Provision of Quality of Service with Router Support

Hongli Luo
Department of Computer and Electrical Engineering Technology and Information System and Technology
Indiana University Purdue University Fort Wayne
Fort Wayne, IN, USA
luoh@ipfw.edu

Mei-Ling Shyu
Department of Electrical and Computer Engineering
University of Miami
Coral Gables, FL, USA
shyu@miami.edu

Abstract

The current Internet servers are susceptible to network attacks. The DDoS attacks consume the network bandwidth and degrade the services provided by the servers. This paper proposed a mechanism to provide security and quality of service (QoS) for a server pool with the support at the edge router. It focuses on the protection of the services based on the priority of different traffic flows and the anomaly degrees of the traffic. Anomaly traffic will be detected using a lightweight anomaly detection method. The result of anomaly detection is sent to the queue management component for resource allocation. Traffic flows are treated with different priorities. The multimedia flows are guaranteed the bandwidth allocation; while the bandwidth allocated for anomaly traffic flows are restricted according to the degrees of the anomaly. Simulation results demonstrate the improvement of service provision for the legitimate traffic flows under a DDoS attack.

1. Introduction

Network applications have different kinds of service requirements. Multimedia applications, such as video streaming and Voice over IP, can tolerate a certain degree of losses but are sensitive to delays. For non-real-time traffic flows, they can tolerate the delays but prefer a high throughput. The Internet is also susceptible to all kinds of the attacks and illegitimate traffic. Distributed Denial of Service (DDoS) can consume the bandwidth, degrade the service provided by the application server, or make the service unavailable. DDoS attacks are difficulty to identify since some malicious traffic can be made similar to legitimate ones. Hence, the legitimate traffic consuming too much network resources is not differentiated from the attacking traffic.

Quality of service (QoS) can be provided using Active Queue Management (AQM) at the router. In RED [5], the drop probability increases with the average queue length. RED works well for TCP flows but fails for unresponsive UDP flows. Class-Based Threshold (CBT) [10] avoids extreme unfairness among different traffics. It categorizes the traffic into three classes: TCP, multimedia UDP, and other UDP. It assigns a static threshold for each of the two UDP categories to regulate the UDP traffic. A dynamic CBT [4] extends CBT by regulate the average queue length of the UDP classes to their fair shares.

Differentiated service (DiffServ) was proposed to provide quality of service in the Internet [1], but it is too complicated and puts the burden on the Internet backbone routers. Resource regulation can be done at the end servers, so each flow can be allocated only a fair share of its resources. However, in DDoS attacks, the traffic from distributed clients are aggregated together to consume the bandwidth at the edge router, which degrades the quality provided for legitimate users. Servers are typically connected to the Internet through the edge router, for example, the servers belonging to an ISP. To mitigate the degradation of the quality of service resulted from distributed attacks, the traffic can be monitored at the ingress router. A coordinated distributed attack targeted at consuming the resource of the server pool can then be identified at the router.

Various research studies have been conducted to provide the quality of service under the network attacks. Some focused on defending DoS attacks with bandwidth restriction. [12] presented the router throttle

approach to protect a server system under DDoS attacks. The rate at which the upstream router can forward packets to the server is limited. The capacity of the server is allocated to the upstream routers in a level-k max-min fairness. In [10], the legitimate traffic is isolated and protected from a huge amount of DDoS attacks. The system can provide adequate service to more clients during DDoS attacks with the provision of adequate resource for legitimate traffic. [6] proposed a metric to classify traffic into different categories, and QoS protocol can use this metric to give different priorities to traffic flows of different categories.

Our approach uses a combination of anomaly traffic detection and bandwidth restriction to regulate the traffic. The purpose is to provide security and QoS for different traffic flows under the DoS attacks or anomalous traffic. The traffic going through the edge router is light compared with the core routers inside the Internet. The traffic monitoring and management at the edge router have a lower overhead in computation. The illegitimate traffic and attacking traffic can be detected. The bandwidth restriction is implemented at the edge router according to the anomaly degrees of the traffic flows. The bandwidth allocated to those traffic flows is proportional to the anomaly degrees. The differentiated services can then be provided by the edge router according to the priorities and the anomaly degrees of the traffic flows.

