Emmanuel Guiton

TKK:n Tietoverkkolaboratorio

Instructor: L.Sc. Jarmo Mölsä

Supervisor: Prof. Jorma Jormakka

A Rate-Limiting System to Mitigate Denial of Service Attacks

Contents

- Overall information
- Intents and scope
- The Rate-Limiting System
- Tests and results
- Analysis
- Areas of application, future research

DoS Attacks

- Attackers aim to disrupt the normal operation of their targets' services. Flooding attacks aim to exhaust resources on the target. Logic attacks rely on intelligent exploitations of software bugs.

- Attacks are distributed (DDoS) when they are carried out using a (large) set of compromised hosts.

- Flooding DoS attacks resemble legitimate traffic, their patterns vary a lot and change quickly (attackers use random addresses and port numbers).

Means of Defense

- Applying security patches.
- Manual and long investigation process involving every-one on the attack path.
- IDSes, blocking
- CITRA [1], ACC [2]

No complete solution!

Intents

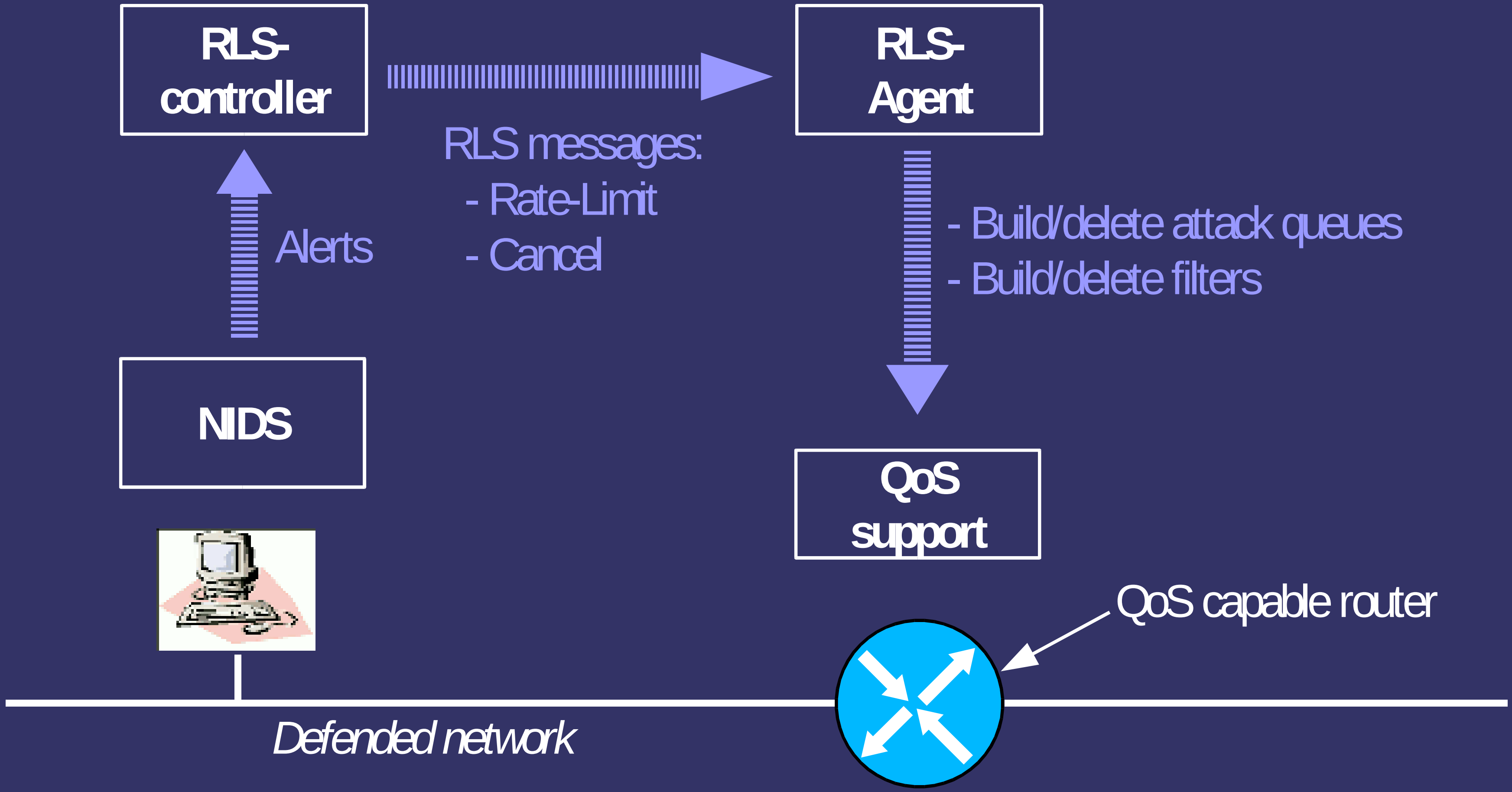
- Automated, early-warning defense mechanism that mitigates DoS attacks. [3, 4]
- Using rate-limiting instead of blocking
- Using IDSes and QoS capabilities

Question:
Is rate-limiting a viable defense mechanism?

