Appmon: An Application for Accurate per Application Network Traffic Characterization

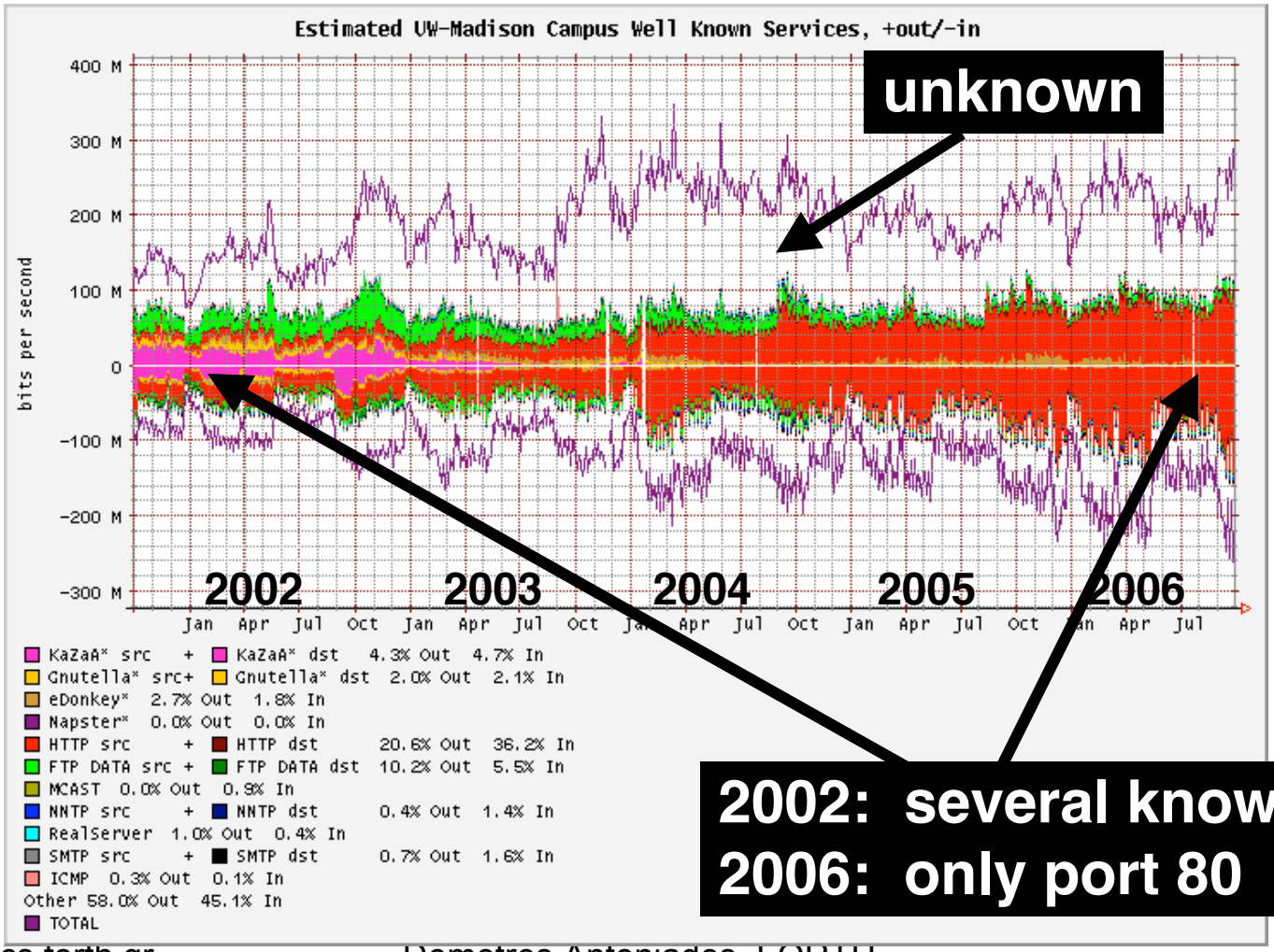
Demetres Antoniades
Michalis Polychronakis
Evangelos P. Markatos

Distributed Computing Systems Lab
Institute of Computer Science
Foundation for Research and Technology Hellas
Crete - Hellas

RoadMap

- Motivation
- Appmon
  - Overall Design
  - Web Interface
- Performance Measurements
- Deployment
- Conclusions

