DIFFERENTIATED SERVICE PROTECTION OF MULTIMEDIA TRANSMISSION VIA DETECTION OF TRAFFIC ANOMALIES

Hongli Luo[1] and *Mei-Ling Shyu*[2*]

[1]Department of Electrical and Computer Engineering Technology
Indiana University – Purdue University Fort Wayne, Fort Wayne, IN 46805, USA
[2]Department of Electrical and Computer Engineering
University of Miami, Coral Gables, FL 33124, USA
luoh@ipfw.edu, shyu@miami.edu

ABSTRACT

Multimedia transmission over the Internet has its quality of service (QoS) requirement. However, Denial-of-Service (DoS) attacks launch large volumes of traffic and consume network bandwidth, thus degrading the quality of the delivered multimedia service. In this paper, we present a differentiated service protection framework consisting of anomaly traffic detection and resource management. Data mining based anomaly traffic detection is implemented at the host; whereas resource management is responsible for the allocation of network resources to the applications. Based on the deviation of the monitored traffic to the normal traffic, differentiated resources are allocated to the traffic. When suspicious traffic is detected, multimedia transmission reacts proactively via adjusting the transmission rate, which can avoid possible packet loss resulting from DoS bandwidth consumption, and thus provide better QoS. The impact of the traffic anomalies on the legitimate services can be mitigated, and the legitimate services can be protected. Simulation results show that better PSNR can be achieved for multimedia transmission during an attack in our proposed framework.

1. INTRODUCTION

Multimedia transmission over the best effort Internet is susceptible to network Denial-of-Service (DoS) attacks or high bandwidth distributed Denial-of-Service (DDoS) attacks, which the malicious users attempt to launch the attacks to exhaust the network resources. DoS attacks can completely occupy the resources of a server, which prevents legitimate users from accessing the services. DoS attacks can also deplete the link bandwidth by injecting the traffic into the router with a high rate. It causes the packets of legitimate traffic being dropped at the router queue due to congestion control. The resulting packet loss will degrade the quality of transmitted video streams. A reliable server should be able to block the attacking traffic or limit the resource consumed by the possible illegitimate traffic, while guaranteeing the resources for the legitimate traffic. Therefore, how to maintain quality of service (QoS) and protect multimedia traffic from the illegitimate users during the DoS attacks is an important issue in Internet transmission. For this purpose, several approaches have been proposed in the literature. As an example, the DDoS attacks were viewed as a resource management problem and implemented via congestion control at the router [2][7], which involves network support. Quality-of-Protection routing is proposed in [8] to protect against network attacks and reduce the impact of the attacking traffic. Moreover, intrusion detection [3] is employed to secure the service under network attacks. An intrusion detection system (IDS) can detect the possible attacks or abnormal network activities and signal an alert. Data mining techniques provide a promising solution to detect the abnormal traffic. Anomaly detection approaches build models from the normal data, and any deviation from the normal model in the new data is detected as anomaly. Anomaly detection has the advantage of detecting new types of attacks, while suffering from a high false alarm rate.

In our earlier study [5], we proposed a secure and adaptive multimedia transmission framework to provide a better QoS protection based on attack detection. In this paper, the focus is on the integration of anomaly traffic detection and adaptive transmission management to provide differentiated services for traffic according to its deviation from the normal traffic. The purpose is to provide a better service for multimedia transmission and mitigate the impact of the attacking traffic. In this manner, the security of both host and network resources can be achieved.

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

* For Mei-Ling Shyu, this research was supported in part by NSF ITR (Medium) IIS-0325260.

2. DIFFERENTIATED SERVICE PROTECTION FRAMEWORK

2.1 Anomaly Traffic Detection

The tasks that the anomaly traffic detection component handles include 1) traffic data collection, 2) data preprocessing, 3) incoming traffic monitoring, and 4) anomaly detection. In anomaly detection, a set of normal data is used to train the model. Anomaly can be defined as those patterns not observed in the normal data set. To detect anomaly from a new set of test data, the detection algorithm needs to decide whether the test data is normal or abnormal. The anomaly traffic detection is designed to target for the detection of selected types of network intrusion, mainly DoS and network Probe attacks. LOF [1] is employed as the anomaly detection approach since LOF has high detection rates when the false alarm rate is larger than 2% [3].

