

Nick Feamster

Assistant Professor

School of Computer Science
Klaus Advanced Computing Building
Georgia Institute of Technology
266 Ferst Drive, Room 3348
Atlanta, GA 30332-0765, USA
+1 404 385 1944
feamster@cc.gatech.edu

Table of Contents

EDUCATIONAL BACKGROUND	3
EMPLOYMENT HISTORY	3
CURRENT FIELDS OF INTEREST	3
I. TEACHING	4
A. Courses Taught	4
B. Curriculum Development	4
C. Individual Student Guidance	5
C.1. Postdocs Supervised	5
C.2. Ph.D. Students Supervised	5
C.3. Masters Students Supervised	7
C.4. Undergraduate Students Supervised	8
C.5. Special Projects	8
II. RESEARCH AND CREATIVE SCHOLARSHIP	10
A. Theses	10
B. Journal Publications	10
C. Books and Book Chapters	10
D. Refereed Conference Publications	10
E. Workshop Publications	13
F. Other	15
F.1. Submitted Journal Papers	15
F.2. Submitted Conference and Workshop Papers	15
F.3. Other Technical Reports, Unrefereed Papers, and Drafts in Preparation	15
F.4. Software	17
F.5. Conference Posters and Demos	18
G. Research Proposals and Grants (Principal Investigator)	19
H. Research Proposals and Grants (Contributor)	23
I. Other	23
J. Research Honors and Awards	23
III. SERVICE	25
A. Professional Activities	25
A.1. Memberships and Activities in Professional Societies	25
A.2. Conference Committee Activities	25
A.3. Workshops and External Courses	26
B. On-Campus Georgia Tech Committees	27
C. Member of Ph.D. Examining Committees	28
D. Consulting, Advisory, and Other External Appointments	29
E. Research Project Reviewer	30
IV. NATIONAL AND INTERNATIONAL RECOGNITION	31
A. Invited Conference Session Chair	31
B. Patents	31
C. Editorial and Reviewer Work for Technical Journals and Publishers	31
V. OTHER CONTRIBUTIONS	31
A. Seminar Presentations	31
VI. PERSONAL DATA	36

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2005	Massachusetts Institute of Technology Cambridge, MA <i>Dissertation:</i> Proactive Techniques for Correct and Predictable Internet Routing <i>Sprolws Honorable Mention for best MIT Ph.D. dissertation in computer science</i> <i>Advisor:</i> Hari Balakrishnan Minor in Game Theory	Computer Science
M.Eng.	2001	Massachusetts Institute of Technology Cambridge, MA <i>Dissertation:</i> Adaptive Delivery of Real-Time Streaming Video <i>Advisor:</i> Hari Balakrishnan <i>William A. Martin Memorial Thesis Award</i> (MIT M.Eng. thesis award)	Computer Science
S.B.	2000	Massachusetts Institute of Technology Cambridge, MA	Electrical Engineering and Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Assistant Professor	Georgia Institute of Technology	2006–Present
Postdoctoral Research Staff	Princeton University	Fall 2005
Research Assistant	Massachusetts Institute of Technology	2000–2005
Intern/Consultant	AT&T Labs–Research	2001–2005
Technical Associate	Bell Laboratories	1999
Intern	Hewlett-Packard Laboratories	1999
Technical Staff	LookSmart, Ltd.	1997

CURRENT FIELDS OF INTEREST

My research focuses on networked computer systems, with a strong emphasis on network architecture and protocol design; network security, management and measurement; routing; and anti-censorship techniques. The primary goal of my research is to help network operators run their networks better, and to enable users of these networks (both public and private) to experience high availability and good end-to-end performance. I have a strong interest in tackling practical problems using a “first principles” approach, designing systems based on these principles, and implementing and deploying these systems in practice.

I. TEACHING

A. Courses Taught

Term	Year	Number of Course Number & Title	Students	Comments
Spring	2010	CS 3251 Computing Networking I	53	
Spring	2010	CS 8803 NGN Next Generation Networking	50	New Course
Fall	2009	CS 7001 Introduction to Graduate Studies	39	
Spring	2009	CS 6262 Network Security	45	Updated Syllabus
Fall	2008	CS 4251 Computer Networking II	16	
Fall	2008	CS 7001 Introduction to Graduate Studies	44	
Spring	2008	CS 4251 Computer Networking II	14	New Syllabus
Fall	2007	CS 7001 Introduction to Graduate Studies	53	
Spring	2007	CS 7260 Internetworking Protocols and Architectures	29	
Fall	2006	CS 7001 Introduction to Graduate Studies	74	New Syllabus
Fall	2006	CS 8001 Networking Research Seminar	30	New Syllabus
Fall	2006	CS 1100 Freshman Leap Seminar	15	
Spring	2006	CS 7260 Internetworking Protocols and Architectures	27	New Syllabus

Tutorials on BGP Multiplexer at GENI Experimenters Workshop and GENI Engineering Conference in Summer 2010.

Tutorial on network security at African Network Operators Group (AfNOG) in Summer 2009. Tutorial on internet routing at Simposio Brasileiro de Redes de Computadores (SBRC) in Summer 2008.

Lecture for DIMACS Tutorial on Next-Generation Internet Routing Algorithms in August 2007.

Guest lecture for CS 6250 (Advanced Computer Networks) in Fall 2007.

Guest lecture for CS 3251 (Computer Networks I) in Fall 2006.

Multiple guest lectures for CS 4251 (Computer Networks II) in Spring 2006.

Guest lecture for MIT Course 6.829 (Computer Networking) in Fall 2005.

B. Curriculum Development

CS 8803 Next-Generation Networking: I have developed a brand-new graduate course that gives students practical experience with a variety of tools for next-generation networking, ranging from the Click software router to the OpenFlow switch framework. The course also teaches students about the state of the art in networking research—students read papers about research and industry trends and do a course project that incorporates aspects of these new technologies. This course relates to the larger nationwide effort on Global Environment for Network Innovations (GENI), which is building infrastructure for researchers to provide the next generation of networking protocols and technologies.

CS 7001 Introduction to Graduate Studies: With Professor Alex Gray, I have developed a new course syllabus and structure to CS 7001 around the larger goal of introducing new students to *how to do great research* as soon as their first term at Georgia Tech. In contrast with previous terms, where CS 7001 consisted of faculty “advertisements” for their research and projects consisted of short “mini-projects” where little research could be accomplished in a short time span of 3 weeks, we have improved the syllabus by bringing in faculty members to talk about research philosophy, exciting new directions, etc. We have also given the students the option to do a research project that is a term-long project in conjunction with CS 8903; our goal is to give students the flexibility to select meaningful research problems based on their research assistantships while helping them learn the skills required for writing papers, finding and evaluating research ideas, and performing other tasks associated with doing great research. Alex Gray and I wrote a conference paper on our development of this course, which appeared at *ACM SIGCSE 2008*.

College of Computing Research Day and Seminar Series: In addition to the course itself, to fulfill some of the functions of the former 7001 course, Alex Gray and I financed and organized a college-wide seminar series and research day in Fall 2009. Throughout the term, faculty speakers from across the college gave one-hour talks about their research; we raised money from Yahoo to support this event. The research day brings together students and faculty from around the college to see talks, demonstrations, and posters from around the college to exchange ideas.

CS 4251 Computer Networking II: *Spring/Fall 2008.* I developed new hands-on assignments to give students experience with real-world networking tools and software (*e.g.*, Emulab, Quagga, Click). I also revamped the course around various high-level themes in networking, including layering, resource sharing, tree formation (routing and forwarding, etc.). Finally, I developed over 20 new lectures for the syllabus, as well as new problem sets which can be re-used for future offerings of the course.

CS 6262 Network Security: *Spring 2009.* I updated the syllabus to include recent network attacks (*e.g.*, spam, botnets, reflection attacks, etc.) and also to integrate more hands-on assignments. Updating problem sets and project lists.

CS 7260 Internetworking Architectures and Protocols: *Spring 2006.* I developed a new project-based graduate course with substantial programming assignments using a wide variety of state-of-the-art networking software tools and platforms (*e.g.*, rcc, PlanetLab, scriptroute, NetFlow, etc.). I contributed questions to a larger bank of questions also used in graduate-level networking courses at Carnegie Mellon and MIT. Finally, I developed 24 new lectures, many based on current “hot topics” in computer networking (*e.g.*, spam, botnets, traffic anomaly detection, etc.)

Spring 2007. I developed two new course modules: (1) sound techniques for network measurement; and (2) evaluation platforms (Emulab, VINI, etc.). I designed new problem sets on these topics. With faculty at Carnegie Mellon, I instituted the use of a cross-institutional online forum for paper discussion. Students read papers from the CS 7260 syllabus and commented on papers before class to help stimulate paper discussion; students also read the discussion blog and could comment on papers being discussed in networking classes at other schools.

C. Individual Student Guidance

C.1. Postdocs Supervised

Cristian Lumezanu College of Computing
Fall 2009 - Present
Research on Internet measurement and economics.

C.2. Ph.D. Students Supervised

Hyojoon Kim College of Computing
Fall 2009 - Present
Research on programmable networks and network configuration.

Robert Lychev College of Computing
Fall 2008 - Present
Research on contract enforcement for transit markets.
Taken qualifier (grading in progress).

Sam Burnett College of Computing

Fall 2008 - Present

Publications: *D.0.2, F.5.2, F.5.7*

Design and implementation of anti-censorship systems.

Taken qualifier (grading in progress).

Srikanth Sundaresan College of Computing

Fall 2008 - Present

Publications: *F.5.3*

Research on access network performance and online traffic engineering.

Taken qualifier (grading in progress).

Bilal Anwer College of Computing

Fall 2008 - Present

Publications: *D.0.1, E.0.1, E.0.4*

Research on support for hardware forwarding in virtual network environments.

Taken qualifier (grading in progress).

Shuang Hao College of Computing

Fall 2007 - Present

Publications: *F.3.7, D.0.9*

Research on botnet detection, network monitoring, and spam filtering.

Taken qualifier (grading in progress).

Maria Konte College of Computing

Fall 2007 - Present

Publications: *D.0.10*

Measurement study of fast-flux networks.

Taken qualifier (grading in progress).

Yogesh Mundada College of Computing

Fall 2007 - Present

Publications: *F.3.8, F.5.9*

Development of experiment specification for VINI and integration of VINI with Emulab.

Taken qualifier (grading in progress).

Vytautas Valancius College of Computing

Summer 2007 - Present

Publications: *D.0.4 E.0.7, E.0.6 F.3.5, F.3.8, F.3.13, F.5.1 F.5.9, F.5.10*

Research on interdomain routing and network virtualization.

Passed qualifier.

Mukarram Bin Tariq College of Computing

Spring 2007 - Spring 2010

Publications: *D.0.13, D.0.7, D.0.6, E.0.8, F.1.1, F.3.6*

Co-advised with Mostafa Ammar. Research on statistical inference methods for network planning and troubleshooting problems. Mukarram's dissertation work is now part of operational systems at Google.

Graduated. Now works full-time at Google in the network monitoring group.

Murtaza Motiwala College of Computing

Fall 2006 - Present

Publications: *D.0.12, E.0.11, F.3.8, F.3.9, F.3.12, F.3.16, F.5.9*

Research on (1) in-band troubleshooting and (2) scalable network architectures for path diversity, including path splicing.

Passed qualifier.

Anirudh Ramachandran College of Computing

Spring 2006 - Present

Publications: *C.0.1, D.0.16, D.0.21, E.0.10, E.0.13, E.0.14, E.0.15, F.3.4, F.3.6, F.5.8, F.5.13*

Research on network-level behavior of spammers and passive botnet detection.

Passed qualifier and proposal defense. Expected graduation Fall 2010.

C.3. Masters Students Supervised

Ankur Nayak College of Computing

Spring 2009 - Spring 2010

Publications: *E.0.5*

Dynamic access control with programmable switches.

Umayr Hassan College of Computing

Fall 2008 - Spring 2010

Research on the design of a market for Internet transit, and on home network configuration.

Umayr now works full-time at Bloomberg.

Nadeem Syed College of Computing

Spring 2007 - Spring 2008

Publications: *F.5.11*

Co-advised with Alex Gray. Developing and implementing new machine learning techniques for fast disruption detection.

Nadeem is in the MBA program at Georgia Tech.

Kaushik Bhandakar College of Computing

Spring 2007 - Summer 2008

Publications: *F.5.8*

Experiments for VINI performance benchmarking; implementation and prototyping for the “Pedigree” packet provenance project; research on incentives in BitTorrent.

Kaushik now works full-time at Google.

Samantha Lo Hong Kong Polytechnic University

Spring 2007

Research on market-based network architectures and inbound traffic engineering.

Samantha is now a Ph.D. student at Georgia Tech.

Manas Khadilkar College of Computing

Fall 2006 - Spring 2007

Publications: *D.0.17*

Research on efficient settings of lease times for DHCP address allocation. Algorithm in development, to be used on the Georgia Tech campus network for optimizing lease time settings.

Manas now works full-time for Expedia.

Han Lu College of Computing

Fall 2006 - Spring 2007

Research on spam traffic patterns by IP address space.

Chris Kelly College of Computing

Fall 2006 - Fall 2007

Developing new software features for the Campus-Wide Performance Monitoring and Recovery (CPR) project.

Chris now works full-time for SugarCRM, an Atlanta-based startup.

Yiyi Huang College of Computing

Spring 2006 - Fall 2009

Publications: *D.0.18, F.3.10*

Co-advised with Jim Xu. Research on fast, distributed network anomaly detection.

Yiyi now works full-time at Microsoft.

