



POLITECNICO DI TORINO
Repository ISTITUZIONALE

Network Highlighter

Original

Network Highlighter / Giordano, Danilo; Traverso, Stefano; Grimaudo, Luigi; Baldi, Mario; Baralis, Elena; Mellia, Marco. - STAMPA. - (2014). ((Intervento presentato al convegno Traffic Monitoring and Analysis (TMA) tenutosi a Londra nel 14 April 2014.

Availability:

This version is available at: 11583/2675282 since: 2017-06-28T10:43:30Z

Publisher:

IFIP

Published

DOI:

Terms of use:

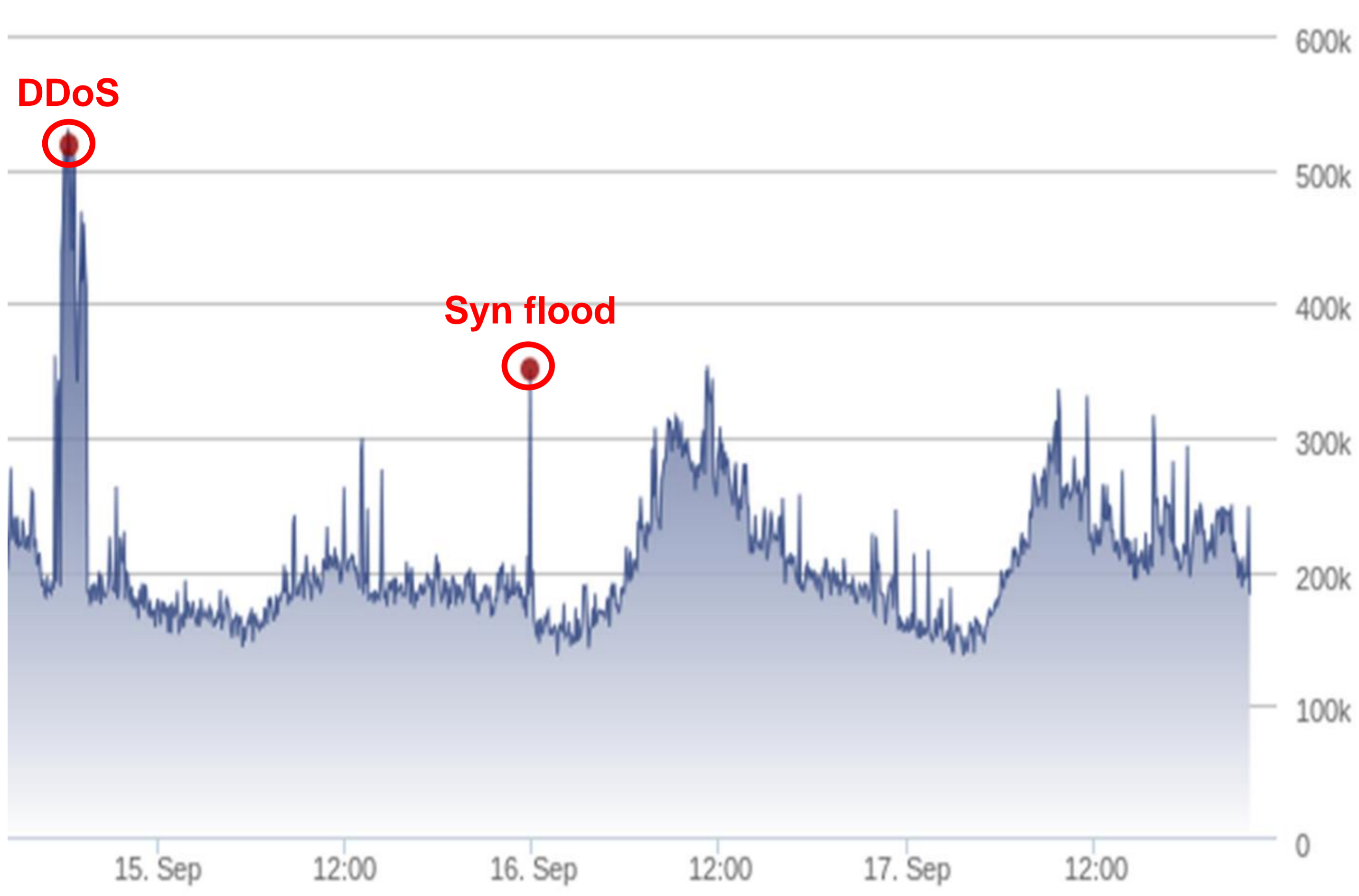
openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

