Mitigating DDoS Attacks using Combined Input-Crosspoint Buffered Switches

Chuan-bi Lin, Yun-Cheng Chang, and Ziqian Dong

***Abstract*—Distributed Denial of Service (DDoS) attack is a major threat to Internet services. We propose a scheduling scheme in a combined input-crosspoint buffered switch to mitigate the DDoS attacks in this paper. The proposed scheduling scheme allows legitimate traffic to pass with high priority and suspected attack traffic to pass however with low priority. By controls the service priority of suspected attack traffic, the method can reduce the damage DDoS attack has on the targeted end hosts.**

***Index Terms*—Distributed Denial of Service, attack, crosspoint buffered switch, legitimate, priority**

I. Introduction

Distributed Denial of Service (DDoS) attack [1] is one of the major threats to Internet services because the legitimate packets are bombarded with high volume of fictitious and malicious packets originated from a large number of computers. The DDoS problem has become an attractive issue for the research community. Moreover, the DDoS attacks exist some different patterns, as the follows:

1) Smurf Attack [2]: The attacker pretends the source to be the attacked IP to send a broadcast address, those receiving this packet in a broadcast area will send reply packets to the attacked host, the victim host cannot respond to these packets within a short period of time and was paralyzed.

2) SYN Flood [3]: The fake IP sends SYN request to the target.The attacked target will respond an ACK+SYN.The host of real IP which was no request and not respond.The victim host receives no response, which will repeat this process three-five times and wait for a SYN Time (generally 30 seconds to 2 minutes), and then finish connection.

3) UDP Flood: UDP Flood: A lot of UDP packets are sent to the victim server of specific service uninterruptedly, such as DNS and media servers. Such attacks will result in a lot of UDP packets flowing in the backbone of network and paralyzes the entire network.

Chuan-bi Lin and Yun-Cheng Chang are with the Department of of Information and Communication Engineering, Chaoyang University of Technology, Wufong Township, Taichung County 41349, Taiwan. Email: {cblin, s9830618}@cyut.edu.tw.

Ziqian Dong is with the Department of Electrical and Computer Engineering, New York Institute of Technology, New York, NY 10023, USA. Email: ziqian.dong@nyit.edu

Corresponded Email is cblin@cyut.edu.tw

4) Fast Adaptive Attack(FAA): Such DDoS attacks are hard to prevent, a sophisticated attacker will try to produce packets periodically to test the condition of defense system, if any packet has broken into the intrusion detection system successfully, the attacker will send the same packet repeatedly to attack.

Therefore, to detect and prevent the DDoS attack packets, a number of methods have been proposed. Some of these proposed methods use traceback protocols to [5]-[7] The another methods use limited statistical traffic profiling at the edge of the networks to stop DDoS attacks, i.e., the ingress routers [8]. The rest of proposed methods use advertise limited support of statistics-based adaptive filtering techniques to filter DDoS attack packet [9][10]. However, most of the proposed methods do not fully filter the suspected attack traffic or automate traffic differentiation. Instead, they use a set of binary filter rules to the network administrator to be installed in their routers or firewalls [11][12]. It was very hard to prevent DDoS in networks.

Therefore, one question arises: is it possible to mitigate suspicious DDoS attacks and achieve the high throughput of legitimate packets by using a scheduling scheme without a set of binary filter rules in the intermediate routers where network packets traverse?

In this paper, we propose a method to mitigate the DDoS attack in the intermediate routers where network packets traverse. The proposed method uses prioritized scheduling scheme in a combined input-crosspoint buffered (CICB) switch. The scheduling scheme allows traffic to pass with different priority. Suspicious DDoS traffic will be delayed when being forwarded, therefore, reduces the transmission rate of suspicious packets and its damage to the end hosts.

This paper is organized as follows. Section II presents a brief description of the pre-existing CICB switch with round-robin input and output arbitrations, and with prioritized priority. Section III presents the throughput performance of the CICB switch with prioritized priority. Section IV presents our conclusions.

