering,
Mahidol University, Thailand
25/25, Salaya, Phuttamonthol, Nakornpathom, Thailand, 73170
E-mail: egstl@mahidol.ac.th, b-bow@live.com, rabu_chan@hotmail.com, st_dragon@hotmail.com

***Abstract*—Denial-of-service attacks (DoS) and distributed denial-of-service attacks (DDoS) attempt to temporarily disrupt users or computer resources to cause service unavailability to legitimate users in the internetworking system. The most common type of DoS attack occurs when adversaries flood a large amount of bogus data to interfere or disrupt the service on the server. By using a volume-based scheme to detect such attacks, this technique would not be able to inspect short-term denial-of-service attacks, as well as cannot distinguish between heavy load from legitimate users and huge number of bogus messages from attackers. As a result, this paper provides a detection mechanism based on a technique of entropy-based input-output traffic mode detection scheme. The experimental results demonstrate that our approach is able to detect several kinds of denial-of-service attacks, even small spike of such attacks.**

Keywords: DoS/DDoS attacks, entropy-based detection

I. Introduction

As stated by Mirkovic and Reiher [9], denial-of-service attacks (DoS) and distributed denial-of-service attacks (DDoS) are a technique aiming to deny access from legitimate users who share service or resources on a computer network. Because the Internet is an open and insecure internetworking system, therefore, it could have some malicious users or adversaries attempting to perform illegal actions to gain benefit over the others in some environments. In some cases DoS/DDoS attacks might not cause permanent harm to the victim, because a computer can restart and continually work again. However, they are able to cause real damage to the victim, especially when a computer is used in a corporate network such as government, commercial websites, bank, or Internet Service Provider (ISP). The growth of these attacks has been officially reported and published by CERT coordination center [5].

Defending against DoS/DDoS attacks is very difficult. Many defending schemes have been proposed to counteract such attacks but all of them can only help to limit the impact, not completely protect the network from denial-of-service disruption. One obvious example of denial-of-service defending approach focuses on detecting the traffic volume and distinguishing between suspicious and legitimate packets. However, this approach seems to be fail in detecting sophisticated DoS/DDoS attacks today. Many short-term denial-of-service attacks cause only minor change in traffic volume. Hence, distinguishing this effect of such DoS/DDoS attacks from legitimate traffic might be difficult or almost impossible when using a volume-based detection approach in this situation.

Another approach, a *feature-based detection* [11] [8], monitors header fields of every incoming packets for examining any changes. This technique fulfills a requirement of detecting DoS/DDoS attacks having a small number of traffic volume. However, the performance of this approach is a major concern because this technique requires real time examination on every packets.

To date denial-of-service defending technique has moved to another approach known as an *entropy-based detection* [6] [10] [1]. Since many applications have their typical packet sizes, for example, FTP can have 40 bytes for acknowledgment packets and 1500 bytes for data packets, Du and Abe [6] observe this fact and propose an IP packet size entropy for detecting DoS/DDoS attacks. In this technique, the concept is to investigate a similarity of IP packets and uses it as a packet size entropy. By investigating time series of packet size entropy, any changes to cause some spikes in observed time slot will be identified as denial-of-service attacks. Although this approach is able to detect both long-term and short-term DoS/DDoS attacks, we have found from the experiment that this technique, sometimes, might shows small number of false positive on the DARPA/MIT Lincoln Laboratory data set [7].

To minimize this false positive, we introduce a technique called *entropy-based input-output traffic mode detection scheme*. By combining packet content observation for identifying DoS and DDoS attacks in the system, this will help our approach not only to increase the accuracy for detecting DoS attacks, but also to effectively discriminate legitimate users from suspicious traffic.

In summary, the major purposes of this paper are

- to propose new entropy-based input-output traffic mode detection scheme for DoS/DDoS attacks; and
- to show the performance of our technique for detecting DoS/DDoS attacks from off-line intrusion detection evaluation data set of DARPA/MIT Lincoln Laboratory.