Features such as the start time and duration, source and destination IP addresses and ports, and protocol type are selected and extracted from the network data. The header information of the packets and some information of the payload are also extracted to construct the statistics of the connection. Since DoS and probing usually make a large number of connections to the host within a period of time from several seconds to several hours, time interval features are also collected to detect these two attacks. After the features are extracted from the processing of the incoming traffic, they are used for anomaly detection. The selection of the features should also be able to reduce the computation cost and achieve a high detection rate. KDD CUP 1999 data [6] were used as the training data set. There are 22 attack types in the training data. Among the original 40 features, 30 of them are selected for anomaly detection, which includes 23 numerical features and 7 nominal features. Different attack types have different important features. For DoS attacks, the important features include count, srv_count, dst_host_srv_serror_rate, serror_rate and dst_host_same_src_port_rate, source bytes and destination bytes [6].

For the incoming traffic to the server, every connection is monitored and kept as a record. When a connection ends, its statistics information is generated for the connection. Based on the statistics information, the selected features are extracted. LOF is performed on the features for each connection record and calculates a distance metric. This distance indicates the deviation of the current record from the normal traffic activity. The larger the distance metric is, the farther the traffic is deviated from the normal traffic. According to the metric calculated for each connection, the traffic is categorized into three traffic classes: normal traffic, suspicious traffic, and attack traffic. Two threshold values, θs and θa, are defined in which θs < θa. θa can be obtained from the training data set.

- If the distance is smaller than θs, the flow belongs to normal traffic.
- If the distance is larger than θs and smaller than θa, the flow is categorized as suspicous traffic. The flow may be from a suspicious node intended for a possible attack.
- If the distance calculated is larger than θa, the flow is categorized as attack traffic.

2.2 Differentiated Service for Multimedia

An adaptive video streaming mechanism was previously proposed in [4]. The transmission rate for multimedia transmission is based on the network delay, buffer occupancy, and playback rate of the video streams. A packet scheduling scheme decides which packets to send to achieve a better presentation quality at the client. A suitable sequence of the transmission rates R_k can be obtained by minimizing the quadratic performance function shown in Equation (1). The purpose of minimizing J_k is to maximize buffer occupancy and minimize bandwidth allocation.

$$J_k = (w_p Q_{k+d_0} - w_q Q_r)^2 + (w_r R_k)^2, \qquad (1)$$

where w_p, w_q, and w_r are the weighting coefficients, Q_r is the allocated buffer size for each client, Q_k denotes the number of packets in the client buffer at the beginning of time interval k, and $d_0 \geq 1$ indicates the network delay. That is, a change of R_k will result in a change of Q_{k+d0} some time interval later. Furthermore, congestion control was implemented via adjusting w_r within [w_r_min, w_r_max] range. A larger w_r will reduce R_k to a smaller value. Under the constraint of R_k, in order to further improve the video quality, a multi-buffer packet scheduling scheme at the source gives a higher priority to those packets of a higher importance. In a compressed video, a GOP (group-of-picture) is composed of I, B, and P frames, which packets from different frames have different effects on the reconstructed video sequences. Hence, packets of a higher importance level should be sent in a higher priority to maximize the presentation quality of the decoded video. This is achieved by developing multiple buffers with different importance levels to hold packets with corresponding importance levels.

The focus of this paper is to provide differentiated services according to the deviation of traffic from the normal traffic. For multimedia transmission, when suspicious traffic or attacking traffic is detected, multimedia transmission takes proactive actions to adjust its transmission rate to avoid possible packet loss resulting from DoS bandwidth consumption. Anomaly traffic detection is performed on each connection. Based on the traffic class, the resource management component provides differentiated services. If the calculated distance metric of the connection is larger than θs, the connection is diagnosed as suspicious traffic. Instead of blocking the traffic immediately, an alert is signaled and sent to the adaptive

transmission management component. In response to this, the values of w_r_max and w_r_min for w_r in Equation (1) are changed to larger values so that the multimedia transmission rates will be adjusted to a lower range. If the calculated distance metric of the connection is larger than θa, the connection is diagnosed as attacking traffic. The attacking traffic will be blocked immediately. Here, we assume the source addresses of the attacking traffic are known, and hence IP spoofing is not considered. The source node of this connection is registered as an attacking node. The current traffic from the attacking node will be discarded. Any future connection request from this attacking node will be rejected. When the attacking traffic from all of the registered attacking nodes is cut off, the anomaly detection component sends a signal to the adaptive transmission management component. The w_r_max and w_r_min values will be reset to the original values, which results in the multimedia transmission rates being adjusted in a larger range.

