# NeuroNet: Towards an Intelligent Internet Infrastructure

Yu Chen
Dept. of Electrical and Computer Engineering
State University of New York – Binghamton
Binghamton, NY 13902, USA
Email: ychen@binghamton.edu

*Abstract* - **Malicious attacks against Internet infrastructure are one of the most damaging threats to modern society. Due to the inter-dependence between networks, attackers can paralyze or isolate the victim network without attacking it directly. Such kind of attacks could be a main weapon of cyber war in the foreseeable future, potentially detrimental to many national interests. Today's network security solutions designed under the end-to-end paradigm cannot address the malicious activities inside the core network effectively. This paper proposed to strengthen the network infrastructure by developing *NeuroNet*, a network neural system that plays a critical role similar to the role of the nervous system in the human body. A distributed information collection and processing mechanism is proposed, which coordinates the activities of core network devices, monitor for anomalies, construct alerts, and initiate countermeasures. Through intensive experiment of a distributed detection scheme against the low-rate TCP-targeted DDoS attacks, the effectiveness of the NeuroNet architecture is verified.**

***Keywords:*** *Network Infrastructure Security, Neural System, Low-Rate TCP-Targeted DDoS Attacks, Shrew Attacks.*

## I. INTRODUCTION

Information technology has revolutionized almost every facet of our lives. Government, commercial, and educational organizations depend on computers and the Internet to such an extent that day-to-day operations are significantly hindered when the networks are "down" [16]. Today's "hackers" aim at attacks against the fundamental Internet infrastructure [8], an activity even more damaging than obtaining unauthorized network accesses or stealing private information. Attacks including DDoS (*Distributed Denial-of-Services*) attacks [18] and Internet worms [29], both of which can lead to enormous destruction, as different infrastructure components of the Internet have implicit trust relationships with each other. Recent research pointed out that infrastructure attacks will be the major weapon of cyber wars in the predictable near future [2]. Therefore, a robust and intelligent infrastructure is vital to protect national interests. Although there are reported works that consider fighting against infrastructure-oriented attacks [3, 13, 23, 29], not one of them can be considered as a comprehensive solution for two reasons.

First of all, the network infrastructure does not provide enough resources to accommodate adequate security functions. When the Internet was created, the end-to-end principle was adopted based on the assumption that the end users, who were mostly engineers and researchers, were willing to behave cooperatively and trustfully to each other. Therefore, security was not considered important to the designers. The Internet protocols and architecture were designed from the perspective of functionalities. In order to support emerging applications, the intermediate network was designed as a purely transparent carrier optimized for *best-effort* packet forwarding. However, today, the Internet is operated in an untrustworthy world and with much more demanding applications [5, 19]. While the end users cannot be trusted, a more reliable and trustworthy network requires a robust and intelligent core network. In addition, end-host based schemes are ineffective to some new attacks patterns [9, 20]. It is mandatory to detect and counteract inside the core networks.

Secondly, infrastructure security is fundamentally different from and even clashes with information security. Most reported information security solutions focus on confidentiality, integrity, and authentication. However, protection of network infrastructure is based mainly on the availability, reliability, and stability of the network services. It is different from information protection that can be achieved by stronger encryption algorithms, stricter authentication policies, or more complex digital signatures. For instance, a strongly encrypted server could be put out of work by a flooding DDoS attack that simply exhausts certain critical resources, i.e. bandwidth. The attacker does not even need to understand the fundamentals of encryption.

The central motivation of our work reported here is the compelling need to secure network infrastructure. For this purpose, technologies need to be integrated into the infrastructure and this needs to be done in a coordinated manner across the core network fabric. One concern is that putting more functions inside the network jeopardizes the generality and flexibility, as well as historic patterns, of innovation under end-to-end paradigms. However, in fact, beside the security concerns, more demanding applications and diversified user groups have been pushing the Internet architecture away from the end-to-end paradigm. A new principle we should follow is that the implementation of functions invisible to the end-to-end application should be "in" the network in general [5].

