International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

Partial Completion Filter Technique for Distributed Denial of Service Attacks

S.S.SARAVANAKUMAR[1], M.PRAVEENKUMAR[2]

[1]*Assistant Professor,*
Department of Information Technology,
Kovai Kalaimagal College of Arts & Science,
Coimbatore-641 109, India.
saravanakumarsssk@gmail.com
[2]*Research Scholar,*
Department of Computer Science
Kovai Kalaimagal College of Arts & Science,
Coimbatore-641 109, India.
praveenmnrp@gmail.com

***Abstract*— A computer system should provide confidentiality, integrity and assurance against denial of service. However, due to increased connectivity (especially Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. When the computer came into existence the minimum security provided is the User Name and Password protection. Through which it is easily detected and misuse can happen very often. Later when the encryption came into existence with various encryption techniques / algorithm, the intruder can able to trace out the encrypted code. Next level of improvement is in the form of Network security. The Network security with various forms and this paper concentrates on the concept of Denial of Service attack. The paper proposes a system with a novel data structure called Partial Completion Filter(PCF), which detects a wide variety of DoS and scanning attacks that belongs to several categories (bandwidth based, claim-and-hold, port-scanning).This system can also detect bandwidth attacks that are scalable in the network.**

Index Terms— **: Intrusion Detection System, Distributed Denial of Service, PCF.** ***(key words)***

I. INTRODUCTION

Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. Intrusion detection does not, in general, include prevention of intrusions. Intrusion detection can be performed manually or automatically. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. A system that performs automated intrusion detection is called an Intrusion Detection System (IDS). An IDS can be either host-based, if it monitors system calls or logs, or network-based if it monitors the flow of network packets.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. It can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

Denial of Service (DoS) attacks and Distributed DoS (DDoS) attacks have become more sophisticated and effective at obstructing this availability. In 2000, several online companies such as eBay, Amazon.com, CNN.com, and Yahoo were all affected by a large scale DDoS attack.

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

During this attack, their websites were rendered virtually unreachable to many Internet users, resulting in severe financial losses, in addition to the many unsatisfied customers. In 2002, several root Domain Name System (DNS) servers were brought down by yet another DDoS attack. This attack demonstrated that attackers were becoming more intelligent because critical systems were now being attacked. The general trend in DoS attacks implies that future attacks are likely to become much worse and more disruptive, affecting a larger number of Internet users.

II. BACKGROUND STUDY

This paper for Network security for available and each of which has got its own drawbacks. Initial when the computer came into existence the minimum security provided is User Name and Password protection. Which is easily detected and misuse can happen very often. Next level, the protections came into existence as encryption form and have various encryption techniques / algorithms are available. Even then the intruder can able to trace out the encrypted code. Next level of improvement is in the form of Network security. The Network security is again in various forms and this project concentrates on the concept of Denial of Service attack.

This paper concentrates on any scalable intrusion detection mechanism must deal with these two issues. Thus, the contributions of this paper are as follows.

1) Framework: Our paper initiates the study of scalable attack detection schemes. Then use behavioral aliasing and spoofing as a framework to analyze such techniques.

Behavioral aliasing: One form of behavioral aliasing occurs when a set of well behaved connections aggregate to look like bad behavior, creating a false positive. A second form of behavioral aliasing occurs when the aggregate behavior of several badly behaved connections looks like good behavior – a false negative.

Spoofing: Spoofing occurs when an intelligent attacker subverts the detection mechanisms by suitably spoofing the attack to appear benign.

2) Technique: As a specific example, we focus on scalable DDoS (Distributed Denial-of-Service Attacks) and scan detection, and propose a specific new scalable technique called Partial Completion Filters (PCFs) and analyze behavioral aliasing and spoofing characteristics of PCFs in different deployment scenarios.

3) Evaluation: To evaluate the efficacy of PCFs, which use a theoretical model later validated by real traces from two different ISPs. For example, in an OC-48 traffic trace for an entire day.

