

2003

# Vulnerabilities and Safe-guards in Networks with QoS Support

Sonia Fahmy

*Purdue University*, fahmy@cs.purdue.edu

Srinivas R. Avasarala

Venkatesh Prabhakar

Report Number:

03-020

---

Fahmy, Sonia; Avasarala, Srinivas R.; and Prabhakar, Venkatesh, "Vulnerabilities and Safe-guards in Networks with QoS Support" (2003). *Computer Science Technical Reports*. Paper 1569.  
<http://docs.lib.purdue.edu/cstech/1569>

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact [epubs@purdue.edu](mailto:epubs@purdue.edu) for additional information.

**VULNERBILITIES AND SAFEGUARDS IN  
NETWORKS WITH QoS SUPPORT**

**Sonia Fahmy  
Srinivas R. Avasarala  
Venkatesh Prabhakar**

**Department of Computer Sciences  
Purdue University  
West Lafayette, IN 47907**

**CSD TR #03-020  
June 2003**

# Vulnerabilities and Safeguards in Networks with QoS support

Sonia Fahmy, Srinivas R. Avasarala, Venkatesh Prabhakar

## Abstract

We identify the security risks involved in quality of service (QoS) enabled networks. Simulation and experimental studies are used to quantify the performance degradation experienced by flows due to security breaches. We propose network monitoring tools, intrusion detection systems and security protocols to safeguard against the security threats in an adaptive manner.

## 1 Introduction

The proliferation of high speed networks and multimedia applications is increasing the demand for high Quality of Service (QoS) in the Internet. Applications such as e-commerce, audio and video conferencing, distance learning have become increasingly popular over the last few years. The best effort network protocols currently deployed are inadequate to handle the service requirements of these applications. Networks with QoS support address these requirements of high bandwidth and low delay. Several components are required to build a QoS framework. Connection admission control, policy control, QoS routing and resource reservations are required to ensure that sufficient resources exist for QoS guarantees to be met. Traffic shaping and policing, scheduling and buffer management are required to control resource usage. Finally, traffic monitoring and feedback control are important to avoid congestion collapse in computer networks. These components form the building blocks of a framework for supporting QoS based applications. These building blocks are used in the Integrated Services and Differentiated Services architectures and with traffic engineering for label switched paths.

The Integrated Services (IS) [13] framework requires resources to be reserved a priori for a given traffic flow (also called micro-flow). The Resource Reservation Protocol (RSVP) [14] establishes distributed state in routers and hosts related to resource reservation if the reservation request is accepted. A packet classifier is used to identify flows that are to receive a certain level of service and a packet scheduler handles the service of different packet flows to ensure that QoS commitments are met. The main problem with the integrated services model has been scalability, especially in large public IP networks which may potentially have millions of concurrent micro-flows.

The Differentiated Services (DS) framework [3] is more scalable for service differentiation in the Internet. The current Internet can be DS enabled without major overhauling. Packets are classified and the DS field in the IP header [2] is marked to receive a particular per-hop forwarding behavior on nodes along their path. Emphasis is placed on shifting the complexity to the edges where ingress and egress router performing traffic metering, policing and shaping. The internal nodes merely forward the packets. Though QoS frameworks like Integrated Services and Differentiated Services have evolved, security threats and vulnerabilities introduced have not been extensively studied.

With the introduction of more points of control that are required to provide QoS, the security threats increase. The potential points of attack increase as additional entities are used to provide service differentiation. Also there is more incentive for a malicious user in terms of the much higher service gained by exploiting these vulnerabilities. In this work, we study such vulnerabilities and classify the risks involved in the terms of potential damage caused. We also provide recommendations and adaptive solutions that use a combination of network monitoring tools, intrusion detection systems and inherently secure protocols.

## 2 Background

In this section we review the background work on Quality of Service with special emphasis on Differentiated Services, and Network Security.

### 2.1 Quality of Service Architectures

The Differentiated Services architecture [1] shifts control functions to the edge of a domain, making the core only responsible for forwarding based on a classification done at the edge. The DS field in the IP packet header is used to indicate the forwarding treatment a packet should receive. While DS standardizes a number of Per-Hop Behavior (PHB) groups, some others have local significance only. A PHB, expedited forwarding (EF) [6] and a PHB group, assured forwarding (AF) [5], have been standardized. Several classes of services are defined using different classification, policing, shaping and scheduling rules.