II. Combined Input-Crosspoint Buffered Switch with Differentiated Priorities

The CICB switch architecture follows the one presented in [13]-[16]. We consider that traffic is classified in two different classes in this paper. A buffered crossbar has N inputs and outputs. A crosspoint (CP) component

would connect the input port i to the output port j in the buffered crossbar, it was defined as $CB(i,j)$. There were $2N$ $VOQs$ in each input. A VOQ in the input i would store cells in the output j of priority p, where $0 \leq p \leq 1$, is denoted as $VOQ(i,j,p)$. Here, we consider that $p = 0$ is presented legitimate traffic and has higher priority, otherwise, $p = 1$ is presented suspicious DDoS traffic. The CP buffer of $CB(i,j)$ was defined as $CPB(i,j)$, and this is not prioritized. The size of $CPB(i,j)$ is k cells, and $k \leq 1$.

There was a credit-based flow control mechanism in this CICB switch, the transfer would be confirmed before Input i sent cell to $CPB(i,j)$. Each VOQ had a credit counter, and the number of this credit counter was the maximum value $CPB(i,j)$ can store. So when the credit counter of VOQ was at its maximum, the input arbitration would regard this VOQ as unqualified to send to $CPB(i,j)$. When $VOQ(i,j)$ sent data to the corresponding $CPB(i,j)$, the credit counter of this $VOQ(i,j)$ would be added by one. When the cell of $CPB(i,j)$ was sent out, the credit counter of $VOQ(i,j)$ would be reduced by one.

An input arbiter at input i selects $VOQ(i,j,p)$ among the eligible VOQs to send a cell to CPB for output j at buffered crossbar. An output arbiter at output port j in the buffered crossbar selects a $CPB(i,j)$, among occupied CPBs from input i, to send a cell to output j. The eligibility of VOQs is determined by the flow control mechanism, as shown in Fig. 1.

This CICB switch has round-robin with strict priority for input and output arbitrations. In this input arbitration scheme, round-robin selection is performed among all queues of the highest priority. If there are no cells of the highest priority, round-robin is performed among the second highest priority. Output arbitration also considers round-robin with differentiated priorities to make starving cells with low priority.

This switch has dedicated crosspoint buffers, this is, $VOQ(i,j,p)$ can access input row i and connect CPB of output j, where each CPB could access through 2 $VOQ(i,j)$ and the same input i and output j. However, if the $CPB(i,j)$ of corresponding input i and output j had no cell, the crosspoint buffer would enter idle.

Figure 1 shows

III. Performance Evaluation

The performance evaluations are produced through computer simulation. This section presents the performance evaluations of a 32×32 CICB switch with two-priority traffics: legitimate and suspected attack, where class legitimate has higher priority than class attack. To analyze the adopted DDoS traffic models, we examine the performance of CICB with two classes under nonuniform prioritized traffic, using the unbalanced and diagonal traffic models. The simulation does not consider the segmentation and re-assembly delays for variable size packets. Simulation results are obtained with a 95% confidence interval, not greater than 5% for the average cell delay.

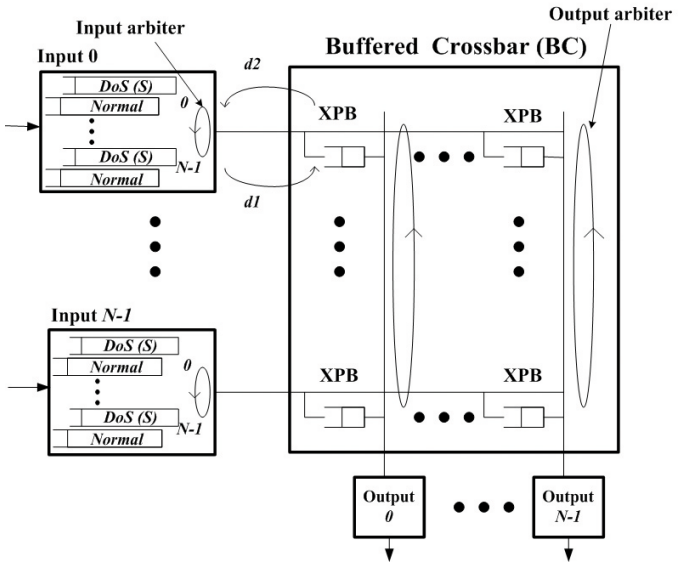

Fig. 1. The CICB switch with differentiated priorities.

A. Unbalanced traffic

The unbalanced traffic model uses a probability, w, as the fraction of input load directed to a single predetermined output, while the rest of the input load is directed to all outputs with uniform distribution. Let us consider input port i, output port j, and the offered input load for each input port ρ. The traffic load from input port i to output port j, $\rho_{i,j}$ is given by,

$$\rho_{i,j} = \begin{cases} \rho\left(w + \frac{1-w}{N}\right) & \text{if } i = j \\ \rho\frac{1-w}{N} & \text{otherwise.} \end{cases} \quad (1)$$

When $w = 0$, the offered traffic is uniform. On the other hand, when $w = 1$, it is completely directional, from input i to output j, where $i = j$. This means that all traffic of input port i is destined for only output port j, where $i = j$.

