Priority Queue-based Scheme to Maintain Quality of Service for Normal Users Suffering from Large DDoS Attacks

Chu-Hsing Lin\textsuperscript{1}, Jung-Chun Liu\textsuperscript{2}, Chien-Ting Kuo\textsuperscript{3}
Department of Computer Science, Tunghai University, Taichung, 40704 Taiwan\textsuperscript{1, 2}
Networks & Multimedia Institute, Institute for Information Industry, Taipei City 105, Taiwan\textsuperscript{3}
\{chlin\textsuperscript{1}, jcliu\textsuperscript{2}\}@thu.edu.tw, ctkuo@nmi.iii.org\textsuperscript{3}

Abstract

In this paper we focus on alleviating malicious traffic from DDoS attacks since many famous websites have been attacked by them and massive losses have been reported in recent years. We propose a Priority Queue-Based scheme to analyze the interval of the arrival times of incoming packets in order to distinguish malicious traffic from normal traffic and to take care of malicious attacks clogging the network. We use the network simulator, NS2, to assess the efficiency of the proposed scheme. Simulation results show that the proposed Priority Queue-based scheme not only effectively decreases the flows of malicious packets from DDoS attacks with various packet rates, but also provides smooth and constant flows for packets sent by normal users. Furthermore, our priority queue-based scheme performs much better than other schemes when the number of the DDoS nodes becomes large.

Keywords: DDoS attack, network simulator, priority queue, QoS.

1. Introduction

With wide-ranging applications and services provided via the network environment, threats to the network become crucial issues nowadays. Numerous kinds of malicious attacks occur on the computer networks, such as SQL Injection, Worm, Trojan, and Distributed Denial-of-Service (DDoS) attacks. In this paper, we focus on defending the DDoS attacks because this type of network attacks has caused many famous websites enormous losses in recent years.

In the previous paper [1], we proposed a Priority Queue-Based scheme to analyze the interval of the arrival times of incoming packets to distinguish malicious traffic from normal traffic and to take care of malicious attacks clogging the network. But in [1], we just compared efficiency of our scheme with the Droptail queuing management algorithm. In this paper, two more experiment sets were conducted to assess the reliability of our priority queue-based scheme. The first experiment set compared our scheme with both Droptail and Random Early Detection (RED) queuing management algorithms under various packet rates; and the second set made comparison of these three schemes while increasing the amount of malicious sources. We used the network simulator, NS2, to verify the effectiveness of our proposed scheme. Simulation results show that the Priority Queue-based scheme not only is superior to DropTail and RED queuing algorithms in detecting and defending DDoS attacks, but also is able to alleviate a great number of malicious flows to maintain quality of service (QoS) for normal users.
2. Related study

Many network attackers employ a number of zombie computers to achieve the goals of bandwidth consumption attacks and resource starvation attacks. These two kinds of attacks belong to DDoS attacks and are very effective.

In the bandwidth consumption attacks, bandwidth of the victim server will be filled with a large number of malicious packets flows created by the zombie computers. The normal users are prevented from connecting with the victim server. The QoS of normal users is lost momentarily since they can not obtain services from the victim server. The bandwidth consumption attack often happens on e-commerce websites. One example of this type of attacks is the ICMP flooding attack.

In the resource starvation attacks, the hardware resources such as memory of the victim server are wasted by the malicious request packets. By exploiting the characteristic of the three-way handshake of TCP protocol, the malicious request packets may ask the victim server for some network service continuously, but the malicious attacker will not respond to the ACK packet from the victim server. By this way the three-way handshake of TCP protocol will be kept in unfinished states, and the resource of the victim server is kept idle. One example of this type of attacks is the SYN flooding attack.

To prevent network attacks, one may adopt methods such as firewalls [2] or intrusion detection system (IDS), which are effective for known attacks or known IP addresses. Other methods include packet filtering [3-5], packet marking, the reverse proxy detection method [6], and ICMP and Traceback [7~13] messages, which are effective for identifying sources of attacks to implement protection measures.

In this paper, we focus on the bandwidth consumption attacks and aim to classify packets as “normal traffic” and “malicious traffic” packets. We analyze the interval time of incoming packets and use the harmonic mean to identify the malicious traffic. The malicious traffic will be pushed into the low priority queue and get low priority services from the server. By this mechanism, the normal user will be able to obtain better QoS from the server.

3. Structure of the Priority Queue-based Scheme

Throughput is often used to assess quality of the network bandwidth in the network environment. From analysis of throughputs of normal and DDoS nodes, a Value of Harmonic Mean (VHM) is assigned to distinguish the normal packets from the malicious ones. Harmonic mean has been used in calculation of average of flows in statistics [14]. The flowchart of our scheme is shown in Figure 1. The records in the Database consist of:

1. Packet address
2. Packet arrival time
3. Average arriving time of the previous packet
4. Average arriving time of the current packet
5. Difference of harmonic means of incoming packets

Each time new incoming data entering the database, formula (1), and (2) are used to calculate the harmonic mean of the arrival time of incoming packets:

\[
H_{n2}(t) = \frac{2}{\frac{1}{t_1} + \frac{1}{t_2}} \quad (1)
\]
\[ H_{ij}(t) = \frac{2}{\frac{1}{t_i} + \frac{1}{t_j}} \]  

(2)

Where suffix \( ij \) indicates that the harmonic mean is for packets coming from the same address with arrival times \( t_i \) and \( t_j \).