The paper is organized as follows. The overview of the proposed framework is presented in Section 2. We present the simulation results and analysis in Section 3. Conclusions are given in Section 4.

2. Provision of the Service with Router Support

Resource control and quality of service are closely related to each other. Some users request too many connections to aggressively consume the bandwidth. Regular active queue management (AQM) cannot differentiate those aggressive users to provide fair bandwidth allocation to each flow. The aggressive users can consume a large portion of the bottleneck bandwidth. Those traffics have a pattern that deviates from the normal traffic flows and can be considered as anomaly traffic. DoS attacks share some similarities with those anomaly traffics in terms of bandwidth consumption. It is not easy to strictly differentiate between DoS attacks and anomaly traffics. Hence, in our proposed approach, we utilize resource restriction to ensure that the attacking traffic and anomaly traffic can only consume a certain portion of network resources, so the legitimate applications can still receive an acceptable quality of service. The advantage of our proposed approach is that it does not require any modification on the server pools being protected.

Our proposed approach is composed of a lightweight traffic monitoring scheme and an active queue management (AQM) component. The calculation of dropping possibility is used in the AQM component.

2.1. The Lightweight Traffic Monitoring Scheme

A lightweight traffic monitoring scheme is implemented at the edge router. It monitors all the incoming and outgoing traffic flows of the edge router. The monitoring scheme targets at any unauthorized bandwidth usage resulted from anomaly traffic or DDoS bandwidth attacks. A lightweight data mining based anomaly detection method such as LOF [2] is used in anomaly traffic detection.

Anomaly detection needs a set of normal data to train the model. An anomaly is a pattern not observed in the normal data. The main idea of LOF is to assign a degree of being outlier to each data example. The degree is called LOF of the data example. LOF has a high detection rate when the false alarm rate is low. The LOF of an object can be computed using the following steps.

- Compute the k-distance neighborhood of each object P in the data set.
- Compute the reachability distance for each object P with respect to an object O.
- Compute the local reachability density of the object P.
- Compute LOF of an object P. An object P is considered to be an outlier if its LOF value exceeds a threshold value.

The KDD CUP 1999 data [8] is used as the training data set in anomaly traffic detection. This data set contains a wide variety of intrusions simulated in a network environment. Each connection in the data set is a sequence of packets with values of 41 features which are either basic features or derived features. The derived features can be the content features within a connection or traffic features computed using a two-second time window. Our anomaly traffic detection scheme only targets at the traffic that consumes too much bandwidth. To reduce the computation and speed up the detection of the anomaly traffic, only features related to the bandwidth attacks will be selected.

For the incoming traffic arriving at the edge router, every connection is monitored and features are extracted as defined in the KDD data. The features are used to construct a record for each connection. LOF is performed on the record to calculate the value of LOF for each connection.

A metric, anomaly degree, is defined here to indicate the possibility of a connection being an anomaly. A higher anomaly degree means the larger deviation the connection is from the normal traffic. The value of anomaly degree is between 0 and 1. The LOF values of all the connections in the training data set are sorted in an ascending order to construct an array *lof_th* which is divided into 100 segments. Each segment consists of an equal number of elements. The obtained LOF for each monitored connection is compared with the beginning value and ending value in each segment of *lof_th*, starting from the first segment. If the LOF value falls into the segment *i*, the anomaly degree of this LOF is *i*/100.

A higher anomaly degree means the connection is using the bandwidth in a pattern quite different from the normal traffic. This connection can belong to a DoS attack, or the user of this connection consumes the bandwidth too aggressively and can be considered as illegitimate. To provide fair services for other traffic, the connections that consume too much bandwidth should be allocated only limited bandwidth. After the anomaly degree is obtained, its value and the related flow information will be sent to the active queue management component and thus the corresponding actions can be taken at the edge router. Flow id, source address, and destination address can all be used to identify a connection at the router.

