

A Proactive Test Based Differentiation Technique to Mitigate Low Rate DoS Attacks

Amey Shevtekar and Nirwan Ansari

Advanced Networking Laboratory
Department of Electrical and Computer Engineering
New Jersey Institute of Technology
Newark, NJ 07102, USA

Abstract— Low rate DoS attacks are emerging threats to the TCP traffic, and the VoIP traffic in the Internet. They are hard to detect as they intelligently send attack traffic inside the network to evade current router based congestion control mechanisms. We propose a practical attack model in which botnets that can pose a serious threat to the Internet are considered. Under this model, an attacker can scatter bots across the Internet to launch the low rate DoS attack, thus essentially orchestrating the low rate DoS attack that uses random and continuous IP address spoofing, but with valid legitimate IP addresses. It is difficult to detect and mitigate such an attack. We propose a low rate DoS attack detection algorithm, which relies on the core characteristic of the low rate DoS attack in introducing high rate traffic for short periods, and then uses a proactive test based differentiation technique to filter the attack packets. The proactive test was originally proposed to defend DDoS attacks and low rate DoS attacks which tend to ignore the normal operation of network protocols, but it is tailored here to differentiate the legitimate traffic from the low rate DoS attack traffic instigated by botnets. It leverages on the conformity of legitimate flows, which *obey* the network protocols. It mainly differentiates legitimate connections by checking their responses to the proactive tests which include puzzles for distinguishing botnets from human users. We finally evaluate and demonstrate the performance of the proposed low rate DoS attack detection and mitigation algorithm on the real Internet traces.

Index Terms— Low Rate DoS, RoQ, TCP, and VoIP.

I. INTRODUCTION

Internet has been plagued by a variety of security threats over the past several years. The security menace in the Internet is exacerbating as more professionals are getting into this lucrative business. A recent article in the New York Times [1] describes one such business of selling the software exploits. Attacks are also getting more sophisticated, as the attackers are not merely interested in achieving publicity. The low rate TCP Denial of Service (DoS) attack is one such intelligent attack, which was first explained in [2], followed by a series of related works [3]-[7]. A low rate DoS attack is typically illustrated by a periodic waveform shown in Fig. 1. T is the time period, t is burst period, and R is the burst rate.

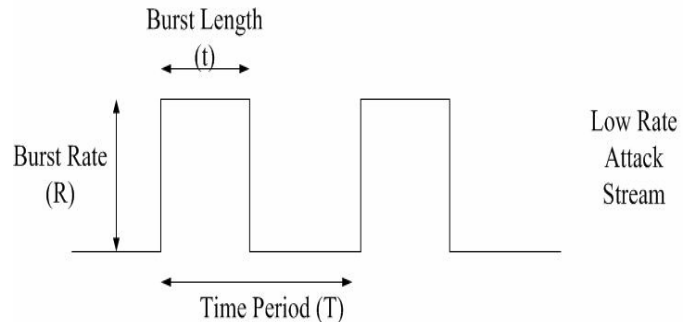


Figure 1: A generic example of low rate DoS attack pattern.

A low rate TCP DoS attack exploits widely implemented minimum RTO [8] property of the TCP protocol. The following characterize the low rate TCP DoS attack:

- It sends periodic bursts of packets at one-second interval.
- The burst rate is equal to or greater than the bottleneck capacity.
- The burst period is tuned to be equal to the round-trip times of the TCP connections; this parameter determines whether the attack will cause DoS to the TCP connections with small or long round trip times.
- The exponential back off algorithm of the TCP's retransmission mechanism is eventually exploited.

