

Curriculum Vitae

Name : Yan Chen

Email: ychen@northwestern.edu

Web Page: <http://www.cs.northwestern.edu/~ychen>

Education

- Dec. 2003 Ph.D. degree in Computer Science, University of California at Berkeley.
Advisor: Randy H. Katz, the United Microelectronics Corporation Distinguished Professor.
Thesis title: *Towards a Scalable, Adaptive and Network-aware Content Distribution Network*.
- May. 1998 M.S. degree in Computer Science, State University of New York at Stony Brook.
Advisor: Arie E. Kaufman, Distinguished Professor.
Thesis title: *Physically Based Volume Graphics Manipulations for Medical Applications*.
- May 1995 Honored B.E. degree in Computer Engineering, Zhejiang University, P. R. China.
Advisor: Jiaoying Shi, ex-Director of the National Lab of Computer Aided Design and Computer Graphics (CAD&CG).
B. E. thesis title: *PVM-G: Parallel Graphics Design Environment*.

Positions, Training, and Experience

- Sep. 2009 – Present Associate Professor, Department of Electrical Engineering and Computer Science, Northwestern University.
- Dec. 2010 – Sep. 2011 Visiting Professor, Department of Computer Science and Technology, Tsinghua University, China.
- Jan. 2004 – Aug. 2009 Assistant Professor, Department of EECS, Northwestern University.
- June 2002 – Oct. 2002 AT&T Shannon Lab, Florham Park, NJ, Researcher Summer Intern. Developed research on network monitoring and anomaly detection on high-speed routers
- May 1999 – Aug. 1999 Lumeria Inc., Berkeley CA, Software Engineer Summer Intern. Developed research on an XML based online transaction system.

Publications

Based on Google Scholar, my papers have been cited for over 3,600 times.

Invited Book Chapters

1. Yao Zhao and Yan Chen, “Algebraic Approaches for Scalable End-to-End Monitoring and Diagnosis”, invited book chapter for “Algorithms for Next Generation Network Architecture”, Springer, 2009.
2. Yan Chen, “Content Replication”, invited book chapter for “Content Delivery Networks: Principles and Paradigms”, Springer, 2008.
3. Zhichun Li, Anup Goyal, and Yan Chen, “Honeynet-based Botnet Scan Traffic Analysis”, invited book chapter for “Botnet Detection: Countering the Largest Security Threat”, Springer, 2008.
4. Ehab Al-Shaer and Yan Chen, Integrated Fault and Security Management, invited book chapter for “Information Assurance: Dependability and Security in Networked Systems”, Morgan Kaufmann Publishers, 2007.