Scope

- Traffic is packet-loss tolerant.
- The attack bandwidth is low.
- The probability of attack is low.
- The attack is non-destructive.
- False-positives are too frequent to use blocking.

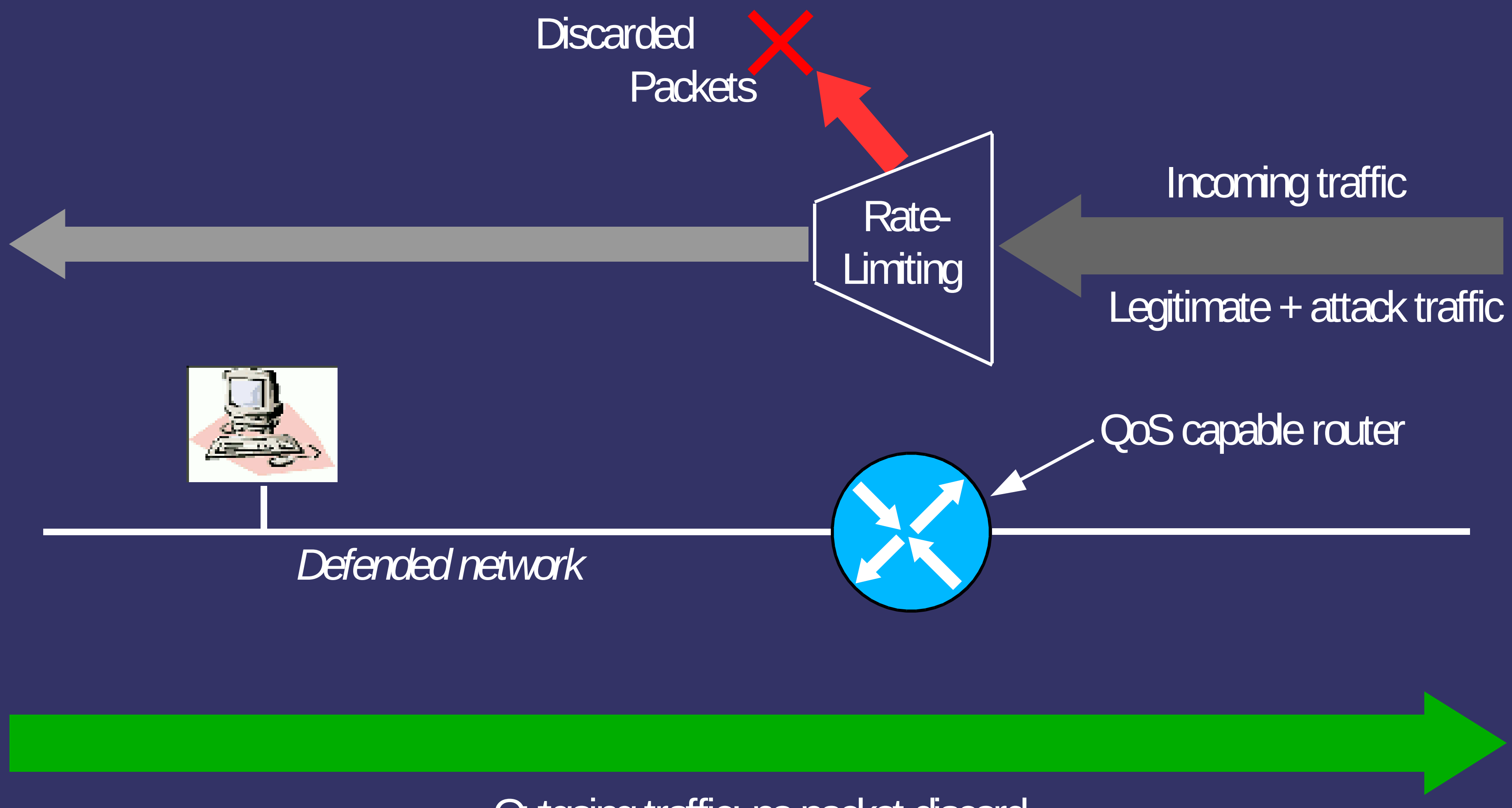
Building blocks of the Rate-Limiting System