This paper proposed to reinforce Internet infrastructure by developing *NeuroNet*, a network neural system that plays a critical role similar to the role of the nervous system in the human body. The NeuroNet is a distributed security system that is capable of monitoring the traffic fluctuation adaptively, detecting the traffic anomalies, and triggering countermeasures in the core network. To verify the effectiveness of the NeuroNet architecture, we also proposed a distributed detection mechanism against the low-rate TCP-targeted DDoS attacks, which is one type of stealthy, hard-to-detect infrastructure-oriented attack [12]. It is also known as shrew attacks [20], periodic pulsing attacks [22] in literatures. For convenience, we will use the term shrew attacks in sequel.

The rest of the paper is organized as follows: Section 2 gives a brief review of related works. Section 3 introduces the rationale and the architecture of our NeuroNet. As a case study, section 4 presents the experiment results of shrew DDoS attack detection on top of the NeuroNet. Section 5 concludes this paper and discusses our on-going works.

## II. Related Work

Network security continues to be a hot topic in the research community. This section presents a brief survey of reported efforts in the areas of new network architecture design and shrew DDoS attack defense schemes.

The Internet has evolved greatly in past decades. Researchers have recognized that new network architecture is needed to adapt to changes in applications and user groups [19]. For instance, as the majority of today's Internet application is data retrieval and service access, data-oriented network architectures have been proposed on name-based routing to improve the data/service access on the Internet [14, 19]. Active network has been suggested to make the Internet infrastructure more adaptive and smart [25, 28], and there was reported countermeasure against DDoS attacks using active networks [26]. Particularly, due to the lack of security functions some researchers are considering a clean-slate design for the next-generation secure Internet [4]. However, since the current Internet cannot be completely replaced by a new network infrastructure in the foreseeable near future, we still need to strengthen the current network infrastructure.

Kuzmanovic and Knightly [20] studied the rationale of the shrew attacks and identified the critical parameters that affect the TCP flows. They indicated the limitation of existing DDoS defense mechanisms against shrew attacks. However, they did not develop specific countermeasures to counter the low-rate shrew attacks. Kwok, et al [21] proposed a HAWK algorithm by judiciously identifying malicious shrew packet flows. However, the HAWK scheme is only effective to single source attacks. Sun *et al.* [27] suggested detecting shrew attacks by matching pattern with prestored attack signature. However, their method cannot distinguish malicious from legitimate flows. Legitimate flows thus suffer in the rate-limit packet filtering process. Luo and Chang [22] have studied shrew attacks using a wavelet approach. Unfortunately, they did not report the detection accuracy achieved. Since the wavelet detection outcomes are largely dependent on the choice of detection parameters, it is difficult to find optimal parameters that are sensitive to detect low-rate distributed attacks while maintaining a low false positive alarm rate.

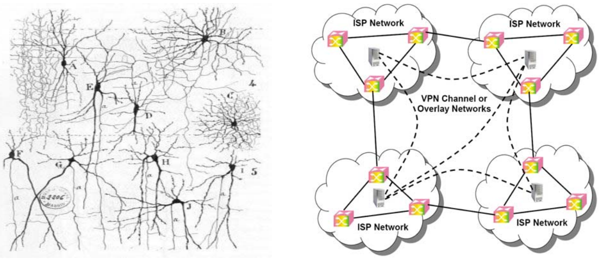
## III. NeuroNet: Rationale and Architecture

The NeuroNet is a nervous system for the Internet infrastructure. Essentially, it is a distributed information collection and processing mechanism, which coordinates the activities of core network devices, monitors the anomalies, constructs senses or alert, and initiates countermeasures.