In this section, we compare the throughput and average delay performance between legitimate and attack traffics under unbalanced traffic with maximum allowable input load, $\rho_i = 1$. Figure 2 shows the throughput of legitimate and suspected attack traffic with unbalanced distribution. This figure shows that legitimate traffic reaches over 99% throughput under the complete range of w and suspected DDoS attack traffic has the low throughput. This is because the legitimate traffic has higher priority to travel to output than DDoS attack traffic under this traffic model.

Here, we use a probability, c, as the proportion of legitimate traffic to whole traffics. Figure 3 shows the throughput of legitimate and suspected attack traffic with different proportions of legitimate traffic and unbalanced distribution, when $w = 0.5$. This figure shows the

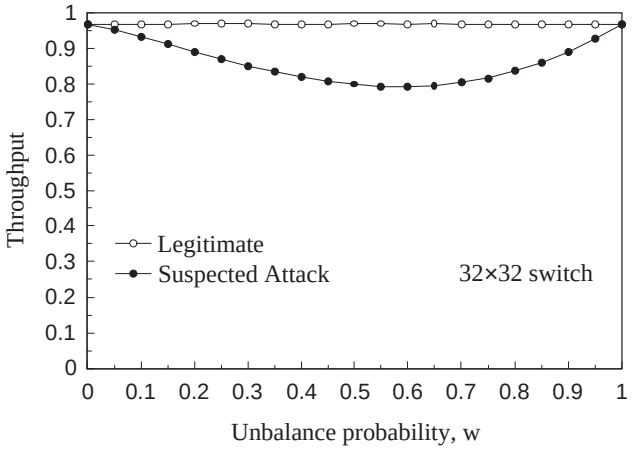

Fig. 2. Throughput of legitimate and suspected attack traffic with unbalanced distribution.

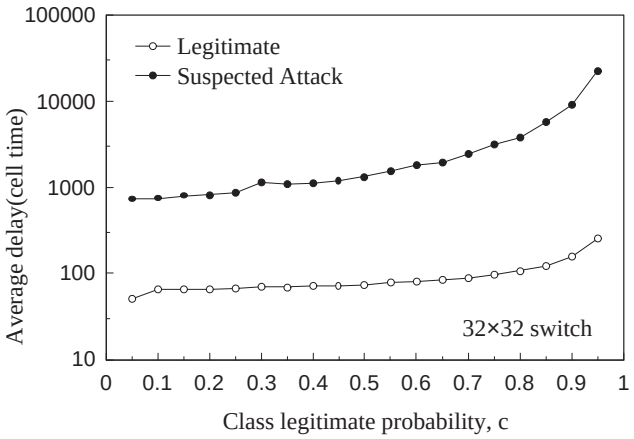

Fig. 4. Average delay of legitimate and suspected attack traffic with different proportions of legitimate traffic and uniform distribution.

legitimate traffic reaches higher throughput than suspected attack traffic under the complete range of c, when $w = 0.5$. The reason is that prioritized scheduling scheme allows traffic to pass with different priority.

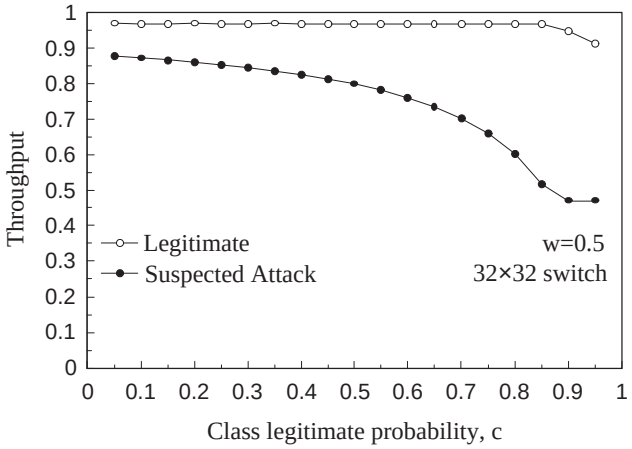

Fig. 3. Throughput of legitimate and suspected attack traffic with different proportions of legitimate traffic and unbalanced distribution, w=0.5.