II. Denial-of-Service Attacks Overview

Denial-of-Service attacks (DoS) are a technique to attack against computers connected to the Internet. DoS attacks exploit bugs in an operating system or vulnerabilities in TCP/IP protocol. In a denial-of-service attack, an attacker attempts to prevent legitimate users from accessing information or

978-1-4244-7010-5/10/$26.00 c2010 IEEE

services. The infected computers may crash or disconnect from the Internet. In some cases they do not cause permanent harm to the victim, because a computer can restart and continually work again. However, they can cause real damage to the victim, especially when a computer is used in a corporate network such as government or ISP.

The most common type of DoS attack occurs when an attacker floods a network with a large amount of information. When a client wants any services from a server, a client will request to establish a connection to that server. The server can only process a certain number of requests at once. Therefore, if an attacker overloads the server with many requests, the server cannot simultaneously process other requests from other legitimate users. Examples of DoS attacks are discussed as follow:

A. TCP SYN attack

Normally, when an Internet user wants to request a service from the server, the user sends an establish-message to let the server know his/her request. The server will send an acknowledge-message back to the user and waits for the reply-message from the user until the connection is established or the timeout period is expired. In the third step, the server will open a socket port waiting for a reply-message from that user. This state is known as server half-open state. The TCP SYN technique [2] uses this flaw of TCP/IP by sending request-message with a large amount of data and source address from a spoofed address that does not exist.

To achieve denial-of-service attack by using this technique, the attacker establishes an uncompleted three-way handshake by sending a large amount of bogus request messages to initiate a connection and waits for a server to reply acknowledge back to the attacker. Because of the non-existent address, the server will not receive any messages back from the attacker. Since the three-way handshake must complete three steps of exchanging messages between a server and client, the server will be waiting for a third message from the attacker for a while. If the attacker sends many bogus requests to open a connection by this method to a server, the server will waste many resources to service these bogus messages and cannot serve legitimate users.

B. ICMP flooding attack

ICMP flooding attack or Ping flooding attack [4], is a Denial of Service attack that sends large amounts of ICMP packets to a victim in order to crash the TCP/IP buffer on the victim's machine and cause it to stop responding to TCP/IP requests. However, this technique does not cause more severe to a victim nowadays. As a result, the attacker needs to magnify the amplitude of attack by increasing a number of attacking packets. This method is also known as Distributed Denial-of-Service attacks (DDoS).

Distributed Denial-of-Service (DDoS) is a technique when an attacker attacks a victim from multiple source systems. An attacker uses a large number of compromised hosts to send useless packets at the same time to crash a victim or Internet connection. These packets are significant enough to break down the system. By taking advantage of security vulnerabilities or weaknesses, the attacker can automatically control other compromised computers, known as zombies, by installing exploit software such as Trojan Horses that contain malicious code into legitimate users' computers. When the attacker decides to launch the DDoS attack to any servers, they send the signal to trigger all compromised computers to make simultaneous requests to the same server. As a result, a large number of packets, which come from many compromised computers could break down the victim system. In this technique, the magnitude of attack is based on the number of compromised computers.

C. Smurf Attack

In the Smurf attack [3], the attacker sends a large amount of ICMP echo to a broadcast address of network (i.e. x.x.x.255 in class C of IPv4 type) and uses a victim's IP address as the source IP address. Therefore, the reply-message from all computers in that network that respond to the broadcast address will flood the victim. There are two parties affected by this attack: the broadcast router known as amplifier and the spoofed address target known as the victim. The victim is the target of a large amount of traffic that the amplifiers generate. The numbers of attack packets sent by the attacker depends on the number of hosts behind the router that reply to the ICMP echo packets. In order to summarize this, the following steps of SMURF attack are;

1) The attacker sends ICMP Echo Request packets where the source IP address has been forged to be the victim's IP address.
2) The attacker sends these ICMP Echo Request packets to a broadcast address of the router. These packets are broadcast to all computers that are connected to the router.
3) All the computers which are alive on that network send an ICMP Echo Reply packet back to the spoofed source IP address of the victim. If many computers are alive on that network, the amplification factor can be very large.