Refereed Journal Publications

1. Chengchen Hu, Kai Chen, Yan Chen, Gao Xia, Bin Liu, Thanos Vasilakos, "A Measurement Study on Potential Inter-Domain Routing Diversity", to appear in *IEEE Transactions on Network and Service Management*, 2012.
2. Chengchen Hu, Bin Liu, Sheng Wang, Jia Tian, Yu Cheng, and Yan Chen, "Adaptive Non-Linear Sampling Method for Accurate Flow Size Measurement", in *IEEE Transactions on Communications*, 2011.
3. Kai Chen, Chuanxiong Guo, Haitao Wu, Jing Yuan, Zhenqian Feng, Yan Chen, Songwu Lu, Wenfei Wu, "DAC: Generic and Automatic Address Configuration for Data Center Networks", to appear in *ACM/IEEE Transaction on Networking (ToN)*, 2011.
4. Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang and Yan Chen, "Security Issues in Online Social Networks", in *IEEE Internet Computing*, Volume 15, No. 4, July/August, 2011, pp. 56-63.
5. Kai Chen, Chengchen Hu, Xin Zhang, Kai Zheng, Yan Chen, and Athanasios V. Vasilakos, "Survey on Routing in Data Centers: Insights and Future", in *IEEE Network magazine - Special Issue on Cloud Computing*, Volume 25, No. 4, July/August 2011, pp. 6-10.
6. Zhichun Li, Anup Goyal, Yan Chen, and Vern Paxson, "Towards Situational Awareness of Large-scale Botnet Probing", in *IEEE Transactions on Information Forensics & Security*, Vol. 6, Issue 1, pp. 175-188, 2011.
7. Zhichun Li, Yan Gao, and Yan Chen, "HiFIND, a High-speed Flow-level Intrusion Detection Approach with DoS Resiliency", in *Journal of Computer Networks*, 2010.
8. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, Chi Yin Cheung, and Xing Li, "POPI: A User-level Tool for Inferring Router Packet Forwarding Priority", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 18, Issue 1, Feb. 2010.
9. Lanjia Wang, Zhichun Li, Yan Chen, Zhi (Judy) Fu and Xing Li, "Thwarting Zero-day Polymorphic Worms with Network-level Length-based Signature Generation," in *ACM/IEEE Transaction on Networking (ToN)*, Volume 18, Issue 1, Feb. 2010.
10. Yao Zhao, Yan Chen, and David Bindel, "Towards Unbiased End-to-End Network Diagnosis", *ACM/IEEE Transaction on Networking (ToN)*, Volume 17, Issue 6 (December 2009), Pages: 1724-1737.
11. Yao Zhao and Yan Chen, "FAD and SPA: End-to-end Link-level Loss Rate Inference without Infrastructure", in the *Journal of Computer Networks*, Volume 53, Issue 9, June 2009, pp1303-1318.
12. Leiwen Deng, Yan Gao, Yan Chen and Aleksandar Kuzmanovic, "Pollution Attacks and Defenses for Internet Caching Systems", *Journal of Computer Networks*. Volume 52, Number 5, April, 2008, pp 935-956.
13. Robert Schweller, Zhichun Li, Yan Chen, Yan Gao, A. Gupta, Y. Zhang, P. Dinda, Ming-Yang Kao, and G. Memik, "Flow-level High-speed Network Monitoring with Reversible Sketches", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 15, Issue 5, Oct. 2007.
14. Yan Chen, David Bindel, H. Song, and R. Katz, "Algebra-based Scalable Overlay Network Monitoring: Algorithms, Evaluation, and Applications", in *ACM/IEEE Transaction on Networking (ToN)*, Volume 15, Issue 5, Oct. 2007.
15. Yao Zhao, Yan Chen, B. Li and Q. Zhang, "Hop ID: A Virtual Coordinate based Routing for Sparse Mobile Ad Hoc Networks", in *IEEE Transactions on Mobile Computing (TMC)*, Volume 6, Number 9, September 2007.
16. Pin Ren, Yan Gao, Zhichun Li, Yan Chen and Ben Watson, "IDGraphs: Intrusion Detection and

Analysis Using Stream Compositing", invited paper for *IEEE Computer Graphics & Applications, special issue on Visualization for Cyber Security*, Volume 26, Number 2, March/April 2006.

17. Yan Chen, Lili Qiu, Wei Chen, Luan Nguyen, and Randy H. Katz, Efficient and Adaptive Web Replication using Content Clustering, *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Internet and WWW Measurement, Mapping, and Modeling*, Aug., 2003.
18. Yan Chen, Chris Overton, and Randy H. Katz, Internet Iso-bar: A Scalable Overlay Distance Monitoring System, in *Journal of Computer Resource Management*, Computer Measurement Group, Spring Edition, 2002.
19. Yan Chen, Khian Hao Lim, Chris Overton, and Randy H. Katz, On the Stability of Network Distance Estimation, in *ACM SIGMETRICS Performance Evaluation Review (PER)*, September issue, 2002.
20. Qinghong Zhu, Yan Chen, and Arie E. Kaufman, "Real-time Biomechanically-based Muscle Volume Deformation using FEM", *Journal of Computer Graphics Forum*, 1998, pp. C275-C284.

Refereed Conference Publications

(Acceptance rates provided when available. The average paper length is about 10 pages.)