Winston Wang M.I.T. EECS

Fall 2002 - Spring 2003

Publications: *E.0.19*

Thesis on an implementation of the Infranet anti-censorship system received MIT's Charles and Jennifer Johnson Thesis Prize.

C.4. Undergraduate Students Supervised

Alex Reimers College of Computing

Spring 2009

Publications: *E.0.5*

Worked on dynamic access control (a replacement of Georgia Tech OIT's current authentication system) with programmable switches. Alex now works full time at Cisco.

Megan Elmore College of Computing

Fall 2007 - Spring 2009

Publications: *D.0.12*

Experiments for interdomain path splicing; design and implementation of the path splicing prototype. Work received 2nd prize in 2008 Georgia Tech College of Computing undergraduate research competition. Megan was also the winner of the 2009 College of Computing Undergraduate Research Award, and the 2009 Sigma Xi Best Undergraduate Researcher Award. Megan is now a Ph.D. student at Stanford University.

Hongyi Hu M.I.T. EECS

Spring 2005 - Fall 2005

*Extensions to the *rcc* router configuration checker tool for static configuration analysis of internal routing protocol configurations.*

C.5. Special Projects

Mona Chitnis College of Computing

Spring 2010

Research on OpenFlow network architectures.

Sravanthi Gondhi College of Computing

Spring 2010

Research on online traffic engineering.

Shruti Gupta College of Computing

Spring 2010

Research on online traffic engineering.

Utkarsh Shrivastava College of Computing

Spring 2010

Research on network-level behavior of spammers.

Pooja Rajanna College of Computing

Spring 2010

Research on network-level behavior of spammers.

Luxmi Saha College of Computing
Spring 2010
Research on data-center scheduling algorithms.

Dongchan Kim College of Computing
Fall 2009
Research on spam filtering.

Sonali Batra College of Computing
Summer 2009
Research on anti-phishing techniques.

Radhika Partharathy College of Computing
Fall 2008
Research on anti-phishing techniques.

Sagar Mehta College of Computing
Fall 2006 - Spring 2008
Research on anti-phishing techniques.

Bhairav Dutia College of Computing
Fall 2006
Research on anti-censorship techniques and countermeasures.

Megan Benoit College of Computing
Fall 2006
Research on spammers' email address harvesting practices.

Amit Khanna College of Computing
Fall 2006
Implemented Secure BGP (S-BGP) in the Quagga software router. Software publically available and operators are using the codebase for ongoing work on certificates for secure routing.

Daniel Mentz College of Computing
Spring 2006
Research on campus network security troubleshooting.

Buddy Moore College of Computing
Summer 2006
Implemented distributed version of the Infranet anti-censorship software. Publicly available.

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Theses

- A.0.1 Nick Feamster. *Proactive Techniques for Correct and Predictable Internet Routing*. PhD thesis, Massachusetts Institute of Technology, February 2006. Winner of the MIT George M. Sprowls Honorable Mention for Best MIT Ph.D. Dissertation in Computer Science.
- A.0.2 Nick Feamster. Adaptive delivery of real-time streaming video. Master's thesis, Massachusetts Institute of Technology, May 2001. Winner of the MIT EECS William A. Martin Memorial Thesis Award.

B. Journal Publications

- B.0.1 Bilal Anwer and Nick Feamster. Building a fast, virtualized data plane with programmable hardware. *ACM SIGCOMM Computer Communication Review*, April 2010.
- B.0.2 Nick Feamster, Ramesh Johari, and Hari Balakrishnan. Stable Policy Routing with Provider Independence. *IEEE/ACM Transactions on Networking*, December 2007.
- B.0.3 Nick Feamster and Jennifer Rexford. Network-Wide Prediction of BGP Routes. *IEEE/ACM Transactions on Networking*, June 2007.
- B.0.4 Nick Feamster, Jaeyeon Jung, and Hari Balakrishnan. An Empirical Study of “Bogon” Route Advertisements. *ACM Computer Communications Review*, 35(1):63–70, November 2004.
- B.0.5 Nick Feamster, Jay Borkenhagen, and Jennifer Rexford. Guidelines for Interdomain Traffic Engineering. *ACM Computer Communications Review*, 33(5):19–30, October 2003.

C. Books and Book Chapters

- C.0.1 Anirudh Ramachandran, Nick Feamster, and David Dagon. *Botnet Detection: Countering the Largest Security Threat*. Springer, 2008. Chapter: Revealing Botnet Membership with DNSBL Counterintelligence.

D. Refereed Conference Publications

- D.0.1 Bilal Anwer, Murtaza Motiwala, Mukarram bin Tariq, and Nick Feamster. SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware. In *Proc. ACM SIGCOMM*, New Delhi, India, August 2010.
Acceptance rate: 12%
- D.0.2 Sam Burnett, Nick Feamster, and Santosh Vempala. Chipping Away at Censorship Firewalls with Collage. In *Proc. 19th USENIX Security Symposium*, Washington, DC, August 2010.
Acceptance rate: 15%
- D.0.3 Manos Antonakakis and Roberto Perdisci and David Dagon and Wenke Lee and Nick Feamster. Building a Dynamic Reputation System for DNS. In *Proc. 19th USENIX Security Symposium*, Washington, DC, August 2010.
Acceptance rate: 15%
- D.0.4 Vytautas Valancius, Nick Feamster, Jennifer Rexford, and Akihiro Nakao. Wide-Area Routing for Distributed Services. In *Proc. USENIX Annual Technical Conference*, Boston, MA, June 2010.
Acceptance rate: 17%

- D.0.5 Roberto Perdisci, Wenke Lee, and Nick Feamster. Behavioral Clustering of HTTP-Based Malware. In *Proc. 7th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, San Jose, CA, April 2010.
Acceptance rate: 16%
- D.0.6 Mohammed Mukarram bin Tariq, Murtaza Motiwala, Nick Feamster, and Mostafa Ammar. Detecting General Network Neutrality Violations with Causal Inference. In *4th International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, Rome, Italy, December 2009.
Acceptance rate: 17%
- D.0.7 Mohammed Mukarram bin Tariq, Ahmed Mansy, Nick Feamster, and Mostafa Ammar. Measuring VLAN-Induced Sharing on a Campus Network. In *Proc. ACM SIGCOMM Internet Measurement Conference*, Chicago, Illinois, October 2009.
Acceptance rate: 22%
- D.0.8 Italo Cunha, Renata Teixeira, Nick Feamster, and Christophe Diot. Techniques for Fast and Accurate Network Tomography. In *Proc. ACM SIGCOMM Internet Measurement Conference*, Chicago, Illinois, October 2009.
Acceptance rate: 22%
- D.0.9 Shuang Hao, Nadeem Syed, Nick Feamster, Alexander Gray, and Sven Krasser. Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine. In *Proc. 18th USENIX Security Symposium*, Montreal, Quebec, Canada, August 2009.
Acceptance rate: 15%
- D.0.10 Maria Konte, Nick Feamster, and Jaeyeon Jung. Dynamics of Online Scam Infrastructure. In *Proc. Passive and Active Measurement Conference*, Seoul, Korea, March 2009.
Acceptance rate: 20% **Best paper award.**
- D.0.11 Anirudh Ramachandran, Srinivasan Seetharaman, Nick Feamster, and Vijay Vazirani. Fast Monitoring of Traffic Subpopulations. In *Proc. ACM SIGCOMM Internet Measurement Conference*, Vouliagmeni, Greece, October 2008.
Acceptance rate: 17%
- D.0.12 Murtaza Motiwala, Megan Elmore, Nick Feamster, and Santosh Vempala. Path Splicing. In *Proc. ACM SIGCOMM*, Seattle, WA, August 2008.
Acceptance rate: 12%
- D.0.13 Mohammed Mukarram bin Tariq, Amgad Zeitoun, Nick Feamster, and Mostafa Ammar. Answering What-If Deployment and Configuration Questions with WISE. In *Proc. ACM SIGCOMM*, Seattle, WA, August 2008.
Acceptance rate: 12%
- D.0.14 David Andersen, Hari Balakrishnan, Nick Feamster, and Scott Shenker. Accountable Internet Protocol (AIP). In *Proc. ACM SIGCOMM*, Seattle, WA, August 2008.
Acceptance rate: 12%
- D.0.15 Nick Feamster and Alexander Gray. Can Great Research Be Taught? Independent Research with Cross-Disciplinary Thinking and Broader Impact. In *ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE)*, Portland, OR, March 2008.
- D.0.16 Anirudh Ramachandran, Nick Feamster, and Santosh Vempala. Filtering Spam with Behavioral Blacklisting. In *Proc. 14th ACM Conference on Computer and Communications Security (CCS)*, Alexandria, VA, October 2007.
Acceptance rate: 24%

- D.0.17 Manas Khadilkar, Nick Feamster, Russ Clark, and Matt Sanders. Usage-Based DHCP Lease Time Optimization. In *Proc. ACM SIGCOMM Internet Measurement Conference*, San Diego, CA, October 2007.
Acceptance rate: 24%
- D.0.18 Yiyi Huang, Nick Feamster, Anukool Lakhina, and Jim Xu. Exposing Routing Problems with Network-Wide analysis. In *Proc. ACM SIGMETRICS*, San Diego, CA, June 2007.
Acceptance rate: 17%
- D.0.19 Feng Wang, Nick Feamster, and Lixin Gao. Measuring the contributions of routing dynamics to prolonged end-to-end internet path failures. In *Proc. IEEE Conference on Global Communications (GlobeCom)*, Washington, DC, November 2007.
Acceptance rate: 40%
- D.0.20 Christopher P. Lee, Keshav Attrey, Carlos Caballero, Nick Feamster, Milena Mihail, and John A. Copeland. MobCast: Overlay Architecture for Seamless IP Mobility using Scalable Anycast Proxies. In *IEEE Wireless Communications and Networking Conference*, Hong Kong, March 2007.
Acceptance rate: 47%
- D.0.21 Anirudh Ramachandran and Nick Feamster. Understanding the Network-Level Behavior of Spammers. In *Proc. ACM SIGCOMM*, Pisa, Italy, August 2006. An earlier version appeared as Georgia Tech TR GT-CSS-2006-001.
Acceptance rate: 12% **Best student paper award.**
- D.0.22 Andy Bavier, Nick Feamster, Mark Huang, Larry Peterson, and Jennifer Rexford. In VINI Veritas: Realistic and controlled network experimentation. In *Proc. ACM SIGCOMM*, Pisa, Italy, August 2006.
Acceptance rate: 12%
- D.0.23 Nick Feamster and Hari Balakrishnan. Correctness Properties for Internet Routing. In *Forty-third Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2005.
- D.0.24 Nick Feamster, Ramesh Johari, and Hari Balakrishnan. The Implications of Autonomy for Stable Policy Routing. In *Proc. ACM SIGCOMM*, pages 25–36, Philadelphia, PA, August 2005.
Acceptance rate: 11%
- D.0.25 Michael Freedman, Mythili Vutukuru, Nick Feamster, and Hari Balakrishnan. Geographic Locality of IP Prefixes. In *Proc. ACM SIGCOMM Internet Measurement Conference*, New Orleans, LA, October 2005.
Acceptance rate: 24%
- D.0.26 Nick Feamster and Hari Balakrishnan. Detecting BGP Configuration Faults with Static Analysis. In *Proc. 2nd Symposium on Networked Systems Design and Implementation (NSDI)*, pages 43–56, Boston, MA, May 2005.
Acceptance rate: 22% **Best paper award.**
- D.0.27 Matthew Caesar, Don Caldwell, Nick Feamster, Jennifer Rexford, Aman Shaikh, and Kobus van der Merwe. Design and Implementation of a Routing Control Platform. In *Proc. 2nd Symposium on Networked Systems Design and Implementation (NSDI)*, pages 15–28, Boston, MA, May 2005.
Acceptance rate: 22%

- D.0.28 Nick Feamster, Zhuoqing Morley Mao, and Jennifer Rexford. BorderGuard: Detecting Cold Potatoes from Peers. In *Proc. ACM SIGCOMM Internet Measurement Conference*, pages 213–218, Taormina, Sicily, Italy, October 2004.
Acceptance rate: 25%
- D.0.29 Nick Feamster, Jared Winick, and Jennifer Rexford. A Model of BGP Routing for Network Engineering. In *Proc. ACM SIGMETRICS*, pages 331–342, New York, NY, June 2004.
Acceptance rate: 12%
- D.0.30 Nick Feamster, David Andersen, Hari Balakrishnan, and M. Frans Kaashoek. Measuring the Effects of Internet Path Faults on Reactive Routing. In *Proc. ACM SIGMETRICS*, pages 126–137, San Diego, CA, June 2003.
Acceptance rate: 12%
- D.0.31 Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, and David Karger. Infranet: Circumventing Web censorship and surveillance. In *Proc. 11th USENIX Security Symposium*, San Francisco, CA, August 2002.
Acceptance rate: 17% **Best student paper award.**
- D.0.32 Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Dos and don'ts of client authentication on the Web. In *Proc. 10th USENIX Security Symposium*, Washington, DC, August 2001.
Acceptance rate: 28% **Best student paper award.**
- D.0.33 Susie Wee, John Apostolopoulos, and Nick Feamster. Field-to-frame transcoding with temporal and spatial downsampling. In *IEEE International Conference on Image Processing*, October 1999.
Acceptance rate: 45%
- D.0.34 Nick Feamster and Susie Wee. An MPEG-2 to H.263 transcoder. In *SPIE Voice, Video, and Data Communications Conference*, Boston, MA, September 1999.