As this paper addresses the issue of developing entropy-based detection for the server, we pay our attention to the flooding attacks targeting only to the server; not covering attacks that overwhelm network bandwidth or legitimate clients. In addition, the result of DoS countermeasures from this work is limited to the protection technique; not including a reaction mechanism that traces back to a source of attacks. The final outcome of our approach, at least, is capable to identify well-known attacks discussed in this section.

III. Entropy-based Detection Technique

Different from a volume-based detection technique that focuses on a capacity of traffic or a number of resource usage of the system, a feature-based detection approach examines a header field of every incoming packets in order to detect denial-of-service and distributed denial-of-service packets. Even though this technique can detect small volume of DoS/DDoS attack packets, it might lead to another susceptibility since this technique requires high computation on the defending machine.

From the observation proposed by Du and Abe [6], basically, the incoming traffic of normal events should not much be identical within period of interest. However, many traditional DoS/DDoS attackers deploy techniques that frequently generate a large number of bogus packets with identical packet size. For example, TCP SYN flooding attack [2] has 40 bytes in length for each packet, and ICMP flooding attack [4] has 1500 bytes in length for each packet. This situation sheds the light on the idea of using Shannon's function to calculate a randomness (*entropy*) of such traffic for identifying denial-of-service packets.

An example of developing an IP packet size entropy (IPSE) to successfully detect DoS/DDoS attacks is proposed by Du and Abe [6]. The concept of their scheme is to investigate a similarity of IP packet size because most of attack traffic contain identical packets. The developer team claims that their technique is capable to detect both long-term; SYN flooding attack at time 11:20, and short-term; ICMP flooding attack at time 9:20 (this attack cannot be detected in a volume-based detection technique), as illustrated in Figure 1.

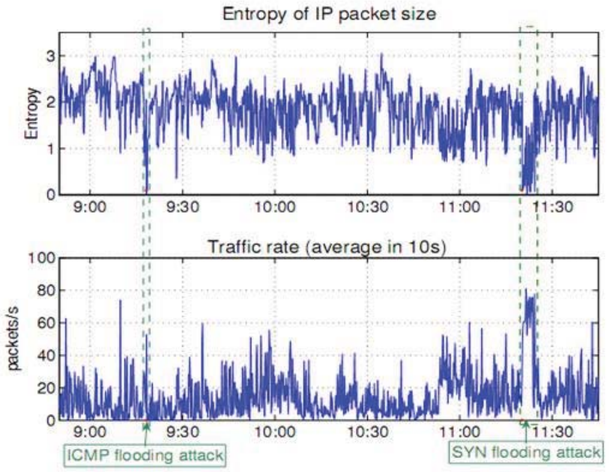


Fig. 1. Du and Abe Entropy Detection Technique [6]

Another one deploys entropy technique to detect attackers sending a large number of DNS query traffic in a campus network [10]. From their experimental result, they are able to identify spam bot as well as distributed denial-of-service (DDoS) attacks in their campus network. The last example goes to the application that uses an entropy detection approach to identify suspicious packets that attempting to stop a firewall [1]. Their goal is to improve the performance of a firewall under DoS/DDoS attacks by removing attacks from a server processing queue. Final outcome shows that a service throughput, queue delay, and availability are improved.

In our entropy-based input-output traffic mode detection scheme, we inspect packet content of traffic by using Shannon's function to compute entropy $H(t)$ at time t, as

$$H(t) = -\sum_{l}(\frac{n_l}{S})\log(\frac{n_l}{S}) \qquad (1)$$

where n_l is the number of packets having a similar size l in the inspection time frame having length S. In addition, packets having a similar length will be grouped and carefully analyzed the packet content for calculating the entropy. From the experiment explained in [6], we select the duration of attacks at least 200 packets similar to Du and Abe's experiment.

The Shannon's function is a useful tool for inspecting a similarity and distribution of traffic in the inspection time frame. When denial-of-service attacks occur in the observation window, the entropy of that traffic will drop noticeably and we can identify that situation as DoS/DDoS attacks. Not similar to other proposed techniques, our detection scheme not only focuses on the entropy of a packet size, but examines packet content as well. The reason why we add this parameter into our approach is that there is a small number of false positive in which some legitimate packets are identified as suspicious traffic in some situation. More details and discussion of this problem, as well as the experimental results are shown in Section IV.

