Exploring Graph-based Network Traffic Analysis

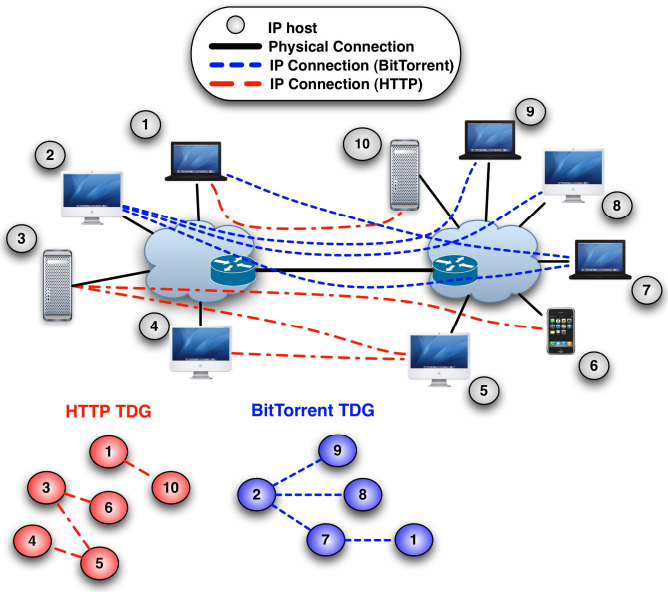
Marios Iliofotou, H. Kim, M. Faloutsos, M. Mitzenmacher, P. Pappu, and G. Varghese
Department of Computer Science and Engineering - University of California, Riverside

Traffic Analysis Using Traffic Dispersion Graphs (TDGs)

❑ What is this poster about

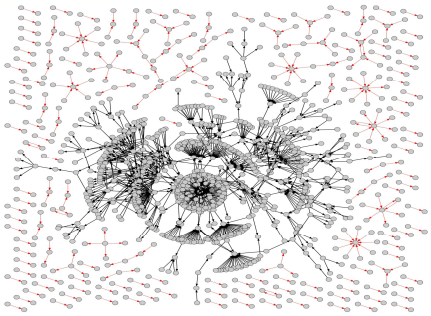
1. How to generate and model TDGs
2. Practical applications of TDGs

❑ Graph formation (toy example)



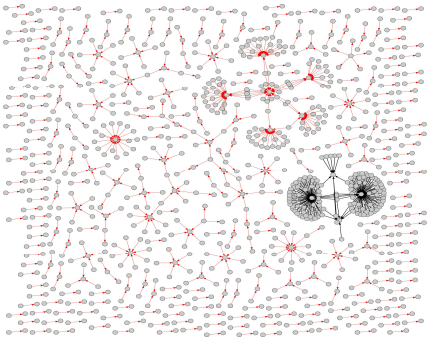
❑ Edge Selection

- Using well-known ports and payload
- Using machine learning classification and clustering methods



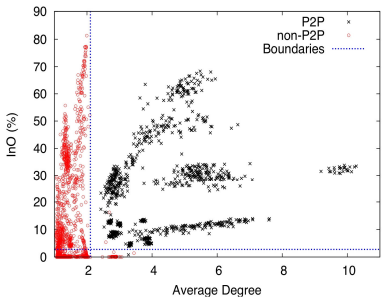
Example of a P2P TDG: Gnutella
- One large connected component
- High average degree

[Trace from: Palo Alto Internet Exchange.]



Example of a Client-Server TDG: HTTP
- Large number of small components
- Graph is less dense compared to P2P TDGs

[Trace from: Palo Alto Internet Exchange.]

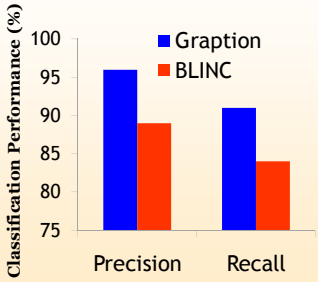


Graph Classification
- Small set of metrics can distinguish between application classes
- Scatter plot shows that fixed threshold can classify TDGs across multiple backbone locations (4 traces)

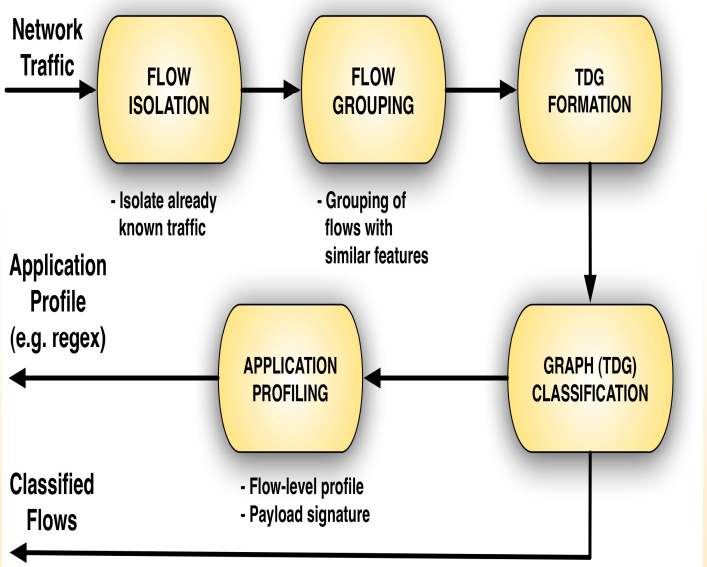
Graption: Graph-based Traffic Classification

❑ About Graption

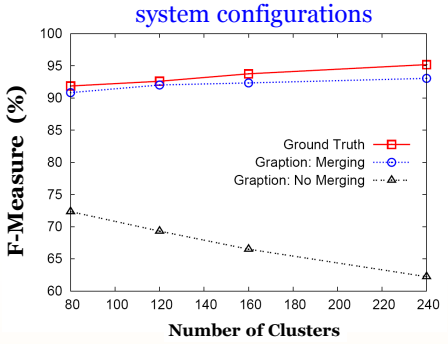
- Classifies network flows using network-wide interactions
- Case study: Use Graption to detect P2P Traffic
- Graption can automate the extraction of application profile
- Performs better than host-based methods at the backbone



The Graption Methodology



Graption over various system configurations



Per application classification performance