Current View of the Network



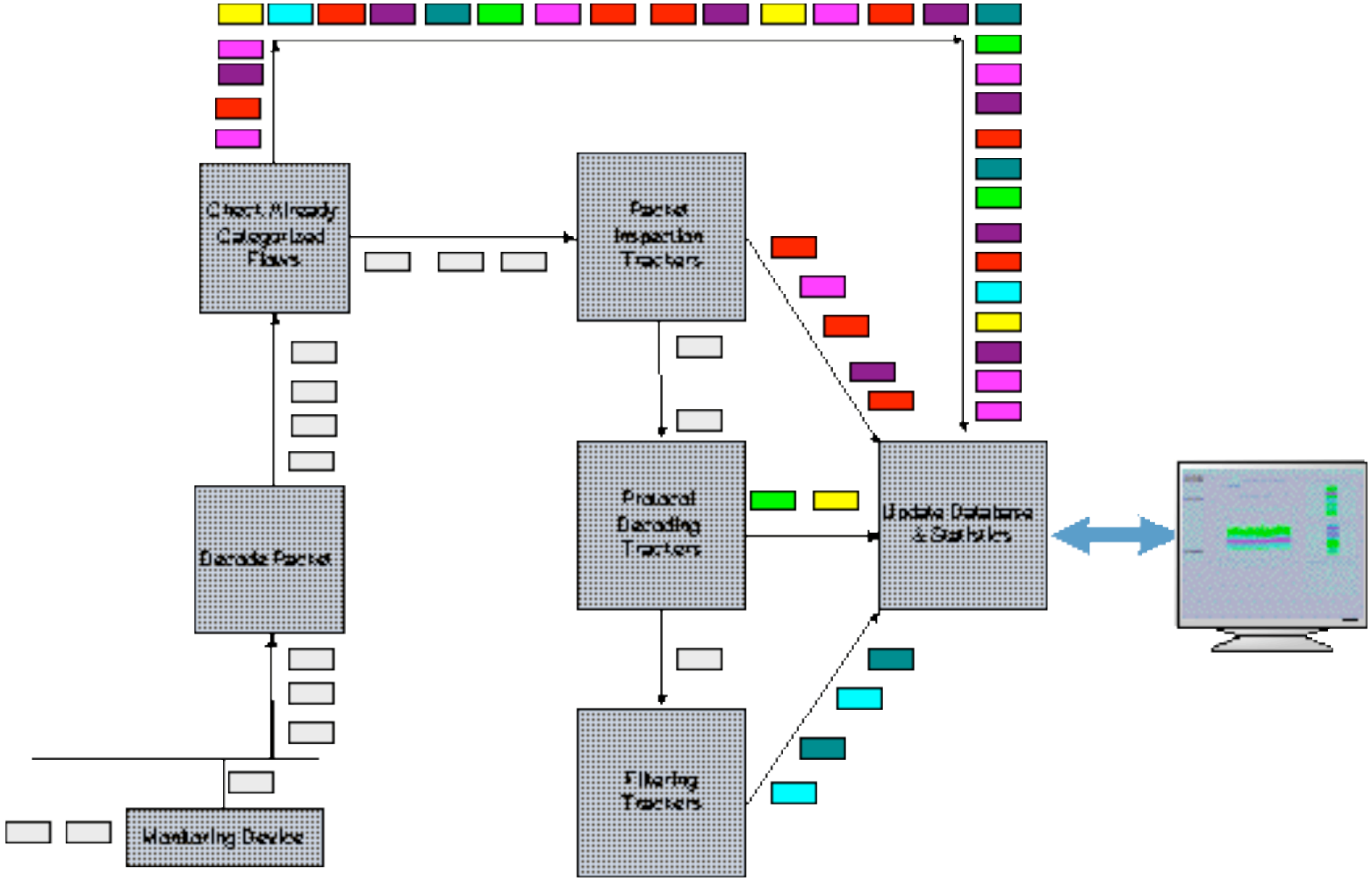
Motivation

- Widely used applications that use dynamic ports
  - Not known in advance
  - Difficult to monitor
- We are not sure even for known ports any longer …
  - Most of port 80 traffic is not web traffic!
- *appmon* uses deep packet inspection to accurately attribute traffic to applications

Our Approach

- Design an application in order to **categorize** and **visualize** in **real-time** per-Application traffic
- Answer common questions
  - What applications are running in my network?
  - Which of them consumes most of the bandwidth?
  - Which hosts are consuming most of my organization's network bandwidth and what applications are they running?