In a Reduction of Quality (RoQ) attack [3], the attacker sends high rate short bursts of the attack traffic at random time periods, thereby forcing the adaptive TCP traffic to backoff due to the temporary congestion caused by the attack bursts. In particular, the periodicity is not well defined in a RoQ attack, thus allowing the attacker to keep the average rate of the attack traffic low to evade the regulation of adaptive queue management (AQM) like random early detection (RED) and RED-PD (Preferential Dropping) [9-11]. RED detects congestion at early stages by monitoring the average queue length. RED - PD is another AQM scheme that regulates the long-lived flows, which occupy most of the bandwidth in the Internet. By sending the attack traffic, the RoQ attack introduces transients and restricts the router queue from reaching the steady state. The open knowledge of these stealthy attacks presses for early fixes. For simplicity, from now on, the term "low rate DoS attack" refers to both the low rate TCP DoS and RoQ attacks, unless otherwise stated. This paper proposes a low rate DoS attack detection and mitigation algorithm that uses different types of IP address spoofing to evade other detection systems. In [12], a proactive test based differentiation technique (PTDT) was proposed to mitigate Distributed Denial of Service (DDoS) packet floods. PTDT relies on differentiating legitimate clients, which follow the standard

protocols. It executes proactive tests to each flow over a period of time to test whether it is benign or malicious. Based on the flow rate, it also computes the probability of each flow of being subject to proactive tests. Our approach combines a slightly modified PTDT with the low rate DoS attack detection algorithm to mitigate the threat by the low rate DoS attacks. The low rate DoS attack detection algorithm, on the other hand, relies on the key characteristic of the Internet traffic, that is, 30-40% of the traffic volume in the Internet is contributed by short-lived flows, and the low rate DoS attacks under consideration in this paper generate short-lived flows. Section II describes the problem and presents the motivation behind the proposed system. Section III describes the proposed detection and mitigation system. Section IV discusses various practical implementation alternatives. Section V presents the evaluation results. Section VI discusses related works, followed by our conclusions in Section VII.

II. PROBLEM DESCRIPTION AND MOTIVATION

In this section, we describe the threat imposed by the low rate DoS attacks which use IP address spoofing, and the low rate DoS attack model using botnets. Owing to the open nature of the Internet, IP address spoofing can still evade ingress and egress filtering techniques at many sites [13]. A low rate DoS attack can use IP address spoofing in a variety of ways like random IP address spoofing and continuous IP address spoofing [10]. The use of IP address spoofing most importantly divides the high rate of a single flow during the burst period of the attack among multiple flows with spoofed identities. This way, an attacker can evade detection systems that concentrate on finding anomalous traffic rate. The detection systems that rely on identifying periodicity of the low rate DoS attack in the frequency domain can detect the periodicity, but they fail to filter the attack traffic as it is difficult to know the IP addresses that an attacker will use in the future. This problem is further exacerbated by the use of botnets; a botnet is a network of compromised real hosts across the Internet controlled by a master [14]. As an attacker using botnets has control over thousands of hosts, it can easily use these hosts to launch a low rate DoS attack[†] like a low rate DoS attack that uses random or continuous IP address spoofing. Now, with the use of botnets, the IP addresses (of compromised hosts) are not spoofed and so these packets cannot be filtered by spoofing prevention techniques. In fact, these attack packets are similar to the HTTP flows. Thus, the objective is to detect a low rate DoS attack that can deploy different IP address spoofing techniques, and then filter the attack traffic. PTDT was demonstrated to defend effectively against DDoS attacks which do not conform to network protocols; it was originally proposed as an end-host defense mechanism. Note that in a low rate DoS attack an attacker usually targets the network element which is a router. The low rate DoS attacks launched by using botnets can behave like normal connections and can go undetected by PTDT which can, however, be used to regulate and limit both the legitimate and attack traffic. These attacks are similar to the low rate DoS attacks that use continuous IP address spoofing described in

[†] Technically speaking, we would coin such an attack launched through botnets as a low rate Distributed Denial of Service (DDoS) attack, though the aggregated traffic received by the victim looks like a low rate DoS attack with IP address spoofing.

[10]. The possibility of an attacker using UDP packets to launch a low rate DoS attack always exists, and PTDT does not provide a provision to mitigate such threat from UDP packets, as it only rate limits UDP traffic. An attacker can use aggregate UDP traffic coming from many networks to launch a low rate DoS attack. In consideration of these issues associated with PTDT, we here propose to enhance PTDT by using the technique described in the next section.

