Yu, Shui, Thapngam, Theerasak, Liu, Jianwen, Wei, Su and Zhou, Wanlei 2009, Discriminating DDoS flows from flash crowds using information distance*, in NSS 2009 : Proceedings of the third International Conference on Network and System Security*, IEEE, Piscataway, N. J., pp. 351-356.

2009 Third International Conference on Network and System Security

Discriminating DDoS Flows from Flash Crowds Using Information Distance

Shui Yu, Theerasak Thapngam, Jianwen Liu, Su Wei and Wanlei Zhou
Deakin University, Burwood VIC 3125, Australia
{syu, tthap, jianwen, suwei, wanlei}@deakin.edu.au

Abstract—**Discriminating DDoS flooding attacks from flash crowds poses a tough challenge for the network security community. Because of the vulnerability of the original design of the Internet, attackers can easily mimic the patterns of legitimate network traffic to fly under the radar. The existing fingerprint or feature based algorithms are incapable to detect new attack strategies. In this paper, we aim to differentiate DDoS attack flows from flash crowds. We are motivated by the following fact: the attack flows are generated by the same pre-built program (attack tools), however, flash crowds come from randomly distributed users all over the Internet. Therefore, the flow similarity among DDoS attack flows is much stronger than that among flash crowds. We employ abstract distance metrics, the Jeffrey distance, the Sibson distance, and the Hellinger distance to measure the similarity among flows to achieve our goal. We compared the three metrics and found that the Sibson distance is the most suitable one for our purpose. We apply our algorithm to the real datasets and the results indicate that the proposed algorithm can differentiate them with an accuracy around 65%.**

Keywords: DDoS Attack; Distance; Measurement

I. INTRODUCTION

It is a tough challenge of identifying DDoS attacks when hackers mimic the normal Internet traffic pattern or hide attack flows in legitimate traffic. Because of the vulnerability of the Internet, it is easy for hackers to spoof source IP addresses of attack packets [24], verifying the pattern of attack flows [14][6], etc. In general, DDoS detection methods include activity profiling [12][21], sequential change-point detection [2][3][7][26], wavelet analysis [1], chi-square/entropy detector [12][16], and so on. All these methods are based on the features or fingerprints of specific DDoS attacks. Unfortunately, it is very easy for hackers to mimic these features to fool user detection methods. For example, because of the open architecture of the Internet, hackers can spoof the source IP addresses of attack packets according to the real Internet IP address distribution to against our source address distribution based detection algorithms [11][28]; hackers can change the TTL value of the attack packets according to the real hop distance between zombies and victim respectively in order to against our hop-count detection methods [27][28]; in order to fly under the radar, attackers may also mimic the behaviors of flash crowds [4][7], a sudden increase of legitimate traffic, e.g. many fans will access the official website when an important match is ongoing; many people will check CNN website when breaking news comes.

DDoS attacks and flash crowds share similar behaviors, and we have to differentiate them effectively, otherwise, we may raise false alarms. In fact, it is a big challenge for defenders to discriminate DDoS flooding attacks from flash events [4][7][15], and the consequences are serious if we can not discriminate them. On one hand, attackers can mimic the traffic features of flash crowds to disable our detectors. On the other hand, our detectors may treat the legitimate flash crowds as DDoS attacks. Research [15] tried to use three dimensions: traffic patterns, client characteristics and file reference characteristics, to discriminate flash crowds from DDoS attacks. Unfortunately, this counter attack method cannot follow the ever changing attack methods, as the attack patterns are changing from time to time, and the attacker may mimic the network traffic patterns of flash crowds, causing the detector to be disabled quickly. The entropy detector mentioned in the survey [4] came from reference [12], which can raise the alarm for a crowd access, however, it cannot discriminate DDoS attacks from the surge of legitimate accesses, e.g. flash crowds. Reference [7] tried to separate flash crowds from DDoS flows using the change-point detection method, but this method can be cheated easily, e.g. zombies can increase the number of attack packets very slowly, which will almost surely disable the change point detectors.