Overall Application Design



Application Tracker Types

- Deep Packet Inspection Trackers
  - Search the packets for specific and unique application strings
- Decoding Trackers
  - Fully decode the protocol in order to extract the used ports
  - Used for protocols that use a predefined control port
- Filtering Trackers
  - Apply BPF filtering for well-known protocols that use predefined ports

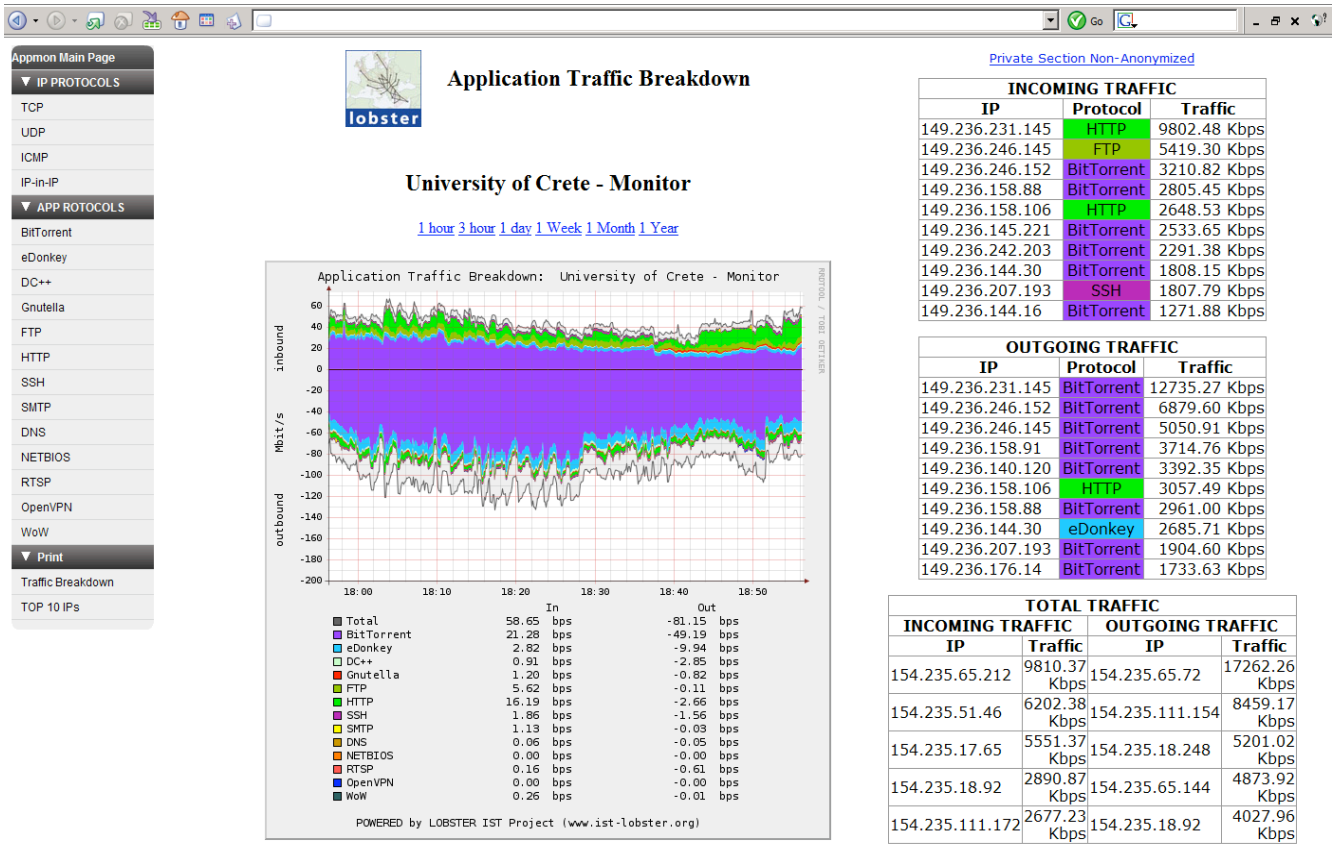
State Keeping

- Keep categorized flows (5-tuples) in order to minimize the number of processed packets.
- Keep per Application TOP bandwidth consuming IP addresses.