21. Xitao Wen, Kai Chen, Yan Chen, Yongqiang Liu, Yong Xia, and Chengchen Hu, "VirtualKnotter: Online Virtual Machine Shuffling for Congestion Resolving in Virtualized Datacenter", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
22. Yi Wang, Keqiang He, Huichen Dai, Wei Meng, Junchen Jiang, Bin Liu, and Yan Chen, "Scalable Name Lookup in NDN Using Effective Name Component Encoding", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
23. Xingyu Ma, Chengchen Hu, Kai Chen, Che Zhang, Hongtao Zhang, Kai Zheng, Yan Chen, and Xianda Sun, "Error Tolerant Address Configuration for Data Center Networks with Malfunctioning Devices", in the Proc. of *IEEE ICDCS*, 2012 (71/515=13%).
24. Yinzhi Cao, Zhichun Li, Vaibhav Rastogi, Xitao Wen, and Yan Chen, "Virtual Browser: a Virtualized Browser to Sandbox Third-party JavaScripts with Enhanced Security", in the Proc. of *ACM ASIACCS*, 2012 (30%).
25. Kai Chen, Ankit Singla, Atul Singh, Kishore Ramachandran, Lei Xu, Yueping Zhang, Xitao Wen, Yan Chen, "OSA: An Optical Switching Architecture for Data Center Networks with Unprecedented Flexibility", in the Proc. of *ACM/USNEIX NSDI*, 2012 (30/169=17.8%).
26. Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia and Alok Choudhary, "Towards Online Spam Filtering in Social Networks", to appear in the Proc. Of *19th Network & Distributed System Security Symposium (NDSS)*, 2012 (46/258=17.8%).
27. Yinzhi Cao, Vinod Yegneswaran, Phillip Porras and Yan Chen, "PathCutter: Severing the Self-Propagation Path of XSS JavaScript Worms in Social Web Networks", to appear in the Proc. Of *19th Network & Distributed System Security Symposium (NDSS)*, 2012 (46/258=17.8%).
28. Yao Zhao, Yinzhi Cao, Anup Goyal, Yan Chen, and Ming Zhang, "Rake: Semantics Assisted Network-based Tracing Framework", in the Proc. of *IEEE/ACM IWQoS*, 2011 (23/80=28.8%).
29. Zhichun Li, Yi Tang, Yinzhi Cao, Vaibhav Rastogi, Yan Chen, Bin Liu, Clint Sbisa, "WebShield: Enabling Various Web Defense Techniques without Client Side Modifications", in the Proc. of *18th Network & Distributed System Security Symposium (NDSS)*, 2011 (28/139=20%).
30. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y. Zhao, "Detecting and Characterizing Social Spam Campaigns", in the Proc. of *ACM SIGCOMM IMC*, 2010 (47/211=22.3%).

31. Zhichun Li, Gao Xia, Hongyu Gao, Yi Tang, Yan Chen, Bin Liu, Junchen Jiang, and Yuezhou Lv, "NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks", in the Proc. of *ACM SIGCOMM*, 2010 (33/276=12%).
32. Kai Chen, Chuanxiong Guo, Haitao Wu, Jing Yuan, Zhenqian Feng, Yan Chen, Songwu Lu, Wenfei Wu, "Generic and Automatic Address Configuration for Data Center Networks", in the Proc. of *ACM SIGCOMM* 2010 (33/276=12%). **Selected as one of three best papers for fast track to ACM/IEEE ToN.**
33. Chengchen Hu, Bin Liu, Hongbo Zhao, Kai Chen and Yan Chen, "DISCO: Memory Efficient and Accurate Flow Statistics for Network Measurement", in the Proc. of *IEEE ICDCS*, 2010 (84/585=14.4%).
34. Zhichun Li, Ming Zhang, Zhaosheng Zhu, Yan Chen, Albert Greenberg, and Yi-Min Wang, "CloudProphet: Automating Performance Prediction for Cloud Services", in the Proc. of *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2010. (29/175=16.6%).
35. Zhichun Li, Anup Goyal, Yan Chen, and Aleksandar Kuzmanovic, "Measurement and Diagnosis of Address Misconfigured P2P Traffic", in the Proc. of *IEEE INFOCOM (main conference)*, 2010 (276/1575 = 17.5%).
36. Chengchen Hu, Kai Chen, Yan Chen and Bin Liu, "Evaluating Potential Routing Diversity for Internet Failure Recovery", in the Proc. of *IEEE INFOCOM (mini conference)*, 2010 (276+106 /1575 = 24.3%)
37. Kai Chen, David R. Choffnes, Rahul Potharaju, Yan Chen, Fabian E. Bustamante, Dan Pei, Yao Zhao, "Where the Sidewalk Ends: Extending the Internet AS Graph Using Traceroutes From P2P Users", in the Proc. of *the Fifth ACM International Conference on emerging Networking Experiments and Technologies (CoNEXT)*, 2009 (29/170=17%).
38. Kai Chen, Chengchen Hu, Wenwen Zhang, Yan Chen, Bin Liu, "On the Eyeshots of BGP Vantage Points", in the Proc. of *IEEE Globecom Next Generation Network (NGN) Symposium*, 2009.
39. Zhaosheng Zhu, Vinod Yegneswaran, and Yan Chen, "Using Failure Information Analysis to Detect Enterprise Zombies," in the Proc. of *the 5th International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2009 (19/75 =25.3%).
40. Yao Zhao, Sagar Vemuri, Jiazhen Chen, Yan Chen, Hai Zhou and Zhi (Judy) Fu, "Exception Triggered DoS Attacks on Wireless Networks", in the Proc. of *the 39th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-DCCS)*, 2009 (37/177 = 21%).
41. Yao Zhao, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Chen, and Eliot Gillum, "BotGraph: Large Scale Spamming Botnet Detection", in the Proc. of *the 6th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2009 (32/162=20%).
42. Yao Zhao, Zhaosheng Zhu, Yan Chen, Dan Pei, and Jia Wang, "Towards Efficient Large-Scale VPN Monitoring and Diagnosis under Operational Constraints", in the Proc. of *IEEE INFOCOM (main conference)*, 2009 (282/1435=20%).
43. Zhichun Li, Anup Goyal, Yan Chen, and Vern Paxson, "Automating Analysis of Large-Scale Botnet Probing Events", in the Proc. of *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, full paper, 2009 (33/147=22.4%).
44. Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, Keesook Han, "Botnet Research Survey," in the Proc. of *the 32nd Annual IEEE International Computer Software and Applications Conference*, 2008, pp.967-972.
45. Yao Zhao, Yan Chen, and Sylvia Ratnasamy, "Load balanced and Efficient Hierarchical Data-Centric Storage in Sensor Networks", in the Proc. of *IEEE Conference on Sensor, Mesh and Ad*