RLS messages:
- Rate-Limit
- Cancel

- Build/delete attack queues
- Build/delete filters

Effects of the RLS on traffic



Discarded Packets

Rate-Limiting

Incoming traffic

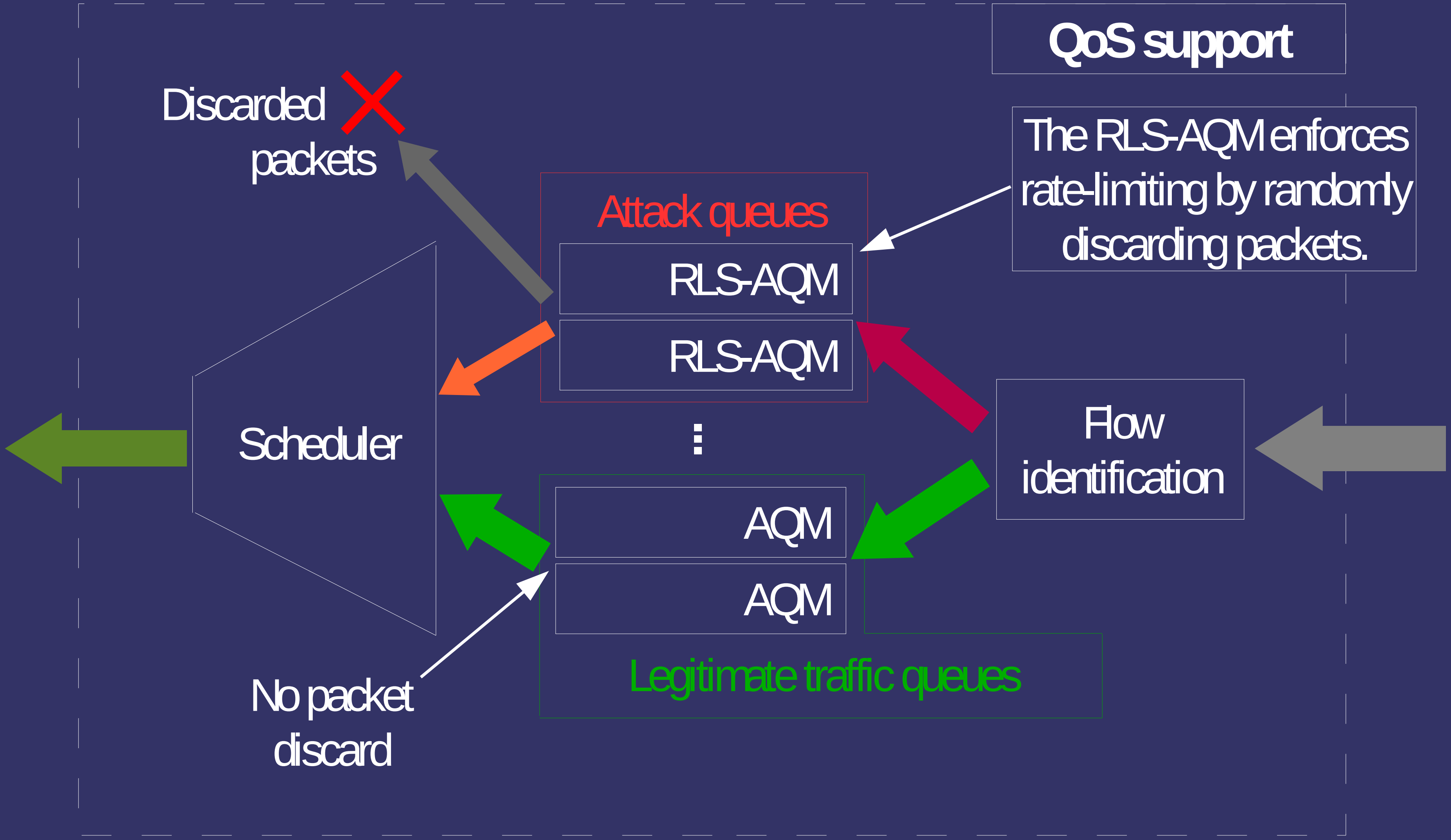
Legitimate + attack traffic

QoS capable router

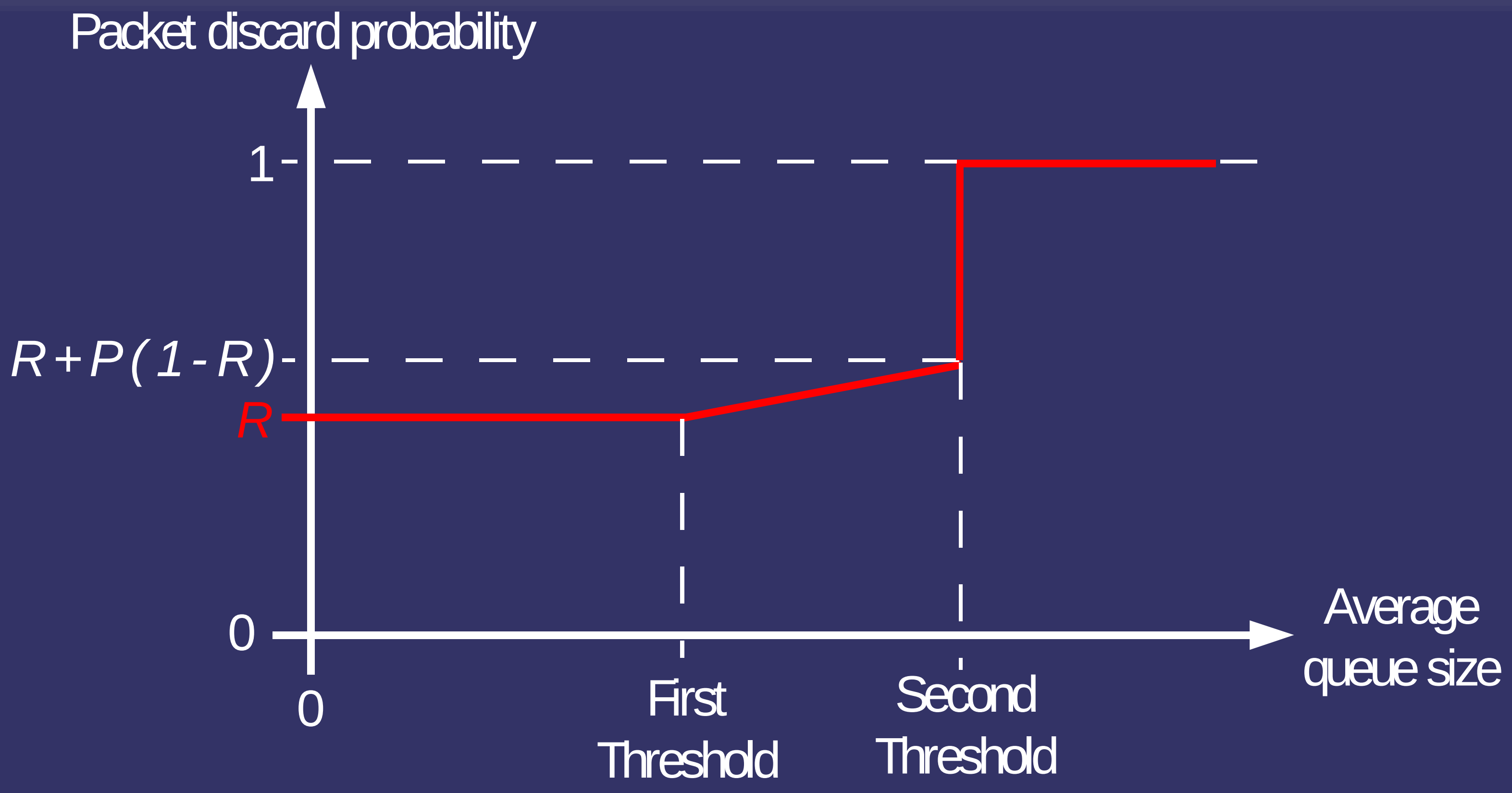