In our proposed approach, when the anomaly degree is larger than 96%, the traffic is considered an attack. The server will then be notified to cutoff any traffic from the attacking source. Future connection requests from the attacking source will be rejected. Instead of determine whether a connection is an attack or not, we are interested in the anomaly degree of the connection which is a measure indicating whether the connection uses the network bandwidth in a normal and fair manner. This is the difference between our proposed approach and other existing methods.

2.2. The Active Queue Management (AQM) Component

In the queue management at the edge router, only one physical queue is maintained. The capacity of the physical queue is divided into 3 isolated virtual queues according to the classes of the traffic. All packets are enqueued and dequeued in a FIFO way. In our proposed approach, traffic flows are categorized into different classes based on their priorities, service requirements, and anomaly degrees. There are three classes, namely the multimedia traffic, other normal traffic, and anomalous traffic. The multimedia flow is given the highest priority in bandwidth allocation. The bandwidth restriction is implemented via packet dropping at the router. The calculation of the dropping probability can also be applied to the calculation of the marking probability.

2.3. Dropping Probability

The edge router monitors the traffic and sends the anomaly detection results to the AQM component. The edge router then uses the packet dropping rate to regulate the anomalous traffic. The AQM component calculates the dropping probability for the traffic flow according to its anomaly degree. This results in better resource utilization and better QoS for different traffic flows.

For the anomalous traffic, the anomaly degree, source and destination address, and flow id will be provided to identify the flow. When a packet arrives, it is classified as being multimedia traffic, other normal traffic, or anomaly traffic.

The purpose of queue management at the edge router is to guarantee the service of multimedia traffic, restrict the bandwidth for anomalous and attacking traffic, and provide fair bandwidth sharing among normal TCP traffic flows. The appropriate dropping probability of packets for each traffic flow is discussed below.

1) Multimedia traffic.

Multimedia traffic has a strict requirement on the delay. We are interested in both dropping rates and the queue length. The increase of the dropping rate is related to the decrease of the queue length, and results in a reduced delay. The queue length for multimedia traffic must be between *max_th_mm* and *min_th_mm*. If the *max_th_mm* is too large, the queueing delay can be excessive. If it is set too low, the bandwidth will be underutilized and packet loss can be very frequent.

Queue length is an indication of delays. To avoid excessive delays, the queue length should also be bounded. The minimum queue length is specified by the service negotiation between the ISP and the users. The negotiated service decides the *min_th_mm* and *max_th_mm* of multimedia flows.

The dropping probability *p* is calculated according to the queue length and packet loss rate to ensure that the previously negotiated service can be guaranteed. The length of the queue for multimedia flow is decided not only by the current queue length but also by the service rates. Service rates are the rates used to transmit packets out of the queue. Probability dropping of multimedia flow happens only when the following two conditions are true: 1) the average queue length is larger than the maximum queue length; and 2) the allocated capacity for a multimedia flow is larger than the incoming rate of the multimedia flow.

The dropping probability of a multimedia flow is calculated as shown in Equation (1).

$$p_{mm} = \frac{qavg\_mm - min\_th\_mm}{max\_th\_mm - min\_th\_mm} * \frac{y(t) - c(t)}{y(t)} \quad (1)$$

where *qavg_mm* is the average queue length of the multimedia flow, *max_th_mm* and *min_th_mm* are the maximum queue length and minimal queue length allocated for the multimedia flow, *y(t)* is the input rate of the multimedia flow, and *c(t)* is the link capacity for the multimedia flow. The multimedia application at the server has congestion control which acts on the detection of the packet loss. The server reduces the transmission rate to alleviate the network congestion and to provide an acceptable level of video quality [7].

2) Normal traffic.