Hoc Communications and Networks (SECON), June 2008 (64/300=21.3%).

46. Chengchen Hu, Sheng Wang, Jia Tian, Bin Liu, Yu Cheng, and Yan Chen, "Accurate and Efficient Traffic Monitoring Using Adaptive Non-linear Sampling Method", in the Proc. of *IEEE INFOCOM*, 2008 (236/1160=20%).
47. Zhichun Li, Lanjia Wang, Yan Chen and Zhi Judy Fu, Network-based and Attack-resilient Length Signature Generation for Zero-day Polymorphic Worms, in Proc. of *the 15th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2007 (32/220=14%).
48. Yan Gao, Yao Zhao, Robert Schweller, Shobha Venkataraman, Yan Chen, Dawn Song, and Ming-Yang Kao, "Detecting Stealthy Spreaders Using Online Outdegree Histograms", in Proc. of *15th IEEE International Workshop on Quality of Service (IWQoS)*, 2007 (17/64=26.6%).
49. Guohan Lu, Yan Chen, Stefan Birrer, Fabian E. Bustamante, Chi Yin Cheung, and Xing Li, "End-to-end Inference of Router Packet Forwarding Priority", in Proc. of *IEEE Infocom 2007* (252/1400=18%).
50. Yao Zhao and Yan Chen, "A Suite of Schemes for User-level Network Diagnosis without Infrastructure", in Proc. of *IEEE Infocom 2007* (252/1400=18%).
51. Yan Gao, Leiwen Deng, Aleksandar Kuzmanovic, and Yan Chen, "Internet Cache Pollution Attacks and Countermeasures", in Proc. of *the 14th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2006 (33/232=14%).
52. Prasad Narayana, Ruiming Chen, Yao Zhao, Yan Chen, Zhi Fu, and Hai Zhou, "Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+", in Proc. of *the Second Workshop on Secure Network Protocols (NPSec)*, co-located with ICNP 2006 (7/21 = 33%).
53. Yao Zhao, Yan Chen, and David Bindel, "Towards Unbiased End-to-End Network Diagnosis", in Proc. of *ACM SIGCOMM*, 2006 (37/340=10%).
54. Zhichun Li, Yan Chen, and Aaron Beach, "Towards Scalable and Robust Distributed Intrusion Alert Fusion with Good Load Balancing", in Proc. of *ACM SIGCOMM Workshop on Large-Scale Attack Defense*, 2006 (11/33=33%).
55. Yan Gao, Zhichun Li and Yan Chen, "A DoS Resilient Flow-level Intrusion Detection Approach for High-speed Networks", in Proc. of *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2006 (75/536=14%).
56. Yao Zhao, Yand Chen, and David Bindel, "Deterministic Overlay Diagnosis", poster paper, in Proc. of *ACM SIGMETRICS*, 2006 (30 full + 17 poster papers out of 217 (14-22%)).
57. Zhichun Li, Manan Sanghi, Brian Chavez, Yan Chen and Ming-Yang Kao, "Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience", in Proc. of *IEEE Symposium on Security and Privacy*, 2006 (23/251=9%).
58. Robert Schweller, Zhichun Li, Yan Chen, Yan Gao, Anup Gupta, Yin Zhang, Peter Dinda, Ming-Yang Kao, and Goken Memik, "Reverse Hashing for High-speed Network Monitoring: Algorithms, Evaluation, and Applications", in the Proc. of *IEEE INFOCOM*, 2006 (252/1800=18%).
59. Yao Zhao, Bo Li, Qian Zhang, Yan Chen, and Wenwu Zhu, Efficient HopID based Routing for Sparse Ad Hoc Networks, Proc. of *the 13th IEEE International Conference on Network Protocols (ICNP)*, 2005 (36/212=17%).
60. Pin Ren, Yan Gao, Zhichun Li, Yan Chen, and Ben Watson, IDGraphs: Intrusion Detection and Analysis Using Histograms, Proc. of *the IEEE Workshop on Visualization for Computer Security (VizSEC)*, 2005.