Categorized Protocols

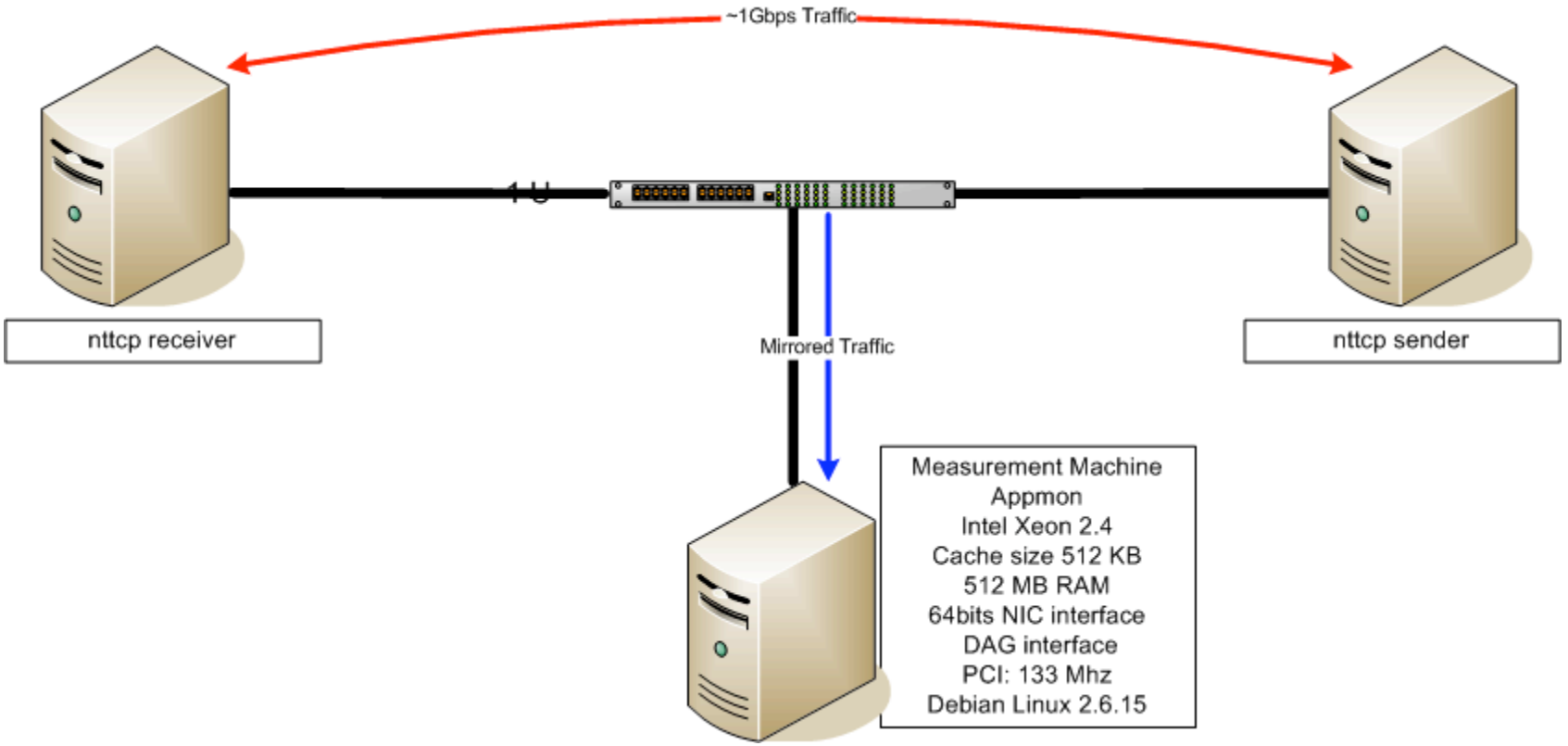
Layer 4 Protocols	**Application Protocols**	
TCP	BitTorrent	eDonkey
UDP	Direct Connect	Gnutella
ICMP	Bluesky	PPStream
IP-in-IP	FTP	HTTP
	SSH	SMTP
	DNS	NetBIOS
	RTSP	OpenVPN