Distance measurement of traffic flows is an effective way to discriminate DDoS attack flows from flash crowds. As we know, zombies use pre-built programs to pump attack packets to the victim, as a result, *the similarity among attack flows are much higher than the similarity between random legitimated flash crowds*. Some researches have been done on solving the similarity problem using stochastic methods in frequency domain [9][17]. Cheng et al. [9] mapped DDoS attacks from time domain to frequency domain, and then transformed it to power spectral density to identify the DDoS attacks. Spectral

978-0-7695-3838-9/09 $26.00 © 2009 IEEE
DOI 10.1109/NSS.2009.29

analysis [8] employed digital signal processing method to expose the hidden shrew DDoS attacking packets. Reference [17] used data mining technology to dig the DDoS attack information, but it is costly in terms of computing and delay. Our previous work [29] explored the similarity methodology preliminarily, and the effectiveness of the proposed method is confirmed. Reference [25] used Hellinger distance to detect VoIP floods in peer-to-peer networks.

In this paper, we employ three abstract distance metrics, the Jeffrey distance, the Sibson distance, and the Hellinger distance [18], to measure the similarity among network flows. A *flow* is defined as the packets which are passing a router and the packets share the same destination address. When a DDoS alarm is raised, we start to sample the suspicious flows, and measure the similarity among the flows using the previously mentioned metrics. If the distance among the flows is sufficiently small, in other words, they are similar enough, we claim them as DDoS attack flows. Otherwise, it is flash crowds.

The major contributions of this paper are as follows:

- We present the three distance measure metrics, and we found that the Sibson metric is the best among them for our discrimination purpose.
- The proposed strategy is scalable and practical. The cooperating routers can be any routers in the Internet, rather than in an ISP network or a community network. We can conduct our detection with only two cooperative routers on the Internet, which is much easy to achieve in the Internet. The attack packets could be discarded far before they reach the victim according to the proposed methodology.
- The proposed method is independent from any specific DDoS flooding attack tools. It therefore can detect any forthcoming new attack fashions actively.
- The proposed algorithm is tested by real datasets, and we can differentiate DDoS flooding attacks from flash crowds with accuracy around 65%.

The remaining of this paper is organized as follows. Section 2 presents the background and the three metrics for distance measurement. In Section 3, we define the problem and specify our goal. Section 4 then explains the design of the discrimination algorithm. The performance analysis of the three metrics is conducted in Section 5, as well as the real dataset experiments for the proposed algorithm. Finally, Section 6 concludes the paper and point out the future work.

II. BACKGROUND

A. Launching DDoS Attacks

DDoS attacks target on exhausting the victim's resources, such as network bandwidth, computing power, operating system data structures, and so on. To launch a DDoS attack, malicious users first establish a network of computers that they will use to generate the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date antivirus software, or those that have not been properly patched. Vulnerable hosts are then exploited by attackers who use the vulnerability to gain access to these hosts. The next step for the intruder is to install new programs (known as *attack tools*) on the compromised hosts of the attack network. The hosts running these attack tools are known as *zombies*, and they can carry out any attack under the control of the attacker. Many zombies together form what we call an *army* [22].

There are two categories of DDoS attacks, typical DDoS attack and DRDoS attacks. In a typical DDoS attack, the army of the attacker consists of *master zombies* and *slave zombies*. The hosts of both categories are compromised machines that have arisen during the scanning process and are infected by malicious code. The attacker coordinates and orders master zombies and they, in turn, coordinate and trigger slave zombies. More specifically, the attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking. Then, master zombies, through those processes, send attack commands to slave zombies, ordering them to mount a DDoS attack against the victim. In that way, the agent machines (slave zombies) begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources.

Unlike typical DDoS attacks, in DRDoS attacks the army of the attacker consists of master zombies, slave zombies, and reflectors [13]. The scenario of this type of attack is the same as that of typical DDoS attacks up to a specific stage. The attackers have control over master zombies, which, in turn, have control over slave zombies. The difference in this type of attack is that slave zombies are led by master zombies to send a stream of packets with the victim's IP address as the source IP address to other uninfected machines (known as *reflectors*), exhorting these machines to connect with the victim. Then the reflectors send the victim a greater volume of traffic, as a reply to its exhortation for the opening of a new connection, because they believe that the victim was the host that asked for it.