Facing the fast growing application and attacking patterns, a more sophisticated and intelligent network infrastructure is desired. A smart Internet architecture is required that is capable of learning the evolution of traffic patterns adaptively and generating new rules and signatures dynamically without human interferences. Adopting artificial neural networks (ANNs) or other artificial techniques in network security is not a new idea [7, 11, 15]. However, built according to a simplified model of a neuron, the ANNs neither really possess properties of the neural network in neurobiology nor reflect the Internet topology or architecture. In fact, the physical architecture topology of the Internet is more similar to the biological nervous system as shown in Fig. 1(a).

Based on this observation, we propose to explore the approach to enable network infrastructure to work coordinately as the human body with a nervous system: which is a real distributed sensing and information processing system. The architecture of the proposed NeuroNet is shown in Fig. 1(b). NeuroNet allows multiple ISP networks or *autonomous systems* (AS) to work collaboratively. Each router works as a neuron, and there is a server in each network that acts as the brain.

Adapting such a model, the basic idea is that NeuroNet plays two roles as neurons do in biological systems: sensing and control. As the brain of the system, the servers located in each ISP network have two responsibilities. Aside from performing complex computing and data analysis work, the servers are also in charge of issuing commands to executors. Similarly, on one hand, routers function as distributed sensors in the procedure of information collection when monitoring the network status. On the other hand, routers also function as distributed executors to make the whole



(a). Biologically based Neural Networks [5]

(b). Proposed NeuroNet Architecture

Figure 1. Illustration of NeuroNet Architecture

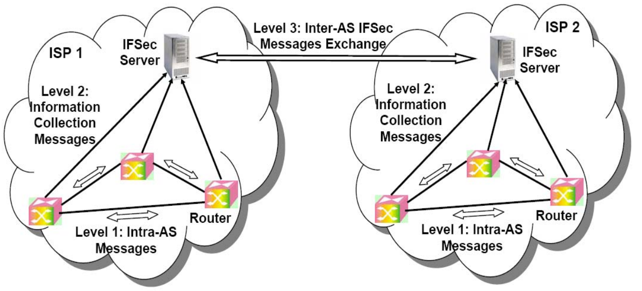

ISP 1
IFSec Server
Level 3: Inter-AS IFSec Messages Exchange
ISP 2
IFSec Server
Level 2: Information Collection Messages
Level 2: Information Collection Messages
Router
Router
Level 1: Intra-AS Messages
Level 1: Intra-AS Messages

Figure 2. Three levels of communication in using the IFSec between two servers in two ASes.

network act correspondently when they are asked to trigger countermeasures against certain on-going attacks.

To provide a secure communication platform for the nervous system, we proposed IFSec, a novel infrastructure security protocol. This protocol is allocated at the network layer (layer 3) and specifies the data format and encryption mechanism for secure information exchange among neurons and between neurons and the server (brain) in the domain.

The IFSec is not an IP multicast protocol in the traditional sense because of two reasons. In the vertical direction of network layer model, it sits on top of the IP layer and it is transparent to transport layer protocols. From the perspective of deployment, IFSec holds its responsibility as limited in layer 3 devices of a physical network. No end hosts or servers are involved. As illustrated by Figure 2, the protocol possesses a three level communication model.

The lowest level enables routers in the same domain to share information for status monitoring. The second level is the communication between the routers and server in each domain. Routers periodically report local traffic detection results to the domain server. At the inter-domain level, the server communicates with its peers located in other ASes. However, due to privacy and security concerns, ISPs are often reluctant to reveal inside information to competitors. Hence, aside from managing the information exchange, servers are also in charge of trust negotiation.

## IV. COLLABORATIVE SHREW DDOS ATTACK DETECTION

To verify the effectiveness of the NeuroNet, we developed a collaborative shrew DDoS attack detection mechanism on top of IFSec and studied its performance through intensive experiment.