The difference of harmonic means of the incoming packets is:

\[ H_{\text{avg}} \_ \text{diff} = H_{i23}(t) - H_{i12}(t) \]  

(3)

4. Experiment environment

We used the network simulator, NS2, to evaluate the effectiveness of the proposed scheme. We compared our scheme with Droptail and RED queuing management algorithms. In the first experiment we adjusted the DDoS packet rates, and in the second experiment we increased the DDoS nodes.

Figure 1. Flowchart of the Priority Queue-based scheme
The experiment environment is illustrated in Figure 2. The target server is connected to a router, which is connected to an external network consisting of four legal users and a group of zombie computers. The zombie computers on the same group can simultaneously launch DoS attacks to the target server to carry out DDoS attacks in the simulation environment.

In the simulation, every link is set up with 1 Mbps bandwidth. The limit of the queue of the priority queue-based scheme in the router is 20 Mbps. The total simulation time is set as 5056 seconds. The legitimate user at normal nodes starts sending packets at 0 second of simulation, with the time interval of incoming packets randomly set by a random number generator to emulate a realistic network environment. The malicious DDoS nodes start sending packets at 20 second of simulation. The average packet rate at each normal node is 100 kbps and the average packet rate in the first experiment of each DDoS node is changed from 0 kbps to 1000 kbps. In the second experiment, numbers of the malicious node are increased. As in [1], we set VHM be 0.07 in simulations.

![Figure 2. A network under DDoS attacks](image)

5. Experiment results

Average throughputs of normal nodes and DDoS nodes, under DDoS attacks by using DropTail, RED, or Priority Queue-based schemes as DDoS defending schemes, are shown in Figure 3 and Figure 4, respectively. From Figure 3, we observe that when the DDoS packet rate is increased, our priority-queue based scheme has better average throughput of normal nodes than the other two schemes. From Figure 4, we observe that when the DDoS packet rates are increased, our priority-queue based scheme allows less average throughput of malicious nodes than the other two schemes. We conclude that the priority-based scheme can effectively enhance QoS of normal users and reduce traffic of malicious users.
Figure 3. Average throughputs of normal nodes under DDoS attacks using DropTail, RED, and Priority Queue-based schemes

Figure 4. Average throughputs of DDoS nodes under DDoS attacks using DropTail, RED, and Priority Queue-based schemes
Figure 5 shows the experimental results when the number of DDoS nodes was varied. By adopting the priority-based scheme, when the number of DDoS becomes tenfold, average throughput for the normal nodes is very smooth and constant about 4,000 kbps (refer to the PQ Normal curve); while average throughput for the DDoS nodes is effectively alleviated (refer to the PQ DDoS curve). It obviously demonstrates that the priority queue-based scheme performs much better than DropTail and RED queuing management algorithms when the number of DDoS nodes becomes large.

6. Conclusion

Simulation results by using the NS2 network simulator show that the DropTail or RED queuing schemes are not very effective in alleviating flows of malicious packets under DDoS attacks. To solve this problem, we propose a Priority Queue-based scheme for defense of DDoS attacks. Simulations of the proposed Priority Queue-based scheme show that, when the number of DDoS nodes becomes large, it not only effectively alleviates the flows of malicious packets from DDoS attack nodes, but also provides smooth and constant flows for packets sent by normal users.

7. Acknowledgement

This work was supported in part by National Science Council under grants NSC-95-2218-E-001-001, NSC-95-2218-E-011-015, iCAST NSC96-3114-P-001-002-Y, NSC95-
8. References


Authors

Chu-Hsing Lin received both of his B.S. and M.S. degrees in applied mathematics from National Tsing Hua University and National Chung Hsing University, respectively. In 1991, he received his Ph.D. degree in computer sciences from National Tsing Hua University, Taiwan. Since then he has been a faculty of the Department of Computer Science and Information Engineering, Tunghai University. Dr. Lin is currently a professor and the chair of the CSIE department of Tunghai University. From 1995 to 1999, he has ever been the Director of the Computer Center of Tunghai. He has also been one of the Board Directors of the Chinese Information Security Association (CCISA) from 2001 till now. Dr. Lin has published over 50 papers in academic journals and international conferences. He has received over twenty project grants from government departments and private companies in recent years. In 2006, he was awarded the Outstanding Instructor Award of Master & Ph.D. Thesis by the IICM (Institute of Information & Computing Machinery). He was the winner of the 1991 Acer Long-Term Award for Ph.D. Dissertation. His current research interests include multimedia information security, wireless ad hoc networks, embedded systems applications.

Jung-Chun Liu received his B.S. degree in electrical engineering from National Taiwan University in 1990. He received M.S. and Ph.D. degrees from the Electrical and Computer Science Engineering Department at University of Texas at Austin, in 1996 and 2004, respectively. He is an assistant professor in the Computer Science Department at the Tunghai University, Taiwan. His research interests include digital signal processing, VLSI design, RF and microwave engineering, watermarking, embedded systems, and computer networks.

Chien-Ting Kuo received his B.S. and M.S. degrees in computer science and information engineering from Tunghai University in 2007 and 2009, respectively. Under the guidance of Professor Chu-Hsing Lin, he has already published one international journal paper and four international conference papers. The topics of his current research interests include network security and distributed denial of service. At now, he is working as a Research and Development engineer on the Institute for Information Industry in Taiwan.