61. Yan Chen, Zhichen Xu, and Chengxiang Zhai, A Scalable Semantic Indexing Framework for Peer-to-Peer Information Retrieval, Proc. of *ACM SIGIR Workshop on Heterogeneous and Distributed Information Retrieval*, 2005.
62. Robert Schweller, Anup Gupta, Elliot Parsons, and Yan Chen, Reverse Hashing for Sketch-based Change Detection on High-speed Networks, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2004 (39/157 = 25%).
63. Yan Chen, David Bindel, Hanhee Song, and Randy H. Katz, An Algebraic Approach to Practical and Scalable Overlay Network Monitoring, Proceedings of *ACM SIGCOMM*, Aug. 2004 (31/340= 9%).
64. Yan Chen, David Bindel, and Randy H. Katz, Tomography-based Overlay Network Monitoring, poster in *ACM SIGCOMM*, 2003. Abstract of the poster in *ACM Computer Communication Review (CCR)*, Jan. 2004.
65. Yan Chen, David Bindel, and Randy H. Katz, Tomography-based Overlay Network Monitoring, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2003 (33/109=30%).
66. Bala Krishnamurthy, Subhabrata Sen, Yin Zhang, and Yan Chen, Sketch-based Change Detection: Methods, Evaluation, and Applications, Proceedings of *ACM SIGCOMM Internet Measurement Conference (IMC)*, Oct. 2003 (33/109=30%).
67. Yan Chen, Lili Qiu, Wei Chen, Luan Nguyen and Randy H. Katz, Clustering Web Content for Efficient Replication, Proceedings of the *10th IEEE International Conference on Network Protocols (ICNP)*, Nov. 2002.
68. Yan Chen, Randy H. Katz and John D. Kubiawicz, SCAN: a Dynamic Scalable and Efficient Content Distribution Network, Proceedings of the *First International Conference on Pervasive Computing*, Zurich, Switzerland, Aug. 2002.
69. B. Raman, S. Agarwal, Yan Chen, M. Caesar, W. Cui, P. Johansson, K. Lai, T. Lavian, S. Machiraju, Z. M. Mao, G. Porter, T. Roscoe, M. Seshadri, J. Shih, K. Sklower, L. Subramanian, T. Suzuki, S. Zhuang, A. D. Joseph, Randy H. Katz, and I. Stoica, The SAHARA Model for Service Composition Across Multiple Providers, *invited paper*, Proceeding of the *First International Conference on Pervasive Computing*, Zurich, Switzerland, Aug. 2002.
70. Yan Chen, Randy H. Katz and John Kubiawicz, "Dynamic Replica Placement for Scalable Content Delivery", Proceedings of *1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.
71. Yan Chen, Adam Bargteil, David Bindel, Randy H. Katz and John Kubiawicz, "Quantifying Network Denial of Service: A Location Service Case Study, Proceeding of the *Third International Conference on Information and Communications Security (ICICS)*, Nov. 2001.
72. John Kubiawicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishna Gummadi, Sean Rhea, Hakim Weatherspoon, Westley Weimer, Chris Wells, and Ben Zhao, "OceanStore: An Architecture for Global-Scale Persistent Storage", Proceedings of *ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, Oct. 2000.
73. Yan Chen, Qinghong Zhu, and Arie Kaufman, "Physically-based Animation of Volumetric Objects", Proceeding of *IEEE Computer Animation*, 1998.