III. DETECTION AND MITIGATION SYSTEM

This section describes the detection and mitigation system in detail. Fig. 2 shows the block diagram of the system.

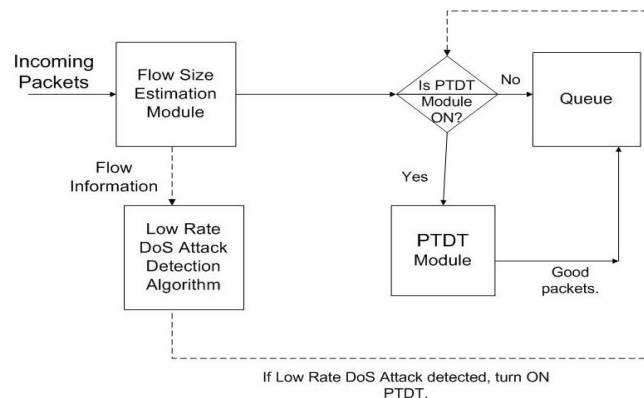


Figure 2: The detection system block diagram.

The detection and mitigation system will operate at routers primarily at the edges of a network, so that all the traffic entering the network can be examined by the system. The low rate DoS attack detection algorithm requires the per flow information of the traffic passing through an edge router. A flow or flow id is defined as a 4-tuple of the source IP address, the source port, the destination IP address, and the destination IP port. The flow size estimation module will provide the necessary per-flow information of the network traffic passing through the router to the low rate DoS attack detection algorithm. Incoming packets are enqueued in the outgoing queue of the router if the PTDT module is not ON. PTDT is activated if the low rate DoS attack detection algorithm detects a low rate DoS attack. Once activated, PTDT allows legitimate traffic to pass through the router, but blocks the attack traffic. We now describe the detailed functioning of the two important modules of the system: the low rate DoS attack detection algorithm and the PTDT module. The low rate DoS attack detection algorithm is based on an important premise about Internet traffic that the majority of short-lived flows occupy only about 30 to 40% volume of the total traffic, and the minority of long-lived flows occupy the rest of 60 to 70% volume of the total traffic [15]-[16]. The low rate DoS attack using IP address spoofing consists of many short-lived flows whose aggregate traffic rate for a short period of time is extremely high, thus violating the characteristics of the normal Internet traffic stated above. The attacker can use different forms of IP address spoofing like random IP address and continuous IP address spoofing, but it will not disrupt functions of our proposed algorithm. The flow information for each flow consists of *the packet count (k)*, *the packet size*, *the createdtime*, and *the lastaccessed time*.

A. Low Rate DoS Attack Detection Algorithm

Fig. 3 shows the low rate DoS attack detection algorithm. In the figure, the $\text{totbytecnt}/\text{flow}$ represents the number of bytes of traffic sent in each flow till lastaccessedtime , the SUM variable represents the total number of bytes of all expired flows, and the THRESHOLD variable will be described in detail later. The algorithm computes the sum of $\text{totbytecnt}/\text{flow}$ of all the flows that are expired in a short period of one second and checks whether the sum is greater than a threshold. If the sum is greater than the threshold, the low rate DoS attack is considered detected. Selecting the threshold is important in detecting a low rate DoS attack, which can keep the burst rate low. The following thresholds are proposed:

$$1) \text{THRESHOLD} \geq C + B$$

$$2) C/2 + B \leq \text{THRESHOLD} < C + B$$

$$3) C/4 + B \leq \text{THRESHOLD} < C/2 + B$$

C is the capacity of the link, and B is the buffer size of the router. As defined in [10] for the random IP address spoofing case, k is one. For the continuous IP address spoofing case, k can be anything; we choose the maximum possible to be less than C/P where P is the minimum packet size. Thus, all the attack flows will be considered by the detection algorithm, and the SUM value will exceed one of the proposed thresholds under the low rate DoS attack. The burst period of a low rate DoS attack in the literature is found to be less than one second, and so we consider one second in the detection algorithm. We still consider higher burst periods in the results, but we argue that the attack is no longer a low rate DoS attack with higher burst period. A higher burst period low rate DoS attack can be easily detected by RED-PD [9]. Thus, our algorithm can successfully detect a low rate DoS attack that uses IP address spoofing. A low rate DoS attack not using IP address spoofing can be easily detected by our previous proposals as well as by the PTDT scheme.