E. Workshop Publications

- E.0.1 Bilal Anwer, Ankur Nayak, Nick Feamster, and Ling Liu. Network I/O Fairness in Virtual Machines. In *ACM SIGCOMM Workshop on Virtualized Infrastructure, Services, and Architectures (VISA)*, New Delhi, India, September 2010.
- E.0.2 Nick Feamster. Outsourcing Home Network Security. In *ACM SIGCOMM Workshop on Home Networking (HomeNets)*, New Delhi, India, September 2010.
- E.0.3 Ken Calvert, W. Keith Edwards, Nick Feamster, Rebecca Grinter, Ye Deng, and Xuzi Zhou. Instrumenting Home Networks. In *ACM SIGCOMM Workshop on Home Networking (HomeNets)*, New Delhi, India, September 2010.
- E.0.4 Bilal Anwer and Nick Feamster. Building a Fast, Virtualized Data Plane with Programmable Hardware. In *ACM SIGCOMM Workshop on Virtualized Infrastructure, Services, and Architectures (VISA)*, Barcelona, Spain, August 2009.
- E.0.5 Ankur Nayak, Alex Reimers, Russ Clark, and Nick Feamster. Resonance: Dynamic Access Control for Enterprise Networks. In *ACM SIGCOMM Workshop on Research in Enterprise Networks (WREN)*, Barcelona, Spain, August 2009.
- E.0.6 Sapan Bhatia, Murtaza Motiwala, Wolfgang Muehlbauer, Yogesh Mundada, Vytautas Valancius, Andy Bavior, Nick Feamster, Larry Peterson, and Jennifer Rexford. Trellis: A Platform for Building Flexible, Fast Virtual Networks on Commodity Hardware. In *3rd International Workshop on Real Overlays & Distributed Systems*, December 2008.

- E.0.7 Vytautas Valancius, Nick Feamster, Ramesh Johari, and Vijay Vazirani. MINT: A Market for Internet Transit. In *ACM SIGCOMM CoNext Workshop on Re-Architecting the Internet*, December 2009.
- E.0.8 Mohammed Mukarram bin Tariq, Murtaza Motiwala, and Nick Feamster. NANO: Network Access Neutrality Observatory. In *Proc. 7th ACM Workshop on Hot Topics in Networks (Hotnets-VII)*, Calgary, Alberta, Canada, October 2008.
Acceptance rate: 20%
- E.0.9 S. Yardi, N. Feamster, and A. Bruckman. Photo-Based Authentication Using Social Networks. In *Proc. ACM SIGCOMM Workshop on Online Social Networks*, Seattle, WA, August 2008.
- E.0.10 Anirudh Ramachandran and Nick Feamster. Authenticated Out-of-Band Communication over Social Links. In *Proc. ACM SIGCOMM Workshop on Online Social Networks*, Seattle, WA, August 2008.
- E.0.11 Murtaza Motiwala, Nick Feamster, and Santosh Vempala. Path Splicing: Reliable Connectivity with Rapid Recovery. In *Proc. 6th ACM Workshop on Hot Topics in Networks (Hotnets-VI)*, Atlanta, GA, November 2007.
Acceptance rate: 18%
- E.0.12 David G. Andersen, Hari Balakrishnan, Nick Feamster, and Scott Shenker. Holding the Internet Accountable. In *Proc. 6th ACM Workshop on Hot Topics in Networks (Hotnets-VI)*, Atlanta, GA, November 2007.
Acceptance rate: 18%
- E.0.13 Anirudh Ramachandran, Atish das Sarma, and Nick Feamster. BitStore: An Incentive-Compatible Solution for Blocked Downloads in Bittorrent. In *ACM Joint Workshop on The Economics of Networked Systems and Incentive-Based Computing (NetEcon)*, San Diego, CA, June 2007.
- E.0.14 Anirudh Ramachandran, Nick Feamster, and David Dagon. Revealing Botnet Membership with DNSBL Counter-Intelligence. In *2nd USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, San Jose, CA, July 2006.
- E.0.15 Anirudh Ramachandran, David Dagon, and Nick Feamster. Can DNSBLs Keep Up with Bots? In *3rd Conference on Email and Anti-Spam (CEAS)*, Mountain View, CA, July 2006.
- E.0.16 Nick Feamster, Hari Balakrishnan, and Jennifer Rexford. Some foundational problems in interdomain routing. In *Proc. 3rd ACM Workshop on Hot Topics in Networks (Hotnets-III)*, San Diego, CA, November 2004.
- E.0.17 Nick Feamster, Hari Balakrishnan, Jennifer Rexford, Aman Shaikh, and Kobus van der Merwe. The Case for Separating Routing from Routers. In *ACM SIGCOMM Workshop on Future Directions in Network Architecture*, pages 5–12, Portland, OR, September 2004.
- E.0.18 Nick Feamster and Roger Dingledine. Location diversity in anonymity networks. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 2004.
- E.0.19 Nick Feamster, Magdalena Balazinska, Winston Wang, Hari Balakrishnan, and David Karger. Thwarting Web censorship with untrusted messenger discovery. In *3rd Workshop on Privacy Enhancing Technologies*, Dresden, Germany, March 2003.
- E.0.20 Nick Feamster. Practical Verification Techniques for Wide-Area Routing. In *Proc. 2nd ACM Workshop on Hot Topics in Networks (Hotnets-II)*, pages 87–92, Cambridge, MA, November 2003.

- E.0.21 Nick Feamster and Hari Balakrishnan. Towards a Logic for Wide-Area Internet Routing. In *ACM SIGCOMM Workshop on Future Directions in Network Architecture*, pages 289–300, Karlsruhe, Germany, August 2003.
- E.0.22 David G. Andersen, Nick Feamster, Steve Bauer, and Hari Balakrishnan. Topology inference from BGP routing dynamics. In *Proc. ACM SIGCOMM Internet Measurement Workshop*, Marseille, France, November 2002. *Acceptance rate: 42%*
- E.0.23 Nick Feamster and Hari Balakrishnan. Packet loss recovery for streaming video. In *Proc. 12th International Packet Video Workshop (PV 2002)*, Pittsburgh, PA, April 2002.
- E.0.24 Nick Feamster, Deepak Bansal, and Hari Balakrishnan. On the interactions between congestion control and layered quality adaptation for streaming video. In *11th International Packet Video Workshop*, Kyongju, Korea, May 2001.

F. Other

F.1. Submitted Journal Papers

- F.1.1 Mohammed Mukarram bin Tariq, Vytautas Valancius, Kaushik Bhandakar, Amgad Zeitoun, Nick Feamster, and Mostafa Ammar. Answering “What-If” Deployment and Configuration Questions with WISE: Techniques and Deployment Experience.
- F.1.2 Nick Feamster and Hari Balakrishnan. Correctness Properties for Internet Routing. *IEEE/ACM Transactions on Networking*, December 2005. *In Submission*.

F.2. Submitted Conference and Workshop Papers

- F.2.1 Mukarram bin Tariq, Jake Brutlag, Natalia Sutin, Nick Feamster, and Mostafa Ammar. Answering How-to Questions for Mitigating High-latency Web Transactions with HIP. *In Submission*.
- F.2.2 Hyojoon Kim, Ankur Nayak, Nick Feamster, Russ Clark, Matt Sanders, and Tim Upthegrove. Realizing Network Policies with Event-Based Programs. October 2010. *In Submission*.
- F.2.3 Yogesh Mundada, Nick Feamster, and Rob Sherwood. Implementing Network-Wide Policies with Distributed Packet Processing. *In Submission*.
- F.2.4 Nick Feamster, Brighten Godfrey, Nick McKeown, Guru Parulkar, Jennifer Rexford, and Scott Shenker. Architecting for Innovation. *In Preparation*.
- F.2.5 Srikanth Sundaresan, Cristian Lumezanu, and Nick Feamster. Autonomous Traffic Engineering with Self-Configuring Topologies. *In Preparation*.
- F.2.6 Srikanth Sundaresan, Lucas Di Cioccio, Nick Feamster, and Renata Teixeira. Which Factors Affect Access Network Performance?, November 2009. *In Preparation*.

F.3. Other Technical Reports, Unrefereed Papers, and Drafts in Preparation

- F.3.1 Vytautas Valancius, Nick Feamster, Ramesh Johari, and Vijay Vazirani. A Market for Internet Connectivity, March 2010. *In Preparation*.
- F.3.2 Robert Lychev and Nick Feamster. Derailing Depeering: Incentives for Interdomain Contracts, March 2010. *In Preparation*.

- F.3.3 Anirudh Ramachandran, Hitesh Khandelwal, Shuang Hao, Nick Feamster, and Santosh Vempala. A Dynamic Reputation Service for Spotting Spammers, March 2010. *In Preparation.*
- F.3.4 Anirudh Ramachandran, Nick Feamster, Kobus van der Merwe, Balachander Krishnamurthy, and Oliver Spatschek. Fishing for Phishing in the Network Stream. March 2010. *In Preparation.*
- F.3.5 Vytutas Valancius and Nick Feamster. Managing BGP Routes with a BGP Session Multiplexer. Technical Report GT-CS-08-05, Georgia Tech School of Computer Science, July 2008.
- F.3.6 Anirudh Ramachandran, Kaushik Bhandakar, Mohammed Mukarram bin Tariq, and Nick Feamster. Packets with Provenance. Technical Report GT-CS-08-02, Georgia Tech School of Computer Science, February 2008.
- F.3.7 Shuang Hao and Nick Feamster. Estimating Botnet Populations from Attack Traffic. April 2008.
- F.3.8 Sapan Bhatia, Murtaza Motiwala, Wolfgang Muehlbauer, Vytutas Valancius, Andy Bavier, Nick Feamster, Larry Peterson, and Jennifer Rexford. Hosting Virtual Networks on Commodity Hardware. Technical Report GT-CS-07-10, Georgia Institute of Technology, Atlanta, GA, October 2007.
- F.3.9 Nick Feamster, Murtaza Motiwala, and Andy Bavier. In-Band Network Path Diagnosis. *In Submission.*
- F.3.10 Yiyi Huang, Nick Feamster, Renata Teixeira, and Christophe Diot. Making Tomography Practical: Scalable Network Monitoring for Fault Diagnosis. *In submission.*
- F.3.11 Nick Feamster, Ramesh Johari, and Vijay Vazirani. AGORA: A Market for Internet Connectivity. In *Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO)*, Princeton, NJ, May 2007.
- F.3.12 Murtaza Motiwala, Nick Feamster, and Santosh Vempala. Improving Interdomain Routing Security with BGP Path Splicing. In *Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO)*, Princeton, NJ, May 2007.
- F.3.13 Vytutas Valancius and Nick Feamster. Layering the Interdomain Routing Layer. In *Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO)*, Princeton, NJ, May 2007.
- F.3.14 Nick Feamster, Lixin Gao, and Jennifer Rexford. How to Lease the Internet in Your Spare Time. *ACM Computer Communications Review*, 37(1), January 2007. Editorial section.
- F.3.15 Nick Feamster. Can Information from End Systems Improve Routing? In *Workshop on Internet Routing Evolution and Design (WIRED)*, Atlanta, GA, October 2006.
- F.3.16 Murtaza Motiwala and Nick Feamster. Network Troubleshooting on Data Plane Coattails. In *Workshop on Internet Routing Evolution and Design (WIRED)*, Atlanta, GA, October 2006.
- F.3.17 David G. Andersen and Nick Feamster. Challenges and opportunities in Internet data mining. Technical Report CMU-PDL-06-102, Carnegie Mellon University, January 2006.
- F.3.18 Nick Feamster and Hari Balakrishnan. Verifying the correctness of wide-area Internet routing. Technical Report MIT-LCS-TR-948, Massachusetts Institute of Technology, May 2004.

- F.3.19 Nick Feamster. Rethinking routing configuration: Beyond stimulus-response reasoning. In *Workshop on Internet Routing Evolution and Design (WIRED)*, Mt. Hood, OR, October 2003.
- F.3.20 Nick Feamster and Jennifer Rexford. Network-Wide BGP Route Prediction for Traffic Engineering. In *Proc. SPIE ITCOM*, volume 4868, pages 55–68, Boston, MA, August 2002.
- F.3.21 Nick Feamster, Jennifer Rexford, and Jay Borkenhagen. Controlling the impact of BGP policy changes on IP traffic. Technical Report 011106-02, AT&T Labs–Research, Florham Park, NJ, November 2001.
- F.3.22 Russ White, B. Akyol, and Nick Feamster. *Considerations in Validating the Path in Routing Protocols*. IETF, June 2005.

F.4. Software

- F.4.1 *Campus-Wide OpenFlow Deployment: Access and Information Flow Control for Enterprise Networks*. Resonance is a system for controlling access and information flow in an enterprise network. Network operators currently use access control systems that are coarse-grained (i.e., it is difficult to apply specialized policy to individual users) and static (i.e., it is difficult to quickly change the extent of a user’s access). Towards fixing these problems, we have developed a system that allows network operators to program network policy using a controller that is distinct from the switch itself and can be programmed to implement network-wide policy. We have implemented and deployed this system in an operational network that spans two buildings on the Georgia Tech campus; the network sees regular use, and a deployment in Georgia Tech dormitories or the wireless network is planned for the near future. We demonstrated the function of this network at the 7th GENI Engineering Conference in March 2010.
See <http://groups.geni.net/geni/wiki/BGPMux> for details.
- F.4.2 *NANO: Network Access Neutrality Observatory*. The Network Access Neutrality Observatory (NANO) is a system to help users determine whether their traffic is being discriminated against by an access ISP. In contrast to existing systems for detecting network neutrality violations, NANO makes no assumptions about the mechanism for discrimination or the services that the ISP might be discriminated against. NANO has been released in collaboration with Google as part of the Measurement Lab project. A preliminary version of the software was released to a small group of users in March 2009 for testing; a complete release is available for download at: <http://gtnose.net/nano/>.
- F.4.3 *Implementation of GENI Prototype: Virtual Networks and BGP Session Multiplexer*. In the process of developing software for the NSF-Sponsored GENI Project Office. This project (1) adds facilities and functions to the VINI testbed to enable experiments to carry traffic from real users; and (2) increases the experimental use of the VINI testbed by providing a familiar experiment management facility. The deliverables for this project all comprise software for supporting external connectivity and flexible, facile experimentation on the GENI testbed. The primary deliverables are a BGP session multiplexer—a router based on the Quagga software routing suite, software support for virtual tunnel and node creation, and integration of the above functionality with clearinghouse services developed as part of the ProtoGENI project.
See <http://groups.geni.net/geni/wiki/BGPMux>.