IV. Experiment and Result

Section IV provides the experiment and results of our approach to detect denial-of-service attacks. In the experiment, the detection first analyses a normal behaviour of a network without any attacks. After that, it creates a network's profile for a normal event. Statistical data of such profile will be stored and used later as a based line. The system can detect the attack by using an entropy detection method because the value drops significantly from the stored profile once the DoS/DDoS attacks occur in the system. We observe that most denial-of-service attacks immediately decrease the entropy of the overall system.

From the data set extracted from Lincoln laboratory at Massachusetts Institute of Technology (MIT) [7], we calculate statistical output by using Equation 1 and separate them into three periods according to the time frame that DoS/DDoS attacks occur as shown in Table I. In a volume-based detection, statistical quantities including *mean*, *median*, and *standard deviation (SD)* of traffic bandwidth (*BW*) and packet rate (*PR*) are calculated. Meanwhile, entropy (*EN*) of these data set are computed as used in our entropy-based approach for comparing with a volume-based detection scheme. To make an important note that, our technique is different from Du and Abe's approach [6] since we incorporate with the packet content in order to analyze a similarity of suspicious packets for guaranteeing that the false positive in our detection technique would be minimum.

To show a functionality and effectiveness of our approach, we pick up a sample data captured by Lincoln laboratory at 1999. In that data set, it contains three kinds of DoS/DDoS attacks including; 1) ICMP flood with 6,105 packets, 2) TCP SYN flood with 111,713 packets, and 3) SMURF attacks with

TABLE I
THE STATISTICAL EVALUATION OF SAMPLE TRAFFIC

	Mean	Median	SD
ICMP			
Packet Rate	8.0	105	16.448
Bandwidth	5786	11064	18873
Entropy	4.4397	4.3164	0.8991
TCP SYN Flood			
Packet Rate	15	21	35
Bandwidth	20100	1440	127115
Entropy	3.1204	3.7529	1.5978
SMURF			
Packet Rate	104	0	302.3012
Bandwidth	835031	0	2592598
Entropy	0.7399	0	1.5962

45,226 packets. In order to discriminate suspicious packets from legitimate packets, Equation 2 and 3 are used for calculating a cutting point for a volume-based detection, while Equation 4 is used for a feature-based detection. The statistical parameters including mean, median, and standard deviation (SD) are used in this calculation for weighting and balancing the final outcome. The output from these equations are shown in Table II.

$$Packet\ Rate = \frac{[mean_{PR} + SD_{PR}] + [median_{PR} + SD_{PR}]}{2} \tag{2}$$

$$Bandwidth = \frac{[mean_{BW} + SD_{BW}] + [median_{BW} + SD_{BW}]}{2} \tag{3}$$

$$Entropy = \frac{|mean_{EN} - SD_{EN}| + |median_{EN} - SD_{EN}|}{2} \tag{4}$$

TABLE II
DETECTING LINE TO ISOLATE DOS/DDOS AND LEGITIMATE PACKETS

	ICMP Flooding	TCP SYN Flooding	SMURF
Packet Rate	73	53	354
Bandwidth	27,299	137,885	3,010,114
Entropy	3.479	1.8391	0.8563

In a volume-based detection technique when the packet rate and bandwidth of incoming traffic are increasing above a calculated value demonstrated in Table II, it considers those traffic as harmful packets. The area above the cutting point will be detected as DoS/DDoS attacks and the system will alert an administrator. In contrast, an entropy-based approach detects DoS/DDoS attacks by investigating a similarity of packet data. Once an entropy decreases below a criteria point shown in Table II, our scheme will consider this situation as DoS/DDoS attacks. Figure 2, 3, and 4 compare the experimental results between a volume-based and our entropy-based detection scheme when using them to detect ICMP flooding, TCP SYN flooding, and Smurf attacks, respectively.