Defended network

Outgoing traffic: no packet discard

QoS operations



Dropping probability function of the RLS-AQM

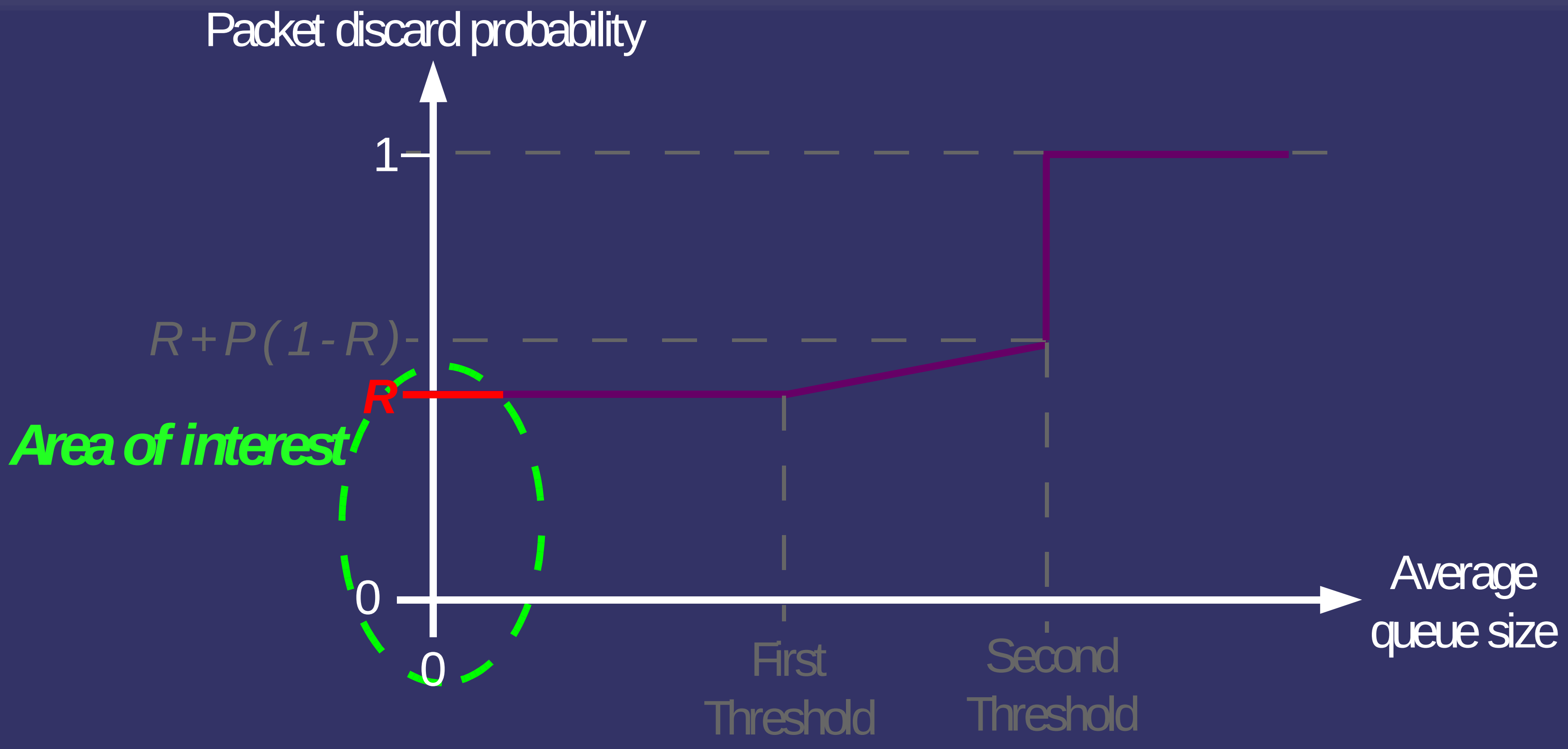


R when average queue size < first threshold

R+ p(1-R) when first threshold < average queue size < second threshold *P=max(p)*