The normal traffic shares the remaining queue occupancy and bandwidth. The normal traffic uses the queue capacity and bandwidth that are not used by the multimedia traffic. If the average queue length for the normal traffic is larger than *max_th_normal*, the packet will be dropped. If the average queue length is larger than the *min_th_normal* and smaller than the *max_th_normal*, the packet will be dropped with a probability. The value of *max_th_normal* is set as follows.

$$max\_th\_normal = max\_th - cur\_len; \quad (2)$$

where *max_th* is the maximum length of the physical queue and *cur_len* is the current length of the physical queue. If a packet is not dropped, it will be subject to the dropping probability of RED before it is passed to the physical queue. In this way, all the normal traffic flows share the available bandwidth in a fair way.

3) Anomaly traffic

For traffic with different anomaly degrees, the bandwidths allocated to them are limited by the dropping probability. The dropping probability according to the queue length only will favor the traffic with a large number of connections. The anomaly traffics launch a large number of connections. Although each connection occupies a small portion of the bandwidth, the aggregate traffic can consume lots of bandwidth. Traffic with a larger anomaly degree should have a higher dropping probability to reduce the bandwidth the aggregate traffic occupies, which is considered as the penalty dropping. To provide a fair bandwidth sharing with normal traffic, the penalty dropping probability of anomaly traffic increases exponentially with the anomaly degree. The penalty dropping probability *d(α)* for anomaly degree α is defined as given in Equation (3).

$$d(\alpha) = 1 - \beta^{-\lambda * \alpha}, \quad (3)$$

where $\beta > 1$ is a constant. The values of β and λ are chosen so that when α approaches 1, the dropping probability approaches 1, too. When α is equal to 1, the flow is identified as an attack. All of the packets belonging to this flow must be dropped. If a packet is not dropped, similar to the normal traffic class, it will be subject to the dropping probability of RED before it is put in the physical queue. Table 1 presents the pseudo code of the proposed AQM component.

Table 1. The proposed AQM component

```
When a packet arrives,
    Categorize the packet into one traffic class.
If multimedia traffic,
    Calculate the dropping probability p_mm;
    If not dropped, put in the physical queue.
If normal traffic,
   Set max_th_normal;
   Calculate the dropping probability using RED;
    If not dropped, put in the physical queue.
If anomaly traffic,
    Calculate the penalty dropping probability d(α);
    If not dropped,
       Calculate the dropping probability using RED;
       If not dropped, put in the physical queue.
```

3. Simulation Results

To evaluate the performance of the proposed approach, the simulations are run in a prototype system implemented using NS2 [9]. The prototype system integrates the lightweight traffic monitoring scheme (including anomaly traffic detection) and the active queue management (AQM) component at the edge router. The server pool of an ISP is simulated. The network topology used in the simulation is displayed in Figure 1.

3.1. Simulation Setup

As can be seen from Figure 1, there are video streaming server, ftp server, and web server inside the server pool. These servers provide the basic services in the Internet, and also have different quality of service requirements. The resulting traffic consists of both TCP and UDP flows. All the traffic flows destined to the servers will go through the edge router. The attackers can launch a large volume of traffics from the

distributed clients to connect to a server inside the server pool. The attacking traffics go through the edge router and consume the bandwidth, thus degrading the services provided by each of the servers behind the edge router. Traffic monitoring and resource allocation are implemented at this edge router to protect the security and service for the server pool.