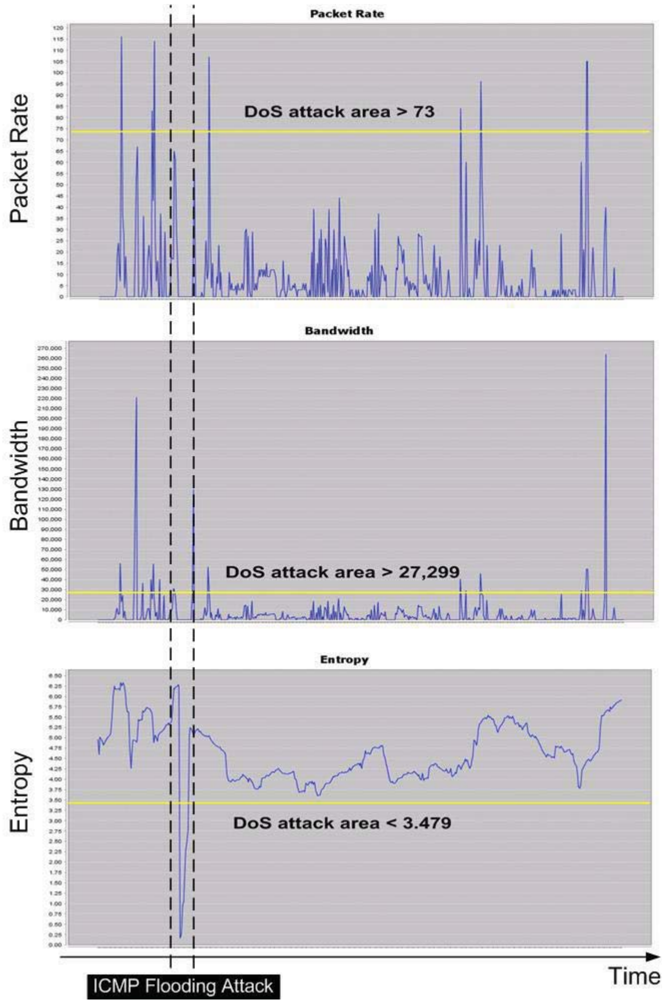


Fig. 2. ICMP flooding: Comparison among Packet Rate, Bandwidth, and Entropy Detection

Comparing both techniques in detection of ICMP flooding attacks shown in Figure 2, measuring the packet rate and bandwidth of traffic to identify suspicious packets discovers more than five times approximately. Meanwhile, detecting DoS/DDoS packets using entropy identifies only one situation as DoS/DDoS attacks. When we compare these results with ones available at the Lincoln laboratory website, our approach correctly identifies DoS/DDoS attacks. Moreover, the time frame detected as ICMP flooding attacks is not identified as the attack by using a packet rate detection method. This is because the attacker only sent small number of bogus packets (6,105 packets) in a short period. Hence, this situation supports

