



lobster

An IST Project



Information Society
Technologies

<http://www.ist-lobster.org>

Summary, Conclusions and future trends

LOBSTER tutorial

6 May 2005

Arne Øslebø

UNINETT

arneos@uninett.no



Packet based monitoring



An IST Project

<http://www.ist-lobster.org>

- PCAP
 - Popular and widely supported
 - BPF filters
- MAPI
 - New powerful API that takes advantage of intelligent hardware
 - Easy to extend
- FFPF



Problems with packet based monitoring

- Large amount of data
- 1 hour trace on a production 1GE link:
 - 37GB (only headers)
- 10Gbps
 - Worst case: ~24Mpps
- Hardware restrictions
 - Memory
 - Bus
 - CPU
 - disk speed



Hardware assisted monitoring

- SCAMPI adapter and DAG cards
 - Based on FPGA
- Hardware functions
 - Header filters
 - Sampling
 - String search
 - Statistics
- More functionality in the future
 - NetFlow



Flow based monitoring

- Less data, but still a lot.
 - UNINETT:
 - Collects NetFlow from 24 routers
 - 30GB per day
- Core routers can not process all packets
 - Sampled netflow
- NetFlow systems often vulnerable during DoS attacks

Future challenges

- Data volume continue to increase
 - Moore's Law
 - CPU processing power doubles every 18 months
 - Gilder's Law
 - Network bandwidth doubles every 12 months
- Sampling will become very important
 - Smart sampling
- Aggregation
 - Need to limit the amount of data that is stored
- Encryption
 - Higher level headers and contents of packets not available for monitoring



Distributed monitoring

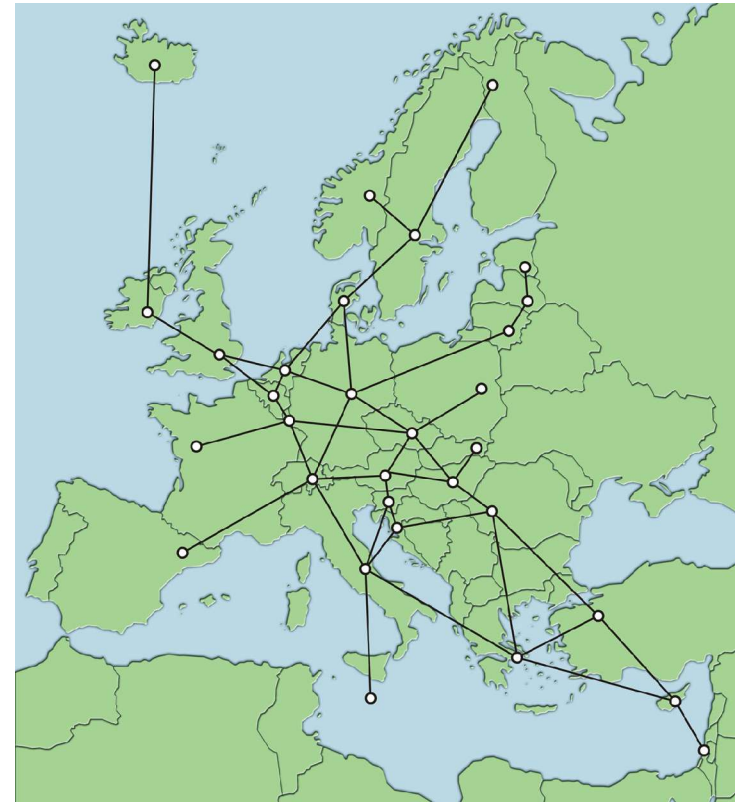


Information Society
Technologies

An IST Project

<http://www.ist-lobster.org>

- Collect data from multiple sensors
- Respond to events faster
- Less false alarms
- Robust against failures
- New challenges
 - privacy
 - anonymization
 - correlate and combine data





LOBSTER

- Specific Support Action project
 - Started 1 October 2004
 - Finishes in December 2006
- Main goal:
 - To develop an advanced European infrastructure for passive network traffic monitoring.
- Technical challenges
 - Distributed access to monitoring probes
 - DiMAPI
 - Admission control and anonymization



Thank you for attending the
LOBSTER tutorial



Information Society
Technologies

An IST Project

<http://www.ist-lobster.org>

<http://www.ist-lobster.org>