Network Highlighter is fundamental to spot unusual and unknown behaviour



Paramount task of network highlighter

- Security
- Performance/Troubleshooting
- Traffic monitoring

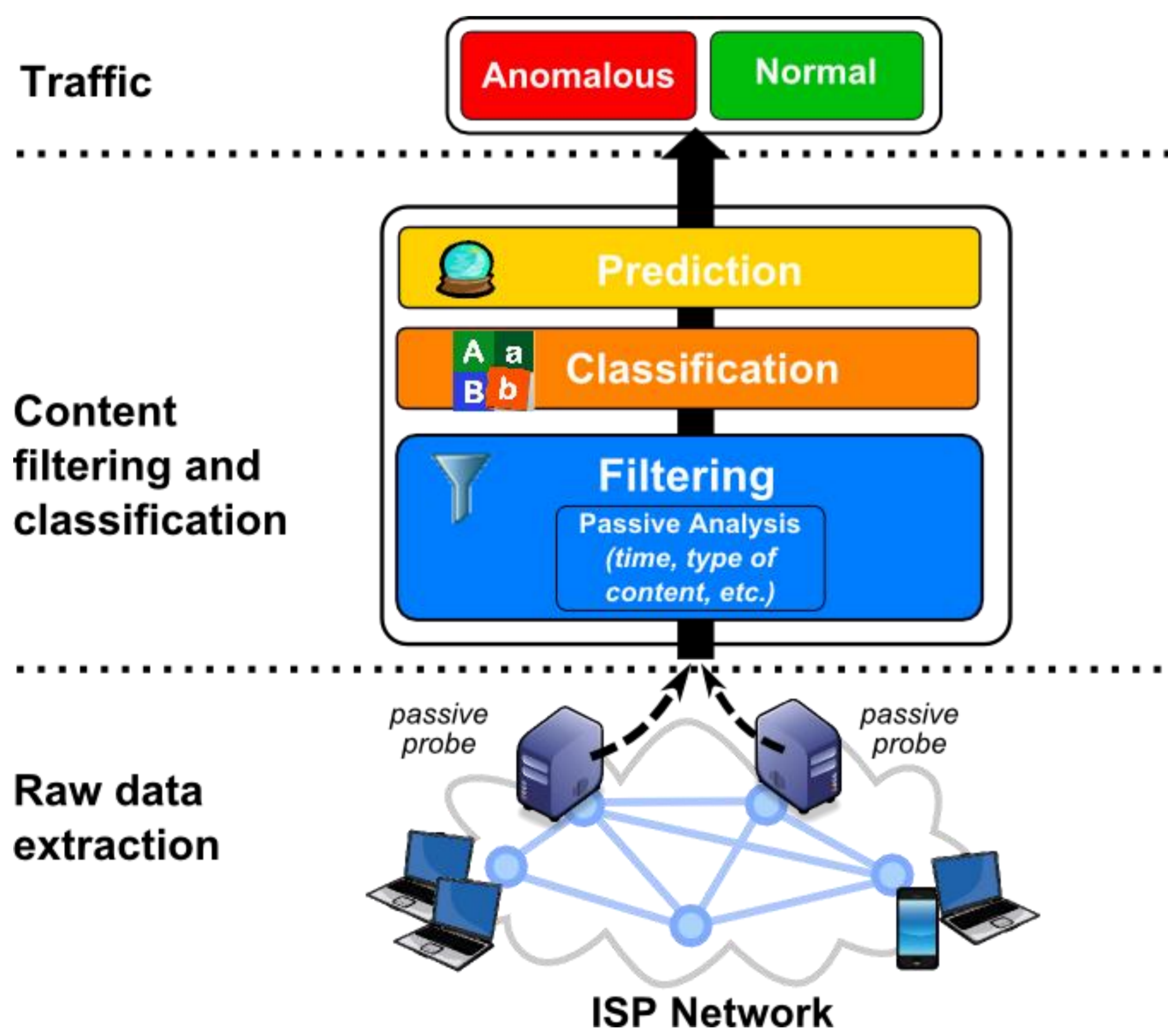
Network behaviour and infrastructure change very fast