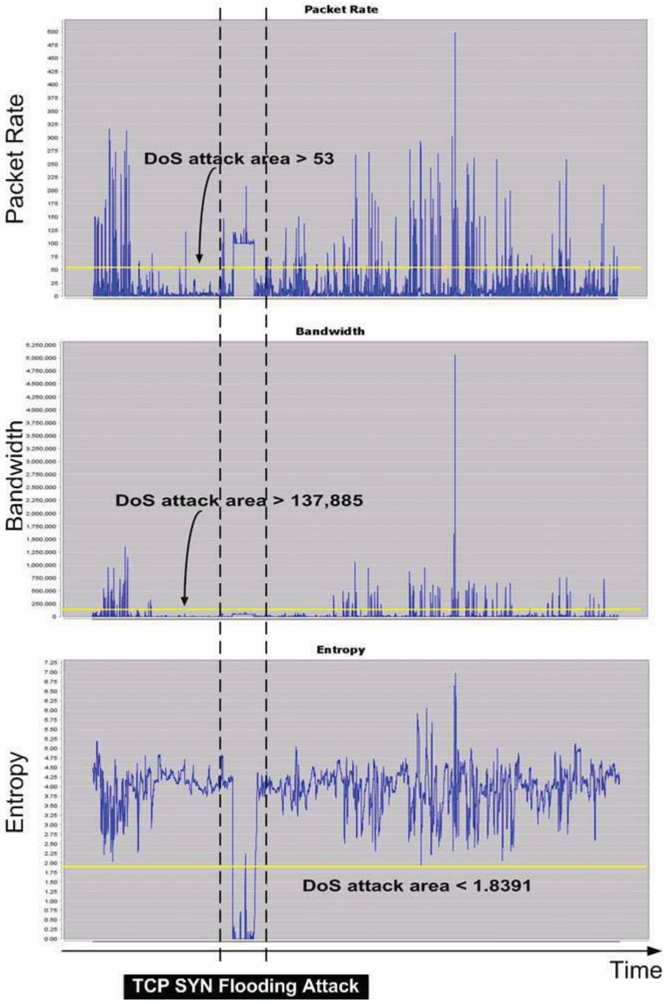


Fig. 3. TCP SYN flooding: Comparison among Packet Rate, Bandwidth, and Entropy Detection

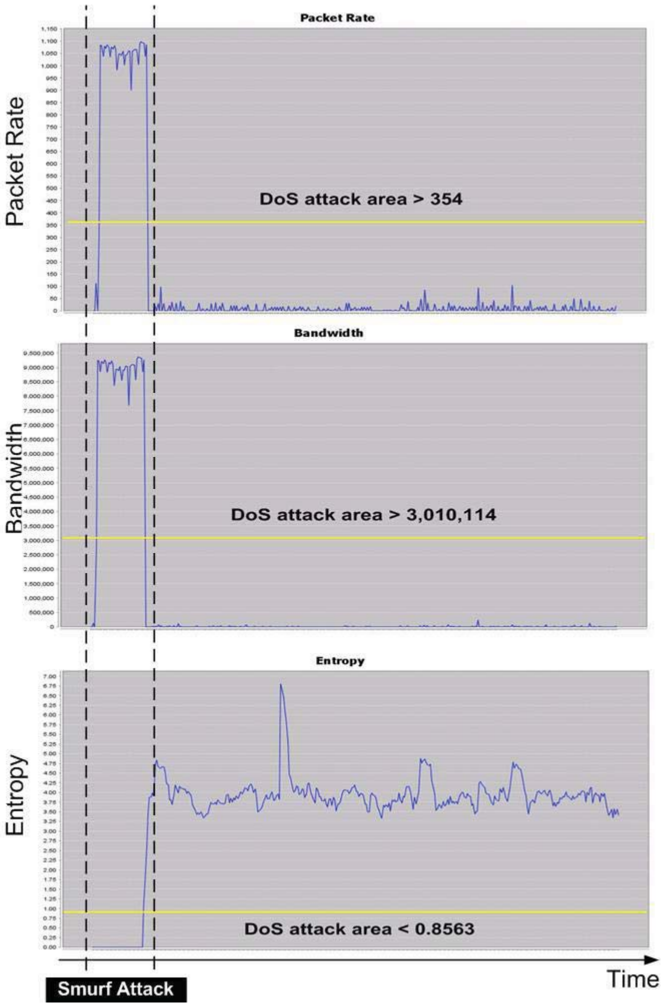
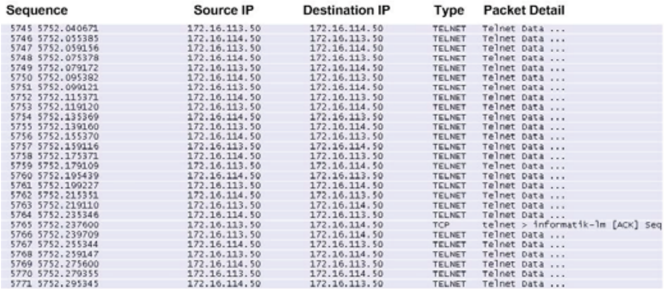