This project contributes to GENI design and prototyping through BGP mux development integration with ISPs; tunnel and topology establishment and management; ProtoGENI clearinghouse integration; and support for isolation and resource swapout. With

researchers at Princeton, we have also built VINI, a large distributed testbed for specifying virtual network topologies and experimenting with routing protocols and architectures in a controlled, realistic emulation environment. See <http://vini-veritas.net/> for details.

- F.4.4 *rcc: router configuration checker*. Static configuration analysis tool for Border Gateway Protocol (BGP) routing configurations. Downloaded by over 100 network operators and many large, nationwide backbone ISPs around the world. See <http://gtnoise.net/rcc/> for details.
- F.4.5 *Infranet*. System for circumventing Web censorship firewalls (e.g., those in China, Saudia Arabia, etc.). Available on Sourceforge. Featured in articles in *Technology Review*, *New Scientist*, and *Slashdot*. See <http://nms.lcs.mit.edu/projects/infranet/>.
- F.4.6 *The Datapostory*. Originally the “MIT BGP Monitor”, the Datapostory is growing to support multiple data feeds (e.g., spam, end-to-end measurement probes, traceroutes, Abilene data, etc.). Currently used by researchers at Georgia Tech, Carnegie Mellon, University of Michigan, Princeton, MIT. See <http://www.datapostory.net/> for details.
- F.4.7 *Secure BGP Implementation*. Implementation of S-BGP in the Quagga software router. Our implementation may be used by Randy Bush and Geoff Huston in their project to develop a certificate infrastructure for secure routing protocols.
- F.4.8 *SR-RTP*. Transport protocol for selective retransmission of packets in an MPEG video stream. Incorporated into “Oxygen TV” for MIT Project Oxygen. Some ideas incorporated into the OpenDivX video transport protocol.

F.5. Conference Posters and Demos

- F.5.1 Vytautas Valancius, Hyojoon Kim, and Nick Feamster. Transit Portal: BGP Connectivity as a Service. In *Proc. ACM SIGCOMM*, New Delhi, India, August 2010. Demo.
- F.5.2 Sam Burnett, Nick Feamster, and Santosh Vempala. Circumventing Censorship with Collage. In *Proc. ACM SIGCOMM*, New Delhi, India, August 2010. Demo.
- F.5.3 Srikanth Sundaresan, Cristian Lumezanu, Nick Feamster, and Pierre Francois. Traffic Engineering with Self-Configuring Topologies. In *Proc. ACM SIGCOMM*, New Delhi, India, August 2010.
- F.5.4 Anirudh Ramachandran, Yogesh Mundada, Mukarram bin Tariq, and Nick Feamster. Securing Enterprise Networks with Traffic Tainting. In *Proc. ACM SIGCOMM*, Barcelona, Spain, August 2009. Demo.
- F.5.5 Vytautas Valancius, Nick Feamster, Jennifer Rexford, and Aki Nakao. Transit Portal: Bringing Connectivity to the Cloud. In *Proc. ACM SIGCOMM*, Barcelona, Spain, August 2009. Demo.
- F.5.6 Murtaza Motiwala, Megan Elmore, Yogesh Mundada, and Nick Feamster. Network and End-System Support for Transparent Use of Multiple Paths. In *Proc. ACM SIGCOMM*, Barcelona, Spain, August 2009. Demo.
- F.5.7 Sam Burnett, Nick Feamster, and Santosh Vempala. Circumventing Internet Censorship with Collage. In *Proc. 6th Symposium on Networked Systems Design and Implementation (NSDI)*, Boston, MA, April 2009. Demo.

- F.5.8 Anirudh Ramachandran, Kaushik Bhandakar, Mohammed Mukarram bin Tariq, and Nick Feamster. Packets with Provenance. In *Proc. ACM SIGCOMM*, Seattle, WA, August 2008.
- F.5.9 Yogesh Mundada, Murtaza Motiwala, Vytas Valancius, Andy Bavier, Nick Feamster, Larry Peterson, Sapan Bhatia, and Jennifer Rexford. Trinity: A Framework for Managing Wide-Area Virtual Networks. In *Proc. 5th Symposium on Networked Systems Design and Implementation (NSDI)*, San Francisco, CA, April 2008.
- F.5.10 Vytas Valancius and Nick Feamster. Multiplexing BGP Sessions with BGP-Mux. In *3rd International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, New York, NY, December 2007.
- F.5.11 Nadeem Syed, Nick Feamster, and Alex Gray. Predicting bad behavior. In *NIPS Workshop on Machine Learning in Adversarial Environments for Computer Security*, Whistler, Canada, December 2007.
- F.5.12 Murtaza Motiwala, Andy Bavier, and Nick Feamster. In-Band Network Troubleshooting. In *Proc. Fourth Symposium on Networked Systems Design and Implementation (NSDI)*, Cambridge, MA, April 2007.
- F.5.13 Anirudh Ramachandran and Nick Feamster. Understanding the Network-Level Behavior of Spammers. In *Proc. Third Symposium on Networked Systems Design and Implementation (NSDI)*, San Jose, CA, May 2006.
- F.5.14 Nick Feamster and Hari Balakrishnan. Detecting BGP Configuration Faults with Static Analysis. In *Proc. First Symposium on Networked Systems Design and Implementation (NSDI)*, San Francisco, CA, March 2004.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

G.1.1 GENI OpenFlow Campus Buildout

Sponsor: GENI Project Office
Investigator(s): N. Feamster (PI), Russ Clark
Amount: \$64,675 for 1 year
Awarded: October 2010

G.1.2 Architecting for Innovation

Sponsor: National Science Foundation
Investigator(s): H. Balakrishnan, N. Feamster, B. Godfrey, N. McKeown, J. Rexford, S. Shenker (PI)
Amount: \$200,000 for 1 year
Awarded: September 2010

G.1.3 Aster*x: Load-Balancing Web Traffic over Wide-Area Networks

Sponsor: National Science Foundation
Investigator(s): N. Feamster (PI), Russ Clark
Amount: \$75,000 for 1 year
Awarded: August 2010

G.1.4 Network-Wide Configuration Testing and Synthesis

Sponsor: National Science Foundation
Investigator(s): N. Feamster (PI), A. Akella
Amount: \$500,000 for 3 years
Awarded: June 2010

- G.1.5 **MEDITA - Multi-layer Enterprise-wide Dynamic Information-flow Tracking & Assurance**
Sponsor: National Science Foundation
Investigator(s): N. Feamster, A. Orso (PI), M. Prvulovic
Amount: \$900,000 for 3 years
Awarded: March 2010
- G.1.6 **Campus Network Access and Admission Control with Openflow**
Sponsor: National Science Foundation
Investigator(s): N. Feamster (PI), R. Clark
Amount: \$300,000 for 3 years
Awarded: January 2010
- G.1.7 **Studying DNS Traffic Patterns**
Sponsor: Verisign
Investigator(s): N. Feamster
Amount: \$30,000 for 1 year
Awarded: November 2009
- G.1.8 **CIFellowship for Cristian Lumezanu**
Sponsor: National Science Foundation
Investigator(s): C. Lumezanu, N. Feamster (PI)
Amount: \$140,000 for 1 year
Awarded: November 2009
- G.1.9 **Military Network Protocol**
Sponsor: DARPA Subcontract
Investigator(s): N. Feamster
Amount: \$37,000 for 1 year
Awarded: November 2009
- G.1.10 **Botnet Attribution and Removal: From Axioms to Theories to Practice**
Sponsor: Office of Naval Research
Investigator(s): W. Lee (PI), D. Dagon, J. Giffin, N. Feamster, K. Shin, F. Jahanian, M. Bailey, J. Mitchell, G. Vigna, C. Kruegel
Amount: \$7,500,000 for 5 years
Awarded: August 2009
- G.1.11 **Taint-based Information Tracking in Networked Systems**
Sponsor: National Science Foundation Trusted Computing Program
Investigator(s): N. Feamster
Amount: \$450,000 for 3 years
Awarded: August 2009
- G.1.12 **Towards a Market for Internet Connectivity**
Sponsor: Office of Naval Research
Investigator(s): N. Feamster (PI), R. Johari, V. Vazirani
Amount: \$350,000 for 1 year
Awarded: March 2009
- G.1.13 **Bringing Experimenters and External Connectivity to GENI**
Sponsor: GENI Project Office
Investigator(s): N. Feamster
Amount: \$320,000 for 3 years
Awarded: September 2008

- G.1.14 **Routing Without Recomputation**
Sponsor: Cisco Systems
Investigator(s): N. Feamster
Amount: \$96,019 for 1 year
Awarded: September 2008
- G.1.15 **CLEANSE: Cross-Layer Large-Scale Efficient Analysis of Network Activities to Secure the Internet**
Sponsor: National Science Foundation Cybertrust Program
Investigator(s): W. Lee (PI), N. Feamster and others
Amount: \$1,200,000 for 5 years
Awarded: September 2008
- G.1.16 **Virtual Center for Network and Security Data**
Sponsor: Department of Homeland Security
Investigator(s): N. Feamster
Amount: \$48,000 for 2 years
Awarded: March 2008
- G.1.17 **Sloan Research Fellowship**
Sponsor: Alfred P. Sloan Foundation
Investigator(s): N. Feamster
Amount: \$45,000 for 2 years
Awarded: February 2008
- G.1.18 **Enabling Security and Network Management Research for Future Networks**
Sponsor: National Science Foundation CRI-IAD Program
Investigator(s): N. Feamster (PI), Z. Mao, W. Lee
Amount: \$397,426 for 3 years
Awarded: February 2008
- G.1.19 **SMITE: Scalable Monitoring in the Extreme**
Sponsor: DARPA BAA 07-52: Scalable Network Monitoring
Investigator(s): N. Feamster (PI), W. Lee
Amount: \$250,000 for 2 years
Awarded: January 2008
- G.1.20 **Countering Botnets: Anomaly-Based Detection, Comprehensive Analysis, and Efficient Mitigation**
Sponsor: Department of Homeland Security BAA07-09
Investigator(s): W. Lee (PI), N. Feamster, J. Giffin
Amount: \$1,050,730 for 2 years
Awarded: January 2008
- G.1.21 **Spam Filtering Research**
Sponsor: IBM Faculty Award
Investigator(s): N. Feamster
Amount: \$ 7,500 (unrestricted gift)
Awarded: June 2007
- G.1.22 **SCAN: Statistical Collaborative Analysis of Networks**
Sponsor: National Science Foundation NeTS-NBD Program
Investigator(s): N. Feamster (PI), A. Gray, J. Hellerstein, C. Guestrin
Amount: \$ 95,000 for 3 years.
Awarded: June 2007

- G.1.23 **Towards an Accountable Internet Architecture**
Sponsor: National Science Foundation CyberTrust Program (Team Proposal)
Investigator(s): D. Andersen, H. Balakrishnan, N. Feamster (PI), S. Shenker
Amount: \$ 300,000 for 3 years.
Awarded: May 2007
- G.1.24 **Fish4Phish: Fishing for Phishing in a Large Pond**
Sponsor: AT&T Labs—Research
Investigator(s): N. Feamster (PI), O. Spatscheck, K. van der Merwe
Amount: Funding for summer intern.
Awarded: February 2007
- G.1.25 **Improving Network Operations with a View from the Edge.**
Sponsor: National Science Foundation CAREER Program
Investigator(s): N. Feamster (PI)
Amount: \$400,000 for 5 years.
Awarded: January 2007
- G.1.26 **Equipment Donation for Network Operations Research**
Sponsor: Intel Corporation
Investigator(s): N. Feamster
Amount: \$30,000
Awarded: October 2006
- G.1.27 **CABO: Concurrent Architectures are Better than One**
Sponsor: National Science Foundation NeTS-FIND Program
Investigator(s): N. Feamster (PI), L. Gao, J. Rexford
Amount: \$ 300,000 for 4 years
Awarded: June 2006
- G.1.28 **Verification and Modeling of Wide-Area Internet Routing**
Sponsor: Cisco Systems University Research Program
Investigator(s): N. Feamster and H. Balakrishnan (PI)
Amount: \$ 95,500 for 1 year.
Awarded: June 2004

2. Pending

- G.2.1 **Wide-Area Networking for Distributed Services**
Sponsor: National Science Foundation CNS Division
Investigator(s): N. Feamster, J. Rexford
Amount: \$600,000 for 3 years
Submitted: September 2010
- G.2.2 **Infrastructure for Home Networking**
Sponsor: National Science Foundation Computing Research Infrastructure Program
Investigator(s): N. Feamster, K. Edwards, K. Calvert
Amount: \$1,200,000 for 3 years
Submitted: August 2010
- G.2.3 **Automatic Configuration Generation for Data Center Configurations**
Sponsor: Yahoo Faculty Research and Engagement Program
Investigator(s): N. Feamster
Amount: \$25,000 for 1 year
Submitted: May 2010

G.2.4 Managing the Cost of Network Traffic

Sponsor: Yahoo Faculty Research and Engagement Program

Investigator(s): N. Feamster

Amount: \$25,000 for 1 year

Submitted: May 2010

3. Not Funded

Available upon request.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

H.1.1 Development of a shared network measurement storage and analysis infrastructure

Sponsor: National Science Foundation Major Research Infrastructure (MRI)

Investigator(s): D. Andersen, D. Song, C. Wang, H. Zhang

Amount: \$ 101,488.96

User and developer for proposed infrastructure; possible equipment money to Georgia Tech .

