

A collection of military medals and a compass on a wooden surface. The medals include a red ribbon with a circular emblem, a blue ribbon with a circular emblem, and two silver Maltese crosses with gold centers. A pair of gold-rimmed glasses is also visible. A compass is in the bottom left corner.

Admission Control with Resource Management for Mitigating Degrading DDoS Attacks

A NISSC Fall 2003 Project

Xiaobo Zhou

C. Edward Chow

Yu Cai

Ganesh Godavari

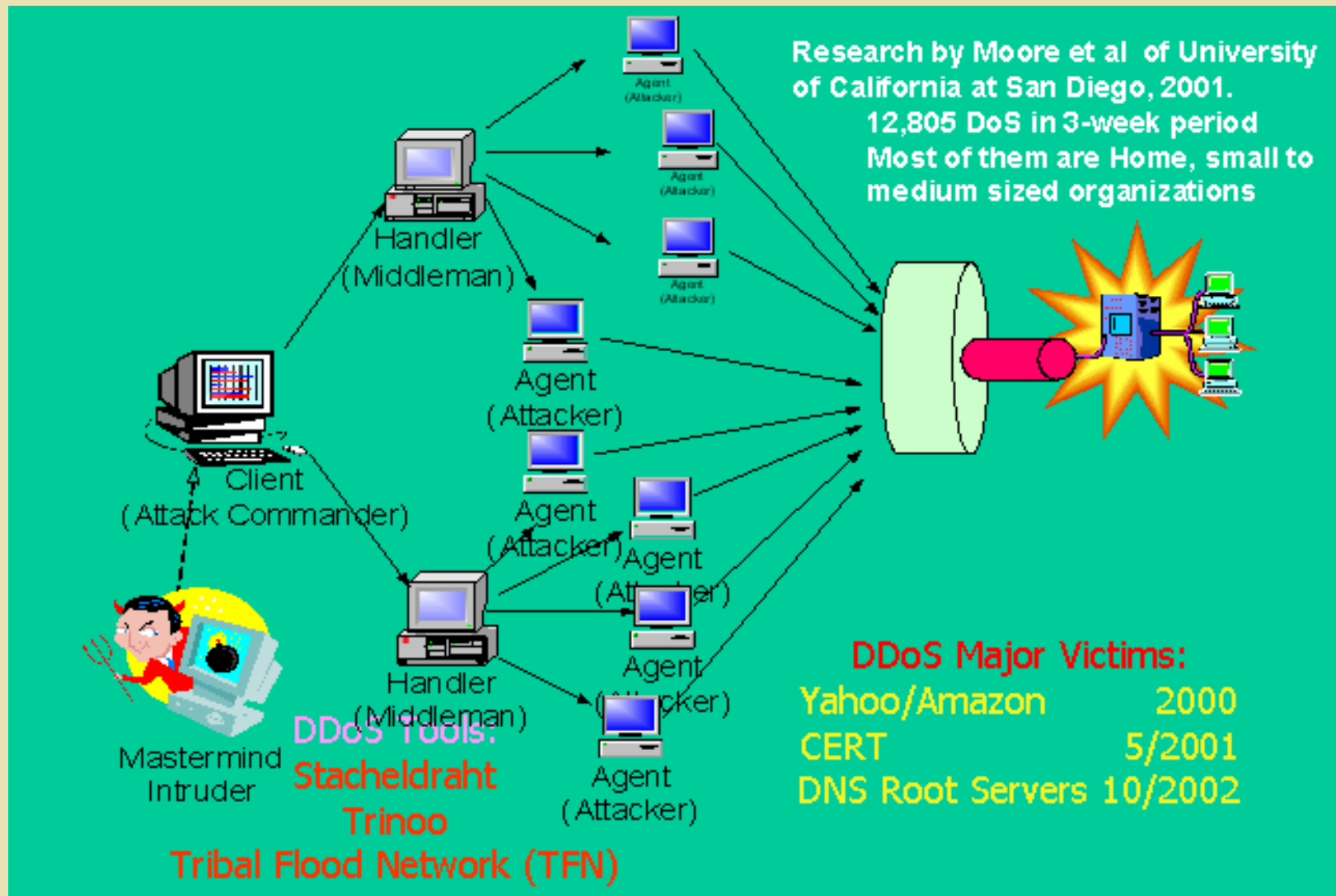
Department of Computer Science

UC. Colorado Springs

<http://www.cs.uccs.edu/~zbo/projects/3DOS.html>

Email: zbo@cs.uccs.edu