Patents

1. B. Krishnamurthy, S. Sen, Y. Zhang, and Yan Chen, "Sketch-based Change Detection in Massive Data Streams", filed on June 14, 2004. U.S. Patent Application No. 10/867,265.
2. Zhichun Li, Lanjia Wang, Yan Chen, and Zhi Fu, "Method and Apparatus to Facilitate Generating Worm-Detection Signatures Using Data Packet Field Lengths", filed on December 18, 2007. U.S. Patent Application No. 11/985,760.

3. Jia Wang, Yan Chen, Dan Pei, Yao Zhao, and Zhaosheng Zhu, "Towards Efficient Large-Scale Network Monitoring and Diagnosis Under Operational Constraints", filed on January 2009. U.S. Patent Application No. 12/186,096.
4. Yan Chen, Zhichun Li, Gao Xia and Bin Liu, "Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense," filed on July 29, 2010, Patent Application No. 12/846,541.

Software Artifacts

All the tools below are available at <http://list.cs.northwestern.edu/projects.html> except denoted otherwise.

- Social network spam campaign analysis data – released the largest social network spam analysis on the spam URLs.
- Hamsa – A system for zero-day polymorphic worm signature generation. The download also includes test cases such as polymorphic engines.
- TOM and LEND – A suite of tools for scalable overlay network monitoring and unbiased overlay network diagnosis.
- FAD – A tools for end user-based based network diagnosis without infrastructure.
- POPI – A tool for router packet forwarding priority inference from end hosts.
- Reversible Sketches – A suite of tools for online high-speed network traffic monitoring and anomaly/intrusion detection.
- ErrorDoS – Tools for novel denial of service (DOS) attacks with error messages for WiFi networks and the corresponding defense.
- CachePollution – Tools for novel DOS attacks on Web caches and the corresponding defense. <http://www.cs.northwestern.edu/~drc915/webBrowsPerf/>

Grants (total grants \$2,455, 779, my share \$1,810,029, no pure equipment grant)

1. "NeTS: Small: Parallax -- Leveraging the Perspective of Ten Million Peers", NSF NeTS Award, co-PI (PI Fabian Bustamante), 9/2009 – 8/2012, \$500,000 (my share \$250,000).
2. "CT-ISG High-Speed Network Defense with Massive and Diverse Vulnerability Signatures", NSF CyberTrust Award, single PI, 9/2008 – 8/2011, \$400,000.
3. "RTFM: Network Penetration and Security Course Development", Walter P. Murphy Society Grant, Northwestern University, single PI, 9/2007 - 8/2008, \$15,000.
4. "Intrusion Detection and Forensics for Self-defending Wireless Networks", Air Force of Scientific Research (AFOSR) Young Investigator Award, single PI, 12/2006 - 11/2009, \$368,326.
5. "CT-ISG: Router-Based Signature Generation for Zero-Day Polymorphic Worms", NSF CyberTrust Award, PI, (co-PI Ming-Yang Kao), 9/2006 – 8/2009, \$200,000 (my share \$100,000).
6. "CT-ISG: Pollution Resilience for Internet Caches", NSF CyberTrust Award, co-PI, (PI Aleksandar Kuzmanovic), 9/2006 – 8/2009, \$350,000 (my share \$175,000).
7. "HPNAIDM: The High-Performance Network Anomaly/Intrusion Detection and Mitigation System", DOE Early Career Award, single PI, 8/2005-8/2008, \$296,980.
8. Microsoft Research Trustworthy Computing Award 2006, PI, (co-PIs: Fabian Bustamante, Peter Dinda and Aleksandar Kuzmanovic), 9/2006-8/2007, \$50,000 (my share \$25,000).
9. "Information and Communication Security Curriculum Development – Phase II: National Accreditation", Walter P. Murphy Society Grant, Northwestern University, single PI, 9/2005 - 8/2006, \$13,393.
10. "A Virtual Lab for Experimental Systems Education", Walter P. Murphy Society Grant, Northwestern University, co-PI, (PI: Fabian Bustamante, Other co-PIs: Brian Dennis, Peter Dinda, and Aleksandar Kuzmanovic), \$35,750, 9/2005 - 8/2006.