III. METHODOLOGY

A. Partial Completion Filters: Algorithm

Partial completion filters identify flows with high imbalance between two types of control packets that are usually balanced. For example, benign TCP connections consist of equal number of SYN and FIN packets — PCFs can be used to detect SYN flooding that involves transmitting only SYN packets (and hence high imbalance between SYNs and FINs). PCF data structure consists of parallel stages each containing a set of counters.

Packets are hashed based on the header fields using multiple independent hash functions (Fig:3.1) and counters indexed by these hash functions are

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

incremented/decremented for the two types of control packets. If all the counters indexed by the hashes of a packet are above a particular threshold (exhibiting high imbalance), the flow is output. At the end of a measurement interval, these counters are all reset.

The expected value of these counters is zero if there are equal numbers of SYN/FIN packets in a given flow. However the standard deviation is after packets. Thus, a benign bucket may have fairly large positive counters (causing false positives) while a bucket containing an attack may be pulled down to zero (causing a false negative). The tricky part is to show that both false negatives and false positives stay within control for reasonable parameter values.

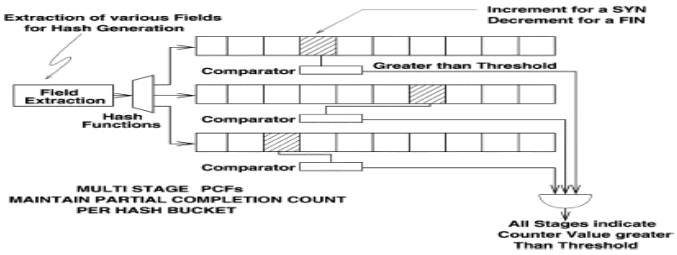

Fig:1 Partial Completion Filters

One might hastily conclude that PCFs are the same as multistage filters first proposed in to detect heavy-hitter flows in the network. This is not true for the following three reasons:

1) Non-monotonicity: In multistage filters (and in fact in all Bloom filter variants), the counters are only incremented and never allowed to be negative.

2) False negatives: Bloom filters and multistage filters have only one-sided errors; there are no false negatives. Unfortunately, since PCFs allow counters to decrease, they can cause false negatives.

3) Different analysis: The analysis of PCFs using the Central Limit theorem is very different from the simple counting argument for multistage filters. Also, the design of a PCF reflects a delicate balance between false positive and false negative rates. For instance, using more than three stages is almost always a bad idea for PCF while it is always a good idea for multistage filters.

B. Behavioral Aliasing in PCFS

In this section, it provides a theoretical analysis that allows predicting the behavior of as well as tuning PCFs in real network settings. The analysis is in three parts. In Part 1, it will use the Central Limit Theorem and tail bounds on Gaussian distributions to bound the false negative and false positive probabilities, which in turn determines the operating range of PCFs. In Part 2, it identify how to use PCFs to detect the flows that greater than a given threshold. Finally, in Part 3, it analyze the false positives and false negatives in the presence of other bad flows.

Before it proceed, note that if a flow begins and ends in a given measurement interval, then the contribution of that flow to the counters would be 0. However, due to the presence of intervals, there can be benign but malformed connections. First, a connection may be long-lived, in which case it contributes its SYN to one measurement interval, and it's FIN to another measurement interval. Second, a connection may retransmit its FIN.

However, as a first-order approximation, it can assume that a connection is equally likely to retransmit its SYN. In practice, TCP has a built-in asymmetry that makes SYN retransmissions happen slightly more often than that of FIN retransmissions. After using the first-order model (with equal retransmission probabilities), it show how this small

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

bias can easily be corrected for in Section IV-A. Third, route churn may cause the SYN to be seen but not the FIN, but in that case, during another interval due to another route churn, it might see the FIN but not the SYN.