1 when second threshold < average queue size

Dropping probability function of the RLS-AQM



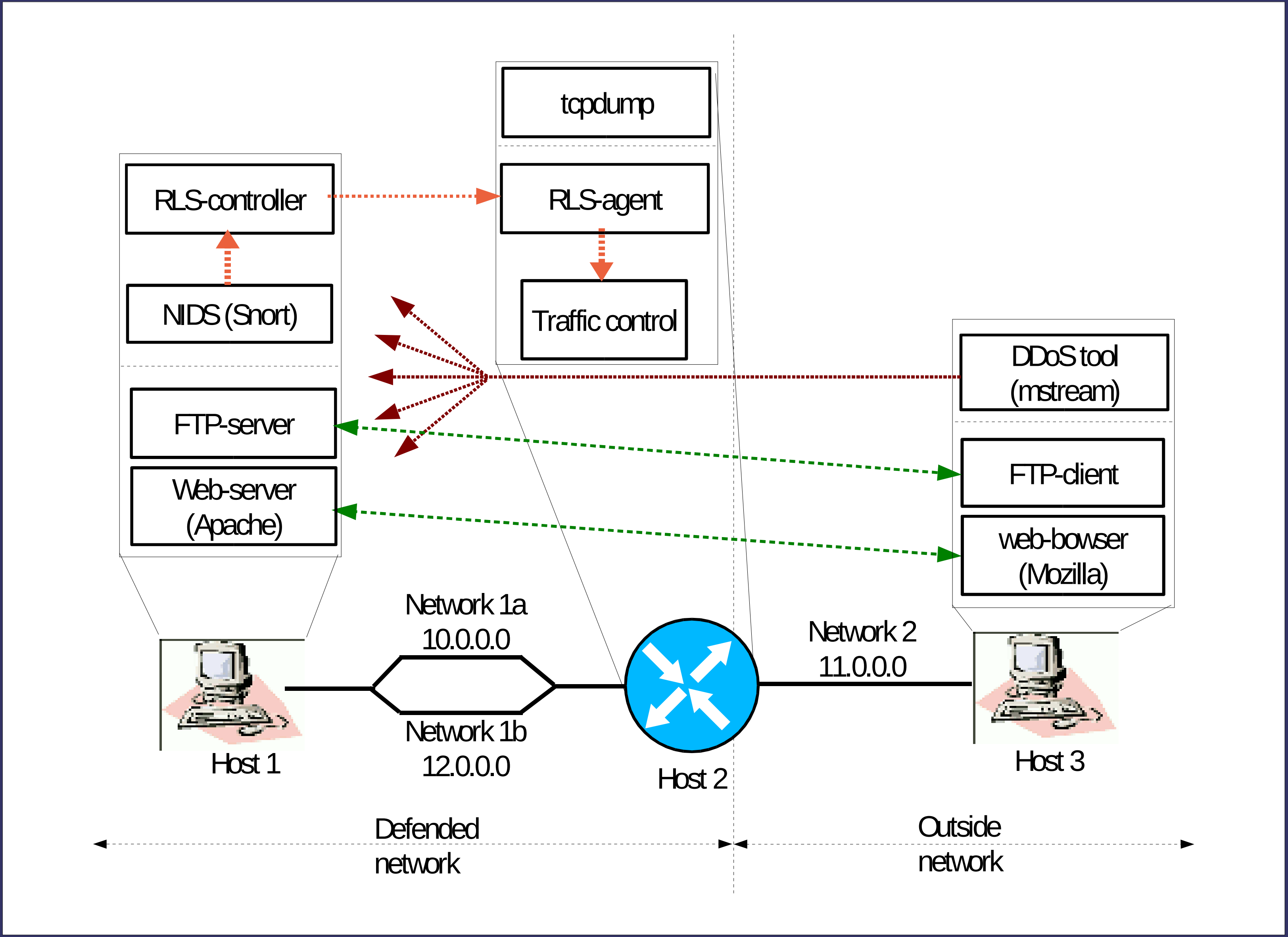
R when average queue size < first threshold

The queue does not get full:
the RLS is intended to work with low-bandwidth attacks.