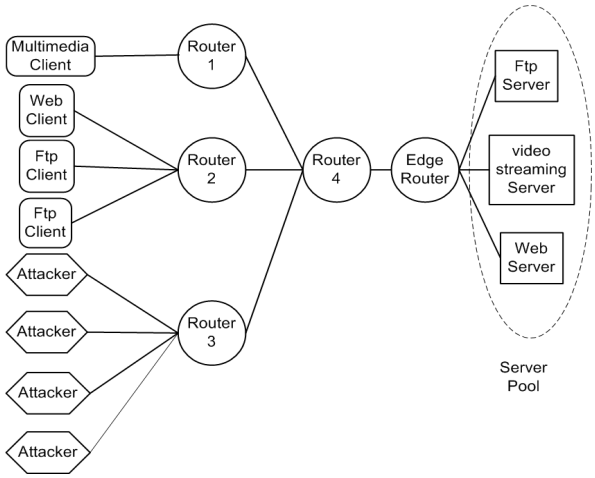
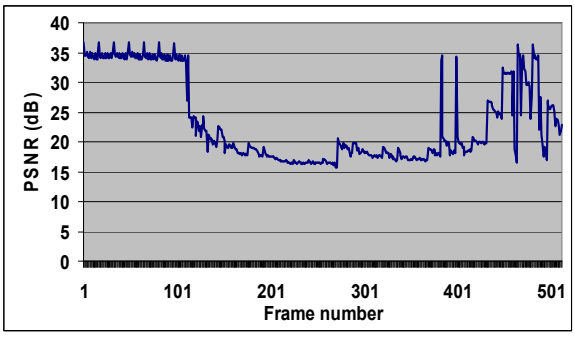


Figure 1. Network topology used in the simulation

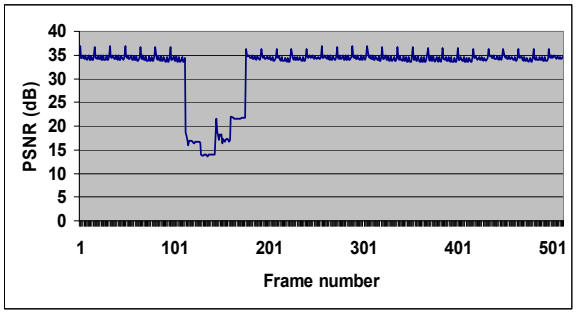
In this network topology, we define the link between Router 4 and edge router as the bottleneck bandwidth. The ftp clients send requests to the ftp server, the Web clients connect to the web server, and the multimedia clients connect to the video streaming server. This generates a variety of traffic flows in the network. One of the attackers is randomly selected to launch the DoS attacks. Each attacker can have simultaneous multiple connections to the servers. The purpose of the attacks is to create a large amount of traffic flows that traverse the edge router to consume the bottleneck bandwidth. This will degrade the services provided by the servers. There are both ftp and udp traffic flows through the edge router, and they should be subject to the resource management mechanism implemented at the router. The standard CIF video sequence Mobile & Calendar is used as the testing video. The training data set consists of 4,000 records selected from the KDD training data set.

3.2. Simulation Results and Analysis

In the simulation, we investigate how the anomaly traffic detection and bandwidth restriction can improve the services for the legitimate users. Both the perceived quality of multimedia services and ftp services are compared between our approach and the RED active queue management.



(a) PSNR values under RED



(b) PSNR values under our approach

Figure 2. Comparison of the PSNR values of received video between RED and our approach

3.1.1. PSNR values of video. The PSNR values of the received video at the client are presented in Figure 2 to demonstrate the quality of multimedia services. The active queue management used in Figure 2(a) is RED, where the average PSNR value of the displayed frames is 23.4 dB. Figure 2(b) displays the PSNR values of the video when the proposed anomaly based bandwidth restriction is used. The average PSNR value of our approach is 32.3 dB, with an improvement of more than 8 dB when comparing to the PSNR values obtained RED. The anomalous traffic started at around the time when Frame 101 was played. Both approaches maintain high PSNR values before the anomalous traffic starts, and then have a degradation of video quality because the anomalous traffic consumes the bottleneck bandwidth. As can be seen from this figure, in our approach, the anomalous traffic can be soon detected, and the edge router begins to drop the anomalous traffic according the anomaly degree. The bandwidth is then efficiently protected for the legitimate traffic, so the PSNR values are recovered and thus the provision of quality of service for the multimedia flow is guaranteed under the anomalous traffic attacks. On the other hand, RED has continuous degradation of video quality with low PSNR values.