On average, a set of measurement intervals should be able to smooth out this noise. In, the authors have experimentally verified that the routes are stable on the scale of a few minutes. So, it believes that the noise generated due to route churn is not really significant. Nevertheless, the analytical model captures this effect as well. In all these cases, it can simply assume that in a given measurement interval, the probability of a SYN or a FIN is 0.5.

C. Applying PCFS to Detect Partial Completion and Scanning Attacks Notation

It use PCF(A, B, C) to denote a PCF that increments (decrements) on a TCP packet with flags A (B), and uses C as the field(s) used to hash the packet.

1. Partial completion detection: For the detection device, the key abstract behavior that signals a SYN flood to a destination is the presence of a destination that receives a large number of SYNs from various sources. Thus, a PCF (SYN, FIN, DIP, DP) can be used to scalably detect a TCP SYN floodattack by hashing based on destination IP address, port pairs.

In the network, if it assumes that the detection mechanism cannot see both directions of the traffic, the attacker can easily spoof the PCF by transmitting an additional FIN packet along with the SYN packet.

It shows how to make SYN flood detection spoof resilient using reverse path deployments in: the trick is to hash source addresses (as opposed to destinations) in the reverse path to identify victims. This is because, without collusion from inside the network, the attacker cannot force the victim to send FIN packets.

2. TCP scanning detection: At a network vantage point, during TCP scanning activity such as port scan, a detection device can observe a large number of SYN packets to a particular port but with no corresponding FIN packets that correspond to legal tearing down of the connection. Therefore, for the detection device the key abstract behavior that signals a TCP scan is the presence of a source that sends a large number of SYNs to various destinations and destination ports without sending a corresponding FIN. Thus, a PCF (SYN, FIN, SIP) can be used to scalably detect a TCP scan by hashing based on source IP addresses and zeroing in on such sources that have a large SYN-FIN imbalance. In the network, if it assume that the detection mechanism cannot see both directions of the traffic as it have assumed, then PCF methods are easily subject to spoofing. One approach is to ignore spoofing because most attackers employ tools such as NMAP that do not spoof today; however, it will show how to make detection spoof-resilient using bidirectional deployments (in scenarios where it can see both directions of traffic) in Section III-E. Next, it apply PCFs for scalable monitoring of partial completion and scanning attacks in the network.

D. Applying PCFS For Attack Monitoring

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

PCFs can be applied to characterize attack flows in an online fashion, in contrast to current approaches that rely on passive traces. Note however that, for the ease of validation, it used real traces to evaluate PCFs in Section IV. Using PCFs, it can identify attack flows (sources and destinations using different PCFs or can be combined into one by hashing each packet twice), count the estimated size and duration of attacks in a scalable fashion. It will show in Section IV-B2 experiences with PCFs in scalable characterization of attack flows. As it have seen earlier, PCF (SYN, FIN, DIP, DP) based on destination IP address, port pairs can detect the destinations under attack in a scalable fashion. It call this the forward path of the attack since it infer DoS activity based on the attack packets going towards a victim. PCF (SYN, FIN, SIP, SP), based on source IP address, port pair can be effective in monitoring based on the reverse path of the attack. This follows the fact that a victim under attack generates several SYN-ACK packets but no corresponding FIN packets. This is because the connection typically does not get established, and even when it does, it does not terminate. Together, the forward and reverse path PCFs can aid in scalable monitoring and characterization of partial completion based DoS activity with an ISP network domain. The forward path PCF however is spoof able, but the reverse path PCF is spoof-resistant.

IV. EXPERIMENTAL RESULT

The purpose of Experimental results is to show synflood attacks in the high speed network. In the High speed network attacker can attack server system by sending more requests as an authorized host. Finally attacker can be denial the service of actual user.