The defense against DDoS attacks is a catch-me-if-you-can game. From the beginning, all legitimate users have tried to respond against these threats. Researchers from academia and industry have proposed a number of methods against the DDoS threat. The basic discrimination is between *preventive* [5][22] and *reactive* [23] defence mechanisms. Despite the efforts, the DDoS attacks still pose a huge threat. Attackers manage to discover new

weaknesses of computer systems and communication protocols when existing weaknesses have been patched up, and—what is worse—they also exploit the defence mechanisms in order to develop attacks to overcome these mechanisms or exploit them to generate false alarms and to cause catastrophic consequences.

B. Metrics for Distance Measures

We discuss three metrics for distance measures for network traffic flows based on literature in this section. There are two categories in this kind of measurement: a) measure based on information theory, and b) measure of affinity [18]. For category a), the original measure is called *Kullback-Leibler distance* [10]. For the given two flows with probability distributions $p(x)$ and $q(x)$, the Kullback-Leibler distance is defined as follow:

$$D(p,q) = \sum_{x \in \chi} p(x) \cdot \log \frac{p(x)}{q(x)} \quad (1)$$

Where χ is the sample space of x. It is obvious that $D(p,q) \neq D(q,p)$, if $p(x) \neq q(x)$. As the result, the previous equation cannot be a measure. *Jeffrey distance* fixes this asymmetric using combination of the Kullback-Leibler distance, which is defined as follows:

$$D_J(p,q) = \frac{1}{2}[D(p,q) + D(q,p)] \quad (2)$$

A further measure for this category is the *Sibson distance* detailed as follows.

$$D_S(p,q) = \frac{1}{2}\{D[p, \frac{1}{2}(p+q)] + D[q, \frac{1}{2}(p+q)]\} \quad (3)$$

The category b) originally came from Bhattacharyya's measure of affinity, $\rho = \sum_{x \in \chi} \sqrt{p(x) \cdot q(x)}$. The major metric used for this category is the *Hellinger distance*, which is defined as follows:

$$D_H(p,q) = \left[\sum_{x \in \chi} (\sqrt{p(x)} - \sqrt{q(x)})^2 \right]^{\frac{1}{2}} \quad (4)$$

It is necessary that we choose the most suitable metrics for specific purposes, e.g. measure the similarity among network flows to discriminate DDoS attack flows.

III. Problem Statement

We consider a very simple network diagram shown as Figure 1, it could be any part of the Internet, which is under control or cooperation of defenders. There are three routers, R_1, R_2 and R_3, and two traffic flows f_p and f_q, which goes through router R_2 and R_3 respectively, and the flows merge at router R_1. The dash lines in the diagram mean that the routers may not immediately connect with each other, in other words, the routers probable separate far away from each other.

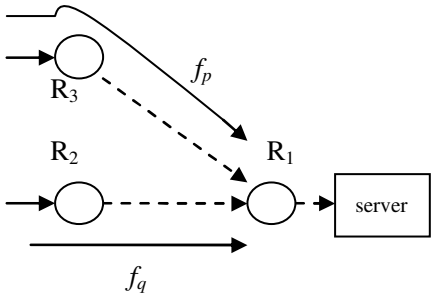

Figure 1. A sample network with two traffic flows.

Let $p(x)$ and $q(x)$ to represent the flow probability distribution of flow f_p and f_q, respectively, and χ be the finite sample space for the flows. Moreover, $p(x)$ and $q(x)$ are *N-tuples* $(p_1, p_2, ..., p_N)$ and $(q_1, q_2, ..., q_N)$, $p_i \geq 0, i = 1,2,...,N$, $q_i \geq 0, i = 1,2,...,N$, and $\sum_{i=1}^{N} p_i = 1$, $\sum_{i=1}^{N} q_i = 1$.

In this paper, our goal is to measure the similarity among the flows, for example f_p and f_q in Figure 1, to differentiate DDoS attack flows from flash crowds.

