Scheme of Defending Against DDoS Attacks in Large-Scale ISP Networks

Zhi-jun Wu and Dong Zhang

Communication Engineering Department, Civil Aviation University of China
Tianjin, 300300, P.R. China
caucwu@263.net, mymailbox66@sohu.com

Abstract. A scheme that defending against distributed denial of service (DDoS) attacks adopts the mechanism of Distribution-based Secure Overlay Nodes (DSON) to a large-scale ISP (Internet Service Provider) network is presented. The scheme uses local BPG announcement to divert traffic to the overlay network when experiencing high load, then filtering algorithm based on the technology of signal processing is applied to the diverted traffic. This algorithm detects and filters out DDoS attacks in frequency domain to allow targets to provide good service to legitimate traffic, with fast reaction and high energy ratio of legitimate to attacks traffic. DSON is implemented and installed on the monitor points of large-scale ISP network associated with the corresponding routers, edge router, border router, and core router, with no requirement for the modifying to network architecture, infrastructure, and protocol.

Keywords: Distributed Denial of Service (DDoS), Distribution-based Secure Overlay Nodes (DSON), China Education & Research Network (CERNET), Router, Large-scale ISP Network.

1 Introduction and Motivation

Distributed Denial of Service (DDoS) attack is a great threat to the quality of service (QoS) of Internet and large-scale Internet Service Provider (ISP) network [1]. In this paper, a network-based defense mechanism called Distribution-based Secure Overlay Nodes (DSON) is proposed to defend against DDoS attacks in large-scale ISP Networks. Since attacker hosts and victim under flood-type attacks are widely distributed, DSON takes a distributed approach to implement defense functions with the features: (i) secure overlay array nodes are installed at every edge or border router and managed by a management center (MC). (ii) no requirements of modifying the architecture, infrastructures, protocol, and routing strategy of existing ISP network, no additional routing path needed, and no physic routing link added.

2 Related Work

There are many network-based mechanisms of handling DDoS problem in large-scale ISP network. Secure overlay Services (SOS) [1] with the goal of routing only

K. Li et al. (Eds.): NPC 2007, LNCS 4672, pp. 296–305, 2007.

authenticated traffic can pass through the overlay network to the target sites, which accepts only packets from the servlets. Traffic that has not been confirmed to originate from a good client is dropped. Clients must use an overlay network, sitting on top of the existing network, to get authentication and reach the servers. Redirection-based defense mechanism [4] is a network-based defense mechanism that reduces the required number of defense nodes based on traffic redirection which allows the edge and border routers to divert suspicious packets to central defense nodes (C-DNs). Such traffic redirection requires an additional forwarding mechanism other than IP-destination-address-based forwarding since suspicious packets must be routed through a C-DN at all times before reaching a final destination. Traffic redirection using tunneling technique to set up tunnels between all the edge and border routers and C-DNs, and the packets destined for a victim are diverted to the C-DNs by configuring policy routing of the edge and border routers. D-ward [5] is a source network-based system aiming to detect attacks before or as they leave the network that the DDoS agent resides on. It is an inline system (transparent to the users on the network) that gathers two-way traffic statistics from the border router at the source network and compares them to network traffic models built upon application and transport protocol specifications, reflecting normal (legitimate), transient (suspicious), and attack behavior[6]. D-ward is a self-regulating reverse-feedback system collaborating with source router. The throttling component of D-ward generates and adjusts rate limit rules, then communicates them to the source router, which filters the attack traffic.

In general, approaches mentioned above depend on modifying the routing configuration policy and adding intelligent algorithm to routers. It is very difficult for a well-design and end-constructed existing large-scale ISP network to do these changes, which may degrade the network QoS, and bring other unexpected problems.

3 D-SON-Based DDoS Defense Mechanism

China Education & Research Network (CERNET) is a national-wide academic network platform. With more and more computers connected to CERNET, system security must be kept up with the increase in connectivity. Many secure measures have been implemented on CERNET with its scale expend. 42 monitor points (MPs) have been designed and installed on distributed 42 region and main network nodes to monitor, detect, and control the outgoing and incoming traffic.