3. SIMULATION RESULTS AND ANALYSIS

The simulations are run in a prototype system integrating anomaly traffic detection and resource management at the server. This prototype system was implemented using NS2.

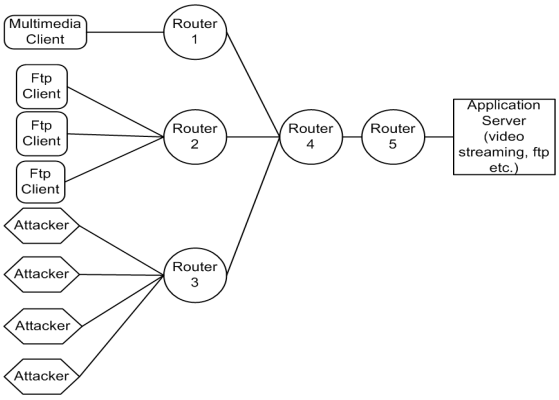


Figure 1. Network topology used in the simulation.

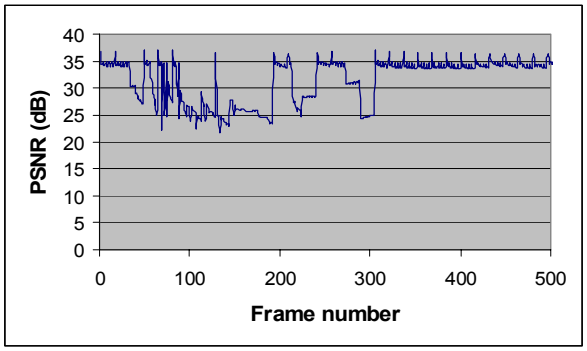
3.1 Simulation Setup

A scenario to simulate an Internet host is used, where an application server can provide video streaming and FTP services. The network topology of the network is presented in Figure 1, where the link between Router 4 and Router 5 is the bottleneck link. All the traffic need to go through this bottle link. The multimedia client requests video streaming services from the multimedia server. Three FTP clients are randomly selected to connect to the application for file transmission. Each time, one of the 4 attack clients is randomly selected as the attacker to launch the DoS attack. The purpose of the DoS attack generated by the attackers is to consume the bottleneck bandwidth. Both of the legitimate FTP traffic and attack traffic conform to TCP congestion control and share the bandwidth equally. The legitimate ftp clients will compete for the bandwidth with the attack ftp traffic. Standard video test sequences, Mobile & Calendar, are used for video streaming.

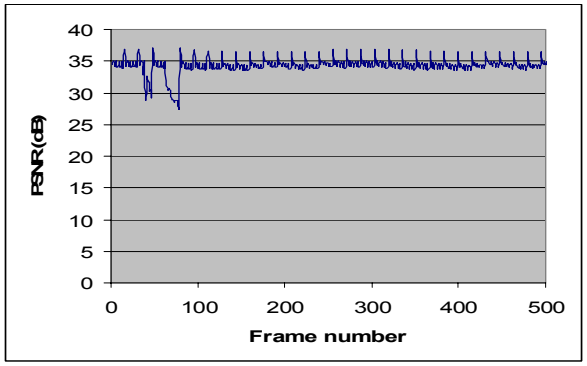
The attack traffic is generated with a large number of connections to the server in a short time. This is a bandwidth consumption attack where a few attacker machines will consume the bandwidth. Since the attack traffic and legitimate traffic conform to TCP congestion control, both normal connection and attack connection get the equal share of the bandwidth. The consequence is that legitimate traffic is unable to compete with the attack flood traffic, and the service it receives will be degraded.

3.2 Performance evaluation

In the simulation, we examine how the interaction between the anomaly traffic detection and adaptive transmission management components can effectively protect QoS for the legitimate user in the delivery of multimedia services when anomaly traffic is detected. First, two cases are studied to see the advantages of our resource management approach.



(a) Without resource management



(b) With resource management

Figure 2. PSNR values of the received video using adaptive video streaming with/without resource management.