The following are the PCF experimental results,

Source IP	Victim IP	Attack Name	No.of Syns
192.168.1.1	192.168.1.2	Syn-flood	512
192.168.1.4	192.168.1.2	Syn-flood	512
192.168.1.5	192.168.1.2	Syn-flood	512
192.168.1.10	192.168.1.2	Syn-flood	512
192.168.1.12	192.168.1.2	Syn-flood	512
192.168.1.14	192.168.1.2	Syn-flood	512
192.168.1.16	192.168.1.2	Syn-flood	512
192.168.1.1	192.168.1.2	Syn-flood	512
192.168.1.1	192.168.1.2	Syn-flood	512
192.168.1.1	192.168.1.2	Syn-flood	512

Table 1 PCF Results

A. Performance Evaluations

In order to evaluate the proposed method, a prototype of DDoS attack system has been established, as an example, the SYN Flooding, which is the most well-known DDoS attacks, is employed in this method. It used this proposed approach for attacking detection, and the proposed method works as the packet filter at the victim side. For contrast, it also implements the 32 bits strict filtering algorithm of PCF. First of all, it examined the false negative

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

and the false positive, when the number of segmentations varies. The number of clients simulated is kept at a fixed level of 20000.

The results are shown as Figure 2.

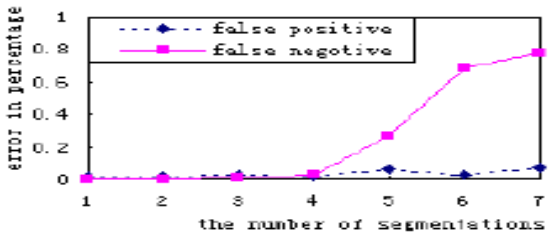

Fig 2 Errors versus number of segmentations

The simulation shows that when the number of segmentations is not greater than 4, both of the errors are quite low (both of them are not greater than 2.5%), and the false negative increases dramatically with the number of segmentations grows. With the growing of the number of segmentations, the proportion of the instances in a segment to the segment's space increases, so the false negative rises in Figure 2.

The false positive keeps stable, because it is related with the number of legitimate clients who never access a server before, which is independent from the number of segmentations.

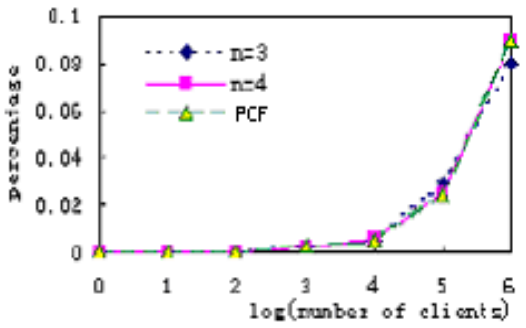

Fig 3 False Positive with IP random spoofing

In the case of random spoofing, Figure 3 and Figure 4 illustrate the relation between error ratio and the number of clients, comparing with PCF algorithm. Therefore, based on the method, When n is equal to 3, the outcome indicates SBF (*Spectral Bloom Filter*) is the same as PCF. With the number of clients growing, the false negative increases relevantly. In fact, the false negative is related closely with the distribution of clients to the server. The false positive increases slowly along with the growing of the number of legitimate clients, because more clients maybe absent in the learning procedure of the algorithm.

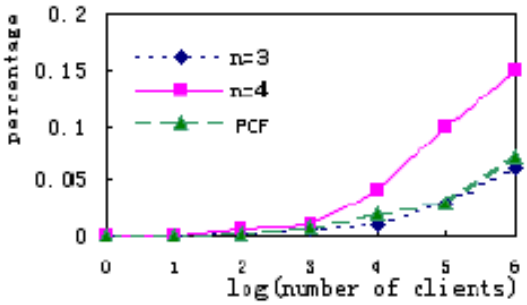

Fig 4 False Negative with IP random spoofing

Then, it contrasts the impact of different methods with subnet spoofing. It deploys the attack packets producing randomly in some subnet of C class. The results are shown as Figure 5 and Figure 6 The figures reveal that the method improves apparently the false negative; yet, the false positive in the method is not as good as PCF. The main reason is that the scoring way influences the legal IP addresses which are identical to subnet spoofed. In the meanwhile, it finds that the efficiency of filtering of the method is connected with time. As the time passes by, the

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

false negative continually decreases, and false positive increases for a while to become steady.

