Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks

Wei-Shen Lai ¹, Chu-Hsing Lin ², Jung-Chun Liu ², Hsun-Chi Huang ², Tsung-Che Yang ²

¹Department of Information Management, Chienkuo Technology University, Taiwan
²Department of Computer Science and Information Engineering, Tunghai University, Taiwan
¹WeiShenLai@gmail.com
²{chlin, jcliu, g922920, f946166}@thu.edu.tw

Abstract

Denial of service attacks occur when the attacks are from a single host, whereas distributed denial of service attacks occur when multiple affected systems flood the bandwidth or resources of a targeted system. Although it is not possible to exempt entirely from denial of service or distributed denial of service attacks, we can limit the malicious user by controlling the traffic flow. In the paper, we propose to monitor the traffic pattern in order to alleviate distributed denial of service attacks. A bandwidth allocation policy will be adopted to assign normal users to a high priority queue and suspected attackers to a low priority queue. Simulations conducted in network simulator of our proposed priority queue-based scheme shows its effectiveness in blocking attacking traffic while maintaining constant flows for legitimate traffic.

1. Introduction

Under distributed denial of service (DDoS) attacks, normal users are affected by attackers who use a number of Handlers to employ bandwidth consumption attacks such as IP spoofing, smurf and fraggle attacks, and resource starvation attacks such as SYN floods [1][2]. Common features of DDoS are observed as follows:

- Public networks are used as springboards
- Attackers are well camouflaged
- Packets sent by the attackers are flooding

To prevent attacks, one may adopt methods such as intrusion detection system (IDS) [3] or firewalls, which are effective for known attacks or IP addresses. Other methods including packet filtering, packet marking, and ICMP Traceback [4][5][6] messages, which are effective for identifying sources of attacks and instituting protection measures but are not easy to be deployed since they need supporting routers to maintain information regarding packets that pass through them. A pushback method [7] categorizes packets into “good traffic”, “bad traffic”, and “poor traffic” packets. It analyzes bad traffic packets and sends signals to upstream routers to control the flow of suspicious packets. If the router cannot correctly categorize packets, it affects flows of all packets through it. Since the normal packets are possible to use the same flow-controlled route to the server, the bandwidth allocated to normal users is also affected. Attacks on the networks, particularly, denial of service (DoS) and DDoS attacks, will paralyze services. We must protect the normal user by removing the malicious attacks on the network.
In this paper, we aim to get rid of malicious attacks clogging the network. We propose a Priority Queue-based scheme to protect bandwidths of normal users so as to improve effectiveness in network services and resources. A traffic factor is tuned to control the rate of the malicious flow and adjust the use of hardware resources. The Network Simulator, NS-2, is used to simulate DoS and DDoS attacks.

2. Priority Queue-based Scheme

For prevention of the DDoS attack [8][9][10][11], we consider the following key issues:
- The bandwidth in use by the network-- Use the bandwidth effectively, and pay attention to the instantaneous increase of the bandwidth
- Preventing IP spoofing
- Reducing loads of hardware resources -- the busy network might deprive available hardware resources.

In order to prevent normal users in an unsafe network from DoS or DDoS attacks, we propose a queuing algorithm for the network to achieve a better performance. By separating normal users from malicious users in view of the Average Packet Rate (APR), and balancing bandwidths according to bandwidth flows, Quality by User (QBU) is attained to safeguard the normal users. To provide smooth services, the network manages quality of service (QoS) by assigning highest priority to packets under service. Since any kind of service can be used as weapons to flood the network, it is not possible to determine beforehand which specific service is used for the DDoS attack. Usually packet flows of normal users are in small amount and in short time span, whereas packet flows of malicious users are in large amount and in long time span, which might flood the network and stop network providers from providing services to users.

For defense of DDoS attacks, we propose a priority queue-based scheme according to
1. Tracking of Intrusion Database (TID) – providing records of sources of attackers
2. Priority Queue Algorithm (PQA) – distinguishing normal users from malicious users to achieve flow controls
3. Traffic Factor Number of Packets – according to the provider’s system resources to adjust allocations of bandwidth
4. Management of queue – a priority queue method is adopted to send normal packets into the high priority queue and malicious packets into low priority queue. All packets in the priority queue have the privilege to be sent before any packets in the low priority queue.

For the priority queue-based scheme to be feasible, we need to correctly classify packets. Mistakes occur if normal packets are sent incorrectly to the low priority queue. PQA is used to tell normal packets from malicious ones. It divides time intervals in a very small unit, and the unit should to be small enough to be applied for classification of packets.