- How to spot anomalies? What is normal and what is not?
- Reactive manual approach completely fails
- Need of automatic tools for anomaly detection in large scale networks
- CDNs/cloud systems make network even more complex: Akamai, YouTube, Amazon

Our proposal is a distributed and comprehensive framework

- To automatically spot anomalous traffic
- To provide administrators with a tool to "understand what is happening" in their networks
E.g.: Capture sudden change in CDN (YouTube, Facebook, etc.) traffic patterns

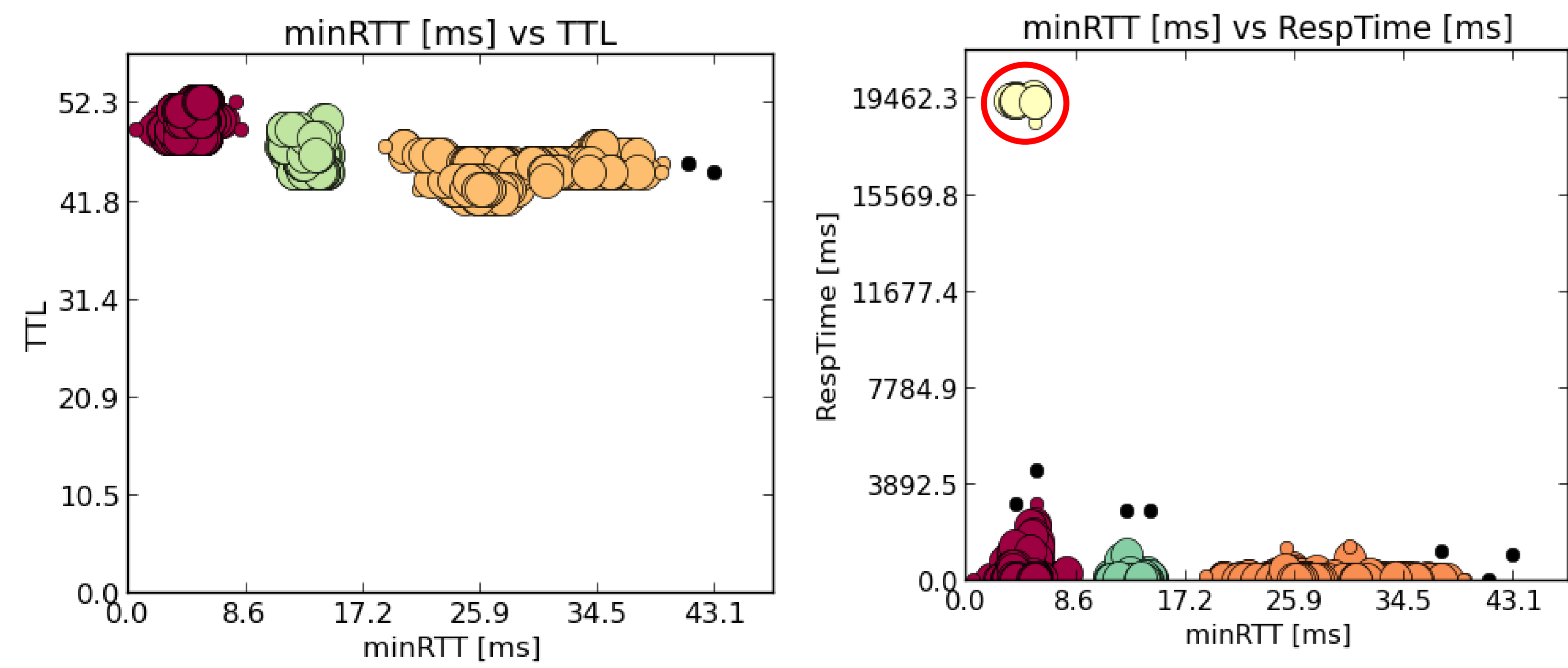
Our network highlighter workflow



Anomalous	Security issue, performance problem, unusual redirect, etc.
Normal	useful to build baselines and normal traffic patterns
Prediction	Kalman filter, Linear/Gaussian Regression
Classification	Data mining and Clustering techniques: DBScan, Multidimensional Subspacing, Ad-Hoc clustering algorithms
Filtering (Feature extractor)	IP address, RTT, TTL, Port Number, service, device, etc.