### *A. Overview of Shrew DDoS Attacks*

The earliest case of shrew DDoS attack was reported in 2001 [12]. But it had not been studied thoroughly until Kuzmanovic and Knight [20] identified and characterized such type of attacks in 2003. They studied the rationale of the shrew attack and analyzed the critical parameters that affect the efficiency on TCP flows. A single source shrew attack could be modeled as a square waveform packet stream with an attack period *T*, length of the burst *L*, and the burst rate *R*. The period *T* is calculated by the estimated TCP RTO timer implementations at legitimate sources. The shrew attacks take advantage of the RTO recovery feature by adjusting the attack period to match with the RTO period. Attacking pulse streams occupy the link bandwidth periodically and make legitimate TCP flows always "see" busy links when they go through the RTO process. In worst cases, the shrew attack can bring down the throughput of legitimate TCP flows lower than 10% of the throughput in normal situation.

### *B. Collaborative Shrew Attack Detection Scheme*

Our previous research [9] discovered that the *Power Spectral Density* (PSD) of traffic with shrew streams embedded has much higher energy statistically located in low frequency band (< 20 Hz) while comparing to traffic flows without such low-rate attack streams. Based on observing the normalized cumulative PSD at 20 Hz, each router detects whether there is shrew stream(s) embedded in flows going through. It is non-trivial for attacker to hide the statistic property in frequency domain,

However, there is a tradeoff because the detection accuracy is related to the false positive rate. If we want to avoid high false positive rate by choosing a higher alert threshold, the detection accuracy is sacrificed. A lower threshold brings a higher detection rate but also a higher false positive rate. With the support of IFSec protocol, we proposed a collaborative distributed detection scheme that solved this dilemma.

The rationale of our algorithm is that routers may detect anomalies more effectively if a wider vision of traffic pattern is available. Two thresholds are adopted. The *local threshold* $\gamma_L$ is set to a higher value to obtain lower false positive rate, while the *cooperative threshold* $\gamma_C$ is set to lower value to make up the sacrificed detection accuracy.

Figure 3 illustrates the operation of the algorithm. Distributed attack is launched from zombies located widely on the Internet and multiple shrew streams are approaching to victim connected to a router in the AS. Due to the random distribution nature of shrew streams, their strengths are not even to each edge router. This mechanism gives routers a clue to check whether they are in the attacking range.

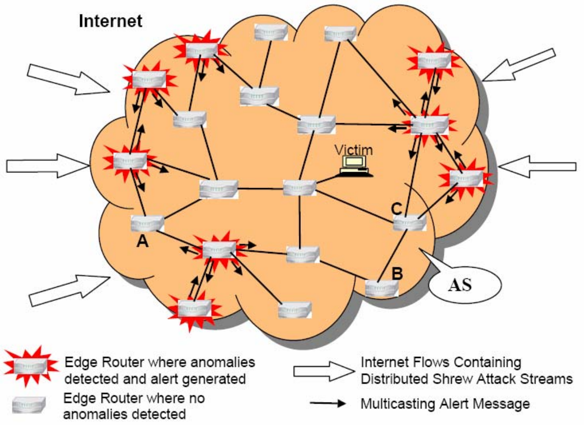

Internet
Victim
A
B
C
AS
Edge Router where anomalies detected and alert generated
Edge Router where no anomalies detected
Internet Flows Containing Distributed Shrew Attack Streams
Multicasting Alert Message

Figure 3. Principle of distributed detection algorithm against shrew attack streams

Edge routers who detected the normalized cumulative PSD *L(x)* > $\gamma_L$ would multicast an alert and start the shrew filtering mechanism [9] to identify malicious flows and cut off them completely. However, as shown in Fig. 3, when *L(x)* < $\gamma_L$ happens at node A, alerts from neighbors tell that there is attack going on. Additionally, the alerts from peers let node A realize that it is located inside the attacking area. Then node A checks the second threshold to see whether *L(x)* > $\gamma_c$, if that is true, node A starts the local shrew filtering mechanism.