Typically, a customer agrees upon a Service Level Specification (SLS) with an Internet Service Provider (ISP) in order to obtain Differentiated Services from it. An SLS may implicitly or explicitly specify a Traffic Conditioning Specification (TCS) which defines classification, metering, marking, discarding and shaping rules. Traffic is conditioned at the ingress router of a DS domain by classification (marking of DS field), shaping (delaying) or policing (dropping). When a packet traverses the boundary between different DS domains, the DS field of a packet may be re-marked according to the existing agreement between the domains.

As Differentiated Services become more widely deployed, interoperability with other technologies becomes important. Typically, edge networks are RSVP enabled and the core transit network is DS enabled. In this scenario, the RSVP networks (on the edges) may be considered as customers of the transit DS network. The edge routers (at the edge of the RSVP and DS networks) are both RSVP and DS capable. RSVP signaling is carried out transparently through the DS network. The DSCP marking can either be done at the host itself or at an intermediate router. RSVP reservations have to be converted into appropriate DS PHBs for achieving end-to-end QoS.

### 2.1.1 Policy Control

A general policy framework identifies the functional elements and protocols required to support QoS policy in the network. Policies for fair access to resources must be stored, accessed, updated and monitored. The COPS protocol [9] provides a client/server model for distributed policy management in a network. COPS can be used within a domain for router policy enforcement points (PEPs) to retrieve policy from policy distribution points. TCP is used as the transport protocol for reliable exchange of messages between policy clients and a server. State management is a large component of COPS. Policy distribution points (PDPs) maintain state for all PEP requests until informed to delete that state. PEPs periodically report status information to the PDP related to accounting and monitoring of requests. The COPS protocol is also being extended for policy provisioning.

## 2.2 Network Security Threats

Well known attacks like IP spoofing, SYN flooding and sequence number guessing have been studied from the perspective of the existing best effort networks. These attacks could have higher motive and wider dimension in a QoS enabled network. Most of the attacks could be classified under the following categories

- Network Denial of Service - An attack in which legitimate users are prevented from using their share of the network or network resources by some malicious users. Service overloading, message flooding and clogging the network are some of the commonly used techniques for performing denial of service.
- Session Hijacking - This involves seizing control of the network connection of a legitimate user. Once an attacker has successfully hijacked the connection, he is able to supply commands on behalf of the user.
- Masquerading - This involves identity theft which is the misuse of another user's identity with the objective of taking actions permitted to the owner of the identity. A common form of this attack occurs when a user executes a protocol with an entity that pretends to be the user with another entity using the same protocol and information passed to itself by the user in the protocol.
- Information Leakage - Failures in the protocol or implementation may lead to an attacker gathering information about a session that he otherwise would not have been able to deduce.
- Unauthorized Resource Use - Compromise of any device on a network constitutes unauthorized resource use.

## 3 Related Work

In this section we discuss related work on network security tools and recent efforts to secure QoS.

### 3.1 Network Security Tools

Several solutions for preventing and recovering from the above attacks exist. Network based tools operate at the network level and typically detect the origin of attack. They are also used to safeguard against attacks by rejecting unauthenticated packets. Host based tools monitor for attacks on the local host. They can also be used to detect if the host is used as the origin of any attack. Some important tools are discussed below.

**Firewall Tools** These are used to safeguard against unwanted intrusion (especially IP address spoofing). These are basically packet filters that are augmented with a lot of rules to accept or reject packets. Firewalls are typically placed at the border of a network, between an organization and the rest of the Internet. They can also be used as an access control measure to prevent misuse of the Internet by the internal network. Drawbridge, SOCKS, Firewall Configuration Tool (FCT) are some of firewall tools developed. Incorporating efficient encryption schemes and lookup algorithms are currently being researched.

**Traceback Tools** Traceback tools are used to trace attacks, especially Denial of Service, to the origin of the attack. Earlier mechanisms used ingress filtering, link testing (by input debugging or controlled flooding) and logging to counter such threats. Recent IP traceback mechanisms include support in the routers to probabilistically mark packets with partial path information[12]. Thus there is a high probability that when an attack occurs at a particular site, a collection of such packets that constitute the attack would yield information about the path and hence the origin of the attack. Another form of traceback, the ICMP traceback [11] emits a traceback packet (a new ICMP message type) to the destination of the traced packet with a probability of about  $\frac{1}{260000}$ . Information about the previous hop, next hop, time-stamp and the traced packet form a part of the traceback message. This helps in detecting the path in event of a denial of service attack.