The Peak Signal-to-noise Ratio (PSNR) metric is used to evaluate QoS. In Figure 2(a), attacking traffic is blocked after the detection, while in Figure 2(b), video transmission service is regulated by differentiated resource management. A DoS attack will result in bandwidth consumption and network congestion. Video transmission reduces its sending

rate in response to the detection of a possible abnormal traffic to avoid the possible degradation of QoS. As can be seen from the decreased PSNR values in both Figures 2(a) and 2(b), the qualities of the video are degraded due to the drastically reduced available bandwidth for multimedia transmission caused by the attacking traffic during an attack. However, in Figure 2(b) which shows the video quality under resource management, PSNR can always be maintained at a higher level. When a possible DoS attack is detected in its initial stage, the server reduces the transmission rate for the multimedia client so that the average PSNR values can be maintained at a higher level than in Figure 2(a). In both cases, the DoS attacks are detected after a period of time. The connections of the attack clients are therefore refused, and the bandwidth resource can be saved for multimedia streaming, so that the PSNR values in both figures are maintained at a high level in the later frames. The provision of the streaming service can then be guaranteed. We also calculated the average PSNR value of the displayed frames is 31.40 without resource management, and is 34.07 with resource management. A performance improvement of 2.67 dB can be achieved with our proposed framework..

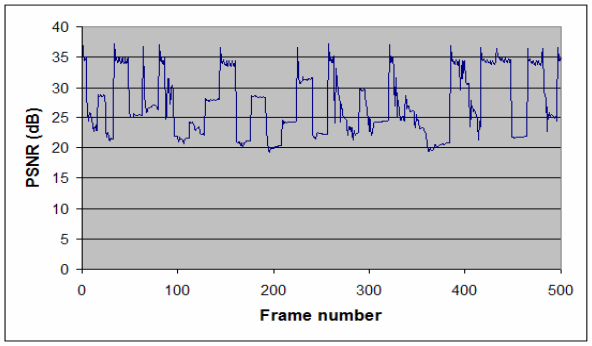


Figure 3. PSNR values of received video using PLUS streaming approach.

Comparison is also made with an existing streaming approach PLUS [9] under the same network scenario with anomaly traffic detection at the server. As can be seen from the Figure 3. The PSNR values of PLUS have continuous degradation of quality because of the attacking traffic. The average PSNR of the video frames of PLUS is 27.30 dB. An improvement of 6.77 dB of the video quality demonstrates the advantage of the proposed framework. Our framework can efficiently mitigate the impact of the attacking traffic and protect the video quality.

4. CONCLUSIONS

Denial-of-Service (DoS) can degrade QoS of multimedia transmission via launching a large volume of traffic into the network. Attack detection and active response to the attacks can mitigate the impact of DoS to provide better QoS. In this paper, we investigate how to provide differentiated resource allocation when anomaly traffic is detected. Actions are taken for traffic flows according to its deviation from the normal traffic. Resource management takes proactive actions to reduce the degradation of the video quality. The prototype of the proposed system is implemented. It includes attacking traffic generation, feature extraction, anomaly detection, and differentiated service provision. Via the early detection of incipient DoS and the interaction with the resource management, QoS of multimedia transmission can be better protected. Simulation results demonstrate the efficiency of our proposed differentiated service protection framework for multimedia transmission.

6. REFERENCES

[1] 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.

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

[3] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur and J. Srivastava, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection," *Proc. of the Third SIAM Conference on Data Mining*, San Francisco, CA, USA, May 2003.

[4] H. Luo, M.-L. Shyu, and S.-C. Chen, "A Multi-Buffer Scheduling Scheme for Video Streaming," *Proc. of the IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1218-1221, Amsterdam, The Netherlands, July 6-8, 2005.

[5] H. Luo and M.-L. Shyu, "The Protection of QoS for Multimedia Transmission against Denial of Service Attacks," *Proc. of the First IEEE International Workshop on Security and Pervasive Multimedia Environments (MultiSec 2005)*, in conjunction with the IEEE International Symposium on Multimedia (ISM 2005), pp. 695-700, December 12-14, Irvine, California, USA.

[6] KDD Cup 1999 Data (available on January 2007), http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[7] R. Mahajan, S. Bellovin, S. Floyd, J. Joannidis, V. Paxson, and S. Shenker, "Controlling High Bandwidth Aggregate in the Network," *Computer Communications Review*, 2001.

[8] 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.

[9] M. Mielke, R. Aygun, Y. Song, and A. Zhang, "PLUS: Probe-Loss Utilization Streaming Mechanism for Distributed Multimedia Presentation Systems," *IEEE Transactions on Multimedia*, Vol. 4, No. 4, pp.561-577, December 2002.