In contrast, node B, who also received alerts, will not trigger further action. As all its immediate neighbors have not raised alert, the received alert just leads to a conclusion that there are suspicious flows coming into the AS, but node B is not in the attacked area. However, the location and distribution of the received alerts would tell nodes C that it is at the edge of attacking area. If there exists *L(x)* > $\gamma_c$, then node C starts the local shrew filtering mechanism.

### *C. Experiment Result*

To verify the effectiveness of the NeuroNet architecture supported distributed detection mechanism against shrew DDoS attacks, we carried out intensive experiments using the NS-2 simulator [24], a widely recognized packet-level discrete event simulator. Our NS-2 simulations were carried out with many topologies generated by the GT- ITM toolkit from Georgia Tech. [17]. We apply each topology for at least 1000 experiments with shrew attack datasets similar to those used by Chertov et al. [10], Kuzmanovic and Knightly [20], and Sun et al. [27].

The simulation assumed default network parameters in link capacity of 2 Mb/s. The RTT of TCP flows are uniformly distributed over 60 ms to 240 ms. Since TCP-Tahoe, TCP-Reno and others present similar vulnerability under shrew attacks [20], we adopt the TCP-Reno standards in our experiments.

We generate shrew attack flows with a period *T* between 0.5 and 3.0 s, the burst period *L* is in the range (30–90 ms). For single-source attacks, the burse rate *R* varies in 0.5–2 MB/s. In distributed attacks from multiple sources, *R* varies in 0.1–2 MB/s. The background traffic without shrew attacks are generated from our analysis of Abilene-I trace dataset released by the PMA Project [1]. This dataset is the first public OC48c backbone trace.

The *anomaly detection rate* $R_d$ is the ratio of detected attack streams over the total number of such traffic streams processed. The *false positive rate* $R_{fp}$ is the ratio of normal traffic flows being wrongly detected as having shrew attacks over total number of legitimate traffic streams. The ROC (*Receiver Operating Characteristics*) curves shown in Fig. 4 present the improvement in performance of cooperative detection on top of the NeuroNet.

The lower curve shows the detection performance when each router works independently. We have to tolerant a false positive rate of 37% for a detection rate of 90%. The detection results in cooperating with neighboring routers are shown in the top two curves. When cooperating with immediately connected neighbors, where distance is 1 hop, a detection rate of 98% is achieved with a false positive rate of 30%.

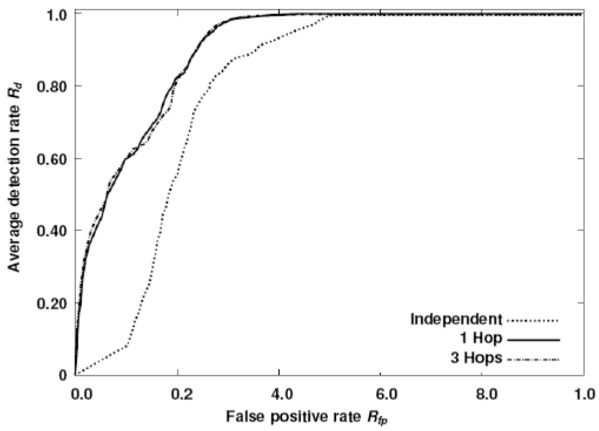


Figure 4. ROC curve illustrating the improvement of detection rate

Note that the false alarm rate does not imply 30% of the legitimate traffic will be cut off or filtered. It could be interpreted as system overhead. The false alarms will unnecessarily launch further countermeasures to investigate which part of the traffic belongs to a malicious attack.

When the false alarm is required to be very low, say below 0.05%, the 3-hop group performs slightly better than the 1-hop group. When the false positive rate exceeds 20% the $R_d$ difference in using large collaborative routers diminishes. However, enlarging the collaborative range may trigger lot more alert messages to propagate among all the routers involved. The neighborhood range has resulted in very little differences.