D-SON is considered as the defense mechanism for CERNET to defend against flood-type attacks based on the experiences of handling DDoS attacks event, and analyzing flow connection and traffic data [4]. We assume all attack traffic is generated by some organized hosts on peer customer networks, or generated from other locations on the Internet and then routed over via neighboring ISPs. CERNET is an autonomous system (AS) constructed by inter-connected core routers forming the backbone network. The sub-networks are connecting to CERNET through border routers or access routers, while the other ISP networks connecting the CERNET through edge routers. The task for CERNET defending against DDoS attack focuses

on two aspects: (i) Stop the CERNET suffering from DDoS attacks coming from outside networks. (ii) Prevent other ISP networks from DDoS attacks by coming from CERNET inside sub-networks.

The scheme for CERNET defending against DDoS attack adopts the distributed defense mechanism, which combining source-end defense with victim-end defense to protect the target inside CRNET from suffering DDoS attack and stop DDoS attack from CERNET to other ISP networks. SONs are installed on the CERNET associated with 42 distributed MPs. MC manages border routers, edge routers, and SONs. 42 MPs constitutes the monitor system of CERNET for detecting of anomaly traffic and attack flow. If MPs report DDoS attack events, MC turns to emergence status immediately and manages the border routers, edge routers, and SONs working together to defend against DDoS attacks.

Figure 1 gives an example of flood-type attacks from one ISP network and one CERNET sub-network. Attack detection is the task of monitor points are installed on the critical nodes of CERNET. The scene of normal and attack traffic flow in CERNET divides the network into three parts: (i) $\mathrm{CERNET}_{\mathrm{BACKBONE}}$ is backbone network of CERNET. (ii) $\mathrm{CERNET}_{\mathrm{Sub1}}$, $\mathrm{CERNET}_{\mathrm{Sub2}}$, and $\mathrm{CERNET}_{\mathrm{Sub3}}$ are three sub-networks of CERNET connect to $\mathrm{CERNET}_{\mathrm{BACKBONE}}$ through border routers. (iii) ISP_1, ISP_2, and ISP_3 are three neighboring ISP networks connected to CERNET through edge routers.

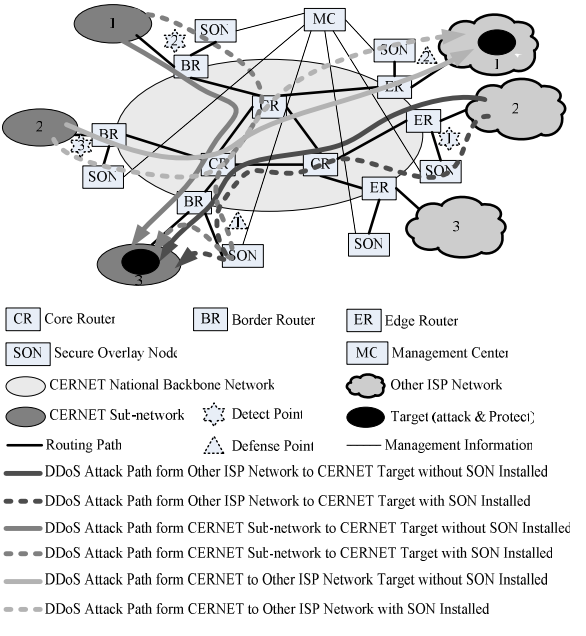


Fig. 1. DDoS defense mechanism of CERNET

Different roles of attacking and defending in Figure 1 are shown as followings:

(i) Two targets (attack and protect)

T_1 is the target located in the $CERNET_{Sub3}$, and T_2 is the target located in the ISP_1.

(ii) Three DDoS attack sources

A_1 is the DDoS attack launched by ISP_2 targeted the T_1 (outside attack)

A_2 is the DDoS attack launched by $CERNET_{Sub1}$ targeted the T_1 (inside attack)

A_3 is the DDoS attack launched by $CERNET_{Sub2}$ targeted the T_2 (inside attack)

(iii) Five defense points

The defense point with six angles means this point has the function of DDoS attack detecting and defending, while the point with triangle means this point only has defending function without detection.

D_{P1} and D_{P2} are the victim-end defense points without the detection function. The detection of DDoS attack is done by the Intrusion Detection System (IDS) installed on the sub-network or ISP network.

D_{P1}, D_{DP2}, and D_{DP3} are source-end defense points with both function of detection and defense.

(iv) Three attack paths

Two defense points are designed for every attack path, one source-end and one victim-end. Each attack path is denoted in two lines, the solid is the real attack path, the while dashed is the path through defense points.