**Intrusion Detection Tools** Intrusion detection tools are used to detect attacks by monitoring system resources. They are both host based and network based. A variety of mechanisms and architectures have been proposed for intrusion detection including using autonomous agents, adaptive and automated methods. SWATCH is a log scanner that monitors messages written to a log file. Trip-wire is a file and directory integrity checker. Internet Security Scanner is a network based intrusion detection tool that is used to detect wrong configuration in networks.

### 3.2 Recent Efforts to Secure QoS

Network administrators are expected to protect network resources by configuring secure policers at interfaces with untrusted customers. Some of the recently developed protocols are briefly examined here.

- **Securing Policy Exchange** - Security considerations are vital to the COPS protocol. The COPS specification discusses an integrity object that must be supported by all COPS implementations. The specification also highlights the use of IPsec to secure the communication between the PDPs and PEPs.
- **Use of IPsec with RSVP** - RSVP was extended to use the Security Parameter Index (SPI) in IPsec to provide similar functionality as the TCP/UDP like ports. RSVP message processing is also modified to handle this case.
- **IPsec with Differentiated Services** - IPsec does not provide any defense against an adversary's modification of the DS field. Only IPsec tunneling capabilities can encapsulate a DS packet so that the DS code-point is protected by the encapsulation.
- **RSVP Integrity Object** - To ensure the integrity of the admission control mechanism, RSVP requires the ability to protect its messages against corruption and spoofing. The RSVP Integrity Object contains a message digest (HMAC-MD5 is recommended but not required) along with a sequence number. These two elements protect against forgery and replay attacks. Confidentiality is not offered by this mechanism. Key management for the Integrity Object mechanism requires further investigation. The requirements for a key management system are presented in the specification along with ideas of possible integration with Kerberos.

## 4 Results

### 4.1 Identification of Top Security Risks in QoS Networks

In this section we present the top security risks in QoS networks. The two most important points of attack are the configuration process and the data forwarding process [4]. Attack operations include injecting malicious packets, modifying information in the packets, delaying and dropping packets, and to a lesser extent eavesdropping. All attack operations aim at either theft of resources or denial of fair share of resources to the legitimate user. Since QoS networks provision resources based on service differentiation, this would lead to a violation of agreed upon policies.

#### Attacking the QoS configuration

- **Modifying configuration information in routers** - The configuration information stored in the edge routers determines how the traffic is shaped, while that at the core routers determines how a packet is forwarded. By altering the information at edge routers, an attacker can cause a change in the implementation of agreed upon TCS, thereby exploiting the change made. By modifying the PHB specifications stored in the core routers the attacker can not only gain better service, but also degrade the service offered to other legitimate users.
- **Altering dissemination of configuration information** - Service Level Agreements (SLAs) are usually decided by exchanging negotiation messages between trusted Bandwidth Brokers (BBs) and the edge routers at DS domains. These negotiations are also done between edge routers of peer DS domains. Additionally PHB specifications are propagated to core routers. These messages form vital points of attack because modifying the negotiation messages alters the configuration information directly which the attacker can later exploit.
- **Compromising Bandwidth Brokers** - Bandwidth brokers maintain the local policy and are responsible for resource allocation in a DS domain. Compromising these would yield the attacker complete control over a DS domain.
- **Configuration information leakage** - A passive attacker can eavesdrop and learn the configuration information and exploit any over-provisioned resources. This could go undetected if proper monitoring tools are not in place.

#### Attacking the packet delivery

- **Theft of service by IP address spoofing** - This attack is possible because of the well known problem of IP spoofing. An attacker can spoof the IP source address and pretend to be a source which gets a better service with a particular Differentiated Services Code Point (DSCP). Thus the attacker gets better service than he should normally get. Also the attacker manages to deny the legitimate user the quality of service that he should get.
- **Modifying header information of packets** - AF service and EF service, the two most widely implemented service differentiation schemes rely on the ingress router performing traffic conditioning by looking at fields in the header. Thus the information in the header is a vital point of attack. If an attacker successfully changes the DSCP field in the header of a packet, he can effectively perform denial or degradation of service to the legitimate user. Since the header fields are currently not protected against modifications, this attack is not very difficult.
- **Maliciously delaying and dropping packets** - This kind of attack occurs on the path between the user and the DS domain. Compromised routers can be used to deliberately delay and drop packets from a legitimate user, while the attacker can make use of the services offered by the DS domain for that user.