Figure 4 shows the average delay of legitimate and suspected attack traffic with different proportions of legitimate traffic and uniform distribution, when $w = 0$. This figure shows the performance of average delay of legitimate traffic is better than that of suspected attack traffic under uniform distribution and the complete range of c.

B. Diagonal traffic

The other nonuniform traffic pattern is diagonal traffic model, which is defined as $d\rho_{i,j} = d\rho_i$ for $j = i$, $(1 - d)\rho_i$ for $j = (i+1) mod N$, otherwise, $\rho_{i,j} = 0$, where ρ_i is the load at input i. This traffic model distributes the load of an input among two outputs only. The distribution is given by the diagonal degree probability, d. Since the results under diagonal traffic are symmetric at $d = 0.5$, the following graphs show throughput results at $0 \leq d \leq 0.5$.

Figure 5 shows the throughput of legitimate and suspected attack traffic with diagonal distribution. The figure shows that legitimate traffic can achieve over 99% throughput, however, the suspected attack traffic has low throughput. Figure 6 shows the throughput of legitimate and suspected attack traffic with different proportions of legitimate traffic and diagonal distribution, when $d = 0.3$. This figure also shows that legitimate traffic reaches high throughput under the complete range of c. Suspicious DDoS attack traffic will be dropped by using the proposed prioritized approach in a CICB switch.

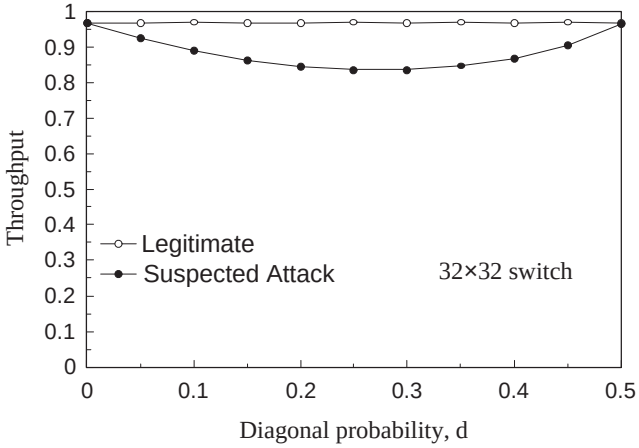

Fig. 5. Throughput of legitimate and suspected attack traffic with diagonal distribution.

Figure 7 shows average delay of legitimate and suspected attack traffic with different proportions of legiti-

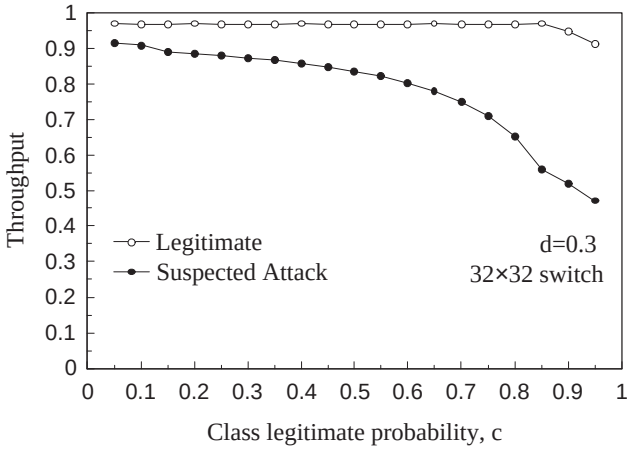

Fig. 6. Throughput of legitimate and suspected attack traffic with different proportions of legitimate traffic and diagonal distribution, d=0.3.

mate traffic and diagonal distribution under the complete range of c, when $d = 0.3$. This figure shows the average delay of legitimate traffic is lower than that of suspected attack traffic under uniform distribution and the complete range of c. This is because suspicious DDoS traffic will be delayed when being forwarded with lower priority by using prioritized scheduling scheme in a CICB switch.