$P_{ISP2-Sub3}$ is the attack path from ISP_2 to $CERNET_{Sub3}$ passing D_{P1} and D_{DP1}.

$P_{Sub1-Sub3}$ is the attack path from $CERNET_{Sub1}$ to $CERNET_{Sub3}$ passing D_{P1} and D_{DP2}.

$P_{Sub2-ISP1}$ is the attack path from $CERNET_{Sub2}$ to ISP_1 passing D_{P2} and D_{DP3}.

Note that in practical application of large ISP networks, the attack targets and sources are changeable, resulting in the change of attack path. In this case, each defense point has the function of both source-end and victim-end defense.

The differences between DSON and redirection-based defense mechanism are that: (i) Redirection modifies router configuration to change the routing policy, while DSON uses diverting algorithm to change the traffic normal path. (ii) Redirection uses Manager Node (MGR) to reconfigure the routing policy of edge and border router, while DSON adopts MC to manage the distributed SONs. The distinguished difference between DSON and D-ward is the executor for traffic limiting. The former is SON, the latter is router. D-ward has the function of traffic observation and rule-based traffic limiting, while SON not only monitors the traffic, also has the ability to remove malicious packets.

4 Design of SON

SON working together with an associated router as Riverhead [8]. If a DDoS attack is detected, all traffic destined to the target (protected and attacked) is then diverted off normal path through the SON, which applies filtering rule (algorithm) and judges

guide-line to identify and eliminate malicious packets, allowing legitimate transactions to pass. Traffic to target is diverted to SON, which works in two operation modes depending on its two main functions: (i) *Defend*: SON actively filters out attack traffic and forwards legitimate traffic to the target. (ii) *Statistic*: if there no attack detected, SON sniffs at the traffic and extracts the data for statistic analysis. This helps SON to learn the normal behavior of every connection and client to establish a standard model. When the standard model is built, SON monitors the traffic behavior. Two situations will make SON switch from *Statistic* mode to *Defend* mode automatically: (i) If SON notices a deviant traffic behavior, which does not match the standard model. (ii) When an alert coming from the MP associated with current SON [8]. The working process of SON is divided into three steps: (i) Charging the target's traffic diverted from the associated router. (ii) Removing malicious packets. (iii) Returning legitimate to router and forwarding them to target.

Three kinds of SONs are designed for cooperation with different routers according to the throughput: (i) Intel network processor platform IXP 2800 is used for first kind of SON, with throughput of 2.5G (test at 256 bytes packet length, at 64 bytes the throughput is 0.75G). (ii) Intel network processor platform IXP 1200 is used for second SON, with throughput of 1G (test at 256 bytes packet length, at 64 bytes the throughput is 0.32G). (iii) AMD 64bits server is used for third SON, with throughput of 0.1G (test at 256 bytes packet length, at 64 bytes the throughput is 0.05G).

5 Key Technologies of SON

In statistic mode, traffic is diverted through the DSON so it could learn the normal behavior of different connections and clients to establish a baseline profile. Once the profile is built, the operator interacts with the DSON and may adjust or accept any of the suggested parameters.

(i) Traffic divert

When an attack has been detected, diversion is achieved by the SON sending out an iBGP announcement, the traffic should be routed to the Label Switching Protocol (LSP) path that ends at the SON's loop-back interface. To ensure that the BGP announcements will not propagate into all the backbone routers' routing tables, no-advertise and no-export BGP is applied on the community strings. As a result, only associated router will receive the BGP announcements about the target, with next hop to the corresponding SON loop-back interface [8].

(2) Detection approach

The detection of DDoS attacks adopts the technology of signal processing based on the frequency-domain characteristics from the autocorrelation sequence of Internet traffic streams [9]. The arrivals of network packet are expressed in a packet process: $\{X(t), t = n\Delta, n \in N\}$, where Δ is the constant interval. N is number of packet. X(t) represents the total number of packet arrivals at one router in $(t-\Delta, t]$ [10][11]. Take a single TCP flow plus one constant rate UDP flow with a rate of 300Kb/sec as the attack flow (Figure 2). The attack flow is destined to the target together with normal traffic. In this case, Δ =5ms.

In order to detect the attack flow from the normal flow, the packet arrivals are converted into frequency domain by adopting Discrete Fourier Transform (DFT):

$$DFT(x(n),k)=\frac{1}{N}\sum_{n=0}^{N-1}x(n)e^{-j2\pi kn/N} \quad (1)$$

Where, $k=0,1,2\ldots\ldots N\text{-}1$. Equation (1) generates the amplitude spectrum of packets arrivals (Figure 3).