Fig. 4. SMURF: Comparison among Packet Rate, Bandwidth, and Entropy Detection



Sequence	Source IP	Destination IP	Type	Packet Detail
5745 5752.040671	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5746 5752.055385	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5747 5752.059156	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5748 5752.075378	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5749 5752.079172	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5750 5752.095382	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5751 5752.099121	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5752 5752.115371	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5753 5752.119120	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5754 5752.135369	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5755 5752.139160	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5756 5752.155370	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5757 5752.159116	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5758 5752.175371	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5759 5752.179109	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5760 5752.195439	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5761 5752.199227	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5762 5752.215351	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5763 5752.219110	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5764 5752.235346	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5765 5752.237600	172.16.113.50	172.16.114.50	TCP	telnet > informatik-lm [ACK] Seq
5766 5752.239709	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5767 5752.255344	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5768 5752.259147	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5769 5752.275600	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...
5770 5752.279355	172.16.113.50	172.16.114.50	TELNET	Telnet Data ...
5771 5752.295345	172.16.114.50	172.16.113.50	TELNET	Telnet Data ...

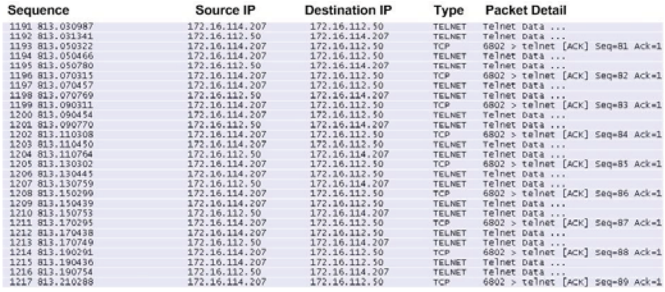
Fig. 5. Details of Packets at the Last Peak of Figure 2 (Packet Rate)

that short-term attacks are able to be successfully detected by the entropy-based detection. This is a major key strength of this approach over the others.

The different result between two approaches leads our attention to carefully investigate the experimental result. By using packet analyzer software for analyzing other peaks detected by a volume-based detection approach, we have found that other remaining areas are not the attacks. An example, which is recorded and illustrated at the last peak area in Figure 2 (Packet Rate), is Telnet data that were being sent back-and-forth between legitimate users and a host computer with high transfer rate. These packets seem to be similar, however, the content inside are totally different. This is because a file size that a legitimate user was exchanging with a host computer are too long, so the protocol break down it to small segment. The detail of these packets is illustrated in Figure 5.

Considering the second attack, TCP SYN flood (Fig 3), a volume-based detection technique identifies almost half of investigated data. In a meantime, our detection technique using entropy of incoming data recognize only one attack. Similar to the previous attack, only one area as discussed on the Lincoln laboratory website is TCP SYN flooding attack. When we carefully analyze those sample data, these false alarms identified by a volume-based detection technique are legitimate users exchanging messages to a host computer. We use a packet analyzer software to capture some samples of these packets around the first peak area of Figure 3 (Packet Rate). The sample result is illustrated in Figure 6.

In term of the accuracy, the successful rate of our technique



```
Sequence                     Source IP        Destination IP   Type    Packet Detail
1191 813.030987              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1192 813.031341              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1193 813.050322              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=81 Ack=1
1194 813.050466              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1195 813.050780              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1196 813.070315              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=82 Ack=1
1197 813.070457              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1198 813.070769              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1199 813.090311              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=83 Ack=1
1200 813.090454              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1201 813.090770              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1202 813.110308              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=84 Ack=1
1203 813.110450              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1204 813.110764              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1205 813.130302              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=85 Ack=1
1206 813.130445              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1207 813.130759              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1208 813.150299              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=86 Ack=1
1209 813.150439              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1210 813.150753              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1211 813.170295              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=87 Ack=1
1212 813.170438              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1213 813.170749              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1214 813.190291              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=88 Ack=1
1215 813.190436              172.16.114.207   172.16.112.50    TELNET  Telnet Data ...
1216 813.190754              172.16.112.50    172.16.114.207   TELNET  Telnet Data ...
1217 813.210288              172.16.114.207   172.16.112.50    TCP     6802 > telnet [ACK] Seq=89 Ack=1
```