Submitted: February 2006.

2. Pending

3. Not Funded

Available upon request.

I. Other

I.0.1 In-Band, Bottom-Up Support for Network Accountability

Sponsor: N. Feamster, W. Lee, M. Ahamad

Investigator(s): DARPA Strategic Technology Office

Amount: *White paper / Request for Information.*

Submitted: February 2007

I.0.2 Towards an Accountable Internet Architecture

Sponsor: D. Andersen, H. Balakrishnan, N. Feamster, S. Shenker

Investigator(s): DARPA Strategic Technology Office

Amount: *White paper / Request for Information.*

Submitted: February 2007

J. Research Honors and Awards

2010	John P. Imlay Distinguished Lecture, Georgia Tech
2010	Panelist for NSF/ <i>Discover Magazine</i> Special Issue on "The New Internet"
2010	<i>Technology Review</i> Top Innovators Under 35
2010	Georgia Tech Sigma Xi Young Faculty Award
2009	Best Paper, <i>Passive and Active Measurement Conference</i>
2009	Georgia Tech Sigma Xi Best Undergraduate Research Advisor
2008	NSF Presidential Early Career Award for Scientists and Engineers (PECASE)
2008	Alfred P. Sloan Fellowship

2008	Georgia Tech College of Computing Outstanding Junior Faculty Research Award
2007	IBM Faculty Award
2007	NSF CAREER Award
2006	Best Student Paper (Advisor), <i>ACM SIGCOMM</i> (Premier Networking Conference)
2006	George M. Sprowls honorable mention for best Ph.D. thesis in computer science, MIT
2005	Best Paper, <i>2nd USENIX Symposium on Networked Systems Design and Implementation</i>
2002	Best Student Paper, <i>11th USENIX Security Symposium</i>
2001	Best Student Paper, <i>10th USENIX Security Symposium</i>
2002–2005	NSF Graduate Research Fellow
2001	MIT William A. Martin Memorial Thesis Award for Best EECS Master's Thesis

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

Member, ACM Special Interest Group on Data Communications (SIGCOMM)

Member, USENIX Technical Association

A.2. Conference Committee Activities

2010	Program Committee, <i>ACM SIGCOMM Poster and Demo Session</i>
2010	Program Committee, <i>ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures (VISA)</i>
2010	Program Committee Co-Chair , <i>USENIX Workshop on Internet Network Management (INM/WREN)</i>
2010	Program Committee, <i>ACM SIGMETRICS</i>
2010	Program Committee, <i>IEEE Symposium on Internet Security and Privacy</i>
2010	Program Committee, <i>USENIX Symposium on Networked Systems Design and Implementation (NSDI)</i>
2010	Program Committee <i>3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '10)</i>
2009	Program Committee, <i>ACM SIGCOMM Workshop on Research on Enterprise Networks (WREN)</i>
2009	Program Committee, <i>ACM SIGCOMM Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO)</i>
2009	Program Committee, <i>USENIX Technical Conference</i>
2009	Program Committee, <i>ACM SIGCOMM Workshop on Economics of Networked Systems (NetE-con)</i>
2009	Program Committee <i>2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)</i>
2009	Poster/Demo Co-Chair , <i>ACM SIGCOMM</i>
2009	Program Committee, <i>ACM SIGMETRICS</i>
2009	Program Committee, <i>6th ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI)</i>
2008	Program Committee, <i>3rd International Workshop on Real Overlays & Distributed Systems</i>
2008	Program Committee, <i>ACM SIGCOMM Internet Measurement Conference</i>
2008	Program Committee, <i>ACM Conference on Computer and Communications Security (CCS)</i>
2008	Program Committee, <i>ACM SIGCOMM</i>
2008	Program Committee, <i>ACM SIGMETRICS</i>
2008	Program Committee, <i>ACM SIGCOMM Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO)</i>
2008	Program Committee, <i>ACM SIGCOMM Workshop on Economics of Networked Systems (NetE-con)</i>

2008	Program Committee, <i>17th International World Wide Web Conference (Security/Privacy Track)</i>
2008	Program Committee, <i>ACM SIGMETRICS Workshop on Internet Network Management</i>
2008	Program Committee, <i>16th IEEE LAN/MAN Workshop</i>
2007	Program Committee, <i>3rd Annual CoNext Conference</i>
2007	Program Committee, <i>ACM SIGCOMM Workshop on Internet Management (INM)</i>
2007	Program Committee, <i>ACM SIGCOMM Student Poster Session</i>
2007	Program Committee, <i>ACM SIGMETRICS Workshop on Mining Internet Data (MineNet)</i>
2007	Co-Organizer , DIMACS Workshop Series on Internet Security
2007	Program Committee, <i>4th Conference on Email and Anti-Spam (CEAS)</i>
2007	Program Committee, <i>3rd USENIX Workshop on Steps to Reduce Unwanted Traffic on the Internet (SRUTI)</i>
2007	Program Committee, <i>USENIX Technical Conference</i>
2007	Program Committee, <i>CoNext</i>
2007	Program Committee, <i>16th International World Wide Web Conference (Security/Privacy Track)</i>
2007	Program Committee Co-Chair, <i>ACM/USENIX Workshop on Networks meet Databases (NetDB)</i>
2006–	Program Committee, <i>North American Network Operators Group (NANOG)</i>
2006	Organizer, <i>Workshop on Internet Routing Evolution and Design</i>
2006	Program Committee, <i>ACM SIGCOMM Internet Measurement Conference</i>
2006	Program Committee Co-Chair , <i>Workshop on the Economics of Networked Systems (NetE-con)</i>
2006	Program Committee Co-Chair , <i>CoNext Student Workshop</i>
2006	Program Committee, <i>2nd Annual CoNext Conference</i>
2006	Program Committee, <i>ACM SIGCOMM Workshop on Internet Network Management</i>
2006	Program Committee, <i>IEEE Symposium on Security and Privacy</i>
2006	Program Committee, <i>IEEE Infocom Student Poster Session</i>
2006	Program Committee, <i>IEEE International Conference on Internet Surveillance and Protection</i>

External reviewer for *IEEE/ACM Transactions on Networking*, *SIGCOMM* (2002, 2003, 2004, 2006, 2007), *SOSP* (2001, 2003), *Infocom* (2004, 2006), *HotNets* (2003), *HotOS* (2001), *USENIX Security Symposium* (2002), *ACM Computer Communication Review*, *IEEE Network Magazine*, *IEEE Journal on Selected Areas in Communications*, *Image Communication (EURASIP)*, *ASPLOS* (2004), *MobiSys* (2004), *USENIX* (2005, 2006), *NSDI* (2005, 2006), *IPTPS* (2005), *Workshop on Privacy Enhancing Technologies* (2006).

A.3. Workshops and External Courses

Unless otherwise noted, all listed activities are invited speaking invitations for workshops, tutorials, and symposia.

July 2010	Routing for Cloud Services Tutorial, GENI Engineering Conference 8, San Diego, CA
-----------	---

July 2010	Routing for Cloud Services Tutorial, GENI Engineering Workshop, Princeton, NJ
June 2010	African Network Operators Group Tutorial, Kigali, Rwanda
March 2010	Co-Organizer , DIMACS Workshop on Secure Internet Routing, New Brunswick, NJ
June 2009	Organizer , NSF Security Driven Architectures Workshop, Arlington, VA
March 2009	Workshop on Re-Architecting the Internet (NetArch), Monte Verita, Switzerland
February 2009	CAIDA Active Internet Measurement Systems (AIMS) Workshop, San Diego, CA
October 2008	Panelist at IEEE CCW, Steamboat Springs, Colorado
October 2008	Panelist at ACM SIGCOMM Internet Measurement Conference, Athens, Greece
June 2008	Google Workshop on Internet Measurement, Mountain View, CA
May 2008	Tutorial at 26th Brazilian Symposium on Computer Networks and Distributed Systems, Rio de Janeiro, Brazil
March 2008	Co-Organizer for DIMACS Workshop on Secure Internet Routing
November 2007	NSF/DARPA/ARO NCDI Workshop, College Park, MD
August 2007	DIMACS Tutorial on Algorithms for Next Generation Networks, New Brunswick, NJ
July 2007	INTIMATE Workshop on Methods and Tools for Network Analysis, Paris, France
May 2007	Workshop on Programmable Routers for Extensible Services of Tomorrow (PRESTO), Princeton, NJ
April 2007	NeXtworking, the Second COST-NSF Workshop on Future Internet, Berlin, Germany
February 2007	GIG Routing and Addressing Workshop, Washington, DC
February 2007	DARPA Workshop on Assurable Global Networking, Washington, DC
December 2006	Next-Generation Internet Workshop, Lisbon, Portugal
September 2006	Clean Slate Network Research Symposium, Cambridge, UK
October 2006	Co-organizer , Workshop on Internet Routing Evolution and Design (WIRED), Atlanta, GA
August 2006	Cisco Routing Research Symposium, San Jose, CA
June 2006	ARO-DARPA-DHS Special Workshop on Botnets, Arlington, VA
June 2006	Microsoft Research EdgeNet Workshop, Snoqualmie, WA
June 2006	Microsoft Research "Networking on the Edge" Workshop on Network Management, Seattle, WA
February 2006	NSF Workshop on Theory of Networked Computation, Princeton, NJ
January 2006	Cisco Network Management Summit, San Jose, CA

B. On-Campus Georgia Tech Committees

Spring 2010	Faculty Recruiting Committee
Fall 2009	Strategic Planning Committee
Spring 2009–10	Dean Search Committee
Spring 2009	Faculty Recruiting Committee

Spring 2008	Faculty Recruiting Committee
Fall 2006–	Area Coordinator, Networking Area Group
Fall 2006	Co-Organizer, Networking and Telecommunications Group Open House
Spring 2006–	College of Computing Strategic Planning Committee
Spring 2006	Ph.D. Recruiting Weekend Organizing Committee, CSS Division Leader

C. Member of Ph.D. Examining Committees

Ph.D. Thesis Committee

1. David Levin, Department of Computer Science, University of Maryland., Fall 2010.
Principal Advisor: Professor Bobby Bhattacharjee.
2. David Dagon, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Wenke Lee.
3. Junjie Zhang, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Wenke Lee.
4. Amogh Dhamdhere, College of Computing, Georgia Tech, Spring 2009.
Principal Advisor: Professor Constantine Dovrolis.
5. Guofei Gu, College of Computing, Georgia Tech, Spring 2008.
Principal Advisor: Professor Wenke Lee.
6. Steve Webb, College of Computing, Georgia Tech, Spring 2008.
Principal Advisor: Professor Calton Pu.
7. Vibhore Kumar, College of Computing, Georgia Tech, Spring 2008.
Principal Advisor: Professor Karsten Schwan.
8. Prahlad Fogla, College of Computing, Georgia Tech, Spring 2007.
Principal Advisor: Professor Wenke Lee.
9. Srinivasan Seetharaman, College of Computing, Georgia Tech, Spring 2007.
Principal Advisor: Professor Mostafa Ammar.
10. Sridhar Srinivasan, College of Computing, Georgia Tech., Spring 2006.
Principal Advisor: Professor Ellen Zegura.
11. Xenofontas Dimitropoulos, Electrical and Computer Engineering, Georgia Tech, Spring 2006.
Principal Advisor: Professor George Riley.
12. Qi Zhao, College of Computing, Georgia Tech, Spring 2006.
Principal Advisor: Professor Jim Xu.
13. Ruomei Gao, College of Computing, Georgia Tech., Fall 2005.
Principal Advisor: Professors Ellen Zegura and Constantine Dovrolis.

Other — Question writer for Ph.D. Qualifying Exam

1. Bilal Anwer, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.
2. Sam Burnett, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.

3. Shuang Hao, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.
4. Partha Kanuparth, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Constantine Dovrolis.
5. Maria Konte, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.
6. Robert Lychev, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.
7. Yogesh Mundada, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Nick Feamster.
8. Cong Shi, College of Computing, Georgia Tech., Spring 2010.
Principal Advisor: Professor Mostafa Ammar.
9. Yiyi Huang, College of Computing, Georgia Tech., Spring 2008.
Principal Advisor: Professor Nick Feamster.
10. Anirudh Ramachandran, College of Computing, Georgia Tech., Spring 2008.
Principal Advisor: Professor Nick Feamster.
11. Murtaza Motiwala, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Nick Feamster.
12. Vytutas Valancius, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Nick Feamster.
13. Mehmet Demirci, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Mostafa Ammar.
14. Ahmed Mansy, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Mostafa Ammar.
15. Tonqing Qiu, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Jim Xu.
16. Nan Hua, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Jim Xu.
17. Chuck Zhao, College of Computing, Georgia Tech., Spring 2009.
Principal Advisor: Professor Jim Xu.
18. Mukarram Bin Tariq, College of Computing, Georgia Tech., Spring 2007.
Principal Advisor: Professor Nick Feamster.
19. Zhenshun Zhang, College of Computing, Georgia Tech., Spring 2007.
Principal Advisor: Professor Raghupathy Sivakumar.
20. Yang Chen, College of Computing, Georgia Tech., Spring 2006.
Principal Advisor: Professor Jim Xu.