2.1. Structure of the Scheme

Based on the interval of transmission time of the incoming packet, a priority value is assigned to distinguish the normal or malicious packets. The block diagram for the structure of the scheme is shown in Fig. 1. The address classifier classifies locations of inbound flows of packets and provides TID with these data for further analyses and references. Records of TID consist of:
1. Packet address: recording locations where the current packet is coming from; information of locations furnishes the basis for packet tracking.
2. Packet arrival time: time for the current packet to enter the queue.
4. Average arriving rate of current packet: the harmonic mean of arrival rate of the previous packet.
5. Difference of harmonic means of incoming packets: the difference of the harmonic means of current and previous packets.

![Figure 1. Block diagram for the structure of the priority queue-based scheme](image)

Whenever TID has incoming data, the priority queue algorithm starts analyzing the data by appropriate division of time. Its analysis is based on the harmonic mean of the arrival rate of incoming packets.

The harmonic mean can be used to compute average velocity of varying speeds at a constant distance. On the other hand, the flow rate on a network is constant but the response time of packets is variable. When the network is flooded, the harmonic mean will no longer be varying but fixed at the allowable bandwidth, which indicating abnormal activities on the network.

In Figure 2, the harmonic mean of the arrival rate for incoming packets from the same source

$$H_{i12}(t) = \frac{2}{\sum_{i=1}^{2} t_i}$$ (1)  

$$H_{i23}(t) = \frac{2}{\sum_{i=2}^{3} t_i}$$ (2)

The difference of harmonic means of the incoming packets is

$$H_{\text{avg\_diff}} = H_{i12}(t) - H_{i23}(t)$$ (3)

TID takes records of all the incoming packets. Note that the amount of inflow is proportional to the difference of harmonic means $H_{\text{avg\_diff}}$ and all segments of networks have limited bandwidth. The difference of harmonic means of the incoming packets is computed whenever TID has incoming data.
Based on difference of harmonic means of the incoming packets, priority queue algorithm decides whether the incoming packet is normal or not, and then passes it in the high priority queue or low priority queue accordingly. Thus, packets from normal users will be sent to the high priority queue and have the priority of services. In contrast, packets from malicious attackers will be sent to low priority queue and will be delayed indefinitely.

2.2. Adaptive Adjustment of Priority Queue

The size of the priority queues affects the transmission time of packets. When malicious packets from attackers flood the entire bandwidth of one network, network hardware resources are in heavy demand. Since bandwidths of networks are growing faster than the upgrades of hardware resources, the malicious packets may stop services from the network providers. An adaptive mechanism to adjust priority queues is provided.

As shown in Fig. 3, the malicious packets from attackers are in the low priority queue, whereas the normal packets from normal users are in the high priority queue. The packets in the low priority queue may accumulate and keep the host busy all the time. Adaptively redirecting packets from the low priority queue into the high priority one will relax accumulation of packets in the low priority queue and speed up the handling of packets in the host. A traffic factor number is used to control the number of re-directed packets. We adaptively redirect packets if the total packets in the low priority queue divided by the factor number is less than the available space in the high priority queue.

![Figure 2. Difference of harmonic means of traffic](image)

**Figure 2.** Difference of harmonic means of traffic

\[ H_{\text{avg \_ diff}} = H_{t_{23}}(t) - H_{t_{12}}(t) \]

\[ H_{t_{12}}(t) \quad H_{t_{23}}(t) \]

\[ t_1 \quad t_2 \quad t_3 \]

**Figure 3.** Adaptive adjustment of priority queues with factor number = 2
3. Experiment Setup

In order to evaluate the effectiveness of the priority queue-based scheme, the Network Simulator, NS-2 [13], was used. NS-2 can simulate behaviors of queues, such as FIFO, RED, FQ [14], CBQ, etc. We added DoS and DDoS attacks into the simulation and investigated the efficiencies of the priority queue and the drop tail queue.

Fig. 4 shows the environment of a network under attacks, including ten source nodes, one main node, and one target node. Packets coming from four nodes, including node 2 to node 5, were from normal users, and packets coming from six nodes, including node 6 to node 11, were from attackers. All packets routed through the main node, node 0, and were sent to the target node, node 1.