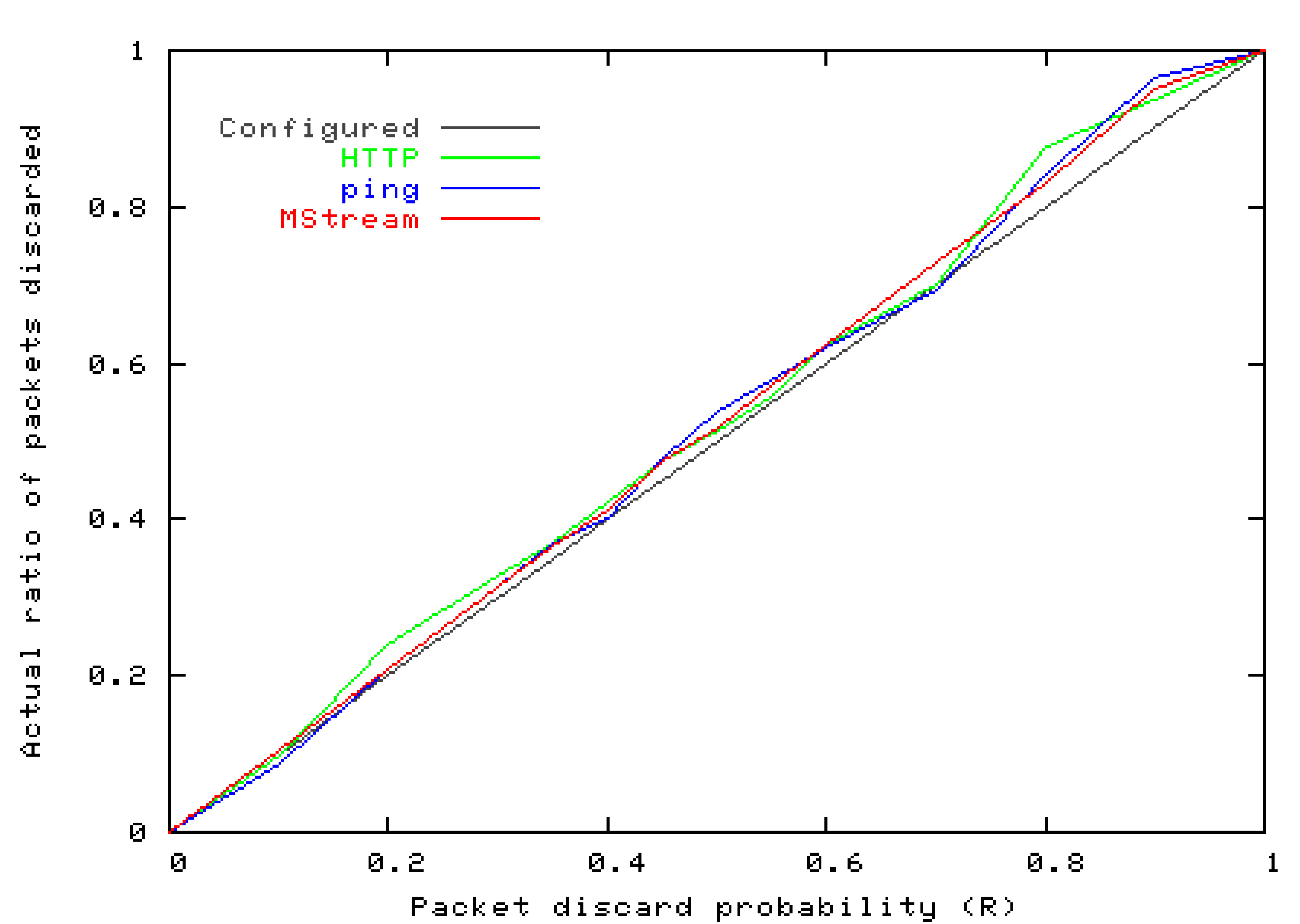
Main tests

- Validating the RLS-AQM behavior
- FTP-uploading / downloading with rate-limiting
- Web-browsing with rate-limiting