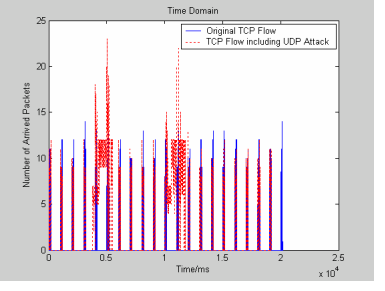


Fig. 2. TCP flow and UDP attack

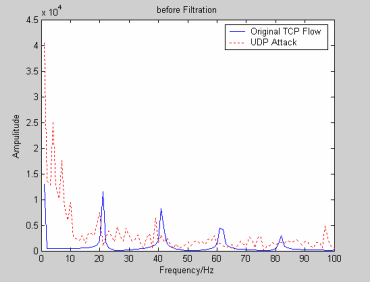


Fig. 3. The amplitude of TCP flow and UDP attack

PSD implies the frequency-domain characteristics from the autocorrelation sequence of Internet traffic streams. The normalized cumulative PSD (NCPSD) curve of autocorrelation function of packet process is shown as Figure 4.

It shows that more than 85% of the packet process's energy distributes in frequency band [0, 50] Hz if the traffic contains a DDoS stream. By contrast, if there is no DDoS stream contained, the energy located in this low frequency band is less than 35%. This implies that NCPSD is a robust criterion in detecting whether current sampled traffic contains shrew streams [10][11].

To detect DDoS attack is to find out the frequency point, called detection point F_D, where the biggest distance between the NCPSD curve of TCP flow and UDP attack occurs. In this case, F_D =50Hz, which corresponds to cutting point where NCPSD=0.6. An optimal tradeoff is made between detection probability PD, false negative alarm rate PFN, and false positive alarm rate PFP during tests. The tests result is shown in Table 1 [10][11].

Table 1. Detection test result

Items	Threshold	NCPSD	F_D	P_D	P_{FN}	P_{FP}
Result	5.45	0.618	50Hz	0.902	0.098	0.154

(3) Filtering algorithm

The filtering algorithm is to design the finite impulse response (FIR) filter $H(\omega)=\sum_{i=1}^{N}H_i(\omega)$ for filtering the illegitimate frequencies in frequency domain and improve the LAR (Legitimate traffic to Attacked traffic Ratio). Where $H_i(\omega)$ is the filter for i-th TCP flow, N is the total number of TCP flow. Based on the result of

DDoS attack detection, the attack and noise flows of network traffic will be filtered out when each packet passing through $H(\omega)$. The filtering result is shown as Figure.5.

Calculate the energy of TCP flow and UDP attack individually; the energy ratio of TCP to UDP is noted as *ERTU*. Test result shows the ERTU increases about 10dB (Table 2).

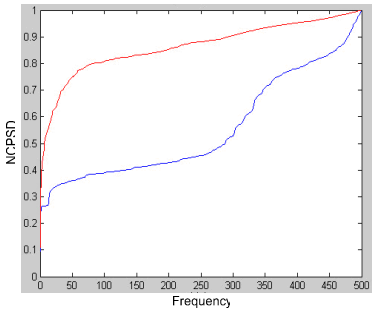


Fig. 4. The NCPSD curve

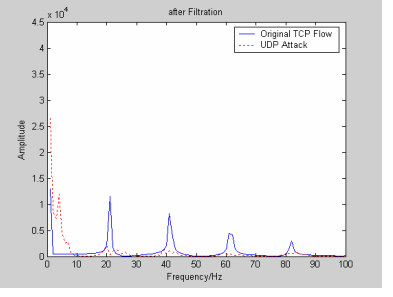


Fig. 5. Filtering result

Table 2. Test result (dB)

Item	Original	Filtering
ERTU	-19.3121	-10.8417

6 Performance Test with CERNET Data

The test of DSON performance is conducted by using the data that collected for CERNET.