- 1) For all the expired flows with k packets in each flow in the persistent storage, C as the link capacity, and P as the minimum packet size, If $\{0 < k < C/P, \& \text{createdtime} > \text{current time} - 1s, \& \text{lastaccessedtime} < \text{current time}\}$,
 $\text{SUM} = \text{SUM} + \text{Totbytecnt}/\text{flow}$.
- 2) If $\text{SUM} > \text{THRESHOLD}$, Low Rate DoS Attack Detected.

B. Proactive Test Based Differentiation Technique Module

We now describe the role of PTDT in Fig. 2. After the low rate DoS attack is detected, PTDT is activated. PTDT also leverages on the fact that TCP traffic is dominant in the Internet [15]. Fig. 4 shows the flowchart of the PTDT module. On arrival of a SYN packet, the PTDT module knows it belongs to a new flow

and sends a puzzle to the source of the packet. The technique of using visual puzzles or CAPTCHA's in our system is similar to several proposals like [16] used to distinguish humans from the attack machines. The user is admitted by the system after having given the correct answer of the puzzle. This way, PTDT can stop an attacker who can send SYN packets to launch a low rate DoS attack, and still allow the legitimate users to access the network. The technique of introducing a puzzle will also confirm that a human user, rather than an automated attack machine, is initiating the communications, and so the flow after having been admitted to the system will follow the standard protocol. The remaining steps in the flowchart for an old flow will typically verify the behavior of the flow over a period of time before being classified as benign.

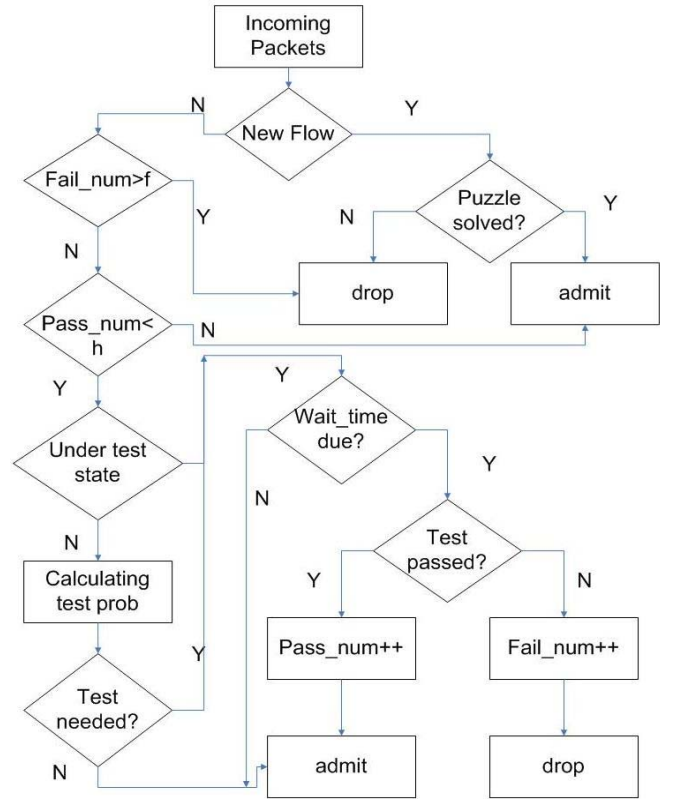


Figure 4: The PTDT module's flowchart.