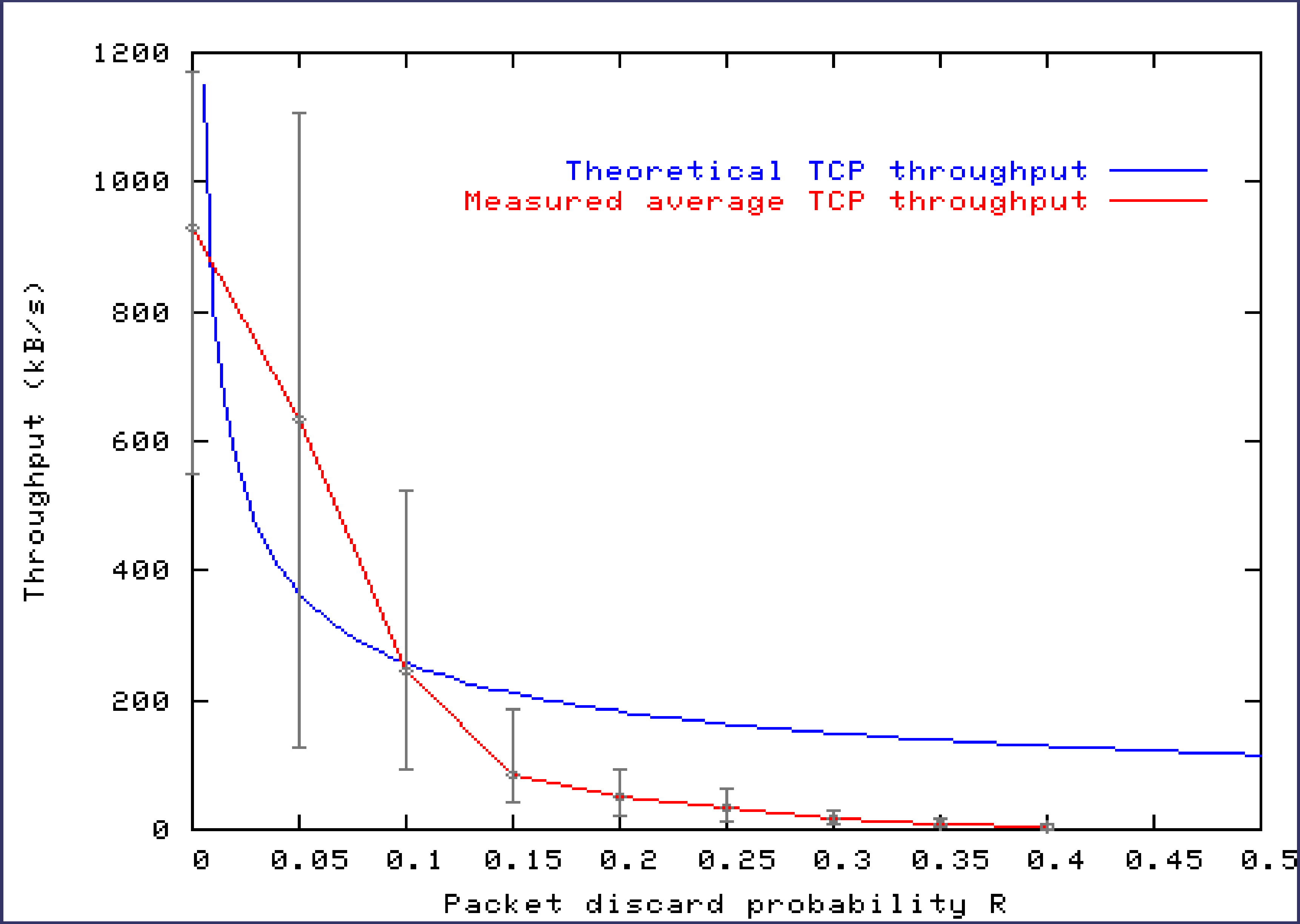
Layout of the test network and the RLS implementation