D. Consulting, Advisory, and Other External Appointments

1. Technical Advisory Board, Guavus, Inc. <http://www.guavus.com/>
2. Technical Advisory Board, Anchor Intelligence, Inc. <http://www.fraudwall.net/>
3. Consultant, Damballa, Inc. <http://www.anchorintelligence.com/>

E. Research Project Reviewer

1. National Science Foundation.
May 2009
2. National Science Foundation.
July 2008
3. National Science Foundation.
June 2008
4. National Science Foundation.
October 2007
5. National Science Foundation.
March 2007
6. National Science Foundation.
February 2007
7. Department of Homeland Security.
Fall 2006 - Present
Department of Homeland Security Predict Review Board

IV. NATIONAL AND INTERNATIONAL RECOGNITION

A. Invited Conference Session Chair

- April 2010 Session chair, *ACM/USENIX Networked Systems Design and Implementation (NSDI)*, San Jose, CA
- October 2008 Session chair, *ACM SIGCOMM HotNets-VII Workshop*, Calgary, Alberta, Canada
- October 2008 Session chair, *ACM SIGCOMM Internet Measurement Conference*, Athens, Greece
- March 2008 Session organizer, *Security for the Future Internet, NSF Cybertrust PI Meeting*, Arlington, VA
- June 2007 Session chair, *Network Virtualization, NSF NeTS-FIND PI Meeting*, Arlington, VA
- June 2006 Session chair, *Mechanism Design and Networking, First Workshop on the Economics of Networked Systems (NetEcon06)*, Ann Arbor, MI

B. Patents

- March 2007 “Method and System for Detecting and Responding to Attacking Networks”, U.S. Patent Application # 11/538,212

C. Editorial and Reviewer Work for Technical Journals and Publishers

- External reviewer for *IEEE/ACM Transactions on Networking*
- External reviewer for *IEEE Journal on Selected Areas in Communications*
- External reviewer for *IEEE Computer Networks*
- External reviewer for *ACM Transactions on Information and Systems Security*

V. OTHER CONTRIBUTIONS

A. Seminar Presentations

- A.0.1 Challenges and Opportunities in Home Network Measurement. In *John P. Imlay Distinguished Lecture*, Atlanta, GA, October 2010.
- A.0.2 SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware. In *ACM SIGCOMM*, New Delhi, India, September 2010.
- A.0.3 Outsourcing Home Network Security. In *ACM SIGCOMM Workshop on Home Networking (HomeNets)*, New Delhi, India, September 2010.
- A.0.4 Challenges and Opportunities in Home Network Measurement. In *ACM SIGCOMM Workshop on Home Networking (HomeNets)*, New Delhi, India, September 2010. Panel Discussion.
- A.0.5 Wide-Area Routing for Distributed Services. In *GENI Experimenters Workshop*, Princeton, NJ, June 2010.
- A.0.6 Wide-Area Routing for Distributed Services: Tutorial. In *GENI Engineering Conference 8*, San Diego, CA, July 2010.
- A.0.7 Network-Level Spam and Scam Defenses. In *African Network Operators Group*, Kigali, Rwanda, June 2010.

- A.0.8 SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware. In *National Institute of Information and Communications Technology*, Tokyo, Japan, June 2010.
- A.0.9 Network-Level Spam and Scam Defenses. In *National Institute of Information and Communications Technology*, Tokyo, Japan, June 2010.
- A.0.10 Wide-Area Routing for Distributed Services. In *University of Tokyo*, Tokyo, Japan, June 2010.
- A.0.11 SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware. In *Stanford Networking Seminar*, Stanford, CA, June 2010.
- A.0.12 Network-Level Spam and Scam Defenses. In *MIT Computer Science Department Colloquium*, Cambridge, MA, May 2010.
- A.0.13 Network-Level Spam and Scam Defenses. In *Harvard University Computer Science Department Colloquium*, Cambridge, MA, April 2010.
- A.0.14 Network-Layer Support for Secure Routing and Access Control. In *DIMACS Workshop on Secure Routing*, New Brunswick, NJ, March 2010.
- A.0.15 Detecting General Network Neutrality Violations with Causal Inference. In *ACM SIGCOMM CoNext*, Rome, Italy, December 2009.
- A.0.16 Dynamic Access Control with Resonance. In *DIMACS Workshop on Network Management*, New Brunswick, NJ, November 2009.
- A.0.17 Network-Level Spam and Scam Defenses. In *Princeton University Computer Science Department Colloquium*, Princeton, NJ, October 2009.
- A.0.18 SNARE: Spatio-Temporal Network-Level Automated Reputation Engine. In *Message Anti-Abuse Working Group (MAAWG) Plenary Session*, Philadelphia, PA, October 2009.
- A.0.19 A Platform for Building Flexible, Fast Virtual Networks on Commodity Hardware. In *Cisco Routing Architecture Workshop*, San Jose, CA, October 2009.
- A.0.20 Network-Level Spam and Scam Defenses. In *EPFL Summer Research Institute*, Lausanne, Switzerland, June 2009.
- A.0.21 Bringing Experimenters and External Connectivity to GENI. In *GENI Measurement Workshop*, Madison, WI, June 2009.
- A.0.22 Network-Level Spam Defenses. In *University of Wisconsin Computer Science Department Colloquium*, Madison, WI, April 2009.
- A.0.23 Trellis: A Platform for Building Flexible, Fast Virtual Networks on Commodity Hardware. In *NSF NeTS FIND PI Meeting*, Arlington, VA, April 2009.
- A.0.24 Dynamics of Online Scam Hosting Infrastructure. In *Passive and Active Measurement Conference*, Seoul, Korea, April 2009.
- A.0.25 Demonstration of Topology Creation Service and BGP Session Multiplexer. In *4th GENI Engineering Conference*, Miami, Florida, April 2009.
- A.0.26 Network Security Research. In *Georgia Tech College of Computing Wine & Cheese Talk*, Atlanta, GA, April 2009.

- A.0.27 Network-Level Spam Defenses. In *Cisco Systems Security Seminar*, San Jose, CA, March 2009.
- A.0.28 Network-Level Spam Defenses. In *Stanford University Networking Seminar*, Stanford, CA, March 2009.
- A.0.29 Network-Level Spam Defenses. In *University of North Carolina Computer Science Department Colloquium*, Chapel Hill, NC, March 2009.
- A.0.30 Dynamics of Online Scam Hosting Infrastructure. In *CAIDA Active Internet Measurement Systems (AIMS) Workshop*, San Diego, CA, February 2009.
- A.0.31 Outsourcing Network Security with Programmable Hardware. In *GENI Security Workshop*, Davis, CA, April 2009.
- A.0.32 Spam, Phishing, and Online Scams:
A View from the Network-Level. In *University of Toronto Computer Science Department Colloquium*, Toronto, Ontario, Canada, December 2008.
- A.0.33 Detecting and Diagnosing Network Performance Degradations with Statistical Methods. In *IPAM Workshop on New Mathematical Frontiers in Network Multi-Resolution Analysis*, Los Angeles, CA, October 2008.
- A.0.34 Fighting Spam, Phishing, and Online Scams at the Network Level. In *Asian Internet Engineering Conference*, Bangkok, Thailand, November 2008.
- A.0.35 Multiplexing BGP Sessions with a BGP Session Multiplexer. In *3rd GENI Engineering Conference*, Palo Alto, CA, October 2008.
- A.0.36 Towards an Accountable Internet Architecture. In *The IEEE 22nd Annual Computer Communications Workshop*, Steamboat Springs, Colorado, October 2008.
- A.0.37 Network-Level Spam Filtering. In *IPAM Workshop on Applications of Internet MRA to Cyber-Security*, Los Angeles, CA, October 2008.
- A.0.38 Spam, Phishing, and Online Scams:
A View from the Network-Level. In *Yahoo Tech Talk*, Sunnyvale, CA, August 2008.
- A.0.39 Path Splicing. In *EPFL Summer Research Institute*, Lausanne, Switzerland, July 2008.
- A.0.40 Spam, Phishing, and Online Scams:
A View from the Network-Level. In *Google Tech Talk*, Mountain View, CA, June 2008.
<http://www.youtube.com/watch?v=IBPg9Lyta3A>.
- A.0.41 Making Tomography Practical: Scalable Network Monitoring for Fault Diagnosis. In *DIMACS Workshop on Network Tomography*, New Brunswick, NJ, May 2008.
- A.0.42 Network-Based Spam Filtering. In *Internet2 Members Meeting*, Arlington, VA, April 2008.
- A.0.43 Path Splicing. In *Carnegie Mellon University Computer Science Seminar*, Pittsburgh, PA, April 2008.
- A.0.44 BGP, Bogons, and Spam. In *DIMACS Workshop on Secure Internet Routing*, New Brunswick, NJ, March 2008.
- A.0.45 Can Great Research Be Taught? Independent Research with Cross-Disciplinary Thinking and Broader Impact. In *ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE)*, Portland, OR, March 2008.

- A.0.46 Path Splicing. In *Colgate University Computer Science Seminar*, Hamilton, NY, November 2007.
- A.0.47 Path Splicing. In *Cornell University Computer Science Symposium*, Ithaca, NY, November 2007.
- A.0.48 Path Splicing. In *Bell Labs Networking Seminar*, Murray Hill, NJ, November 2007.
- A.0.49 Usage-Based DHCP Lease-Time Optimization. In *ACM/USENIX Internet Measurement Conference*, San Diego, CA, October 2007.
- A.0.50 Network-Based Spam Filtering. In *University of Southern California Computer Science Symposium*, Los Angeles, CA, October 2007.
- A.0.51 Path Splicing with Network Slicing. In *Georgia Tech Algorithms and Randomness Center (ARC) Symposium*, Atlanta, GA, October 2007.
- A.0.52 Internet Availability. In *DIMACS Tutorial on Algorithms for Next-Generation Networks*, New Brunswick, NJ, August 2007.
- A.0.53 Towards an Accountable Internet Architecture. In *INTIMATE Workshop on Methods and Tools for Network Analysis*, Paris, France, July 2007.
- A.0.54 Path Splicing with Network Slicing. In *UCL Networking Seminar*, Louvain La Neuve, Belgium, July 2007.
- A.0.55 Composing Virtual Networks. In *Third NSF-NeTS FIND PI Meeting*, Arlington, VA, June 2007.
- A.0.56 Path Splicing with Network Slicing. In *UCSD Networking and Systems Seminar*, San Diego, CA, June 2007.
- A.0.57 Path Splicing with Network Slicing. In *NANOG 40*, Bellevue, WA, June 2007.
- A.0.58 AGORA: A Market for Internet Connectivity. In *Workshop on Programmable Routers for Extensible Services of Tomorrow*, Princeton, NJ, May 2007.
- A.0.59 Path Splicing with Network Slicing. In *NeXtworking 2007, the Second COST-NSF Workshop on Future Internet*, Berlin, Germany, April 2007.
- A.0.60 Towards an Accountable Internet Architecture. In *DARPA GIG Routing and Addressing Workshop*, Arlington, VA, February 2007.
- A.0.61 Towards an Accountable Internet Architecture. In *DARPA STO Assurable Global Networking Workshop*, Arlington, VA, February 2007.
- A.0.62 Improving Network Operations with a View from the Edge. In *National Science Foundation CyberTrust PI Meeting*, Atlanta, GA, January 2007.
- A.0.63 Network Virtualization for Experimentation and Profit. In *University of Michigan Networking Seminar*, Ann Arbor, MI, December 2006.
- A.0.64 Network Virtualization for Experimentation and Profit. In *Stanford Networking Seminar*, Stanford, CA, November 2006.
- A.0.65 Network Architecture Research. In *National Science Foundation NeTS-FIND Informational Meeting*, Reston, VA, November 2006.
- A.0.66 Network Virtualization. In *National Science Foundation NeTS-FIND PI Meeting*, Reston, VA, November 2006.

