# Network measurement activities at UPC Barcelona

June 3, 2011

# About us

- Advanced Broadband Comm. Center (CCABA)
  - Research center at UPC
  - Several topics: optical networking, new Internet arch., nano-networking, network measurements, …
- People (in network measurements)
  - Jordi Domingo-Pascual, Josep Solé-Pareta (Full profs.)
  - Pere Barlet-Ros (Assistant prof.)
  - Josep Sanjuàs-Cuxart (PhD student)
  - 3 more PhD students (V. Carela, J. Mikians, I. Paredes)

# Research topics (outline)

- Traffic analysis
- Monitoring systems
- Efficient measurement algorithms
- Interdomain TM characterization
- Traffic classification
- Anomaly detection
- (Bandwidth estimation in WLAN)

# Traffic analysis

- Monitoring platforms
  - CESCA NREN (10 GbE)
  - UPC network (1 GbE)
  - Several Endace cards (1 and 10 GbE)
  - Live traffic, full packet traces, HTTP logs
  - GÉANT NetFlow data (18 POPs)
- Traffic studies
  - HTTP traffic analysis (one-click file hosting)
  - Network anomalies in backbone networks
  - World IPv6 day (ongoing)

# Monitoring systems

- CoMo
  - Joint work with Gianluca Iannaccone (Intel labs)
  - Modular passive monitoring system (open source)
  - Involvement in its design and development
  - Predictive resource management (load shedding)
- Promoting CoMo within the COST-TMA
  - “Code-to-the-data” approach for data sharing
- SMARTxAC
  - Ad-hoc monitoring system for CESCA NREN

# Efficient measurement algorithms

- Joint work with R. Kompella (Purdue), N. Duffield (AT&T)
- Efficient passive delay measurement
  - Outperforms existing techniques (both active and passive)
  - Overcomes linear relationship sample size/net. overhead
  - Improved analysis of LDA (unknown loss, net. overhead)
  - Per-flow delay measurement (delay sketching)
- Adaptive flow sampling with a fixed memory budget
  - Cuckoo sampling (inspired in Cuckoo hashing)
  - Extremely simple data structure and algorithm
  - Outperforms Adaptive NetFlow (packet sampling)
  - Cost independent of mem. size, normalization not needed

# Efficient measurement algorithms

- Trade (some) accuracy for performance
  - Fit data structures in SRAM
  - Few memory accesses per packet
- Measurement over sliding windows
  - Bitmaps (counting active flows)
  - Bloom filters (traffic filtering)
  - Approximate expiration (not full timestamps)
- Portscan detection
  - Early filtering, whitelist known servers, top-k detection

# Interdomain TM characterization

- Joint work with C. Dovrolis (Gatech), A. Dhamdhere (CAIDA)
- Studying statistical properties of the Interdomain TM
  - Obstacle: Lack of adequate traffic data
  - NetFlow data from GÉANT (18 POPs) and Internet2
  - Characterize row distributions (impact of congestion)
  - Sparsity, low rank, prefix popularity, etc.
- Future work
  - Study temporal properties and longitudinal evolution
  - Synthetic generation of realistic ITM

# Traffic classification

- Addressing practical problems
  - Joint collaboration with two Spanish companies
  - Developing a commercial prototype
  - Multi-gigabit performance (> 200 Gb/s)
  - Reduce deployment and operational costs
    - Sampled NetFlow (no packet level access)
    - Autonomic training (no human intervention)
    - Combine multiple state-of-the-art techniques
  - Reduce impact of (aggressive) sampling

# Anomaly detection

- Investigating important aspects to operators
  - Joint work with DANTE, UK
  - Comparison of three commercial AD products
  - Study of the anomalies in the GEANT backbone
- Automatic extraction of anomaly evidence
  - Joint work with X. Dimitropoulos (ETH Zurich)
  - Frequent itemset mining algorithms
- Anomaly detection with Sampled NetFlow
  - Evaluation/reduction of the impact of sampling

# (Bandwidth estimation in WLAN)

- Analysis of current mechanisms in WLAN links
  - Measure the achievable throughput
  - Dispersion-based measurements are biased
  - Solution: ignore first samples (transient state)
- Ongoing work
  - Poisson-based probing in WLAN links
  - Bandwidth estimation in hybrid paths
- Contact: Albert Cabellos (acabello@ac.upc.edu)

# Summary

- Working on several topics
  - Traffic classification, anomaly detection, traffic analysis, monitoring systems and algorithms, …
- Access to multiple sources of data
  - 1 and 10 GbE academic networks (packet level)
  - GÉANT backbone (NetFlow)
- Future work
  - Further analyze these data …

# References


- **Monitoring systems**
  - P. Barlet-Ros, G. Iannaccone, J. Sanjuàs-Cuxart, Amores-López, J. Solé-Pareta. “Load shedding in network monitoring applications”. USENIX ATC, 2007.
  - P. Barlet-Ros, G. Iannaccone, et al. “Robust network monitoring in the presence of non-cooperative traffic queries”. Computer Networks, 2009.
  - P. Barlet-Ros, G. Iannaccone, et al. “Predictive resource management of multiple monitoring applications”. Transactions on Networking, 2011.

- **Traffic analysis**
  - J. Sanjuàs-Cuxart, P. Barlet-Ros, et al. “Measurement Based Analysis of One-Click File Hosting Services”. Journal of Network and Systems Management, 2011.

- **Efficient measurement algorithms**
  - J. Sanjuàs-Cuxart, P. Barlet-Ros, J. Solé-Pareta. “Counting flows over sliding windows in high speed networks”. IFIP Networking, 2009.
  - J. Sanjuàs-Cuxart, P. Barlet-Ros, J. Solé-Pareta. “Validation and improvement of the Lossy Difference Aggregator to measure packet delays”. TMA, 2010.
  - J. Mikians, P. Barlet-Ros, J. Sanjuàs-Cuxart, J. Solé-Pareta. “A practical approach to detect port scans in very high speed links”. PAM, 2011.

- **Traffic classification**
  - V. Carela-Español, P. Barlet-Ros, M. Solé-Simó, A. Dainotti, W. Donato, A. Pescapé. “K-dimensional trees for continuous traffic classification”. TMA, 2010.
  - V. Carela-Español, P. Barlet-Ros, A. Cabellos-Aparicio, et al. “Analysis of the impact of sampling on NetFlow traffic classification”. Computer Networks, 2011.

- **Anomaly detection**
  - I. Paredes-Oliva, X. Dimitropoulos, et al. “Automating root-cause analysis of network anomalies using frequent itemset mining”. SIGCOMM (demo), 2010.
  - M. Molina, I. Paredes-Oliva, W. Routly, P. Barlet-Ros. “Operational experiences with anomaly detection in backbone networks”. Submitted to Comsec, 2011.

- **Bandwidth estimation in WLAN**
  - M. Portoles, A. Cabellos, J. Mangues, A. Banchs, J. Domingo. “Impact of transient CSMA/CA access delays on active bandwidth measurements”. IMC, 2009.