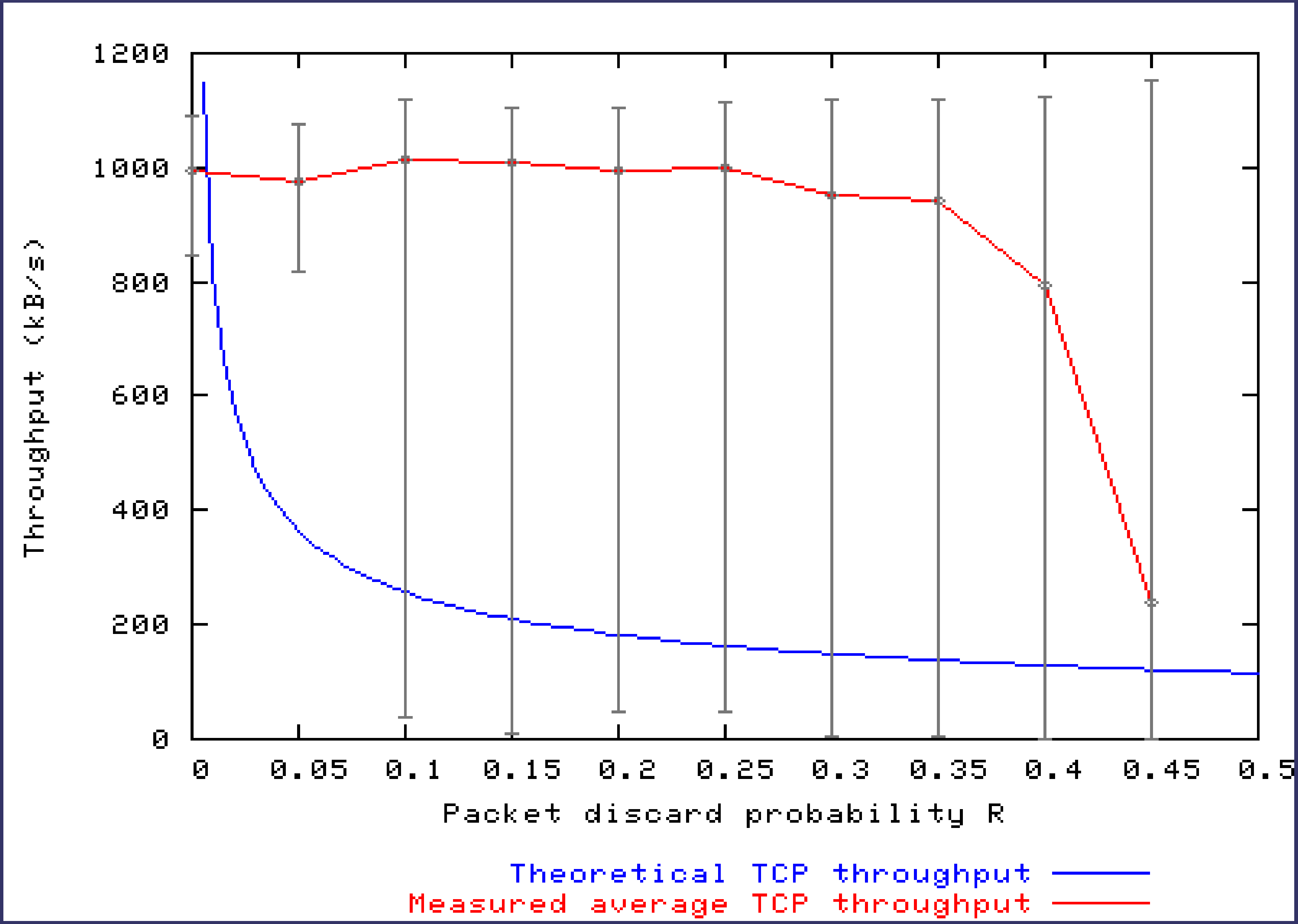
Experienced packet loss ratios using the RLS-AQM compared to configured values



FTP-upload rates for different packet discard probability values.



FTP-downloading rates for different packet discard probability values.



Analysis

- Uploading: data packets are discarded. Every lost data packet has to be retransmitted.
- Downloading: ACKs are discarded. A lost ACK does not necessary need to be retransmitted: following ACKs can recover the information.
- The theoritical model only takes into account the loss of data packets. [5]

Areas of application

- Test HTTP: handle up to 55% packet discard
  Test FTP-downloading: up to 40% packet discard

- HTTP and FTP-downloading are the two most common services offered by websites.

- Flooding DoS attacks (i.e. TCP SYN flooding, ICMP Echo Request flooding) are the most common DoS attacks and very often aim well-known websites (e.g. Yahoo!, eBay, Amazon, CNN... shut down by the same attack in February 2000).

Future Research

- Designing a complete system
- More exhaustive and precise tests, including more realistic network conditions
- Managing several attack and legitimate queues according to the characteristics of traffic flows
- Finding the right communication protocols between components

Kysymyksiä?

- Questions?

Congratulations

- Read aloud:
  - " Bravo "
  - " Viva "
  - " Bis "
- Applause, make a stand-up ovation
- You can throw:
  - Roses
  - Hats
  - Wallets

References

[1] D.Schnackenberg, H. Holiday, R. Smith, K. Djahandari, and D. Sterne. (2001, June). "**Cooperative Intrusion Traceback and Response Architecture**", in *Proceedings of the Second DARPA Information Survivability Conference and Exposition (DISCEX II).* Anheim, California, USA.

[2] R. Majahan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. (2001. July 13). "**Controlling High Bandwidth Aggregates in the Network (Extended Version)**". Draft paper pushback-Jul01.ps, work in progress. [On-line]. Available: http://www.icir.org/pushback

[3] J. Mölsä, "**Mitigation of Denial of Service Attacks**", submitted.

[4] J.Mölsä, E.Guiton, "**Rate-Limiting as an Automatic Reaction against Flooding DoS Attacks**", submitted.

[5]J. Padhye, V. Firoiu, D. Towsley, and J. Kurose. (1998, September). "**Modeling TCP Throughput: A Simple Model and its Empirical Validation**", in *Proceedings of the ACM SIGCOMM conference*. Vancouver, Canada.