We now explain the functions of the remaining blocks of the flowchart, which are similar to the original proposal in [12]. The two counters fail_num and pass_num achieve a balance between the conservative and aggressive approach against individual flows. A flow is allowed to prove its innocence by failing no more than a certain number of tests maintained by the fail_num counter; otherwise, it is dropped. Similarly, a good flow after having passed a certain number of tests maintained by the pass_num counter is trusted as innocent, and is not required to take further tests. Then, the PTDT module checks the current state of the flow; for a flow under test, its current rate should not exceed its previous rate. This can be achieved by dropping a single data packet, so that the legitimate TCP flow will reduce its sending rate. The attack flows will not reduce their rates, and thus can be distinguished. If a flow passes this test, its pass_num value is increased by one, and vice versa. The default values of various thresholds like certain

numbers of tests that can be failed, though are applications specific, can be kept the same as in the original proposal [12]. Another advantage of using these proactive tests is to detect intelligent attackers who can overcome CAPTCHA's by using intelligent image recognition softwares [17].

Thus, by employing the PTDT module, the legitimate TCP traffic can still access the network in the presence of the low rate DoS attack. The PTDT module can also monitor the rates of some common UDP applications like VoIP and Video traffic, and if the rates conform to the standard application rates, then these flows can also be admitted into the network.

IV. PRACTICAL IMPLEMENTATION

To realize the proposed detection system at high speeds is the key to our proposal. As network security is becoming important, advances in hardware technologies are critical to support complex operations at high speeds. Our proposal mainly needs per flow information for the low rate DoS attack detection algorithm, and per flow processing for the PTDT module. There have been many proposals to estimate per flow information like [18] [19]. In [19], the authors proposed to tune the sampling frequency of Internet traffic such that an accurate estimate of both long-lived and short-lived flows can be made. They alleviate the common drawback of the uniform sampling, which just provides the information of the long-lived flows in the Internet, i.e., the dominant traffic at both the byte-level and packet-level. There have also been proposals such as CYSEP [20], which perform complex network security operations like encryption/decryption, and intrusion detection at gigabit speeds. Such architectures can be easily modified to implement the PTDT module. Currently, our entire detection system can work at network edges where such tasks can be performed by using a combination of different hardware implementations. It can be typically suitable for medium and small-sized networks, which host web servers.

V. TRACE EVALUATION

We decide to evaluate the low rate DoS attack detection algorithm using the real Internet traces provided by CAIDA [21]. The OC48 traces were recorded during August 2002 and April 2003. The flow information was obtained from the traces using the coralreef software [22]. The low rate DoS attack detection algorithm was then executed on the flow information. The results indicating the nature of the *SUM* variable are shown in Figs. 5 and 6. In Fig. 6, the burst period of the attack is two second and in Fig. 5 the burst period is 1 second to verify the validity of the proposed thresholds to detect the low rate DoS attack. The low rate DoS attack with burst periods greater than one second can be easily mitigated by several AQM schemes like RED-PD. For the OC48 ($C = 2.5\text{Gbps}$) speed, $C/2$ is 1.25Gbps , and $C/4$ is 625Mbps . We can observe from Figs. 5 and 6 that the sum variable is around 5 to 15Mbps which is less than both $C/2$ and $C/4$. Thus, the proposed low rate DoS attack detection algorithm can detect a low rate DoS attack which employs IP address spoofing. We did preliminary investigation to validate the proposed detection and mitigation system by using the ns2 simulator. We used a well-known dumbbell topology network with a single bottleneck link of 10Mbps. The access links were 100Mbps with random delays on each link to