(1) Flood-type DDoS attack to CERNET

Reports from CERNET NOC and CERNET Computer Emergency Response Team (CCERT) show that many mission-critical web sites of CERNET experienced many times flood-type DDoS attacks. Traffic Accounting record of CERNET show that a DDoS attack happened from AM 6:25 to 8:15, July 14, 2005, congestion in the rush hour is so serious (max traffic up to 453,667kpps) that lead to a lot of packets (Legitimate and attack) dropped, the traffic accounting of inbound and outbound descended shapely. Obviously, this attack causes big economy loss to CERNET [7], because this attack leads to a wrong traffic account.

At PM 1:10, Mar. 28, 2005, monitor center of CERNET record the detail information about one important Web page server of CERNET suffer from TCP SYN flood attack. This attack directs about 100 of compromised zombie hosts, all IP are spoofed. It adopts TCP protocol, average packets length is 60 Bytes [7].

Table 3 shows the records for 4 zombie hosts (in shorten, only list 4 of 100 zombie hosts' records). Table.4 is the analysis result to one zombie host. For privacy purpose, the destination (target) IP and source IP is omitted. These data of attack traffic are collected and stored in disc array storage for future testing of DSON performance.

Table 3. Records of four zombie hosts (4 sources IP) TCP SYN flood attack

Protocol	Bandwidth (Mbps)/Percent	Packets/sec/Percent	Average packet (Bytes)
TCP	12.43 (1.45%)	27161 (7.56%)	60
TCP	7.55 (0.88%)	16496 (4.59%)	60
TCP	7.13 (0.83%)	15589(4.34%)	60
TCP	6.63 (0.78%)	14497(4.04%)	60

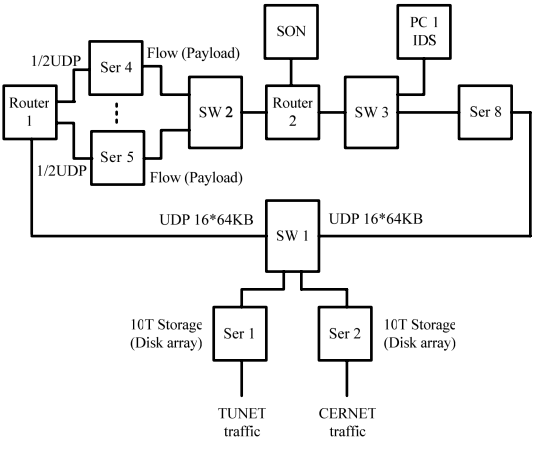
Note: Percent in bandwidth means every attack TCP link occupies in total practical bandwidth 857.9 Mbps, and percent in packets expresses the packets of every attack TCP link sending occupies in total practical packets 359390.

Table 4. Analysis result to one zombie host(Single source IP)

Src_port	Dst_port	Protocol	Bandwidth (Mbps)	PPS	Average packet (Bytes)
329	80	6 (TCP)	0.033	72	60
718	80	6 (TCP)	0.032	70	60
851	80	6 (TCP)	0.032	69	60
833	80	6 (TCP)	0.031	68	60

(2) Defending against DDoS attack test

Every SON assigns an IP address. The management information of communication between SON and MC adopts the TCP/IP protocol. The former executing as a detector and the latter acting as a controller of the flood-type DDoS attack. MP detects the traffic destined to a certain network that are exceed "normal" levels, then SON examines the traffic of different port numbers, and/or different sources in order to detect the offending source or the characteristic port number. Experiment environment for testing the performance of DSON scheme is built by connecting to CERNET and TUNET (Tsinghua University Campus Network) as Figure 6.



PC1— Computer for IDS SW1、SW2、SW3— Giga Switcher

Ser1、Ser2—1U server with two giga network cards and 10T disc array storage

Ser3、Ser4、Ser5、Ser7、Serv8—1U server with two giga network cards

Ser6—2U server with three giga network cards

Fig. 6. Test environment

The flows in this environment are composed of two kinds traffic: (i) Background flow come from the real flow of CERNET and TUNET. (ii) Attack flow is the playback of attack traffic, which is collected and stored in disc array. The background flow combines attack flow in the UDP (User Datagram Protocol) of 64KB in length. Each flow consists of 16 UDP packets.

In the experiment environment, router 1 and ser 4, 5 insert the payload to the packet and assign the flow to construct the attack path. Router 2 acts as the edge router cooperated with the SON to defend the attack. Ser 8 plays three roles: (i) Target for the attack. (ii) Indicator for the test result evaluation. (iii) Playback of attack scenery circularly for repeat testing.