Application Web Interface

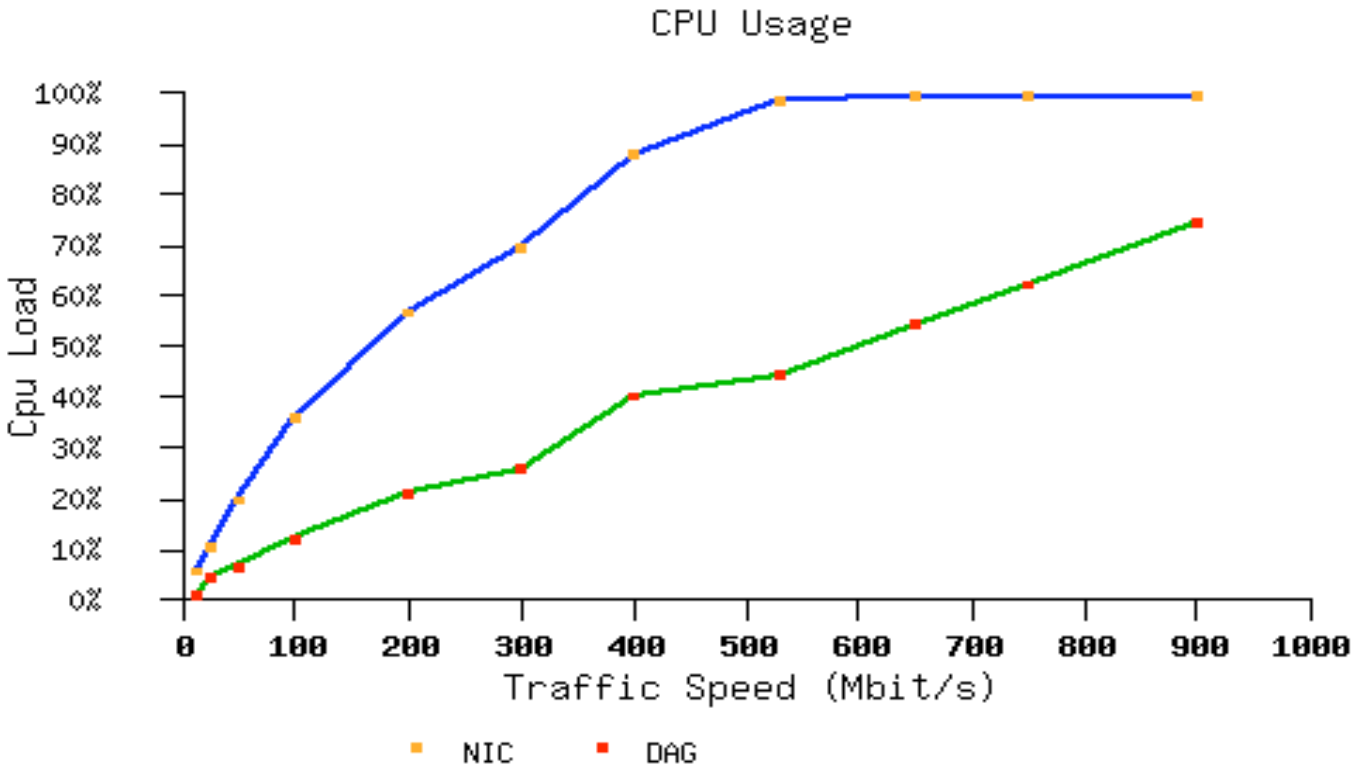


- Graph representation of each categorized per-application traffic portion
- Presentation of ***"Top 10"*** bandwidth consuming IP addresses
  - *Prefix Preserving Anonymization* for public view
- Menu Selection for explicit application view