simulate varying roundtrip-time for each connection. We used ten FTP flows and one attack flow in the network. The FTP traffic used TCP sack with a window size of 43 packets, segment size 1460bytes, and the other parameters were default values. The attack flow was a UDP constant bit rate traffic with the burst period of 0.4seconds, the burst rate 15Mbps, and the time period one second. The attack traffic was using random IP address spoofing. In the ns2 simulations, we could not serve the puzzles before the connections were established, and so we assumed that the FTP connections had solved the puzzles. We plan to implement this functionality in the future in the Linux prototype of the detection system. We imposed the proactive tests on these connections to verify their legitimacy. Fig. 7 shows the throughput of the legitimate FTP flows under different scenarios. Note that using the detection and mitigation system the throughput is restored back. Fig. 8 shows the sending rate of a legitimate flow with and without the proactive test, respectively. Typically, the legitimate flow that uses a stock TCP should reduce its rate after its packet is dropped. An attack flow will not obey the stock protocol which was shown in the original PTDT [12]; this was reinforced by our simulations. Our contribution here has been augmenting the PTDT approach with the low rate DoS attack detection algorithm to mitigate the low rate DoS attacks orchestrated through botnets.

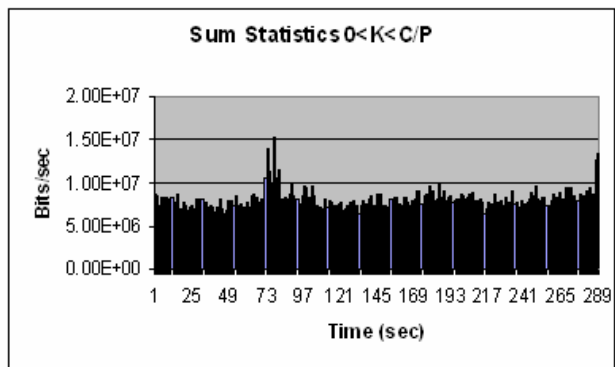


Figure 5: Sum statistics for every second.

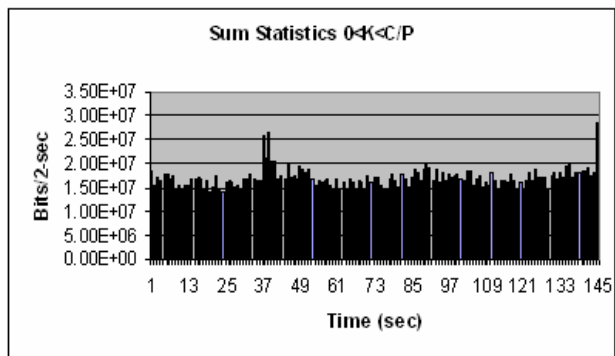


Figure 6: Sum statistics for every two seconds.

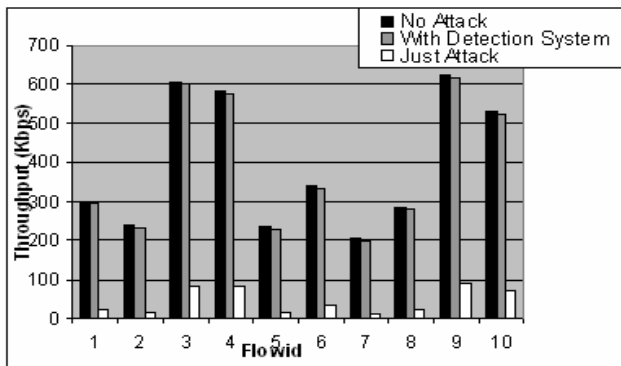


Figure 7: Throughput of the legitimate FTP flows.

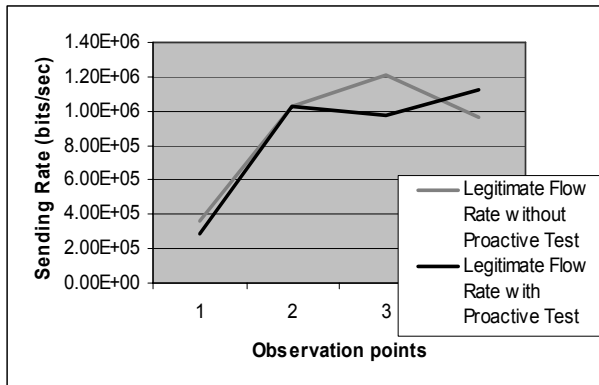


Figure 8: A proactive test demonstration on a legitimate FTP flow.