3.1.2. Downloading time for the normal ftp connection. Downloading times for the normal ftp connections starting at different times are compared and shown in Figure 3. The smaller the downloading time, the higher throughput the ftp connection can achieve. The solid line is for RED; whereas the dashed line is for our approach. As can be seen from this figure, the downloading time increases when the anomalous traffic begins and it decreases when the anomalous traffic stops. In our approach, when the anomalous traffic is detected, the bandwidth allocated to this anomalous traffic is restricted, so the service for legitimate ftp traffic can be effectively protected.

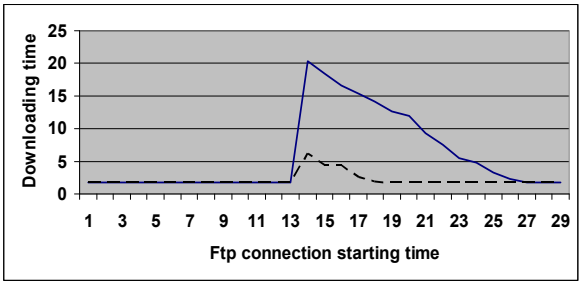


Figure 3. Comparison of downloading time for normal ftp connections between RED and our approach

4. Conclusions

This paper addresses the problem of how to provide differentiated quality of service with the support of active queue management at the edge router during DoS attacks. A traffic monitoring and anomaly detection scheme is implemented at the edge router. Bandwidth restriction will be enforced on different traffic flows with different anomaly degrees. The multimedia traffic will be allocated bandwidth with a higher priority. The bandwidth restriction is performed via packet dropping at the router. The packet dropping rate is proportional to the anomaly degree of the traffic. By restricting the bandwidth for anomalous traffic and attacking traffic, the bandwidth can be effectively saved for the legitimate traffic. The multimedia streaming can provide a higher video quality, and the non-real time application can achieve a higher throughput. Simulation results demonstrate that the quality of service of the legitimate applications can be provided under DoS attacks in our proposed approach.

5. References

[1] S. Blake, et al. "An Architecture for Differentiated Services,", *RFC 2475*, Dec. 1998.

[2] M.M. Breunig, H.-P. Kriegel, R. Ng, and K. Sander, "LOF: Identifying Density-Based Local Outliers," *Proc. of the ACM SIGMOD Conference*, pp. 93-104, Dallas, Texas, 2000.

[3] S. Chen and Q. Song, "Perimeter-Based Defense against High Bandwidth DDoS Attacks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 16, No. 6, July 2005, pp.526-537.

[4] J. Chung and M. Claypool, "Dynamic-CBT and ChIPS – Router Support for Improved Multimedia Performance on the Internet", *Proceedings of the eighth ACM international conference on Multimedia*, pp. 239-248, Marina del Rey, California, 2000.

[5] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance", *IEEE/ACM Transactions on Networking*, vol. 1, No. 4, August, 1993, pp. 97-413.

[6] S. Hariri, G. Qu, R. Modukuri, H. Chen, and M. Yousif, "Quality-of-Protection (QoP) – An Online Monitoring and Self-Protection Mechanism," *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 10, October 2005.

[7] H. Luo, M.-L. Shyu, and S.-C. Chen, "Video Streaming over the Internet with Optimal Bandwidth Resource Allocation", *Multimedia Tools and Applications*, Vol. 40, No. 1, October, 2008, pp. 111-134.

[8] KDD Cup 1999 Data (available on August 2008), http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[9] http://www.isi.edu/nsnam/ns/. Network Simulator, 2008.

[10] M. Parris, K. Jeffay, and F. D. Smith, "Lightweight Active Router-Queue Management for Multimedia Networking", *Multimedia Computing and Networking, SPIE Proceedings Series*, Vol. 3020, San Jose, CA, January 1999.

[11] J. Xu and W. Lee, "Sustaining Availability of Web Services under Distributed Denial of Service Attacks", *IEEE Transactions on Computers*, Vol. 52, No. 2, February 2003, pp.195-208.

[12] D. K. Y. Yau, J. C. S. Lui, F. Liang and Y. Yam, "Defending against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles", *IEEE/ACM Transactions on Networking*, vol. 13, No. 1, February 2005, pp. 29 – 42.