It is very important to have an effective algorithm that responds very fast against attacks, since traffic flows of DDoS attacks are rather great. Our priority queue approach can efficiently compute and respond fast to attacks in the simulations. When the method is implemented in real-life networks, computational speeds of facilities of the networks need to be high enough to effectively defend attacks. We used tcl files and simulates in NS-2. In the tcl files, we describe the simulation environments, record the network status, and make them into graphs. For example, we defined the network bandwidth using the following line:

\[
\text{ns duplex-link node1 node2 10Mb 1ms DropTail}
\]

The priority queue-based scheme was used to control flows of packets from node 0 to node 1. There was a duplex link with bandwidth of 1 Mbps between these two nodes. In the NS-2 simulations, we used a bandwidth of 1Mbps and an average packet traveling time, $H_{avg_dif}$, of 0.07 second. Normal packets coming from node 2 to node 5 had flows of 100Kbps. Node 6 was used by a DoS attacker with a flow of 800Kbps. Node 7 to node 11 were used by DDoS attackers, each with a flow of 1Mbps.

![Figure 4. A network under DoS and DDoS attacks](image)

Figure 5 shows the progress of simulation:
1. At the beginning of simulation, we started sending packets from normal nodes, node 2 to node 5, each with a flow of 100Kbps and kept sending them until the end of simulation. From 0 to 10 second, only normal packets were sent on the network.
2. The packets from a DoS attacker with a flow of 800 Kbps were sent for a range of ten seconds, from 10 to 20 second of simulation.
3. The packets from DDoS attackers with a flow of 1MKbps were sent after 20 second of simulation.

![Figure 5. Progress of simulation](image)

4. Results

To evaluate the effectiveness of our proposed scheme, we compare the simulation results of our priority queue-based scheme with those of the DropTail queue scheme provided by NS-2.

Fig. 6 to Fig. 8 shows the results of the Drop Tail queue scheme, whereas Fig. 9 to Fig. 11 shows the results of the priority-based scheme.

The throughput (800 Kbps) of the DoS attack in Fig. 6, and throughputs (1Mbps) of DDoS attacks in Fig. 7 show that the DropTail queue cannot effectively block the malicious packets. Fig. 8 shows that DropTail queue cannot guarantee bandwidths required by normal users. There are obvious drops of throughput of normal packets at node 4 and node 5 at time of 10 second when the DoS attacker starts sending packets. Flows through DropTail queue at all normal nodes decrease to 0 Kbps about 20 second when DDoS attackers launch attacks.

The throughput (600 Kbps) of the DoS attack in Fig. 9, and throughputs (500 Kbps at nodes 7, 9, 10, 11, and 100 Kbps at node 8) of the DDoS attacks in Fig. 10 show that the priority queue effectively decreases the flow of the malicious packets.

Fig. 11 shows that priority queue safeguard bandwidths required by normal users. There are constant flows of normal packets at all normal nodes through the whole simulation time, in other words, the flows of the normal packets are sustained and the normal users are not affected by the DoS or DDoS attacks.
Figure 6. Throughput of DoS attack on DropTail queue

Figure 7. Throughputs of DDoS attacks on DropTail queue
Figure 8. Throughputs of normal traffic through DropTail queue

Figure 9. Throughput of DoS attack on priority queue
DDoS Nodes Network by Priority Queue

Figure 10. Throughputs of DDoS attacks on priority queue

Normal Nodes Network by Priority Queue

Figure 11. Throughput of normal traffic through priority queue
5. Discussion

NS-2 network simulator shows that the DropTail queue is not effective in alleviating flows of malicious packets under DoS and DDoS attacks. To solve this problem, we propose a priority queue-based scheme with an adaptive bandwidth allocation mechanism to defend DoS and DDoS attacks. Simulation results of the proposed priority queue-based scheme shows that it not only effectively decreases the flows of malicious packets from DoS or DDoS attackers, but also provides smooth and constant flows for packets sent by normal users.

6. Acknowledgement

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under grants NSC-95-2218-E-001-001, NSC-95-2218-E-011-015, iCAST NSC96-3114-P-001-002-Y, NSC95-2221-E-029-020-MY3, and NSC 97-2221-E-029-023.

7. References

Authors

Wei-Shen Lai received his B.S. and M.S. degrees in computer science and information engineering from Feng Chia University and National Chiao Tung University, respectively. In 2002, he received his Ph.D. degree in computer science and information engineering from National Chiao Tung University, Taiwan. In 2004, he has been a faculty of the Department of Information Management, Chienkuo Technology University. His current research interests include network security and cryptography.

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.

Hsun-Chi Huang received his M.S. degree in computer science and information engineering from Tunghai University in 2008. he has work experience in information security for more than ten years. The topics of his research interests include firewall, virtual private network, and certification authority. His current research focus on distributed denial of service, and intrusion detection system.
Hsung-che Yang is a graduate student in computer science and information engineering at Tunghai University, Taiwan. The topics of his research interests include firewall, cryptography, key management, multimedia, and energy analysis on embedded systems.