DDoS: Distributed Denial of Service





What is Degrading DDoS (3DoS)

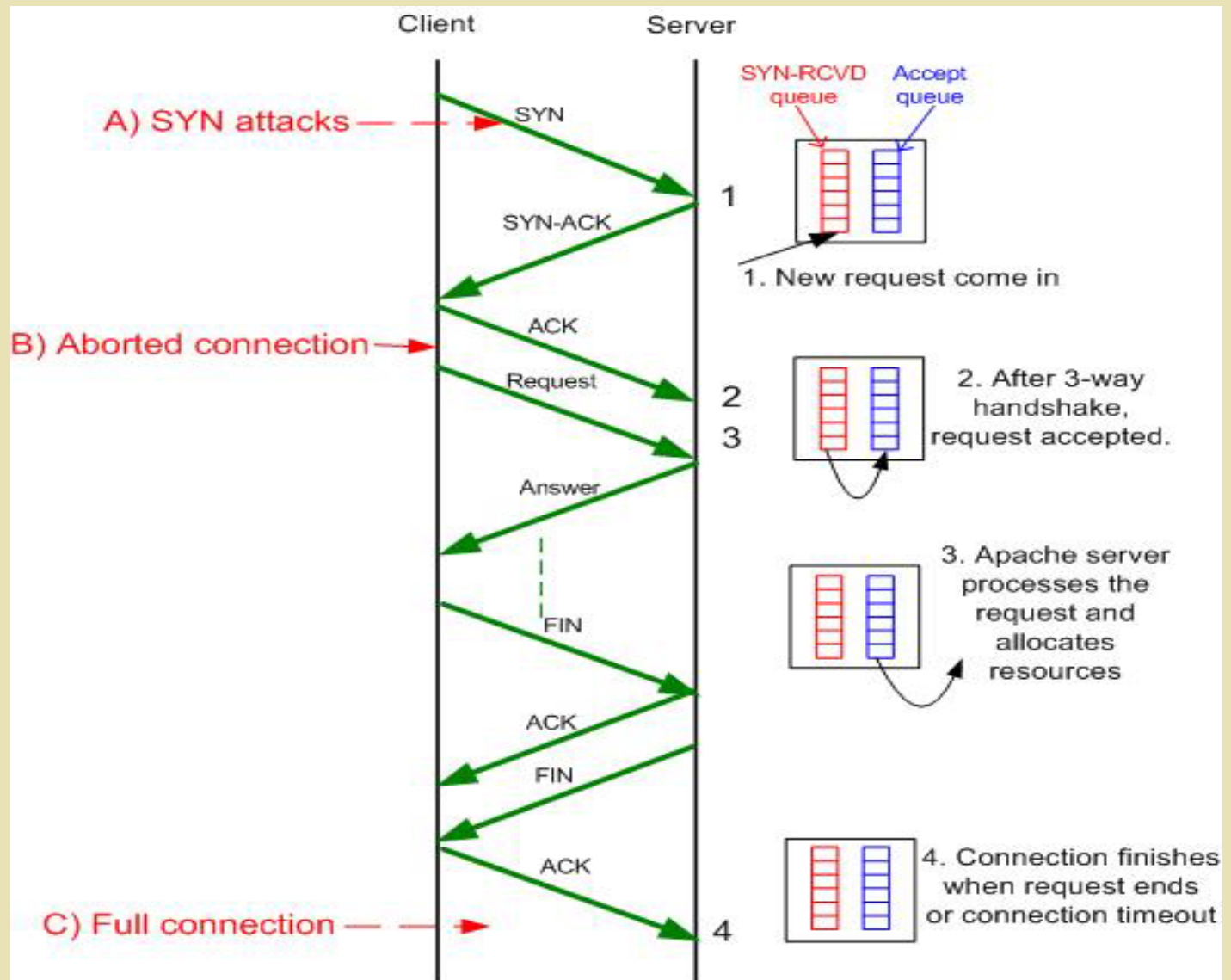
- ◆ According to the impact of a Distributed Denial of Service (DDoS) attack, DDoS attacks can be classified into two categories.
 - **Traditional DDoS attacks:** disruptively and completely disable the victim system's service to its clients. Most known attacks belong to this category.
 - **Degrading DDoS attacks:** increasingly and/or periodically consume portions of a victim system's resources so as to result in denial of service or poor quality of service (QoS) to some legitimate clients during high load periods.