Fig. 6. Details of Packets at the First Peak of Figure 3 (Packet Rate)

to detect ICMP flooding attacks is 99.48%, TCP SYN flooding attacks is 99.40%, and SMURF attacks is 99.52%. On the other hand, the accurary of legitimate traffic identification is 98.14% in case of ICMP flooding attacks, 99.92% in case of TCP SYN flooding attacks, and 99.71% in case of SMURF attacks. This result ensures that our approach is able to correctly detect DoS/DDoS attacks not only long-term attacks as similar as other approaches, but also short-term attacks which are unable to be discovered by volume-based detection schemes.

In summary, an entropy-based technique provides more accurately denial-of-service detection than a volume-based technique. Moreover, the detecting time to discover both long-term and short-term denial-of-service attacks in our scheme is another key strength over a feature-based detection approach. These two major advantages are supported by the experimental results as demonstrated in this section.

V. Conclusion

This paper introduces an alternative technique to detect denial-of-service and distributed denial-of-service attacks by using packet size and packet content entropy-based technique. By combining with an IPSE-based DoS detection scheme, the major strength over existing ones is that our approach functions correctly and is able to successfully detect both long-term and short-term denial-of-service attacks that might not be able to detect at the same time with other approaches. To support this, we set up the experiment and show the result in Section IV. Definitely, only the experiment of DoS/DDoS detection using the data set from DARPA/MIT Lincoln Laboratory might not enough to cover all denial-of-service attacks in the world, we plan to test our approach with other kinds of DoS/DDoS attacks in the future work. Moreover as discussed in [6], if sophisticated attackers completely understand our detection mechanism, they might be able to modify their attacking technique that cause vulnerability to our defending approach.

References

[1] F. Al-Haidari, M. Sqalli, K. Salah, and J. Hamodi. An Entropy-Based Countermeasure against Intelligent DoS Attacks Targeting Firewalls. In *POLICY '09: Proceedings of the 2009 IEEE International Symposium on Policies for Distributed Systems and Networks*, pages 41–44, Washington, DC, USA, 2009. IEEE Computer Society.

[2] Computer Emergency Response Team (CERT). TCP SYN Flooding and IP Spoofing Attacks. [Online]. Available: http://www.cert.org/advisories/CA-1996-21.html, 1996.

[3] Computer Emergency Response Team (CERT). Smurf Attack. [Online]. Available: http://www.cert.org/advisories/CA-1998-01.html, 1998.

[4] Computer Emergency Response Team (CERT). Tribe Flood Network. [Online]. Available: http://www.cert.org/incident_notes/IN-99-07.html, 1999.

[5] Computer Emergency Response Team (CERT). Denial-of-Service Attack Articles and Reports. [Online]. Available: http://www.cert.org/nav/allpubs.html, 2006.

[6] Ping Du and Shunji Abe. Detecting DoS Attacks Using Packet Size Distribution. In *2nd Bio-Inspired Models of Network, Information and Computing Systems (Bionetics 2007)*, Dec 10-12 2007.

[7] Lincorn Laboratory. DARPA Intrusion Detection Evaluation. Online Webpage, Jan 2010. [available] http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.

[8] A. Lakhina, M. Crovella, and C. Diot. Mining Anomalies using Traffic Feature Distributions. In *SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 217–228, New York, NY, USA, 2005. ACM.

[9] J. Mirkovic and P. Reiher. A Taxonomy of DDoS attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computing and Communication Review*, 34(2):39 – 53, 2004.

[10] Dennis Arturo Ludena Romana and Yasuo Musashi. Entropy based analysis of dns query traffic in the campus network. In *The 4th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA 2007)*, July 12-15 2007.

[11] H. Wang, D. Zhang, and K. G. Shin. Detecting SYN Flooding Attacks. In *In Proceedings of the IEEE Infocom*, pages 1530–1539. IEEE, 2002.