## V. CONCLUSIONS AND DISCUSSIONS

Protecting the Internet infrastructure from malicious attacks has been a compelling task. As tremendous damages may be caused before the end hosts realize, end hosts based defense systems cannot response to anomalies inside the network effectively. To address the malicious activities inside the core networks, we propose to develop a nervous system for the network infrastructure. To support the collaborative operation between neurons, a layer 3 IFSec protocol enables intermediate network devices to communicate with each other safely.

We verified the effectiveness of the NeuroNet architecture and the IFSec protocol through intensive experiment on a distributed cooperative DDoS attack detection scheme. Implemented on top of IFSec, our distributed detection algorithm effectively improved the detection accuracy against low-rate DDoS attack streams. The experiment on NS-2 revealed that NeuroNet is a promising idea based on that network infrastructure security scheme can be implemented.

Essentially, NeuroNet architecture provides a distributed information collecting and processing framework. Inspired by the form of biological nervous system in human body, it is different from ANNs. There is no training phase, instead, the intelligence is achieved by the adaptive information processing algorithm and updating the attack signature database in a real time manner.

Actually, this paper merely verified the concept of NeuroNet by presenting some preliminary results of a case study. Our ultimate goal is to really achieve an intelligent Internet infrastructure and to understand the impact of applying a nervous system model to the next generation Internet infrastructure. There are still considerable works and multiple open problems to be addressed.

The first challenge is to identify the metrics, parameters, and data format each individual neuron (a network layer device, i.e. a router) uses to monitor the traffic and describe what it observed. As both new applications and attack patterns keep merging quickly, it is mandatory to have a systematic way to describe the status of traffic and an adaptive approach to abstract the common characteristics to distinguish "legal" and "illegal" activities.

The second challenge is the development of mathematical application models. To describe the profile of network traffic in a more precise manner, a quantitative abstraction of data is needed. Such a data set is critical for automatic data processing.

Thirdly, we will investigate the mechanism to coordinate network activities. Particularly, this is difficult when certain actions involve multiple domains. To enable different ISP networks to work seamlessly for security purposes, one major obstacle are trust and privacy concerns. Therefore, a trust negotiation scheme will be investigated.

## ACKNOWLEGEMENT

The author would like to thank the anonymous reviewers for their valuable comments and suggestions.

## REFERENCES

[1] Abilene-I data set, the Passive Measurement and Analysis (PMA) project, http://pma.nlanr.net/traces/long/ipls1.html.

[2] P. Allen and C. Demchak, "The Palestinian-Israel: Cyberwar," *Military Review*, March-April, 2003.

[3] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," *RFC 4033*, 2005

[4] S. Bellovin, D. Clark, A. Perrig, and D. Song, "A Clean-Slate Design for the Next-Generation Secure Internet," *Report of an NSF workshop held at CMU*, 12-14 July 2005.

[5] M. Blumenthal and D. Clark, "Rethinking the Design of the Internet: the End-to-End Arguments vs. the Brave New World," *ACM Transactions on Internet Technology*, Vol.1, No.1, Aug. 2001.

[6] S. Cajal, P. Pasik, and T. Pasik, "Texture of the Nervous System of Man and the Vertebrates: Volume I," 1 edition, Springer, Feb. 1, 1999.

[7] J. Cannady, "Artificial neural networks for misuse detection," *In Proceedings of the 1998 National Information Systems Security Conference* (NISSC'98), pages 443--456, October 5-8 1998. Arlington, VA.

[8] A. Chakrabarti and G. Manimaran, "Internet Infrastructure Security: A Taxonomy", *IEEE Network*, Nov. 2002.

[9] Y. Chen and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks using Spectral Analysis," *Journal of Parallel and Distributed Computing, special issue on Security in Grids and Distributed Systems*, Vol. 66. No. 9, September 2006.