IV. The Discrimination Algorithm Design

In this section, we describe the design of the discrimination algorithms, and present the details of the algorithm.

When there is a surge of network flows, we are not sure whether it is DDoS attack or flash crowds. We name the surge flows as *suspicious flows* at the moment, and the cooperating routers will activate the discrimination algorithm to make the decision further.

Once the discrimination process is activated, the cooperating routers start to sample the suspicious flows for a sufficient time slot *t*, and the sampling is repeated until there are sufficient samples for decision making. The cooperative routers, e.g. router R_2 and R_3 in Figure 1, will exchange data when the sampling process is done. Then the routers can calculate the similarity of the flows independently using anyone of the previous mentioned metrics (we use the Sibson distance in this paper). If the distance is smaller than a given threshold, then the flows are DDoS attack flows, otherwise, the flash crowds.

The discrimination algorithm is detailed as follows:

The Discrimination Algorithm

1. Identify the suspicious flow, f_i, on a router *i (i>1)*, and initialize sample slot *t*, sample size *n*, and the discrimination threshold δ.
2. Take samples on flow f_i until the sample size $\geq n$, therefore, we obtain samples of number of packets as $x_1^i, x_2^i, \ldots, x_n^i$.
3. Calculate the probability distribution of the flow as $p(x^i) = x_k^i \cdot \left(\sum_{k=1}^{n} x_k^i \right)^{-1}$, noted as $p(x)$.
4. Router *j* will obtain its probability distribution of the flow as $p(x^j) = x_k^j \cdot \left(\sum_{k=1}^{n} x_k^j \right)^{-1}$, noted as $q(x)$.
5. Exchange $p(x)$ and $q(x)$ between router *i* and *j*.
6. The distance between $p(x)$ and $q(x)$ is calculated at router *i* and *j* independently using the Sibson distance metric, and noted as $D_s(p, q)$.
7. If $D_J(p, q) \leq \delta$, it is a DDoS attack and discard the related packets; otherwise forward the packets to the destination.
8. Go to step 2.

Figure 2. The discrimination algorithm

V. Performance Analysis on Metrics

A. *Metric Performance Analysis*

In order to find out which metric is the most suitable one for flow similarity measurement for DDoS attacks, we conducted a number of simulations carefully. In general, people believe that the Internet traffic obeys the Normal distribution pattern or the Poisson distribution pattern. Moreover, any distribution can also be represented by combination of a series of normal distributions with different parameters. Therefore, we examine the attributes of the three metrics using Normal distribution and Poisson distribution, respectively. There are two critical attributes that we use to compare the metrics: accuracy and sensitivity.

We arrange two flows with Normal distribution, $\mu = 10, \sigma = 1$, and the three distance metrics are applied to these two flows to measure the information distance. The simulation is conducted for 100 times, and the results are shown in Figure 3. On the other hand, we did the same simulation on two Poisson distribution flows with $\lambda = 10$, and the results are shown in Figure 4.

For two flows share the same distribution and parameter(s), the distance between them suppose to be zero in terms of statistics. From Figure 3 and Figure 4, we found that the Sibson's information radius is the best measure among the metrics in terms of accuracy.

In order to examine the metrics' sensitivity to traffic flows variations, two more simulations have been performed. We first investigate the metrics' sensitivity against standard variations of Normal distribution flows with $\mu = 10$ and σ that varies from 0.1 to 3.0, namely 1% to 30% variation from the mean. The results are shown in Figure 5.