What is the Impact of 3DoS

- ◆ A 3DoS attacker may launch a low rate attacking traffic, and it can remain undetected for a long time period since it doesn't lead to total service disruption.
- ◆ 3DoS attacks might not always have significant impact on server performance.
- ◆ But because of the characteristic of some Internet services, e.g., Apache web server and DNS server, under certain circumstances (like heavy load conditions), small amount of 3DoS traffic can degrade server performance or affect the QoS significantly.
- ◆ Therefore, the behavior of “aggressive” and “malicious” clients should be differently controlled and handled.

Http Connection Establishment



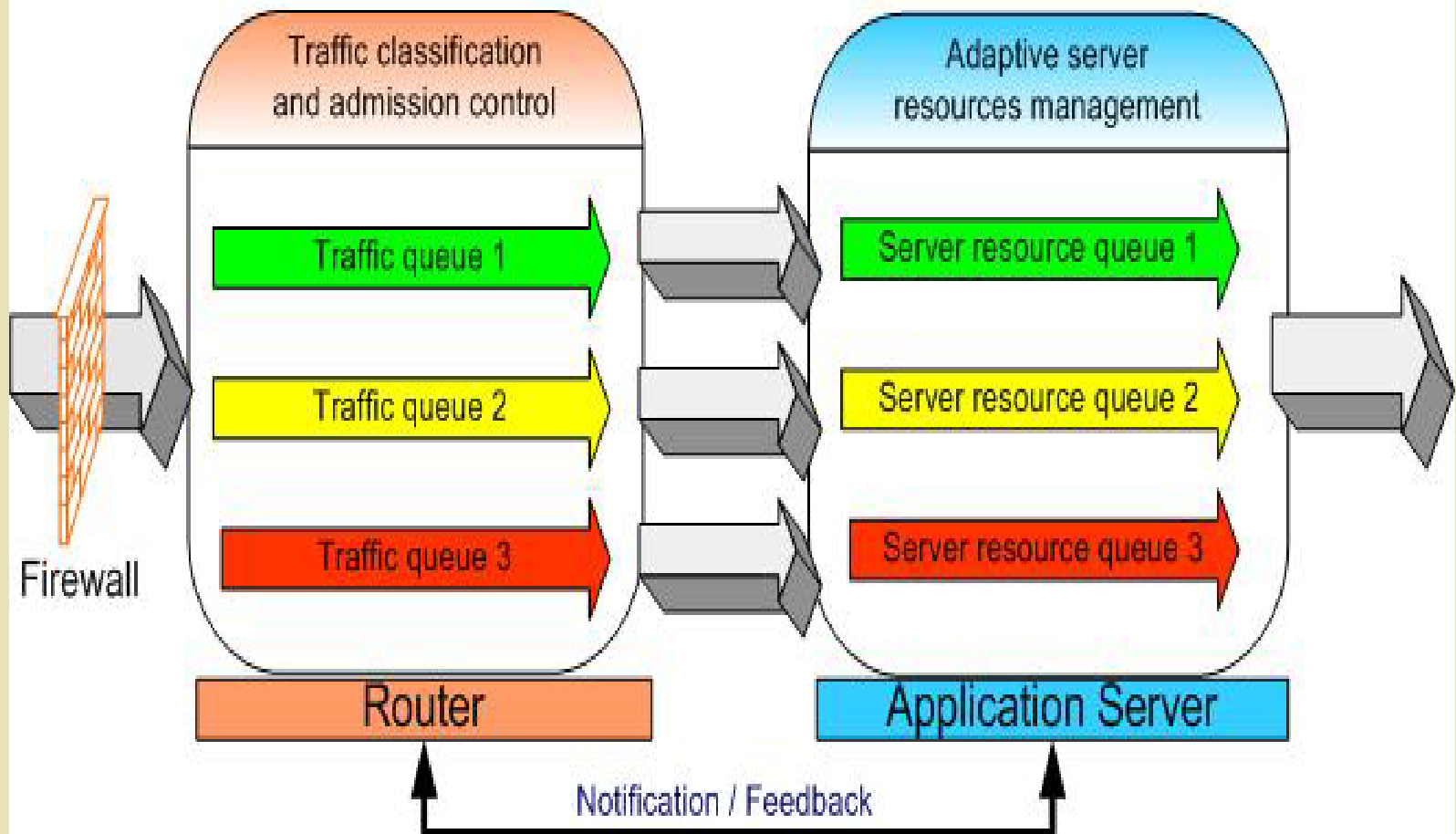


Project Goal

- ◆ The project goal is to design an effective admission control strategy in combination with adaptive resource management mechanisms to mitigate the impact of degrading DDoS attacks.
- ◆ Specifically, we plan to do:
 - A **measurement-based admission control mechanism** that can admit and classify incoming traffic into multiple classes with different QoS expectations according to clients' behaviors.
 - A **demand-driven resource management mechanism** that can provide QoS isolation to the multiple classes by regulating the movement of traffic.

3DoS Mitigation Overview

Overview of Degrading DDoS attacks Defense Mechanism





An Admission Control Strategy

- ◆ To adaptively categorizes the incoming traffic into different classes based on their behavior patterns.
 - **Arrival rate:** how many packets or requests / seconds
 - **Abort ratio:** how many aborted sessions over all sessions
- ◆ Defining a fidelity factor for admission control decisions.
$$FF = \alpha * \text{ArrivalRate} + (1 - \alpha) * \text{AbortRatio}$$

(α is a parameter set by user)