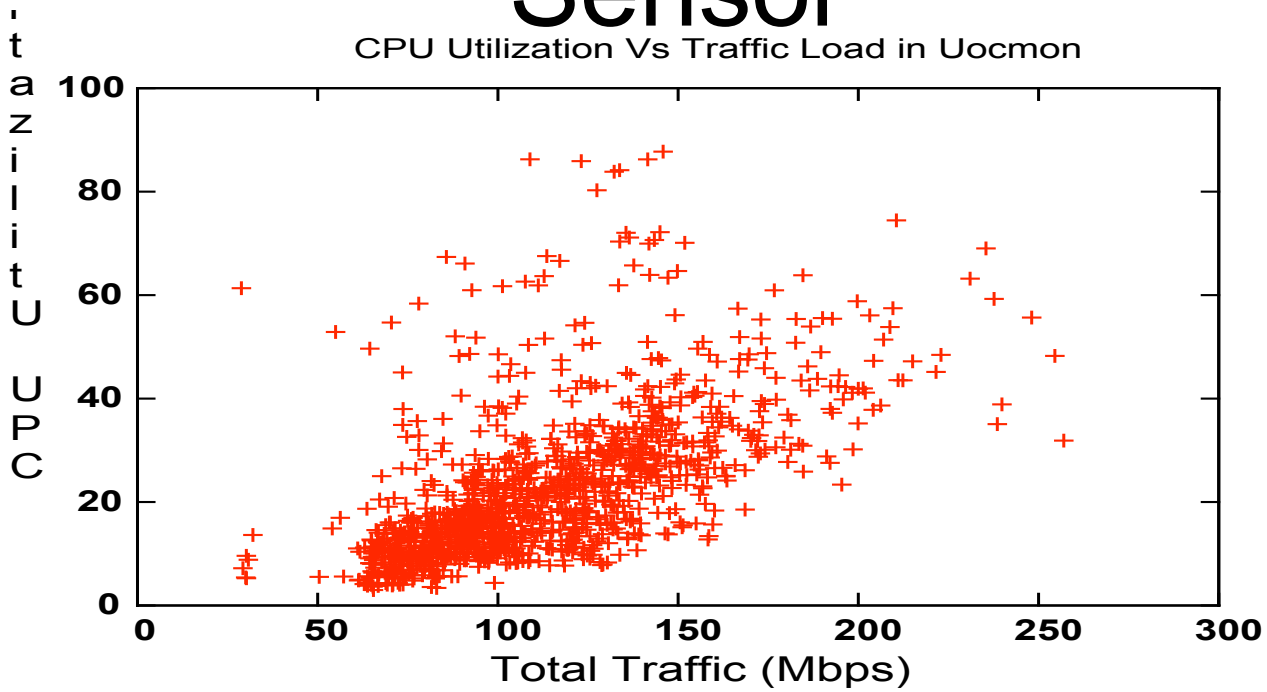
Experimental Setup



Processed Traffic Vs. CPU Load



Performance on a fully Operational Sensor

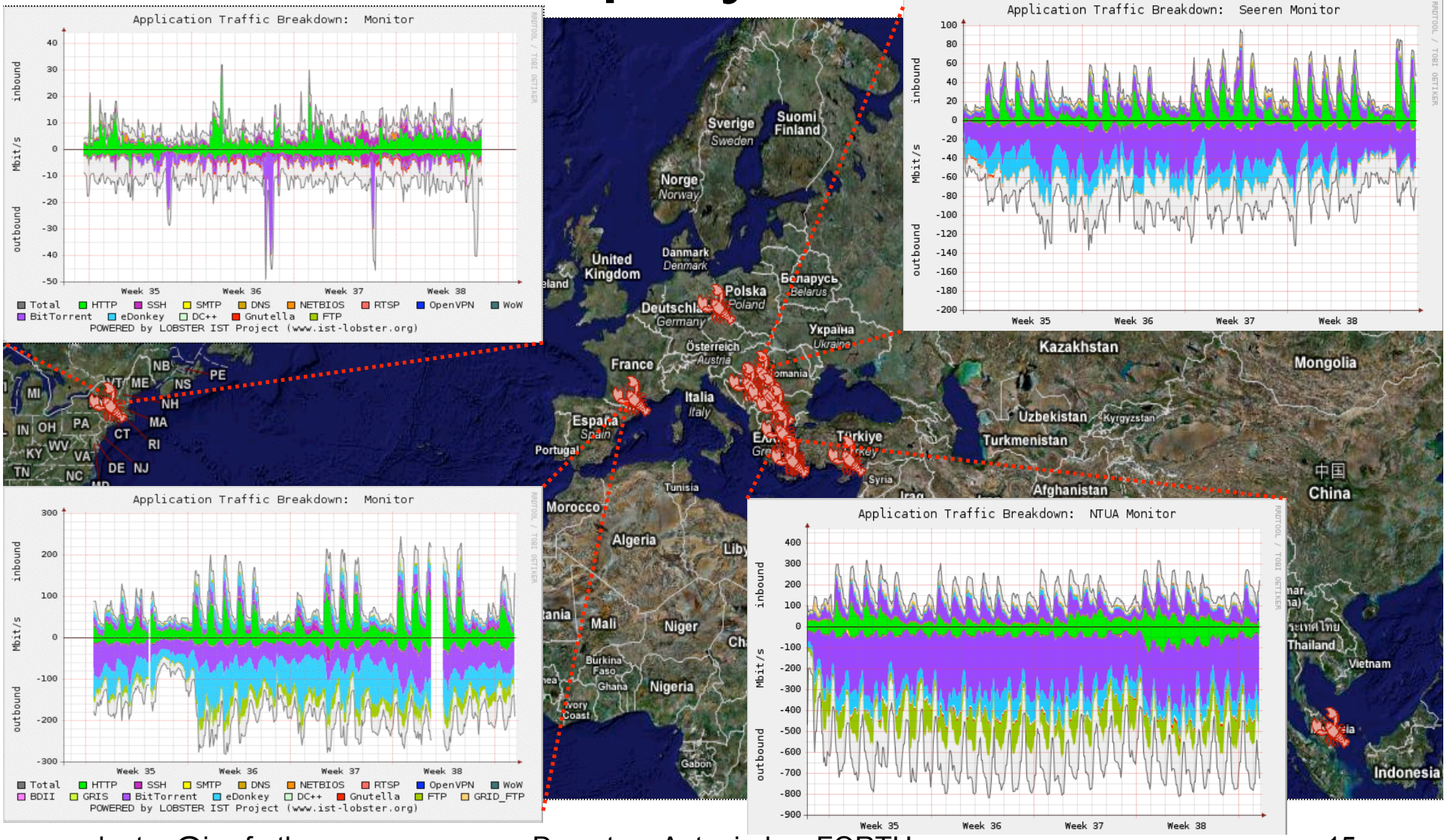


- Monitoring traffic at University of Crete
- Measuring traffic and CPU load every 10 seconds