**Simulation results for attacks on differentiated service networks** Simulation experiments were carried out to determine the effect of DSCP changes of unauthorized traffic flows on the throughput of authorized flows. These were carried out on the Network Simulator-2(ns). The Diffserv implementation for ns [7] was used to augment it to provide service differentiation capabilities like AF and EF PHBs. We implemented functions to update the DSCP and to perform dropping of EF packets when the traffic was above the committed rate irrespective of the queuing function used. The setup consisted of two traffic sources and a single destination through a bottleneck path as shown in figure 1.

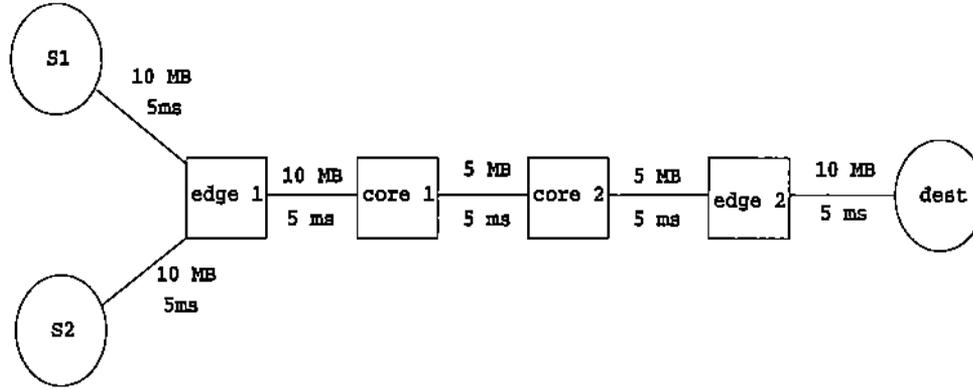


Figure 1: Simulation Experiment Setup

A Time Sliding Window (TSW) tagger was used to meter the packets. Policing was done by a Time Sliced Window Three Color Marker (TSW3CM) policer. The scheduler used was a Weighted Round Robin (WRR) scheduler with two RED queues(70%, 30% weights) and three drop precedences within each queue. Experiments were carried out for both AF and EF PHBs with CBR, FTP and Telnet traffic.

For both sources S1 and S2, we used a committed rate of 10 Mb/s, a peak rate of 50 Mb/s and an actual data rate of 7 Mb/s. The experiments were carried out for 150 seconds. For the initial 50 seconds of the simulation, source S2 uses a lower PHB than the one used by source S1. During the next 100 seconds of the simulation the DSCP used by source S2 was changed to that of source S1 to study the effect bandwidth stealing on authorized users like source S1. The summary of results is shown in the table below.

Source S1 PHB/Agent	Source S2 PHB/Agent	Normal Throughput (S1/S2) (kb/s)	Changed Throughput (S1/S2) (kb/s)
EF/CBR	BE/CBR	3519.04/1483.63	2862.56/2140.69
EF/CBR	AF11/CBR	3502.13/1502.61	2854.66/2148.48
EF/CBR	AF12/CBR	3502.72/1500.91	2849.60/2153.71
EF/CBR	AF13/CBR	3517.17/1486.03	2854.77/2148.53
EF/CBR	AF21/CBR	3527.68/1474.83	2863.36/2139.89
AF11/CBR	BE/CBR	4998.35/4.0	2665.01/2339.68
AF12/CBR	BE/CBR	4996.59/4.0	2663.52/2339.63
AF13/CBR	BE/CBR	4991.31/4.0	2661.92/2340.0
AF21/CBR	BE/CBR	4979.19/4.0	2657.81/2341.01
AF11/CBR	AF12/CBR	4996.64/6.13	2662.88/2341.54
AF11/CBR	AF13/CBR	4998.07/4.21	2664.75/2340.16
AF11/CBR	AF21/CBR	4997.97/4.16	2664.90/2339.73
EF/FTP	AF11/CBR	2725.49/2276.85	918.29/4083.41
EF/Telnet	AF11/CBR	8.10/4993.97	6.40/4995.84

It is observed in all the cases that there is a marked difference in the throughput achieved by the source 1 between the normal run and the run when source 2 steals bandwidth from it.