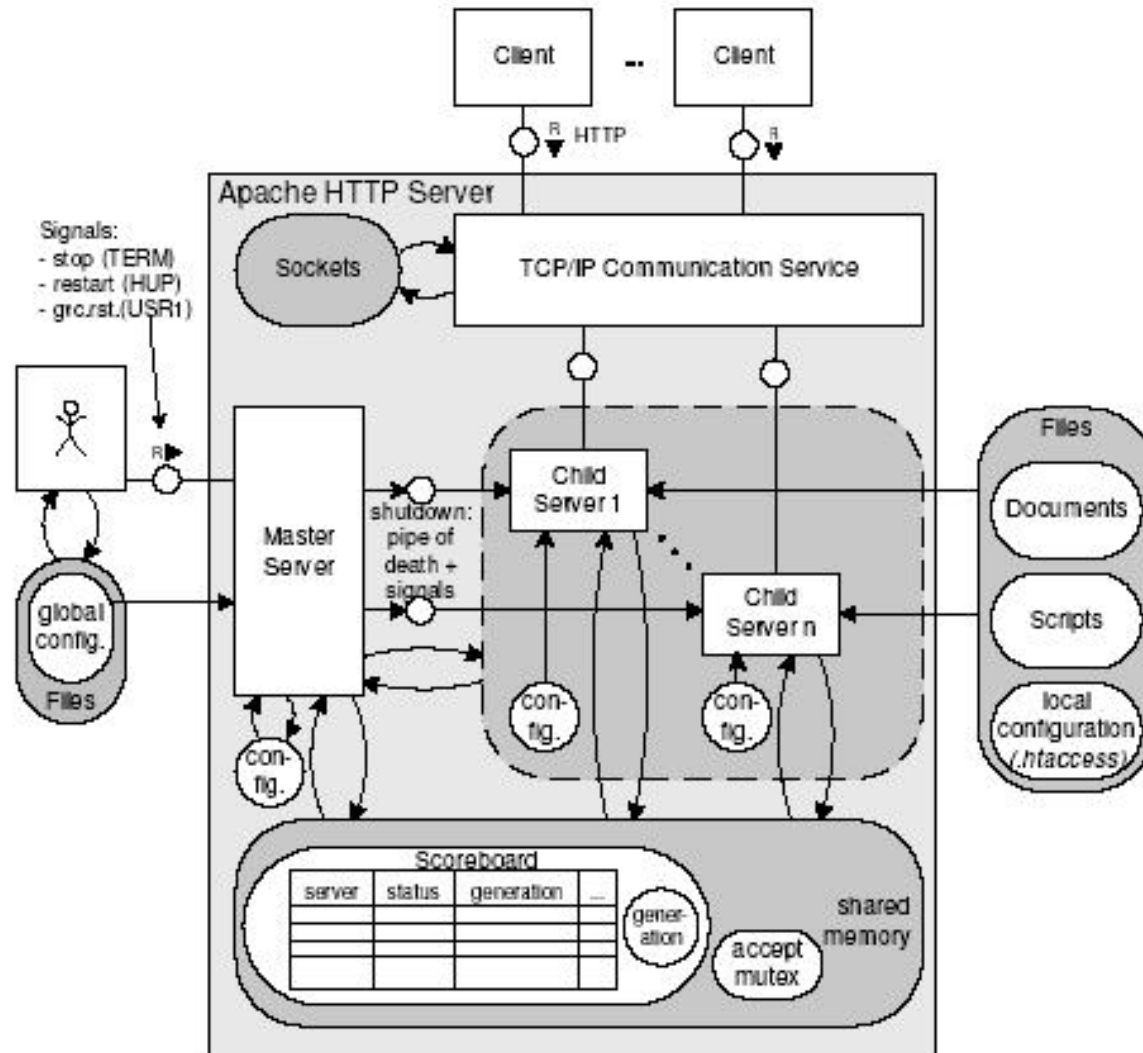
 - The arrivalRate and abortRatio can be obtained by sniffing sampling, and analyzing the clients' traffic.
- ◆ Based on FF values, we classify the clients' traffic into different classes with different QoS expectations.