- A.0.67 Understanding the Network-Level Behavior of Spammers. In *Johns Hopkins Security and Applied Research Lab Seminar*, Baltimore, MD, October 2006.
- A.0.68 Revealing Botnet Membership with DNSBL Counter-Intelligence. In *NANOG 38*, St. Louis, MO, October 2006.
- A.0.69 VINI: A Virtual Network Infrastructure. In *Centre national de la recherche scientifique (CNRS)*, Paris, France, September 2006.
- A.0.70 Botnets and Spam. In *Seminar: Laboratoire d'informatique de Paris 6*, Paris, France, September 2006.
- A.0.71 Network Virtualization and Graph Embedding. In *Georgia Tech Algorithms and Randomness Center Seminar*, Atlanta, GA, September 2006.
- A.0.72 Cabo: Concurrent Architectures are Better than One. In *Cisco Internet Routing Research Symposium*, San Jose, CA, August 2006.
- A.0.73 Botnets and Spam. In *ARO-DARPA-DHS Special Workshop on Botnets*, Arlington, VA, June 2006.
- A.0.74 Understanding the Network-Level Behavior of Spammers. In *CS 548: Internet and Distributed Systems Seminar*, Stanford, CA, June 2006.
- A.0.75 Understanding the Network-Level Behavior of Spammers. In *NANOG 37*, San Jose, CA, June 2006.
- A.0.76 Campus and Personal Network Troubleshooting. In *Microsoft Research EdgeNet 2006*, Snoqualmie, WA, June 2006.
- A.0.77 Infranet: Circumventing Web censorship and surveillance. In *Georgia Tech NTG Seminar*, Atlanta, GA, April 2006.
- A.0.78 Filtering: Sharpening Two Sides of a Double-Edged Sword. In *Interzone 5*, Tucker, GA, March 2006.
- A.0.79 Theory of Measurement and Monitoring. In *Workshop on the Theory of Networked Computation*, Princeton, NJ, February 2006.
- A.0.80 Challenges and Opportunities in Internet Data Mining. In *Cisco Network Management Summit*, San Jose, CA, February 2006.
- A.0.81 BGP Spamming Agility. In *NANOG 36*, Dallas, TX, February 2006.
- A.0.82 Spam Forensics. In *IEEE Security and Privacy Crystal Ball Workshop*, Berkeley, CA, February 2006.
- A.0.83 Network Security. In *Georgia Tech Information Security Center Lunch*, Atlanta, GA, January 2006.
- A.0.84 Geographic Locality of IP Prefixes. In *NANOG 35*, Los Angeles, CA, October 2005.
- A.0.85 rcc demonstration. In *NANOG 35*, Los Angeles, CA, October 2005.
- A.0.86 Detecting BGP Configuration Faults with Static Analysis. In *Princeton University Systems Reading Group*, Princeton, NJ, October 2005.
- A.0.87 Proactive Techniques for Correct and Predictable Internet Routing. In *University of Cambridge Symposium*, England, United Kingdom, June 2005.

- A.0.88 Proactive Techniques for Correct and Predictable Internet Routing. In *Hewlett-Packard Laboratories*, Palo Alto, CA, October 2005.
- A.0.89 Open problems in BGP anomaly detection. In *CAIDA Workshop on Internet Signal Processing*, San Diego, CA, November 2004.
- A.0.90 On end-to-end path failures and routing instability. In *CAIDA Workshop on Internet Signal Processing*, San Diego, CA, November 2004.
- A.0.91 Wide-area network data and analysis at MIT. In *CAIDA Internet Measurement Data Catalog Workshop*, San Diego, CA, June 2004.
- A.0.92 Verifying wide-area routing configuration. In *NANOG 31*, San Francisco, CA, May 2004.
- A.0.93 Verifying wide-area routing configuration with *rcc*. AT&T Labs; Florham Park, NJ, February 2004.
- A.0.94 Verifying wide-area routing configuration with *rcc*. In *NYU Systems Reading Group*, New York, NY, February 2004.
- A.0.95 A systematic approach to BGP configuration checking. In *NANOG 29*, Chicago, IL, October 2003.
- A.0.96 Characterizing path failures: Location, characterization, correlation. In *CAIDA Internet Statistics, Metrics, and Analysis Workshop*, Leiden, The Netherlands, October 2002.
- A.0.97 Infranet: Circumventing Web censorship and surveillance. In *Harvard Kennedy School of Government Seminar*, Cambridge, MA, November 2002.
- A.0.98 Infranet: Circumventing Web censorship and surveillance. Hewlett-Packard Laboratories; Palo Alto, CA, August 2002.
- A.0.99 Infranet: Circumventing Web censorship and surveillance. In *Carnegie Mellon University SDI Seminar*, Pittsburgh, PA, April 2002.
- A.0.100 Controlling the impact of BGP policy changes on IP traffic. In *NANOG 25*, Toronto, Ontario, Canada, June 2002.

VI. PERSONAL DATA

Born: Stanford, CA
Home Address: Atlanta, GA 30308-1490
Citizenship: USA
Email: feamster - cc.gatech.edu
WWW: <http://www.cc.gatech.edu/~feamster>

Teaching Statement

Nick Feamster

I believe that students learn best by doing. Hands-on experience and real-world exercises not only make classes more exciting, but they also provide memorable examples and analogies. Our ability to understand abstract concepts is more limited than our ability to process concrete examples that relate to familiar ideas. Some of my own memorable classroom experiences were lectures with concrete examples; I apply a similar approach in my courses, tying abstract concepts to relevant concrete examples and hands-on experience. For example, “route hijacking” is more concrete when students can actually see network traffic going where it isn’t supposed to go. Routing protocols make more sense when students can configure routers, induce failures on an experimental network, and watch the behavior of traffic over that network.

To this end, my first goal in teaching both networking and security classes is to connect textbook material with (1) real-world examples; and (2) hands-on experience. At both the undergraduate and graduate levels, I have incorporated course material that familiarizes students with the state of the art in network design, implementation, and experimentation; for example, I have students run experiments on network testbeds like Emulab and VINI, with real software routers that they can configure. Where appropriate, I have also allowed students to shape the course themselves by bringing in real-world examples, from which I will design a lecture. For example, in my undergraduate networking course, I maintain a wiki where students could post relevant “current events” in networking and vote on which topics they would like to see covered. Based on that input, I incorporate new material into the syllabus—teaching not just the current event itself, but also the relevant foundational material. I also bring my own current events to lecture and relate them to the textbook being covered. This takes more effort than dusting off old notes, but it keeps students engaged and helps me stay abreast of what is happening both in industry and in research.

My second goal is to elevate course material so that students are not just learning mechanics of protocols and systems, but also gaining a deeper understanding of the *concepts* that underlie their design. My reasoning here is two-fold. First, I believe that the traditional classroom lecture is “going the way of the blackboard”. With so many computing and communications tools for aggregating and processing information, conventional lectures are no longer always the most efficient way to convey textbook information. In my lectures, I try to go beyond what is taught in the textbook—rather than teaching only mechanics, I ask students about design rationales, and whether they would make the same choices today, given the changing roles of communications networks. Given that networking is still maturing as a field, there is a tendency to focus on protocol details, which may change over time. Ten years from now, I would like someone who took my class to be able to say that the concepts they learned have remained applicable. I try to organize topics around higher-level concepts (*e.g.*, randomization, caching, tree formation, identity), so that even as protocol details continue to change, the concepts that they learn remain valuable.

I enjoy teaching students how to think. With Alex Gray, I have designed a graduate course that focuses on teaching first-year graduate students how to do research. The course includes topics ranging from paper reading to fellowship applications to generating (and executing) research ideas. The value of the course is evident from student response: Students at various points along their Ph.D.—even more senior students—sit in on lectures. We presented a paper on the course at SIGCSE in 2008, and other computer science departments (*e.g.*, Duke, Princeton) are now starting to adopt some of the material.

I have a strong mentoring and advising record. My graduate students have received best paper awards at top conferences (including SIGCOMM), and my undergraduate students I have advised have garnered publications in top conferences and have gone to the best computer science graduate schools in the country. One of my most rewarding advising experiences was with undergraduate student Megan Elmore. When I first began working with undergraduate student Megan, she lacked confidence that she could be good at research. I taught her not only about research and computer networking, but I also continually encouraged her to continue in research and helped her realize her talents. Under my advisement, she received the Sigma Xi Undergraduate Research Award, the CoC undergraduate research award, and an NSF Graduate Fellowship; she is now a Ph.D. student at Stanford University.

Research Statement

Nick Feamster

Summary

My research focuses on developing tools, algorithms, and protocols that make the network easier to manage, more secure, and more available.

Nobody notices when the network works well, but everyone suffers when it doesn't. Thus, communications networks should be both secure and available. Network *security* has many facets, ranging from the ability to stop "unwanted traffic" (e.g., spam and denial-of-service attacks) to the ability to trace back attacks to their perpetrators ("accountability"). *Availability* means that the network must provide good performance for users whenever they want to use it—unfortunately, the increasing complexity of the network, coupled with hardware faults, software bugs, misconfigurations, and malice, make it difficult to achieve this goal. Unfortunately, these two important goals have also been among the most evasive. Breakthroughs require not only extensive domain knowledge, but also the ability to techniques from a wide range of areas, ranging from economics to machine learning. My work combines domain knowledge, extensive interactions with network operators, techniques from a wide range of disciplines, and—perhaps most importantly—the competence and tenacity to implement and deploy these systems in practice. This unique combination has allowed me to build one of the few networking research groups in the world that interacts directly with network operators to deploy fundamentally new systems and technologies in real-world networks.

I discover interesting and challenging practical problems through frequent discussions and meetings with network operators and people in industry. I then tackle these problems from first principles, develop new methods, and transfer these solutions back to practice in the form of working systems. I have tackled a variety of problems in network operations, ranging from real-time network diagnosis to stemming unwanted traffic like spam to architectures for fast failure recovery. Many people—most notably, operators "in the trenches"—are also working on these problems. Unfortunately, many of the people who have the domain knowledge that best equip them to solve these problems are busy with day-to-day operations, putting out fires as they arise but rarely taking time to think about fundamental changes to the network that might eradicate these problems. My research fills this niche. I first devise methods to understand the nature of the problem in practice. I tackle domain-specific problems with tools and techniques from other disciplines—ranging from machine learning to economics to program analysis—whose principles might provide insights into a new, previously undiscovered solution. I then devise a new approach or solution, and I transfer it to practice through implementation and deployment of real-world systems.

My work in this broad area follows three specific themes: (1) making the network more secure; (2) improving network availability and performance by making the network easier to operate and manage; (3) designing platforms for virtual networks that facilitate technical innovation in both network security and operations. The first two themes involve developing solutions that make the network more robust and resilient in the face of faults, misconfiguration, and malice; the third theme provides an avenue to evaluate and deploy these solutions in practice.

Theme 1: Network Security

Summary of work. My research explores the role that communications networks—in particular the network layer—can play in improving computer and communications security. This line of research began with my arrival at Georgia Tech in 2006. A cornerstone of this research is a system that was published in August 2009 called "SNARE" (Spatio-temporal Network-level Automated Reputation Engine). This work appeared at the *USENIX Security Symposium*, a top-tier security conference. The main idea behind

SNARE—and the key insight behind my research in spam filtering—is that spammers have different sending behavior than legitimate senders. Therefore, filters can distinguish spammers from legitimate senders by examining their *sending behavior* (i.e., how they send traffic), rather than what is in the messages themselves.

Prior to my research, conventional spam filters attempted to distinguish spam from legitimate email by looking at message contents: that is, they would look at the words or language used in the messages themselves and try to detect spam based on what the message said. This approach has become increasingly untenable, since spammers have begun to embed their messages in all sorts of media, ranging from images to PDFs to audio files to spreadsheets—by the time developers perfected their content filters for one type of medium, spammers moved onto the next. My line of work has taken an entirely different, but complementary approach: I look at features of the senders' *behavior* (e.g., the time of day they are sending, whether there are other “nearby” senders on the network, whether and how the sizes of the messages of the senders vary over time) to distinguish spamming behavior from legitimate email use. The method is harder for spammers to evade, it is more flexible because it can be deployed anywhere in the network, and it can work at much higher traffic rates than conventional approaches. This idea was first laid out in the initial award paper at SIGCOMM and finally realized in the SNARE paper from August 2009 at *USENIX Security*.

I have also worked on sweeping changes to the Internet architecture that could improve *accountability*, thus making it more difficult for malicious parties to operate unfettered in the first place. The current Internet architecture provides little to no accountability. Malicious end systems can conceal the source of their traffic (“spoofing”), and edge networks can provide false information about their reachability to various Internet destinations (“route hijacking”); both of these attacks make it difficult to track down perpetrators of attacks. Current approaches to solving these problems require manual configuration and operator vigilance, which make them weak and error-prone. Towards building networks that are inherently accountable, I have developed the Accountable Internet Protocol (AIP). One of my contributions to the design was to make the addresses in this protocol self-certifying, which forms the cornerstone of the basic design. I also demonstrated how to apply AIP to secure BGP, the Internet's interdomain routing protocol.

Impact. My research in network security has had impact in research, in industry, and on the national level. My research on this topic has earned the Presidential Early Career Award for Scientists and Engineers (PECASE), a Sloan fellowship, and the Best Paper Award at ACM SIGCOMM (the premier computer networking conference). Aspects of my work have also been incorporated into commercial spam filtering products and Web mail clients at companies including Yahoo, Cisco/Ironport, and McAfee, as well as a project for the Department of Defense on high-speed network monitoring. My paper on understanding the network-level behavior of spammers—which won the Best Student Paper award at SIGCOMM in 2006—has been cited over 200 times since its initial publication in August 2006—it spawned a variety of high-impact follow-on work, including looking at network-level behavior not only to develop better spam filters, but also to detect botnets more effectively and defend against phishing attacks, click fraud, and other serious threats to the Internet infrastructure. I have also been working on similar approaches to help detect and dismantle the Internet's scam hosting infrastructure (e.g., Web sites that attempt to steal user passwords, money, and so forth). My initial paper on this topic (“Dynamics of Online Scam-Hosting Infrastructure”) won the Best Paper award at the *Passive and Active Measurement* conference in April 2009.

My work on SNARE has also garnered significant attention in industry. This work was featured in *Technology Review* and on Slashdot (a popular, high-traffic site for news in information technology). Several companies including Yahoo have incorporated the network-level features that SNARE identifies into its spam filters, and companies that develop spam filtering appliances, such as McAfee, are also using these features to improve the accuracy and performance of their spam filtering appliances.

AIP appeared in ACM SIGCOMM in 2008; an early version of the design also appeared in *ACM Workshop on Hot Topics in Networking (HotNets)*. I am incorporating a version of this technology into a working system and transferring them to practice. I am working with BBN on a DARPA project that will ultimately result in incorporating AIP's mechanisms into a military network protocol that allows attribution of traffic to sources

(the details may ultimately be classified).