False Positives

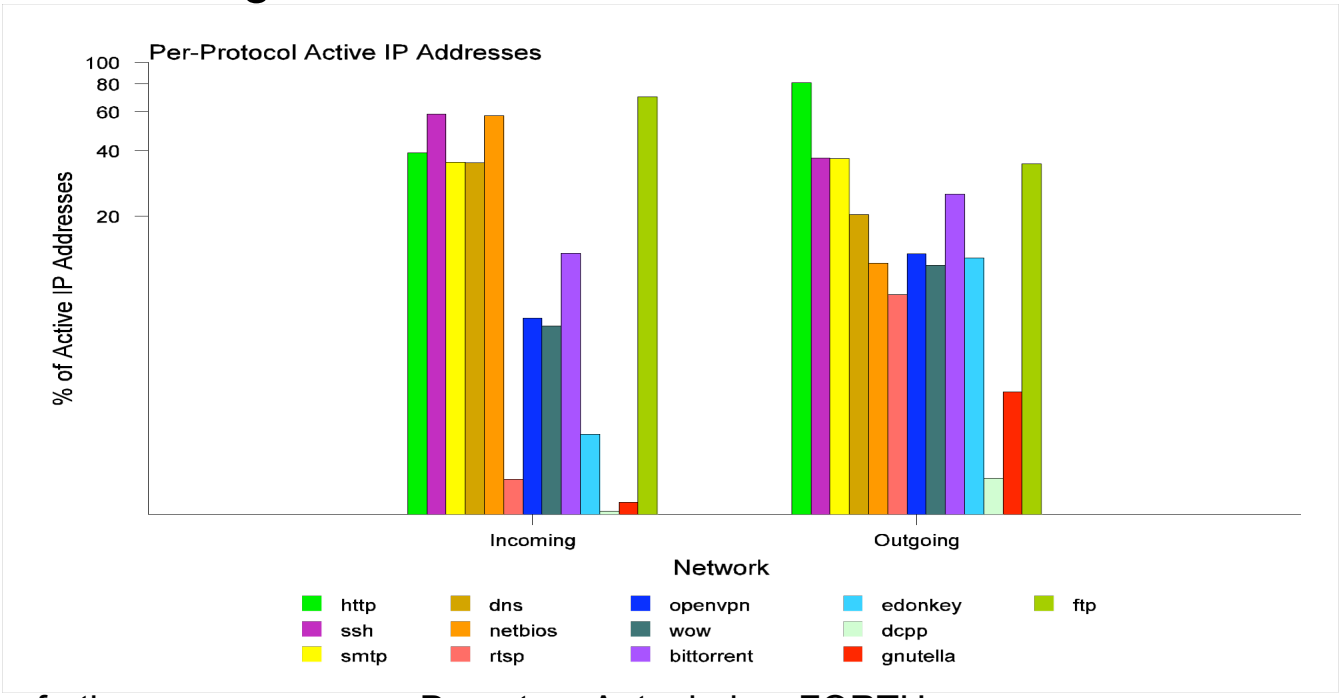
- Tested Deep Packet Inspection and Decoding Trackers
- 3 1Gbyte Web traces
  - No classified traffic from any tracker function
- Specific Application Traces
  - Only the corresponding tracker reported classified traffic

Deployment


Application Traffic Breakdown: Monitor
Application Traffic Breakdown: Seeren Monitor
Application Traffic Breakdown: Monitor
Application Traffic Breakdown: NTUA Monitor
inbound
outbound
Mbit/s
Week 35
Week 36
Week 37
Week 38
Total HTTP SSH SMTP DNS NETBIOS RTSP OpenVPN WoW
BitTorrent eDonkey DC++ Gnutella FTP
BDII GRIS GRID_FTP
POWERED by LOBSTER IST Project (www.ist-lobster.org)
Sverige Sweden
Suomi Finland
Norge Norway
United Kingdom
Danmark Denmark
Беларусь Belarus
Polska Poland
Deutschland Germany
Україна Ukraine
Österreich Austria
France
Italia Italy
España Spain
Portugal
Kazakhstan
Mongolia
Uzbekistan
Kyrgyzstan
Turkmenistan
Türkiye
Syria
Afghanistan
中国 China
Tunisia
Morocco
Algeria
Mali
Niger
Burkina Faso
Ghana
Nigeria
Ivory Coast
Gabon
Thailand
Vietnam
Indonesia
NB PE NS ME VT NH MA CT RI MI IN OH PA WV KY VA TN NC DE NJ