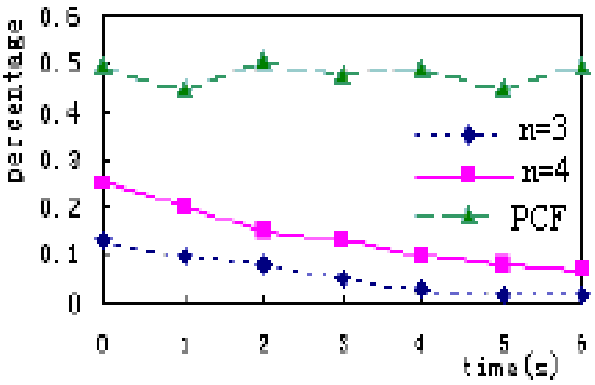

Fig 5 False negative with IP subnet spoofing

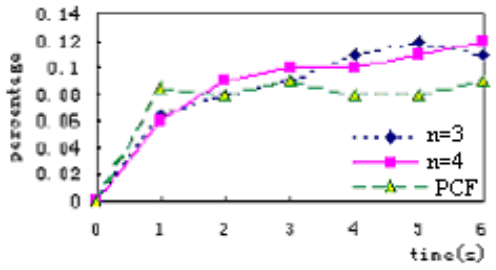

Fig 6 False Positive with IP subnet spoofing

Besides, this method accommodates automatically the attack intensity. For one hop of m, it adds up all the incoming packets. In terms of the normal statistics of bm and current statistics of am, the attack intensity 'w' can be calculated. The proposed approach improves the defense effect and decreases the false for the different hops have various attack intensity.

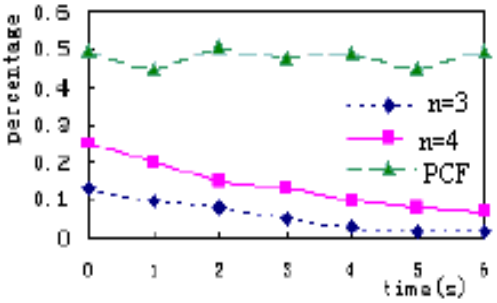

Fig 7 Performance of Proposed methodology

Finally, the scheme is capable of corresponding for the change of the attacks way. It previously analyze that SBF adapts to the attacks of random spoofing and subnet spoofing. In addition, if attackers fake the TTL (*Time To Live*) values to deceive by getting error hops, the method would get a good result as well. It is mostly because attackers are not able to alter the profile of the hop, as set forth, the attack packets would be filtered according to the regularity stated previously.

V.CONCLUSION

This paper explores this possibility in the specific context of DoS attacks and scan attacks. While it have not harped on this point, doing DoS detection in the network also finesses the need for traceback and/or manual intervention, and allows enterprise networks and ISPs to automatically filter out attacks before they enter (or leave) their networks. More fundamental than the specific techniques discussed in this paper is the general question of scalable behavior-based detection of attacks within the network. This project concentrates on many other network functions (forwarding, classification, QoS) have already

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

received considerable attention in the research and product literature, and solutions that scale to 40 Gb/s already exist.

As security functions become more prevalent in the edge first and then the core, it is natural to expect the same attention to be paid to scalable security solutions. More than just introducing the question and suggesting a specific mechanism for some problems, this paper shows that the issues of behavioral aliasing and spoofing are key questions that must be addressed in any scalable solution, even if the only response is to simply ignore the problem. For example, it may be reasonable to ignore spoofing until the bar is raised. These two provide a simple lens to view existing and future work in attack detection, and can perhaps suggest new solutions to an even broader class of attacks. In future plan to conduct on-line, almost everything that it does in life, it is crucial to consider the responses and preventive measures to these threats.