Test result (Table 5) from the output of ser 8 shows that the SON has a good performance in filtering attack packets.

Table 5. Records of four zombie hosts (4 sources IP) TCP SYN flood attack survival

Protocol	Bandwidth (Mbps) /Percent	Packets/sec/Percent	Average packet (Bytes)
TCP	0.1864 (0.0217%)	407 (0.1133%)	60
TCP	0.0083 (0.0088%)	165 (0.0459%)	60
TCP	0.0071 (0.0083%)	156 (0.0434%)	60
TCP	0.0066 (0.0077%)	145 (0.0404%)	60

Statistics to the experiment result shows (Table 6) that the average ratio of legitimate traffic passing is more than 92%, legitimate traffic dropping is less than 8%, attack traffic filtering is more than 98.5%, and attack traffic passing is less than 1.5%.

Table 6. Test statistics result

Item	Average Percent
Legitimate traffic passing	More than 92%
Legitimate traffic dropping	Less than 8%
Attack traffic Filtering	More than 98.5%
Attack traffic passing	Less than 1.5%

7 Conclusion

In this paper, a distribution-based defense mechanism against flood-type attacks is proposed for protecting the targeted sub-networks and mission-critical Web sites of CERNT. For a well-constructed large-scale ISP networks, any small modification to the routing policy and network devices will lead to big troubles. Based on the principle of no requirements of modification to the topology and protocol of existing large-scale ISP networks, this ISP level mechanism using DSON to divert the traffic with suspicious packets to the SONs by sending a BGP announcement to the associated edge or border routers. Then, a filtering algorithm in frequency domain is applied to filter out attacks.

We will further study how to improve the accuracy of the malicious packet search process, develop the IP trace-back system to catch attacking source sites against a variety of attacks, and protect large-scale ISP network from vicious attacks to ensure business continuity.

Acknowledgement

The authors like to thank the CERNET NOC and CCRET for providing network data, and thank the anonymous reviewers for their hard works.

References

1. Keromytis, A.D., Misra, V., Rubenstein, D.: SOS: Architecture for Mitigating DDoS Attacks. Journal, IEEE Journal on selected areas in communications 22(1), 176–188 (2004)
2. Keromytis, A.D., Misra, V., Rubenstein, D.: SOS: Secure Overlay Services. In: Proc. of ACM SIGCOMM' 2002, August 2002, ACM Press, New York (2002)
3. Chen, S., Chow, R.: A New Perspective in Defending against DDoS. Distributed Computing Systems. In: FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends, 26-28 May 2004, pp. 186–90 (2004)
4. Hamano, T., Suzuki, R., et al.: A Redirection-based Defense Mechanism against Flood-type Attacks in Large-scale ISP Networks. In: Proceedings, 10th Asia-Pacific Conference on Communications and 5th International Symposium on Multi-Dimensional Mobile Communications, Taiwan, pp. 1–15 (2001)
5. Mirkovic, J., Prier, G., Reiher, P.: Attacking DDoS at the source. In: Proceedings, 10th IEEE International Conference on Network Protocols, Paris, France, November 2002, pp. 312–321. IEEE Computer Society Press, Los Alamitos (2002)
6. Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P.: Internet Denial Service: Attack and Defense Mechanisms. In: Prentic Hall Professional Technical Reference, Coirier in Stoughton, Massachusetts (December 2004) ISBN: 0-13-147573-8
7. Technical report, DDoS attack and defense of CERNET, CCERT, report, Network Research Center, Tsinghua University (March 2005)
8. DDoS Mitigation: Maintaining Business Continuity in the Face of Malicious Attacks, report, Technical Note, Riverhead, Cisco (2004)
9. Cheng, C.-M., Kung, H.T., Tan, K.-S.: Use of Spectral Analysis in Defense Against DoS Attacks. In: Proceedings, IEEE GLOBECOM (2002)
10. Chen, Y., Hwang, K., Kwok, Y.-K.: Filtering of Shrew DDoS Attacks in Frequency Domain. In: Proceedings of the IEEE Conference on Local Computer Networks, 30th Anniversary, 15-17 November 2005, pp. 786–793 (2005)
11. Chen, Y., Hwang, K., Kwok, Y.-K.: Collaborative Defense against Periodic Shrew DDoS Attacks in Frequency Domain. Journal, ACM Transactions on Information and System Security (TISSEC), 1–30 (May 3, 2005)