Another interesting scenario is the division of excess bandwidth between various flows at the routers when the DS domains are over provisioned. We used a topology similar to the one in figure 1, but with all the links between edge, core and destinations as 12Mb/s links. The traffic policies for the flows from sources S1 and S2 were altered to allow a peak rate of 6Mb/s and a committed rate of 5Mb/s. The actual sending rates of the sources was 7Mb/s. In an initial run, we let only source S1 send data. We notice that though its sending rate is higher than its committed and peak rates, it still achieves a throughput equal to

its sending rate due the over-provisioning in the DS domain. This is despite the downgrading of its PHB due to overshooting the committed rate. We then let source S2 also send data. In this case we notice that S2 achieves a bandwidth of 5.23 Mb/s, using up some of the over-provisioned bandwidth in the DS domain. Source S1 achieves a bandwidth of 6.75 Mb/s, below its sending rate of 7 Mb/s.

## 4.2 Proposed Solutions

**Protecting flows entering a DS domain** In a DS domain, the authentication of user traffic is done by the edge routers. Edge routers are configured with the user profiles, as SLAs, and must do DSCP validation to allow only valid user traffic flows. Since traffic flows are identified using IP source addresses, IP spoofing is a serious security threat. Another threat to user traffic flows are modification of packets on the way to the edge routers. This modification will alter information in the packet used for identifying valid users. Both the above problems can be handled by using IPSec tunnels between the host and its ingress router, i.e., an edge router of the DS domain. Since IPSec tunneling uses the inner packet for its cryptographic calculations, the packet fields are secure against any modifications on the way. Also, this end-to-end security mechanism prevents any malicious user from taking on the identity of another user for stealing bandwidth.

**Protecting BBs, Edge and Core Routers** All the components of a DS domain, the BBs, the Edge and the Core routers, contain sensitive information that can be subject to attacks. Bandwidth brokers contain SLAs, and configuration information for edge and core routers. The Edge routers contain user traffic profiles along with traffic conditioning parameters like token bucket rates, committed rates and peak rates. The Core routers contain PHB setup information and buffer management parameters for schemes like RED, RIO. Attacks on this information can be detected using intrusion detection tools. Intrusion detection has two major areas of research, anomaly detection and pattern recognition. Anomaly detection is based on determining patterns of normal behavior for networks, hosts and users and then detecting behavior that is significantly different. Pattern recognition aims to detect patterns of activity that match known intruder attack scenarios.

**Protecting Configuration Messages** Bandwidth Brokers disseminate configuration information to edge and core routers using protocols like RSVP, SNMP, COPS or other similar signaling mechanisms. Recent research suggests using IPSec along with COPS or RSVP to secure communication between the PDPs (like BBs) and PEPs (like edge/core routers). The RSVP integrity object can also be used to ensure integrity of signaling messages. Hop integrity in networks is another interesting approach to this problem [10]. The authors suggest addition of a secret exchange layer and an integrity check layer above and below the network layer respectively. This is aimed at detecting message modification and message replay between any two communicating devices.

**QoS Monitoring Tools** Continuous monitoring of network activity is required to maintain confidence in the security of the network. Network monitors can be installed at strategic locations in a DS domain to collect information from all the DS components and examine the information continuously to identify suspicious activity. Collected information can include among other things, the configuration data of each router, the current bandwidth usage of each router etc. At regular intervals, the configuration data at a router can be verified to be the same as the one computed at a PDP (a BB). Also one can monitor the bandwidth usage of a router and compare it with the sum of traffic profiles configured at that router to indicate any theft.

**Traceback Mechanisms** In addition to measures for preventing attacks, we also need mechanisms in place to trace attacks back to their source. As explained in an earlier section there are two interesting schemes proposed in this area. One of them uses special ICMP messages [11] to probabilistically send information about a traced packet traversing through the router. The information contains, among other things, the back link and the front link used by the packet, a time-stamp and the traced packet. A second scheme relies on encoding the path in the IP header's ID field [12]. This scheme has an advantage that no extra traffic is generated. Another advantage is that the trace information is bound to the packet itself and hence will not follow a different path and will not be differentially blocked by firewalls.

## 5 Future Work

In this section we describe additional simulation experiments, testbed setup, and tools that we propose to implement. We will be focusing mainly on the monitoring tools, but will also complete the simulation and testbed setup, and investigate other tools if time allows.