[10] R. Chertov, S. Fahmy, and N. Shroff, "Emulation versus Simulation: A Case Study of TCP-Targeted Denial of Service Attack," in *Proc. of 2nd International IEEE CreateNet Conference on Testbeds and Research Infrastructures*, March 2006.

[11] D. Dasgupta and F. Gonzalez, "An Intelligent Decision Support System for Intrusion Detection and Response," *Proceedings of the International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security* (MMM-ACNS), St. Petersburg, Russia, 2001.

[12] M. Delio, "New Breed of Attack Zombies Lurk", Wired News, http://www.wired.com/news/technology/0,1282,43697,00.html, 2001.

[13] D. Ellis, "Worm Anatomy and Model," *Proc. 2003 ACM Workshop Rapid Malcode* (WORM '03), pp. 42-50, 2003.

[14] P. Francis and R. Gummadi, "IPNL: A NAT-extended Internet Architecture," *In Proc. of ACM SIGCOMM '01*, pages 69–80, San Diego, CA, USA, Aug. 2001.

[15] J. Frank, "Artificial intelligence and intrusion detection: Current and future directions," *Proceedings of the 17th National Computer Security Conference*, October 1994.

[16] L. Gordon, M. Loeb, W. Lucyshyn, and R. Richardson, "10th Annual CSI/FBI Computer Crime and Security Survey," *Computer Security Institute* (CSI), 2005.

[17] GT-ITM: Georgia Tech Internet Topology Models, (http://www.cc.gatech.edu/projects/gtitm/), November, 2005

[18] K. J. Houle and G. M. Weaver, "Trends in Denial of Service Attack Technology," CERT Coordination Center, Carnegie Mellon Software Engineering Institute, 2002, (http://www.cert.org/archive/pdf/DoS_trends.pdf).

[19] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. Kim, S. Shenker, and I. Stoica,"A Data-Oriented (and Beyond) Network Architecture," *SIGCOMM'07*, Aug. 27 – 31, 2007, Kyoto, Japan.

[20] A. Kuzmanovic and E. W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks — The Shrew vs. the Mice and Elephants," *Proceedings of ACM SIGCOMM 2003*, Aug. 2003.

[21] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, "HAWK: Halting Anomaly with Weighted ChoKing to Rescue Well-Behaved TCP Sessions from Shrew DoS Attacks," in *Proceedings of the 2005 International Conf. on Computer Networks and mobile Computing* (ICCNMC'05), Zhangjiajie, China, August 2-4, 2005.

[22] X. Luo and R. Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense," in *Proceedings of Network and Distributed System Security Symposium* (NDSS'05), San Diego, CA., February 2-5, 2005.

[23] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM Computer Communications Review*, vol. 34, no. 2, Apr. 2004.

[24] NS-2, http://www.isi.edu/nsnam/ns/, 2004.

[25] B. Schwartz, A. Jackson, W. T. Strayer, W. Zhou, R. D. Rockwell, C. Partridge, "Smart Packets: Applying Active Networks to Network Management," *ACM Trans. Computer Systems*, V 18, N 1, 2000.

[26] D. Sterne, K. Djahandari, R. Balupari, W. La Cholter, B. Babson, B. Wilson, P. Narasimhan, and A. Purtell. "Active Network Based DDoS Defense," in *the Proceedings of the DARPA Active Networks Conference and Exposition* (DANCE 02), 2002.

[27] H. Sun, J. Lui, and D. Yau, "Defending Against Low-rate TCP Attacks: Dynamic Detection and Protection," in *Proceedings of 2004 IEEE International Conference on Network Protocols* (ICNP), Berlin, Germany, October 5-8, 2004.

[28] D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, G. J. Minden, "A Survey of Active Network Research," *IEEE Communications Magazine*, V. 35, N. 1, January 1997.

[29] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms," *Proc. 2003 ACM Workshop Rapid Malcode* (WORM '03), Washington, D.C., Oct. 27, 2003, pp. 11-18.