

240 - Topics for projects

1-- Detecting patterns and anomalies in BGP traffic

- Identify patterns and anomalies in BGP data
- Correlate and compare traffic patterns across different links and routers
- "BGP-lens: Patterns and Anomalies in Internet Routing Updates"
B. A. Prakash, N. Valler, D. Andersen, M. Faloutsos and Christos Faloutsos
ACM SIGKDD'09, industrial track, Paris 2009.
- An Internet Routing Forensics Framework for Discovering Rules of abnormal BGP events, Li et al.,
Computer Communication Review, vol 35, No. 5, 2005 (I have hardcopy)
- Realistic BGP Traffic for Test Labs. Olaf Maennel and Anja Feldmann
<http://www.acm.org/sigcomm/sigcomm2002/papers/bgplab.html>
- Siganos and Faloutsos. "BGP Routing: A study at Large Time Scale" Global Internet Symposium, Taipei, Taiwan, November 17-21, 2002

Resources: www.BGPmon.io we know the director
<https://www.caida.org/data/overview/> ready to download traces

2-- Model and Generate realistic Internet and BGP graphs

- Generate realistic topologies that match properties of real communication networks
- Identify patterns and anomalies in real network topologies
- "Policy-Aware Topologies for Efficient Inter-Domain Routing Evaluations"
Yihua He and Michalis Faloutsos and Srikanth V. Krishnamurthy and Marek Chrobak IEEE INFOCOM 2008
Mini-Conference, Phoenix, AZ, USA, April 2008.
- Y. He et al "A systematic framework for unearthing the missing links: Measurements and Impact" NSDI 07
(email yhe@cs for preprint)
- On the Hierarchical Structure of the Logical Internet Graph, ,
Z. Ge, D.R. Figueiredo, S. Jaiwal, L.Gao ITCOM'2001.
- "On Inferring Autonomous System Relationships in the Internet " Lixin Gao,
Global Internet Symposium in Globecom 2001
- Reducing Large Internet Topologies for Faster Simulations, V. Krishnamurthy et al, Proceedings of IFIP
Networking 2005, Waterloo, Ontario, Canada, May 2-6, 2005

3-- Modeling virus and instability propagation

- Given a virus or some information that is spreading in a network, while it spread or die out quickly?
- Consider two competing virus in one network and ask the same question.
- Consider a non-binary entity that propagates in the network and model and predict its outcome.
- 1-- Non-Binary Information Propagation: Modeling BGP Routing Churn,
Nicholas Valler, M. Butkiewicz, B. Aditya Prakash, Michalis Faloutsos, Christos Faloutsos
In Network Science for Communication Networks, NetSciCom 2011
- 2-- Competing Memes Propagation on Networks: A Network Science Perspective.
Xuetao Wei, Nicholas Valler, B. Aditya Prakash, Iulian Neamtiu, Michalis Faloutsos, Christos Faloutsos: IEEE
Journal on Selected Areas in Communications 31(6): 1049-1060 (2013)

Related reading

- Information Survival Threshold in Sensor and P2P Networks D. Chakrabarti, J. Leskovec, C. Faloutsos, S. Madden, C. Guestrin and M. Faloutsos
IEEE INFOCOM 2007, Anchorage, Alaska.

Resources: python has powerful graph libraries, the grafos.ml project at Telefonica

4-- Graph-based techniques for traffic analysis

- Classify traffic by modeling it as an interaction graph
- Entelecheia: Detecting P2P botnets in their waiting stage.
Huy Hang, Xuetao Wei, Michalis Faloutsos, Tina Eliassi-Rad: Networking 2013: 1-9
- Profiling-By-Association: a resilient traffic profiling solution for the internet backbone.
Marios Iliofotou, Brian Gallagher, Tina Eliassi-Rad, Guowu Xie, Michalis Faloutsos: ACM CoNEXT 2010

5-- Analyzing router behavior: hacking, detecting and malware

Routers have started to be hacked and exploited and there is limited work on protecting routers.

- (a) How can we hack a router?
- (b) Understanding the malware of a router?
- (c) Detecting infected routers: distinguishing them from non-infected routers

-- Don't Trust Your Router: Detecting Compromised Routers

A Darki, A Duff, Z Qian, G Naik, S Mancoridis, M Faloutsos ACM CONEXT student workshop