### 5.1 Simulation Experiments

We have shown the effect of performance degradation that occurs because of DSCP modification attacks in QoS networks. We plan to simulate further attack scenarios using the following topologies.

- A network of clients, a DS domain as the transit network and a network of servers. This would be useful in studying attacks outside the DS domain.
- Using several DS domains in the transit network. This would help in studying flaws in negotiations between DS domains like the effects of code point re-marking.
- Non DS enabled nodes in DS domains. This would help in studying both the dissemination of configuration information within the DS domain and also routing the packets within the domain as per the specified PHBs.

We further plan to study the effects of altering the configuration process by simulating a bandwidth broker.

### 5.2 Linux Testbed Setup

We will implement some of the attacks on a Linux testbed to study the performance degradation and uncover possible security holes and bugs in the implementations. We plan to use PCs running Linux as nodes in the network. We shall be using the Differentiated Services support for the Linux implementation [8]. This implementation uses additional fields in packet headers for classifying them. A queuing discipline to support multiple drop priorities is used for supporting AF PHB. EF PHB is built using the Class Based Queuing (CBQ). The authors have designed GRED, a generalized RED mechanism for buffer management in the queues. A Token Bucket Filter is used to shape the traffic. The implementation allows a node to be configured as an Edge router or as a Core router.

### 5.3 Monitoring Tool Implementation

We plan to implement a monitoring tool that would reside at the edge routers and constantly monitor bandwidth and other system resources that are specific to Diffserv. These include configuration information, PHB specifications, current bandwidth usage and provisioned bandwidth. This would enable us to detect any theft of over-provisioned resources. Also we could monitor the resource usage of flows periodically to guarantee appropriate service levels are not compromised.

### 5.4 Traceback Tool Implementation

We plan to implement a traceback tool on the Linux testbed. We will adopt the approach of probabilistically encoding the path in the IP header's field [12]. We will include this functionality in the edge router as the complexity would be at the edges and also because that would enable us to pin down the route to the DS domains through which the packet passed.

### 5.5 Securing Message Exchanges

We plan to implement a way to secure the message exchanges for disseminating the configuration information between the BBs and the edge routers and the PHB specifications between the edge and the core routers. We plan to use the hop integrity approach to secure the message exchanges [10]. This would entail using a secret exchange layer and the integrity layer. We plan to augment it with the use of time-stamps to prevent replays.

## References

- [1] S. Blake D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, An architecture for Differentiated Services, RFC 2475, IETF, December 1998.
- [2] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 headers, RFC 2474, IETF, December 1998.
- [3] Yoram Bernet, James Binder, Steven Blake, Mark Carlson, Brian E. Carpenter, Srinivasan Keshav, Elwyn Davies, Borje Ohlman, Dinesh Verma, Zheng Wang, Walter Weiss, A Framework for Differentiated Services, Internet Draft, IETF, February 1999.
- [4] Zhi Fu, S Felix Wu, T.S. Wu, He Huang, Security Issues for Differentiated Service Framework, Internet Draft, IETF, October 1999.
- [5] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, Assured Forwarding PHB group, RFC 2597, IETF, June 1999.
- [6] V. Jacobson, K. Nichols, K. Poduri, An Expedited Forwarding PHB, RFC 2598, IETF, June 1999.
- [7] Peter Peda, Jeremy Ethridge, Mandeep Baines, Farhan Shallwani, A Network Simulator Differentiated Services Implementation - Open IP, Nortel Networks, July 2000.
- [8] Werner Almesberger, Jamal Hadi Salim, Alexey Kuznetsov, Differentiated Services on Linux, June 1999.
- [9] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan. E. Sastry, The COPS (Common Open Policy Service) Protocol, RFC 2748, IETF, January 2000.
- [10] M.G. Gouda, E.N. Elnozahy, C.-T. Huang, T.M. McGuire, Hop Integrity in Computer Networks, ICNP 2000.
- [11] Steven Bellovin, ICMP Traceback Messages, Internet Draft, March 2000.
- [12] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, Practical Network Support for IP Traceback, Department of Computer Science and Engineering, University of Washington, Technical Report UW-CSE-2000-02-01.
- [13] R. Braden, D. Clark, and S. Shenker, K. Poduri, Integrated Services in the Internet Architecture: An Overview, RFC 1633, July 1994.
- [14] B. Braden et. al., Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, RFC 2205, IETF, September 1997.