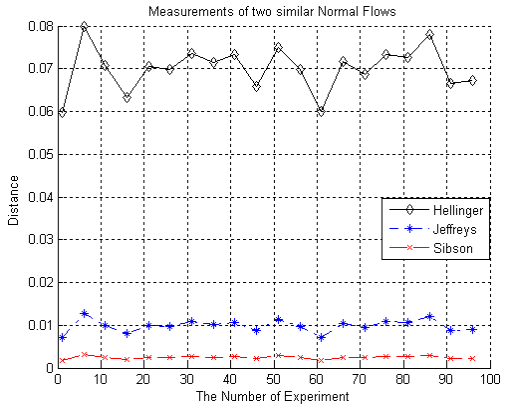

Figure 3. The measurements of two normal flows ($\mu = 10, \sigma = 1$)

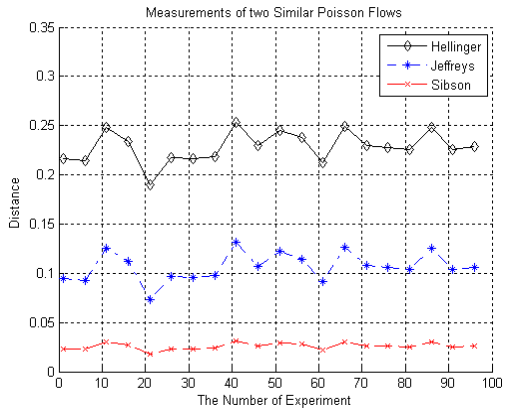

Figure 4. The measurements of two Poisson flows ($\lambda = 10$)

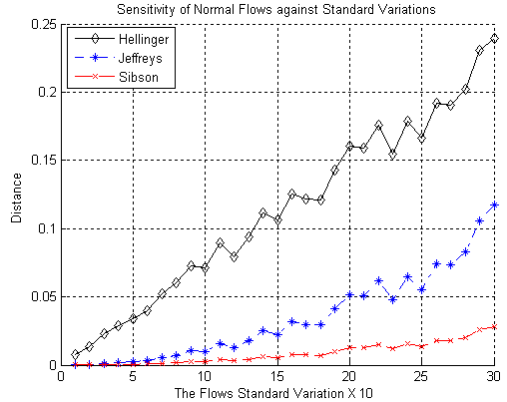

Figure 5. The metric sensitivity of normal flows ($\mu = 10$) against standard variation

