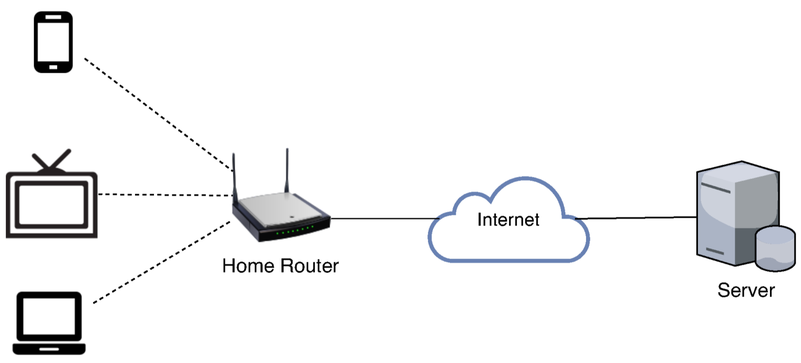
INSaNE: Improving Network Security at the Network Edge

CO-Pis: Edmundo de Souza e Silva (UFRJ), Antônio Abelém (UFPA), Don Towsley (UMass, Amherst)

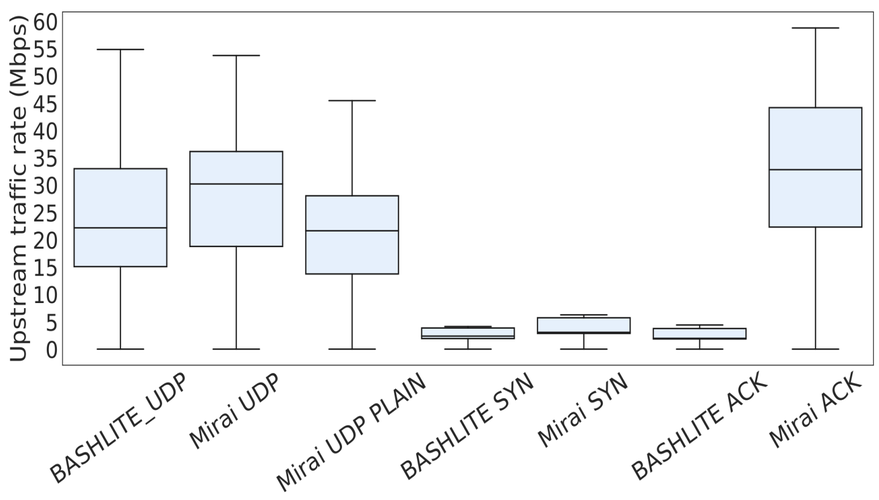
Measurement Infrastructure



- Over 4,000 home-routers
- Latency, loss
- Upstream / downstream packet and byte rates

Lightweight Approach for DDoS Detection at Home Gateways

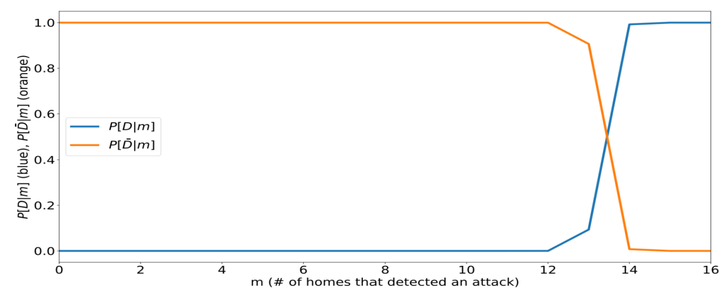
- Experiments with malwares



- Machine Learning classifier

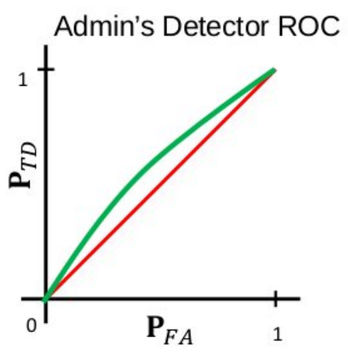
	Accuracy	Precision	Recall	F1 Score
Results	0.9998	0.9966	0.9838	0.9901

- Spatio-temporal correlation



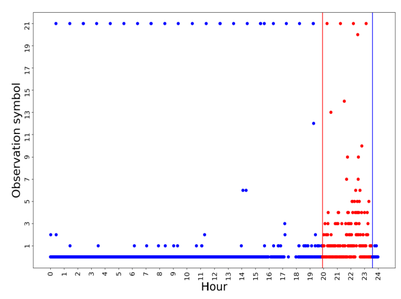
Covertness model for botnets

- Net admin controls N homes
- Adversary controls M <= N homes
- How much damage can attacker do without being detected?
  - Statistical hypothesis testing
- **Result**: Attacker cannot launch from W($\sqrt{n}$) homes without being detected

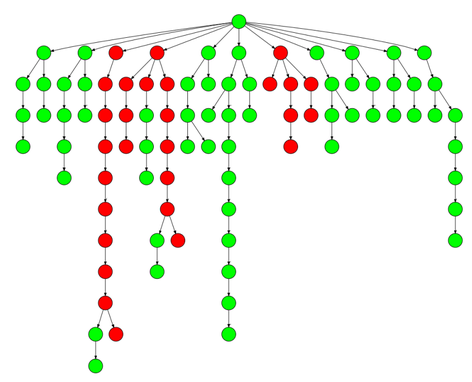


Anomaly detection based on QoS metrics

- Packet loss model



- Spatio-temporal correlation



Detecting home user traffic anomalies

- Tensor Decomposition (PARAFAC)
- DDoS attacks detected from model residuals