ACKNOWLEDGMENT

I am greatly indebted to my parents and department faculties for their great encouragement and co-operation in all aspects to develop this paper. I wish to thank everyone who helped us directly or indirectly for the successful completion of this paper.

REFERENCES

[1] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies", in Proc. 2nd ACM SIGCOMM Internet Measurement Workshop, 2002, pp. 71–82.

[2] B. H. Bloom, "Space/Time Tradeoffs in Hash Coding with Allowable Errors", Communication ACM, vol. 13, no. 7, pp. 422–426, Jul. 1970.

[3] L. Carter and M. N.Wegman, "Universal Classes of Hash Functions", Computer. System Science. vol. 18, no. 2, pp. 143–154, 1979.

[4] C. Estan and G. Varghese, "New Directions in Traffic Measurement and Accounting", in Proc. ACM SIGCOMM, 2002, pp. 271–282.

[5] C. Gilbert, S. Guha, P. Indyk, S. Muthukrishnan, and M. J. Strauss, "Quicksand: Quick Summary and Analysis of Network Data", DIMACS, Tech. Rep. 2001-43, 2001.

[6] T. M. Gill and M. Poletto, "MULTOPS: A Data-Structure for Bandwidth Attack Detection", in Proc. 10th USENIX Security Symp., 2001, pp. 23–38.

[7] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A Network Security Monitor", in Proc. IEEE Symp. Research in Security and Privacy, 1990, pp. 296–304.

[8] Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks", in Proc. ACM SIGCOMM, 2003,pp. 99–110.

[9] J. Jung, V. Paxson, A. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing", in Proc. IEEE Symp. Security and Privacy, 2004, pp. 211–225.

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-029 PAGE NO: 150-158

[10] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, "Sketch-Based Change Detection: Methods, Evaluation, and Applications", in Proc. 3rd ACM SIGCOMM Internet Measurement Conf., 2003, pp. 234–247

[11] J. Lemon, "Resisting SYN Flooding DoS Attacks with a SYN Cache", in Proc. USENIX BSDCon'2002, pp. 89-98.

[12] K. Levchenko, R. Paturi, and G.Varghese, "On the Difficulty of Scalable Detecting Network Attacks", in Proc. 11th ACM Conf. Computer and Communications Security, 2004, pp. 12–20.

[13] R. J. Larsen and M. L. Marx, "An Introduction to Mathematical Statistics and its Applications", Upper Saddle River, NJ: Prentice-Hall, 2001.

[14] D. Moore, G. Voelker, and S. Savage, "Inferring Internet Denial of Service Activity", in Proc. 10th USENIX Security Symp., Aug. 2001, pp. 9–22.

[15] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-time", Computer Networks, vol. 31, no. 23–24, pp. 2435–2463, 1999.

[16] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial of Service Attacks", Computer Communication. Rev., vol. 31, no. 3, Jul. 2001.

[17] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance Detection in High Bandwidth Environments", in Proc. 2003 DARPA DISCEX III Conf., pp. 229–238.

[18] S. J. Staniford, "Containment of Scanning Worms in Enterprise Networks", Computer Security, 2004, to be published.

[19] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time", in Proc. 11th USENIX Security Symp., Aug. 2002, pp. 149–167.

[20] E. Shenk, "Another New Thought on Dealing with SYN Flooding", 1996

[21] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms", in Proc. ACM Workshop of Rapid Malcode (WORM), 2003, pp. 11–18.

[22] H.Wang, D. Zhang, and K. Shin, "Detecting SYN Flooding Attacks", in Proc. IEEE INFOCOM, 2002, pp. 1530–1539.

[23] H. Wang, D. Zhang, and K. Shin, "SYN-Dog: Sniffing SYN Flooding Sources", in Proc. IEEE Int. Conf. Distributed Computing Systems (ICDCS), 2002, pp. 421–428.

[24]Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate Ddos Flooding Attacks", in Proc. IEEE Symp. Security and Privacy, 2004, pp. 130–143