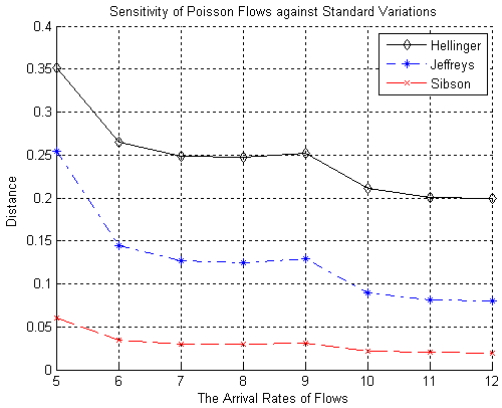

Figure 6. The metric sensitivity of Poisson flows against arrival rate

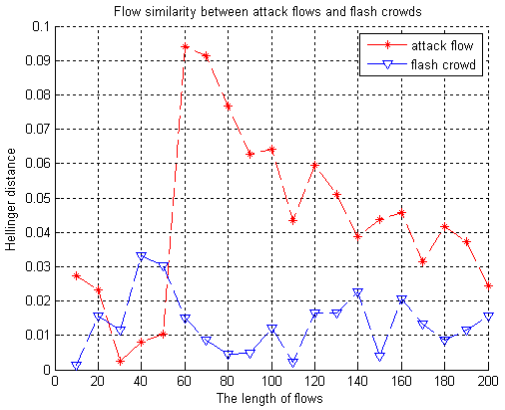

Figure 7. Similarity measure with the Hellinger distance

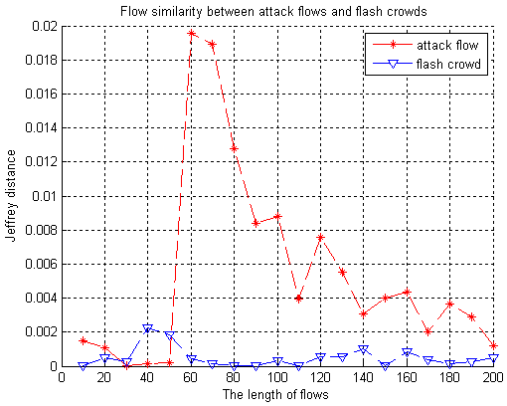

Figure 8. Similarity measure with the Jeffrey distance

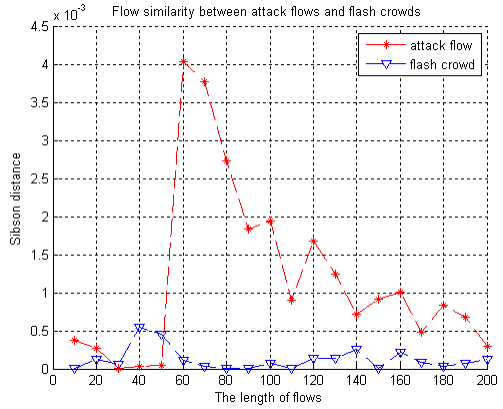

Figure 9. Similarity measure with the Sibson distance

For the Poisson flows, we examine the metric sensitivity against arrival rate, which varies from 5 to 12. The results are shown in Figure 6.

Based on Figure 5 and 6, we found that the Sibson's information radius is the least sensitive metric among the three metrics. The simulations demonstrated that it is quite stable for the change of parameters for both standard variation of Normal flows and arrival rate of Poisson flows.

B. *Performance Evaluation of the Discrimination Algorithm*

In this section, we examine the performance of the proposed discrimination algorithm against the real datasets. We use the NLANR PMA Auckland-VIII dataset [20] as the flash crowds, and the MIT LLS DDOS 1.0 intrusion dataset [19] as DDoS attack dataset. For each dataset, we count the number of packets which is addressed to the server (for flash crowds) or the victim (for DDoS attacks), the sample interval is 100 ms, and the size of samples is 200.

We processed the flows with the three metrics the Hellinger distance, the Jeffrey distance, and the Sibson distance respectively. The results are shown in Figure 7, 8 and 9 respectively.

Following the results of Figure 7, 8 and 9, we conclude two preliminary findings:

- The proposed strategy can differentiate DDoS attack flows and flash crowds more than 65% (13 out of 20) of the time.
- The Sibson distance is best metric among the three metrics for discriminating DDoS attack flows from flash crowds.

VI. SUMMARY AND FUTURE WORK

In this paper, we proposed the discrimination algorithm to differentiate DDoS attack flows from flash crowds employing information distance to fulfil the task. We presented three metrics for information distance measures, the Jeffrey distance, the Hellinger distance, and the Sibson distance. Our simulations and real data experiments indicate and confirm that the Sibson distance is the best metric among the previously mentioned metrics for flow distance

measure. Moreover, the proposed discrimination algorithm can identify DDoS attacks flows from flash crowds with an accuracy around 65% in the real dataset experiments.

Our future work focus on the follows: improving the accuracy of the flow based discrimination strategy with more side information, such as other independent attack features; extend the experiments to a large scale to observe the performance of the discrimination algorithm.

REFERENCES

[1] P. Barford, J. Kline, D. Plonka and A. Ron, "A Signal Analysis of Network Traffic Anomalies", *Proc. ACM SIGCOMM Internet Measurement Workshop,* ACM Press, November 2002, pp. 71–82.

[2] R.B. Blazek, H. Kim, B. Rozovskii, and A. Tartakovsky, "A Novel Approach to Detection of 'Denial-of-Service' Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods", *Proc. IEEE Workshop Information Assurance and Security*, IEEE CS Press, June 2001, pp. 220–226.

[3] R.R. Brooks, *Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks*, CRC Press, Boca Raton, 2005.

[4] G. Carl, G. Kesidis, R.R. Brooks, and S. Rai, "Denial-of-Service Attack Detection Techniques", *IEEE Internet Computing*, Vol. 10, No. 1, January 2006, pp. 82-89.

[5] CERT, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", *CERT Coordination Center*, 29 November 2000. http://www.cert.org/advisories/CA-1996-21.html

[6] Y. Chen and K. Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks", *the 2007 IEEE International Conference on Communications (ICC'07)*, June 2007, pp. 1203–1210.