Preliminary Results on YouTube infrastructure

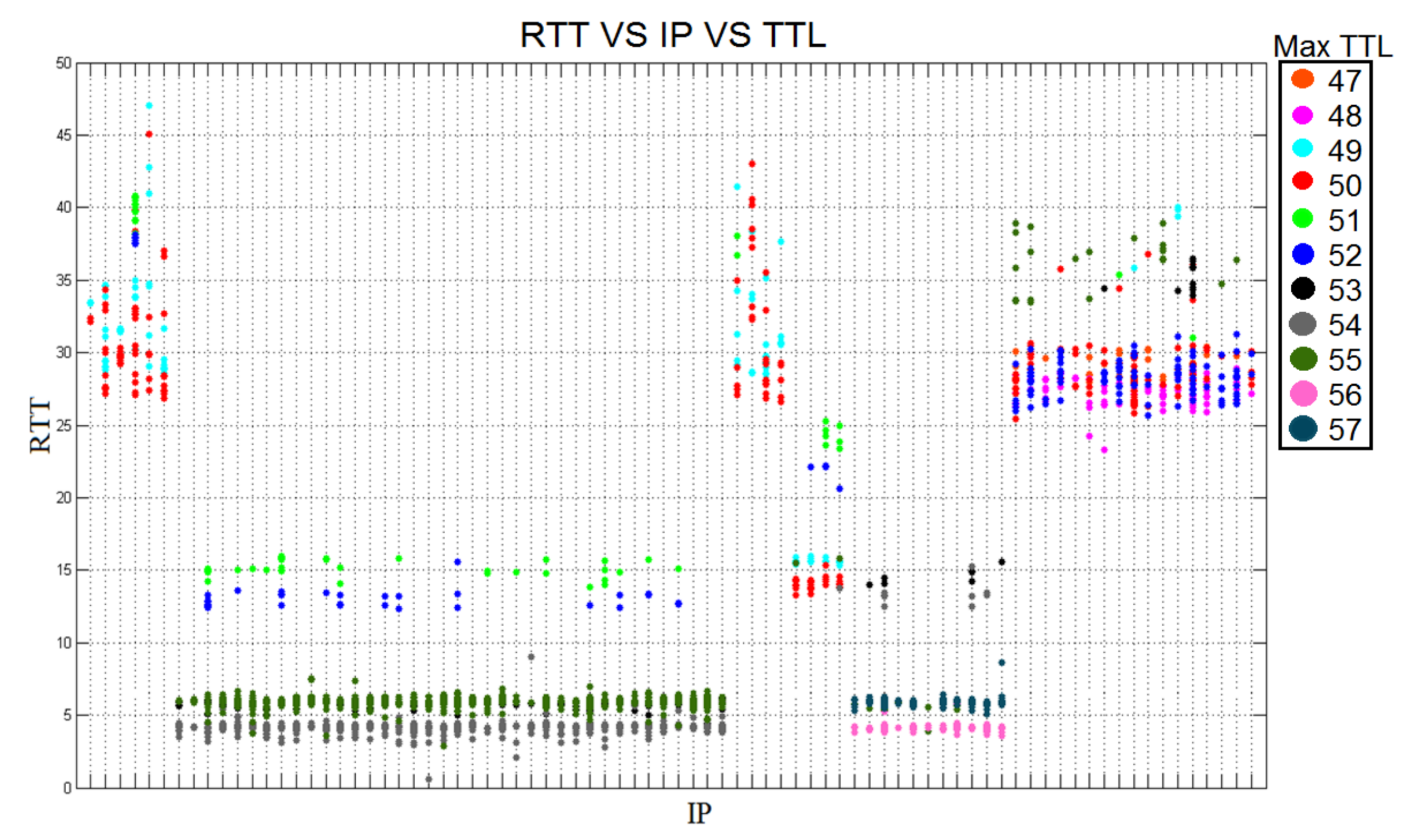
Clustering Technique



- ✓ Three different clusters
- ✗ A single IP address can be present in two clusters

- ✓ Four distinct clusters
- ✓ A single client creates an outlier cluster
- ✗ The outlier cause a wrong normalization
- ✗ Automatic crosscheck still needed

Multi-Dimensional Visual Technique



- ✓ Easier to detect server classic behaviour
- ✗ Harder to identify anomalies

Classic clustering techniques are not adequate for network modelling, new ad-hoc solutions have to be developed