My impact on the broader field of cybersecurity goes beyond my own research. I am also having impact in the national arena in several ways. Last year, I was involved in setting the nation's agenda for cyber security, through multiple additional activities. First, with leadership from Jeannette Wing at NSF, I led a community-wide effort to develop a "wish list" document that describes the security community's needs for access to better data—ranging from network traffic data, to data about our country's infrastructure. This report was ultimately delivered to Tom Kalil, the deputy director for policy in the Office of Science and Technology Policy. Second, with program managers Karl Levitt and Lenore Zuck at NSF, I organized a community-wide, multi-agency workshop on "Security-Driven Architectures". The workshop included participants from all areas of computer science (ranging from theory and cryptography to networking to systems to hardware), with an eye towards setting a research agenda for developing more holistic approaches to computer security that consider *all* aspects of computer and communications systems, rather than just a single piece (like the network). Finally, my work on developing next-generation Internet protocols to improve accountability (which could eradicate spam in the first place), based on work that appeared at *ACM SIGCOMM* in 2008, were also included in reports for the National Cyber Leap Year.

Representative Publication

S. Hao, N. Syed, N. Feamster, A. Gray and S. Krasser. "Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine". *USENIX Security Symposium*, August 2009. Montreal, Quebec, Canada.

Most Cited Publication (236 Citations)

A. Ramachandran and N. Feamster. "Understanding the Network-Level Behavior of Spammers". *ACM SIGCOMM*, August 2006. Pisa, Italy. **Best Student Paper Award.**

Theme 2: Network Operations

Summary of work. A second major theme of my work is *network operations*, which is what I call the field of designing networks so that they are easier to run and manage. Much of my work in this area has focused on fault detection and troubleshooting. Prior to my dissertation work, operators relied on detecting problems with networks "at runtime" on a live network. My dissertation work demonstrated that, in fact, many routing problems could be detected simply by examining the configuration of the routing protocols, before the configuration is even deployed. I applied techniques from static program analysis to routing configuration to help network operators catch mistakes and predict dynamic network behavior before the configurations are deployed on a live network, preventing costly and catastrophic network downtime.

Beyond predicting behavior and proactively detecting configuration faults, operators must understand the network's behavior *as it is running* (e.g., to detect equipment failures, attacks, or unplanned shifts in network traffic). Unfortunately, operators are drowning in heterogeneous data. To help operators better understand network faults "at runtime", I have applied unsupervised learning techniques to Internet routing data to help them efficiently mine the data for network events that require corrective action. This work appeared in *ACM SIGMETRICS* in 2007. My work has also applied statistical inference techniques to help network operators determine the answers to "what if" configuration questions in content distribution networks; we developed a system called "WISE" (What-If Scenario Evaluator) to help network operators determine the effects of configuration changes on network response time. A paper on this system appeared at *ACM SIGCOMM* in 2008 and is now used by operators and network designers at Google. A more mature version of this work that also describes deployment experiences at Google is in submission to *IEEE/ACM Transactions on Networking*.

Users of communications networks also face the potential of intentional performance degradation or manipulation by Internet Service Providers (ISPs); these problems are popularly referred to as “network neutrality violations”. This transparency can help users determine whether their network is the cause of performance degradation, or whether performance problems that they are seeing are due to some other cause. With students, I designed, built, and deployed the *Network Neutrality Access Observatory (NANO)*, a system that aggregates measurements from end systems to help users and operators of edge networks infer when transit networks may be discriminating against certain types of traffic. This work appeared in *ACM SIGCOMM CoNext* in 2009, and we have deployed the system on Google’s Measurement Lab (<http://www.measurementlab.net/>). More recently, we have been looking at methods for helping users diagnose general problems with access network performance and examining which factors have the most influence on access network performance.

I have developed new network protocols and architectures that improve availability and accountability in communications networks in the face of both faults and malice. Networks face the continual threat of failures and attacks that disrupt end-to-end connectivity. Prior to my work, one promising approach to improving connectivity involved routing traffic along multiple paths between two endpoints (“multi-path routing”); despite the promise of this approach, previous approaches encountered two significant challenges: First, previous approaches for disseminating information about multiple paths through the network did not scale to large networks. Second, end systems had no way to signal to the network that an end-to-end path had failed or was providing inadequate performance. My research applied a new perspective to this problem: rather than simply routing traffic on one of multiple paths to a destination, allow traffic to switch paths at intermediate points en route to the destination, and allow end systems to signal to the network when it should attempt to use a different path to the destination using a small number of bits that can be carried in the traffic itself. This system, called *path splicing*, provides up to an exponential improvement in reliability for only a linear increase in the amount of state that each router in the network must store.

Impact. The foundation of this research theme comes from a system I built called “rcc” (router configuration checker). This system was the centerpiece of my doctoral dissertation and has had significant impact in both research and industry. The work received the Best Paper Award at *ACM/USENIX Networked Systems Design and Implementation (NSDI)* in 2005 and has been used by hundreds of Internet Service Providers (ISPs) around the world to check their network configurations for errors.

The NANO project is among the most visible of my research projects at Georgia Tech: The project page receives about 2,000 unique visitors every month, and, between January and March 2010, about 300 users have downloaded the code. The system is deployed on Google’s Measurement Lab, and we are exploring a version of NANO that could be incorporated into the Google Toolbar with Google’s Broadband Access Transparency (BAT) team.

The path splicing work resulted in a Sigma Xi undergraduate research award for Megan Elmore. The work was funded by Cisco, and they have considered the possibility of extending their existing multiple routing configuration (MRC) function to support path splicing. A more likely deployment scenario, however, may be the incorporation of path splicing into a network where network elements are more programmable (I discuss the promise of programmable networking in “Future Challenges” below.) We have published an open-source implementation of path splicing on several programmable networking platforms.

Representative Publication

M. Tariq, A. Zeitoun, V. Valancius, N. Feamster, and M. Ammar. “Answering What-if Deployment and Configuration Questions with ‘WISE’”. *ACM SIGCOMM*, August 2008. Seattle, WA.

Most Cited Publication (137 Citations)

N. Feamster and H. Balakrishnan “Detecting BGP Configuration Faults with Static Analysis” *2nd Symposium on Networked Systems Design and Implementation (NSDI)*, Boston, MA, May 2005. **Best Paper Award.**

Theme 3: Virtual Networking

Network virtualization allows multiple networks to operate in parallel on the same physical infrastructure. Although this concept is not new (commonly used Virtual Private Networks, or “VPNs”, come to mind as a prominent real-world example of network virtualization), virtualizing all aspects of the network infrastructure—in particular, both the links *and* the routers themselves—holds great promise for enabling innovation. In 2002, Larry Peterson, Scott Shenker, and Jon Turner argued that networking research had “ossified”, because researchers faced a huge deployment hurdle for deploying their research in production environments, and also because the large stakeholders had little incentive to allow disruptive innovation to take place. Their argument was essentially that, by “letting a thousand flowers bloom”, multiple networking technologies could be deployed in parallel, thereby providing researchers a path to innovation. The main research challenge was how to design and implement a virtual network infrastructure that supported this philosophy.

Towards solving this challenge, I began working on network virtualization during my postdoc at Princeton. Jennifer Rexford and I wanted to implement a new network protocol we had designed at the end of my graduate career. Our plan was to use PlanetLab—a large testbed with virtualized servers distributed around the world—to do it. Unfortunately, we quickly realized that PlanetLab did not have the necessary functions to instantiate test *networks*; in particular, PlanetLab offered no functions for building virtual routers and links, and also had no support for forwarding traffic at high rates for virtual routers (e.g., every packet needed to be copied several times at each node, significantly slowing the packet forwarding rates). These shortcomings caused us to pursue a larger project to build such a testbed that would support the kinds of experiments that we wanted to run. With Andy Bavier and Larry Peterson, we built a Virtual Network Infrastructure (VINI), a testbed that allows researchers to build virtual networks. This work appeared in *ACM SIGCOMM* in 2006. Although we still strive for more widespread adoption, the testbed is regularly used by several research groups around the country.

Since this initial work, I have focused on two aspects of network virtualization: (1) providing Internet connectivity and routing control to virtual networks; (2) designing very fast packet forwarding technologies for virtual networks. A virtual network—either an experiment or a distributed “cloud” service—typically needs connectivity to the rest of the Internet so that users can actually exchange traffic with it. To provide such connectivity, and to give each virtual network direct control over how user traffic reaches it, I designed, implemented and deployed the Transit Portal. This work will appear in *USENIX Annual Technical Conference* in June 2010; it is also a cornerstone of the larger nationwide GENI effort (featured here, for example: <http://www.geni.net/?p=1682>). Our work on designing faster packet forwarding technologies for virtual networks started with the Trellis project, which moved packet forwarding for virtual networks into the kernel; although this work resulted only in a workshop publication, the software itself was adopted by University of Utah’s Emulab, the most prominent emulation-based testbed for networking research. Our current efforts have focused on accelerating packet forwarding further by supporting custom packet forwarding for virtual networks in Field Programmable Gate Arrays (FPGAs); our work on Switch-Blade, a platform for rapidly developing and deploying custom forwarding engines in hardware for virtual networks, will appear at *ACM SIGCOMM* in August 2010.

Impact. The impact of this work thus far has been to support network experimentation for researchers; many other virtual network technologies and platforms have built on this work. Our work on virtual

networks has been cited nearly 300 times (the VINI paper has been cited 200 times, and our work describing a network architecture based around network virtualization has been cited over 100 times).

The Transit Portal is currently deployed in five locations, and I am using it in my courses to provide students with hands-on experience configuring networks of routers and connecting them to real BGP-speaking routers on the Internet. The course I have developed that uses this technology is likely serves as the first course where students can directly configure networks of routers that are connected to the global Internet.

Representative Publication

B. Anwer, M. Tariq, M. Motiwala, N. Feamster. "SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware" *ACM SIGCOMM*, New Delhi, India, August 2010.

Most Cited Publication (200 citations)

A. Bavier, N. Feamster, M. Huang, L. Peterson, J. Rexford. "In VINI Veritas: Realistic and Controlled Network Experimentation". *ACM SIGCOMM*, August 2006. Pisa, Italy.

Future Challenges

In my future work, I plan to take a proactive approach to network security and operations by developing protocols from the ground up that make networks fundamentally more secure and easier to manage. Networks are large, distributed systems that operators "program" with network configuration. Unfortunately, this configuration still takes place at the granularity of individual network devices and relies on low-level, mechanistic, and unintuitive commands. Improving network security and reliability ultimately requires raising this level of abstraction, which will most likely require developing protocols and languages that allow network operators to configure networks from a much higher layer of abstraction than they do today. It also entails fundamental changes to both the network devices and protocols. To achieve this goal, I see opportunities to draw on techniques from other disciplines. For example, my most recently awarded NSF grant proposes applying programming language and software engineering techniques to help operators configure networks.

Along these lines, my long-term goal is to *design networks that permit a range of policies but still have provable correctness and security properties*. In recent years, I have been redesigning network protocols so that operators can more easily control which users have access to which parts of the network ("access control"); I have also been building host and network support to prevent unauthorized access and data leaks ("information flow control"). My goal is to make it easier for operators to express—and verify—these policies in an operational network. I have made some early progress on these problems: we have built a system called Resonance that allows operators to express access control policies at a higher level of abstraction and may ultimately replace the current campus access control system. (A working version of this system was demonstrated at the GENI Engineering Conference in March 2010.) We are also building a system called Pedigree, which allows network operators to prevent certain types of data leaks. Finally, I have begun to design new protocols and systems to make home networks easier to configure and more secure.

My continued efforts will not only help advance network operations, but also to help shape the future of networking research towards more "hands on", operationally relevant problems. My approach will not only define new areas for networking research, but will also take better advantage of Georgia Tech's unique facilities and research-minded network operators. I aim to make Georgia Tech the top destination for performing experimental, systems-focused research on network operations and security.

Suggested Letter Writers

Nick Feamster

1. Jennifer Rexford (Princeton), Full Professor (postdoc mentor and regular collaborator)
2. Scott Shenker (UC Berkeley), Full Professor (occasional collaborator)
3. Larry Peterson (Princeton), Full Professor (previous collaborator)
4. Farnam Jahanian (Michigan), Full Professor
5. Jim Kurose (UMass Amherst), Full Professor
6. David Clark (MIT), Senior Research Scientist
7. Nick McKeown (Stanford), Associate Professor
8. Vern Paxson (UC Berkeley), Associate Professor
9. Stefan Savage (UCSD), Associate Professor
10. David Wetherall (Univ. of Washington), Associate Professor

Representative Publications

Nick Feamster

1. S. Hao, N. Syed, N. Feamster, A. Gray and S. Krasser. "Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine". *USENIX Security Symposium*, August 2009. Montreal, Quebec, Canada.
2. M. Tariq, A. Zeitoun, V. Valancius, N. Feamster, and M. Ammar. "Answering What-if Deployment and Configuration Questions with 'WISE'". *ACM SIGCOMM*, August 2008. Seattle, WA.

Note: A more recent version of this paper is submission to *IEEE/ACM Transactions on Networking*; it was submitted in January 2010. A version of the *Transactions on Networking* submission is available at <http://www.cc.gatech.edu/~feamster/rpt/papers/wise:ton10.pdf>

3. B. Anwer, M. Tariq, M. Motiwala, N. Feamster. "SwitchBlade: A Platform for Rapid Deployment of Network Protocols on Programmable Hardware" *ACM SIGCOMM*, New Delhi, India, August 2010.