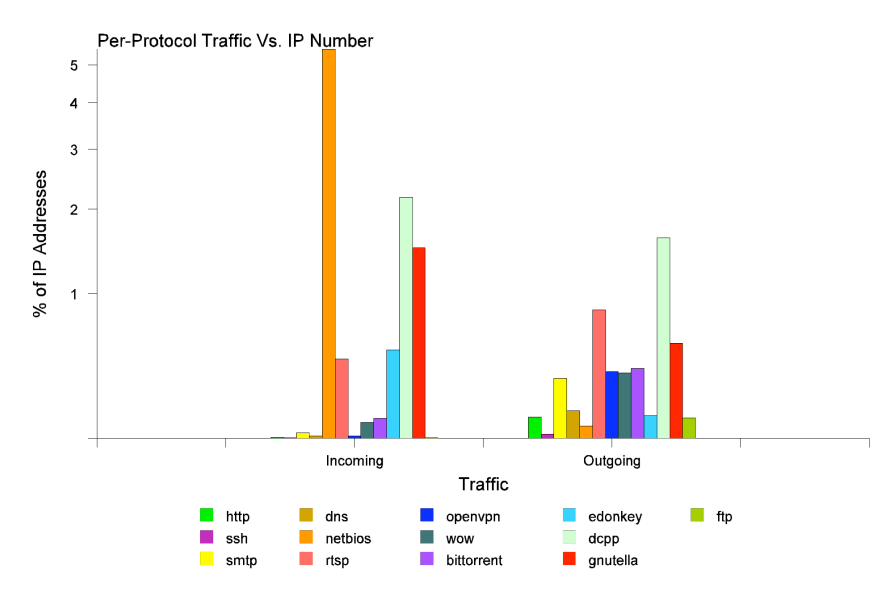
Real World Observations 1/2

- BitTorrent & eDonkey are the most bandwidth consuming protocols
- HTTP is still the most widely used client-server protocol
  - Has the largest number of Active IP addresses

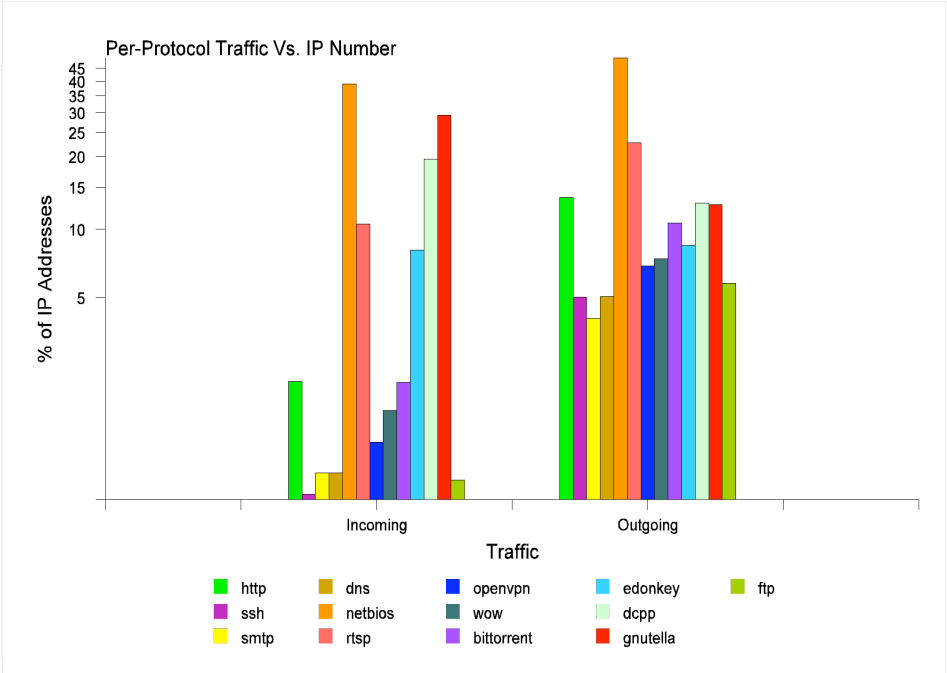


Real World Observations 2/2

- "Elephants" are getting larger
  - A small portion of IP address contributes most of the traffic



50% of Traffic



99% of Traffic

Conclusions

- Presented *“appmon”* an application for Accurate per Application Network Traffic Characterization.
- Able to monitor traffic in Gbit speeds, using a DAG card and 500 Mbits using a regular Ethernet interface.
- Steady performance when deployed in a real production environment.
- World wide deployment.

Thank You!!!


QUESTIONS COMMENTS
FEEDBACK QUESTIONS
COMMENTS FEEDBACK QUESTIONS
COMMENTS

Appmon: An Application for Accurate per Application Network Traffic Characterization

Demetres Antoniades
Michalis Polychronakis
Evangelos P. Markatos

Distributed Computing Lab
Institute of Computer Science
Foundation for Research and Technology Hellas
Crete - Hellas