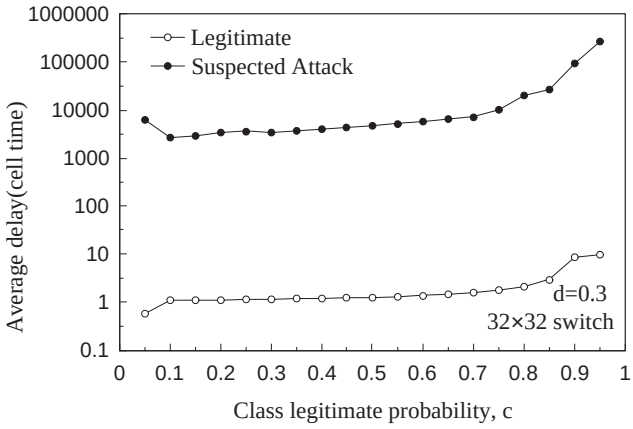

Fig. 7. Average delay of legitimate and suspected attack traffic with different proportions of legitimate traffic and diagonal distribution, d=0.3.

IV. Conclusions

DDoS attack is a major threat to continuity of network services. The counter measures are mainly focused on end server side to block suspicious DDoS traffic. We propose in this paper a method to mitigate the DDoS attack in the intermediate routers where network packets traverse. The proposed method uses prioritized scheduling scheme in a combined input-crosspoint buffered switch. The scheduling scheme allows traffic to pass with different priority. Suspicious DDoS traffic will be delayed when being forwarded, therefore, reduces the transmission rate of suspicious packets and its damage to the end hosts. Simulation results show that actual delay of suspicious DDoS packets with our proposed scheme is larger than that of legitimate packets. When a large amount of traffic overloads the switch, legitimate packets will not suffer from throughput degradation which DDoS packets are dropped for its low priority. We also refer to several methods of detecting DDoS traffic in network routers/switches that can work together with the proposed scheme to mitigate DDoS attack on the network path.

References

[1] F. Lau, S.H. Rubin, M.H. Smith, and L. Trajkovic, "Distributed denial of service attacks," *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, vol. 3, pp. 2275 - 2280, Oct 2000.

[2] CERT Co-ordination Centre, 2000, "CERT Advisory CA-98.01 SMURF IP Denial of Service Attacks," *online http://www.cert.org/advisories/CA-98.01.smurf.html -smurf Attack*

[3] CERT Co-ordination Centre, 2000, "CERT advisory CA-1996-21,TCP SYN flooding and IP spoofing attacks," *online http://www.cert.org/advisories/CA-1996-21.html*

[4] F.A. El-Moussa, N. Linge, and M. Hope, "Active router approach to defeating denial-of-service attacks in networks," *Communications, IET*, vol.1, no.1, pp.55-63, February 2007

[5] S. Bellovin, M. Leech, and T. Taylor, ICMP Traceback Messages, *draft-ietf-itrace-01.txt, Internet draft*, Oct 2001.

[6] K. Park and H. Lee, On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack, *Infocom*, 2001.

[7] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, Network Support for IP Traceback, *IEEE/ACM TON*, Vol. 9, no. 3, June 2001.

[8] J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the Source, *ICNP*, Nov. 2002.

[9] Mazu Networks Inc. http://www.mazunetworks.com

[10] Riverhead Networks Inc. http://www.riverheadnetworks.com

[11] H. Sun, W. Ngan, and H. J. Chao, "RateGuard: A Robust Distributed Denial of Service (DDoS) Defense System," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp.1-8, Nov. 30 2009

[12] M. C. Chuah, W. C. Lau, Y. Kim, and H. J. Chao, "Transient performance of PacketScore for blocking DDoS attacks," *2004 IEEE International Conference on Communications*, vol.4, no., pp. 1892- 1896 Vol.4, 20-24 June 2004

[13] R. Rojas-Cessa, E. Oki,Z. Jing, and H.J. Chao, "CIXB-1: combined input-one-cell-crosspoint buffered switch," *High Performance Switching and Routing, 2001 IEEE Workshop on*, pp.324-329, 2001

[14] R. Rojas-Cessa, E. Oki, and H.J. Chao, "CIXOB-k: combined input-crosspoint-output buffered packet switch ," *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE* , vol.4, no., pp.2654-2660 , 2001

[15] Z. Dong and R. Rojas-Cessa,"Long Round-Trip Time Support with Shared-Memory Crosspoint Buffered Packet Switch," *High Performance Interconnects, 2005. Proceedings. 13th Symposium on*, pp. 138- 143, Aug. 2005.

[16] Z. Dong and R. Rojas-Cessa,"NXG05-5: Shared-Memory Combined Input-Crosspoint Buffered Packet Switch for Differentiated Services," *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, pp.1-6, Nov. 27 2006