Adaptive Resource Management

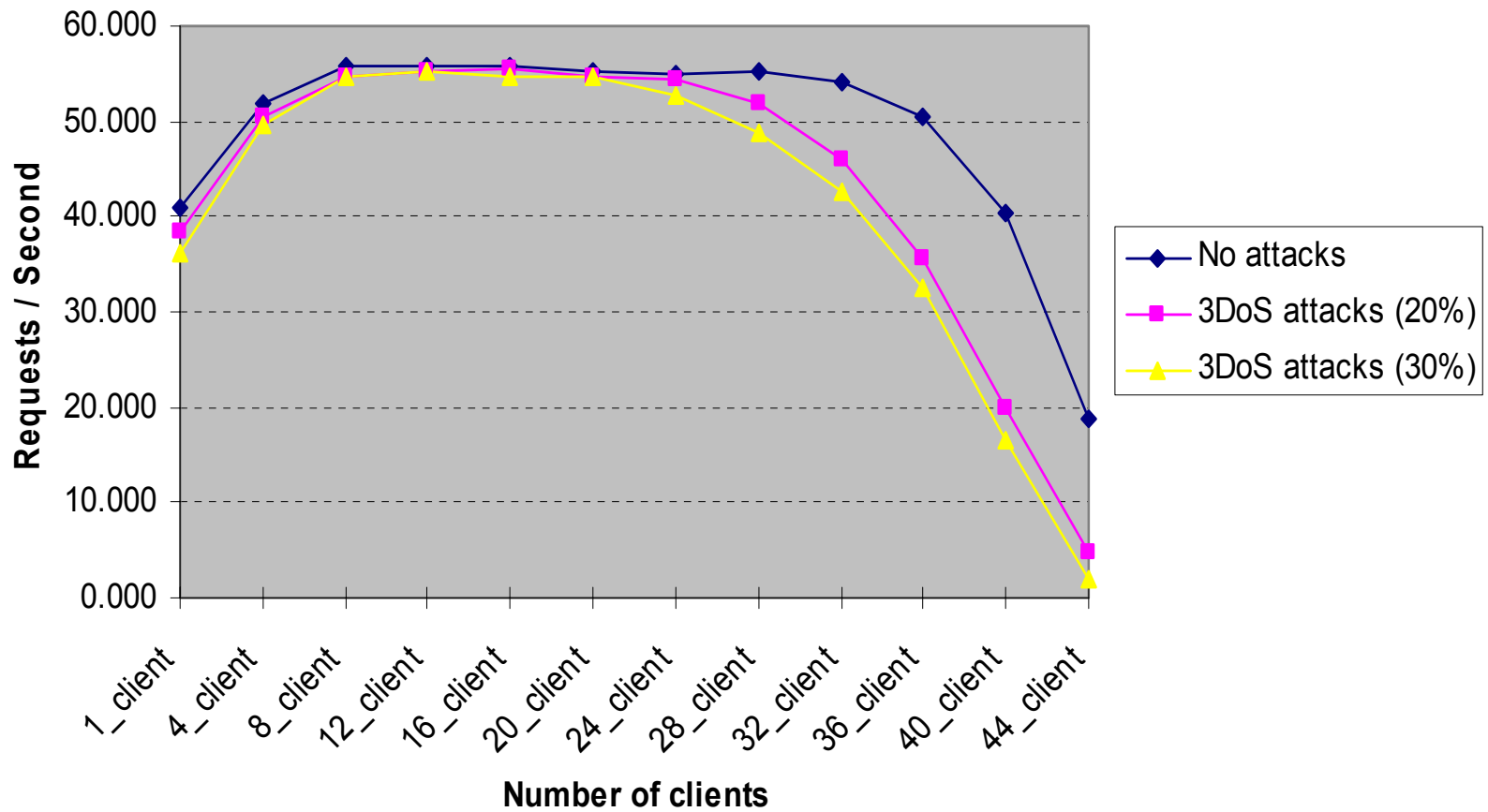
- ◆ The overall goal of adaptive management is not to maintain an optimal condition of the resource, but to develop optimal management capacity.
- ◆ A resource management mechanism is being developed to allocate the server's resources to handle traffic in different classes based on clients' behavior patterns and servers' workload conditions.
- ◆ We are currently modifying Apache web server scheduling policy to provide differentiated resource allocation and management to various classes of queue where each class of queue is a virtual host.

Apache Process Scheduling



Preliminary Results

Benchmark of apache ssl request under 3DoS attacks





Future Work

- ◆ Simulate 3DoS attacks and further study the potential impact on server performance.
- ◆ Define effective and efficient schemes for 3DoS traffic pattern classifications.
- ◆ Enhance the traffic sniffer and traffic analyzer.
- ◆ Enhance the process scheduling approaches based dynamic resources allocation.
- ◆ Extend the current work to DNS server, FTP server.
- ◆ 3DoS defense mechanism performance evaluation.