VI. RELATED WORKS

The end host based defense strategy against the low rate TCP DoS attack is randomization of the minimum RTO [2] [23], but it cannot defend against an RoQ attack as it exploits the network element, and not the end host's vulnerability. A few router based defense systems have been proposed to mitigate the low rate DoS attacks. In [24], a modified AQM scheme is proposed to penalize bursty flows, but it lacks accurate identification of the attack flow, and can penalize legitimate bursty short-lived TCP flows. It does not consider the spoofing problem of an RoQ attack. The RoQ attacks can use source and destination IP address spoofing, and they do not have well-defined periodicity, and so schemes like [25]-[27] may not filter these attack packets *accurately*. The scheme proposed in [28] may not be scalable, and can be deceived by the IP address spoofing, although it can detect any periodic pattern in the flows. The wavelet based approach [5] relies on detecting variability of the incoming traffic rate and outgoing acknowledgments for detecting the low rate TCP DoS attack, but this approach cannot mitigate the RoQ attack which does not try to completely shutdown the competing flows. The extent of the IP spoofing problem in the Internet today is demonstrated in [13], and thus the spoofing issue cannot be ignored. Sarat and Terzis [29] suggested to decrease the buffer size by means of a mathematical analysis based on [30] to expose the attack flow to the AQM schemes like RED-PD, but unfortunately it cannot mitigate the RoQ attack, in which the average rate is lower than the low rate TCP DoS attack.

VII. CONCLUSION AND FUTURE WORK

We have proposed a detection system to detect new breed of DoS attacks in the Internet known as low rate DoS attacks. Our detection system was shown to detect and mitigate these attacks even if an attacker uses IP address spoofing. We have evaluated the feasibility of the proposed low rate DoS attack algorithm on real Internet traces. As part of the future work, we are planning to test the effectiveness of the proposed detection system by using the NSF Deterlab test bed.

REFERENCES

- [1] A Lively Market, Legal and Not, for Software Bugs [online]. Available: <http://www.nytimes.com/2007/01/30/technology/30bugs.html?ex=1327813200&en=99b346611df0a278&ei=5088&partner=rssnyt&emc=rss>
- [2] A. Kuzmanovic and E. Knightly, "Low-Rate TCP -Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)," Proceedings of ACM SIGCOMM 2003, Karlsruhe, Germany, August 2003, pp. 75-86.
- [3] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources," Proceedings of IEEE ICNP 2004, Berlin, Germany, October 2004, pp. 184-195.
- [4] S. Ebrahimi-Taghizadeh, A. Helmy, and S. Gupta, "TCP vs. TCP: a Systematic Study of Adverse Impact of Short-lived TCP Flows on Long-lived TCP Flows," Proceedings of IEEE INFOCOM 2005, Miami, USA, March 2005, pp.926-937.
- [5] X. Luo and R. K. C. Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense," Proceedings of NDSS 2005, San Diego, USA, February 2005.
- [6] A. Shevtekar and N. Ansari, "Do Low Rate DoS Attacks Affect QoS Sensitive VoIP Traffic?," Proceedings of IEEE ICC 2006, Istanbul, Turkey, June 2006, pp. 2153-2158.
- [7] R. Chertov, S. Fahmy, and N. Shroff, "Emulation versus Simulation: A case study of TCP-Targeted Denial of Service Attacks," Proceedings of Tridentcom 2006, Barcelona, Spain, March 2006, pp. 316-325.
- [8] V. Paxson and M. Allman, "Computing TCP's Retransmission Timer," RFC 2988, November 2000.
- [9] R. Mahajan, S. Floyd, and D. Wetherall, "Controlling High-Bandwidth Flows at the Congested Router," Proceedings of IEEE ICNP 2001, Riverside, California, November 2001, pp.192-201.
- [10] Y. Xu and R. Guerin, "On the Robustness of Router-based Denial-of-Service (DoS) Defense Systems", ACM Computer Communications Review, July. 2005, pp. 47-60.
- [11] S. Floyd and V. Jacobson, "Random Early Detection gateways for Congestion Avoidance," IEEE/ACM Transactions on Networking, Vol.1, No. 4, August 1993, pp. 397-413
- [12] Z.Gao and N. Ansari, "Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests," IEEE Communication Letters, Vol. 10, No. 11, November 2006, pp.793-795.
- [13] R. Beverly and S. Bauer, "The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet," Proceedings of USENIX SRUTI, Cambridge, MA, July 2005, pp. 53-59.
- [14] D. Dagon, Z. Zhou, W. Lee, "Modeling Botnet Propagation Using Time Zones," Proceedings of NDSS 2006, San Diego, USA, February 2006.
- [15] M. Fomenkov, K. Keys, D. Moore, and K. Claffy, " Longitudinal study of Internet traffic from 1998-2003," Proceedings of the Winter International Symposium on Information and Communication Technologies, Cancun, Mexico, January 2004, pp.1-6.
- [16] S. Kandula, D. Katabi, M. Jacob, and M. Berger, "Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds," Proceedings of USENIX NSDI, Boston, MA, May 2005.