[7] Y. Chen and K. Hwang, "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks", *the IEEE International Symposium on Collaborative Technologies and Systems (CTS 2006)*, May 2006, pp. 401-410.

[8] Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis", *Journal of Parallel and Distributed Computing*, Vol. 66, No. 9, September 2006, Academic Press, Orlando, pp. 1137-1151.

[9] C.M. Cheng, H.T. Kung and K.S. Tan, "Use of Spectral Analysis in Defense Against DoS Attacks," *IEEE Global Communications Conference*, 2002, pp. 2143-2148.

[10] T.M. Cover and J.A. Thomas, *Elements of Information Theory*, 2nd edition, Wiley-Interscience, June 2006.

[11] Z. Duan, X. Yuan and J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters", *IEEE Trans. on Dependable and Secure Computing*, Vol. 5, No. 1, January-March 2008, pp. 22-36.

[12] L. Feinstein, D. Schnackenberg R. Balupari and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," *Proc. DARPA Information Survivability Conf. and Exposition,* Vol. 1, IEEE CS Press, 22-24 April 2003, pp. 303–314.

[13] S. Gibson, "Distributed Reflection Denial of Service Description and Analysis of a Potent, Increasingly Prevalent, and Worrisome Internet Attack", *Gibson Research Corporation*, February 2002. http://grc.com/dos/drdos.htm

[14] M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End Systems", *Proc. IEEE INFOCOM*, Vol. 2, March 2005, pp. 1362-1372.

[15] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash Crowds and Denial-of-Service Attacks: Characterization and Implications for CDNs and Web Sites", *Proc. International World Wide Web Conferences*, ACM Press, New York, May 2002, pp. 293-304.

[16] K. Kumar, R.C. Joshi, and K. Singh, "A Distributed Approach using Entropy to Detect DDoS Attacks in ISP Domain", *The International Conference on Signal Processing of Communications and Networking (ICSCN '07),* February 2007, pp. 331–337.

[17] K. Lu, D. Wu, J. Fan, S. Todorovic and A. Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet," *Computer Networks*, Vol. 51, September 2007, pp. 5036-5056.

[18] G.J. McLachlan, *Discriminant analysis and statistical pattern recognition*, Wiley-Interscience, March 1992.

[19] MIT Lincoln Laboratory, "Lincoln Laboratory Scenario (DDoS) 1.0", *Massachusetts Institute of Technology (MIT)*, 1999. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000/LLS_DDOS_1.0.html

[20] Passive Measurement and Analysis (PMA) Project "Auckland-VIII", *The National Laboratory for Applied Network Research (NLANR)*, December 2003. http://pma.nlanr.net/Special/auck8.html

[21] D. Moore, G.M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," *Proc. 2001 USENIX Security Symposium,* Vol. 10, USENIX Association, August 2001.

[22] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks", *The Internet Protocol Journal*, Vol. 7, No. 4, December 2004.

[23] D. Radcliff, "Cybersleuthing solves the case", *Computerworld*, 14 January 2002. http://www.paypal.com/html/computerworld-011402.html

[24] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems", *ACM Computing Surveys*, Vol. 39, No. 1, April 2007.

[25] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 6, June 2008. pp. 794-805.

[26] H. Wang, D. Zhang and K.G. Shin, "Change-Point Monitoring for the Detection of DoS Attacks", *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 4, October-December 2004. pp. 193-208.

[27] H. Wang, C. Jin, and K.G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", *IEEE/ACM Transactions on Networking*, Vol. 15, No. 1, February 2007, pp. 40-53.

[28] F. Yi, S. Yu, W. Zhou, J. Hai, and A. Bonti, "Source-Based Filtering Algorithm Against DDOS Attacks", *International Journal of Database Theory and Application*, Vol. 1, No. 1, December 2008, pp. 9-20.

[29] S. Yu, W. Zhou and R. Doss, "Information Theory Based Detection Against Network Behavior Mimicking DDoS Attack", *IEEE Communications Letters*, Vol. 12, No. 4, April 2008, pp. 319-321.