- [17] G. Mori and J. Malik, "Recognizing Objects in Adversarial Clutter – Breaking a Visual CAPTCHA," Proceedings of IEEE CVPR 2003, Madison, WI, June 2003, pp. 134-141.
- [18] A. Kumar, J. Xu, L. Li, and J. Wang, "Space-Code Bloom Filter For Efficient Per-Flow Traffic Measurement," Proceedings of IEEE INFOCOM 2004, Hong Kong, March 2004, pp.1762-1773.
- [19] A. Kumar and J. Xu, "Sketch Guided Sampling - - Using Online Estimates of Flow Size for Adaptive Data Collection," Proceedings of IEEE INFOCOM 2006, Barcelona, Spain, April 2006.
- [20] H. J. Chao, R. Karri, and W. Lau, "CYSEP: a cyber-security processor for 10Gbps networks and beyond," Proceedings of IEEE MILCOM 2004, Monterey, CA, USA, Oct-Nov 2004, pp.926-937.
- [21] The OC48 Data [online]. Available:
<http://www.caida.org/data/passive/index.xml#oc48>
- [22] The Coral Reef Software [online]. Available:
<http://www.caida.org/tools/measurement/coralreef/>
- [23] G. Yang, M. Gerla and M. Y. Sanadidi, "Randomization: Defense against Low-Rate TCP-targeted Denial-of-Service Attacks," proceedings IEEE Symposium on Computers and Communications, Alexandria, Egypt June - July 2004, pp.345-350.
- [24] Y. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: Halting Anomaly with Weighted ChoKing to Rescue Well-Behaved TCP Sessions from Shrew DoS Attacks," Technical Report, USC Internet and Grid Computing Lab (TR 2005-5), February 2005.
- [25] H. Sun, J. C. S. Lui and D. K. Y. Yau, "Defending Against Low-rate TCP Attack: Dynamic Detection and Protection," Proceedings of IEEE Conference on Network Protocols (ICNP 2004), Berlin, Germany, October 2004, pp. 196-205.
- [26] K. Chandrayana and S. Kalyanaraman, "Uncooperative Congestion Control," Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems, New York, NY, June 2004, pp. 258-269
- [27] Y. Chen, K. Hwang, and Y. Kwok, "Collaborative Defense against Periodic Shrew DDoS Attacks in Frequency Domain," Technical Report, USC Internet and Grid Computing Lab (TR 2005-11), May 2005.
- [28] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communication Letters, Vol. 9, No. 4, April 2005, pp.363-365.
- [29] S. Sarat and A. Terzis, "On the Effect of Router Buffer Sizes on Low-Rate Denial of Service Attacks," Proceedings of IEEE ICCCN 05, San Diego, California, October 2005, pp..281-286.
- [30] G. Appenzeller, I. Keslassy, and N. McKeown, "Sizing Router Buffers," Proceedings of ACM SIGCOMM 2004, Portland, Oregon, August-September 2004, pp.281-292.