11. "Adaptive Intrusion Detection and Mitigation Systems for WiMAX Networks", Northwestern-Motorola Center for Telecommunications, PI (co-PI Hai Zhou), 9/2005-8/2007, \$150,000 (my share \$110,000)
12. Microsoft Research Trustworthy Computing Award 2005, PI (co-PI: Andrea Matwyshyn), 9/2005-8/2006, \$50,000 (my share \$30,000)
13. "Information and Communication Security Curriculum Development", Walter P. Murphy Society Grant, Northwestern University, single PI, 09/01/2004 to 08/31/2005, \$26,330.

Honors

- Selected to Attend the University Leadership Program offered by the Kellogg School of Management, 2009
- Top EECS Researcher Award, Northwestern University, 2009
- DoD (Air Force of Scientific Research) Young Investigator Award, 2007
- Department of Energy (DOE) Early CAREER Award, 2005
- Microsoft Trustworthy Computing Awards, 2004 (with Andrea M. Matwyshyn) and 2005 (with Fabian Bustamante, Peter Dinda and Aleksandar Kuzmanovic)
- AGEF Professor, Midwest Crossroads AGEF (Alliances for Graduate Education and the Professoriate) - a partnership of Northwestern, Indiana and Purdue University to increase minority participation in graduate studies and academia, 2005
- Searle Junior Fellow, Northwestern University, 2004

Synergistic Activities

- Vice Chair of World Wide Web conference in charge of the "Security, Privacy, Trust, and Abuse" track, 2012.
- General Chair, the 18th ACM Conference on Computer and Communication Security (CCS), 2011.
- Poster Co-chair, the 41st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2011.
- Steering Committee member, the IEEE International Workshop on Quality of Service (IWQoS), 2007 – 2010.
- TPC Co-Chair, the Next Generation Networking Symposium (NGN) of the IEEE GLOBECOM 2010.
- TPC Co-Chair, the 5th International Conference on Security and Privacy on Communication Networks (SecureComm) 2009.
- Founding Editorial Board (EB) of ICST Transactions on Security and Safety, 2009 – present.
- Local Arrangement Committee Chair, the ACM Conference on Computer and Communication Security (CCS), 2009 and 2010.
- Local Arrangement Committee Co-Chair, the ACM/USENIX Internet Measurement Conference (IMC) 2009.
- Organization and TPC Co-Chair, the 15th IEEE International Workshop on Quality of Service (IWQoS) 2007.
- TPC member, IEEE INFOCOM 2007, 2008, 2009, 2010, 2011, 2012, 2013.
- TPC member, Network & Distributed System Security Symposium (NDSS) 2010, 2011, 2012.
- TPC member, IEEE ICNP 2007, 2011, 2012.
- TPC member, IEEE ICDCS 2007, 2008, 2011.
- TPC member, International Conference on Security and Privacy on Communication Networks (SecureComm) 2008, 2011.
- TPC member, the 40th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2010.
- TPC member, IEEE ICPP 2009

- TPC member, IEEE International Workshop on Network Security and Privacy (NSP) 2008
- TPC member, IEEE International Conference on Broadband Communications, Networks, and Systems (BroadNets), 2008
- TPC member, IEEE International Conference on Sensors and Ad Hoc Communications and Networks (SECON) 2008
- TPC member, the IEEE International Workshop on Quality of Service (IWQoS), 2006, 2008-2010
- TPC member, ACM MobiCom 2007
- TPC member, IFIP/IEEE International Symposium on Integrated Management (IM) 2007
- TPC member, the International Conference on Mobile and Ad-hoc and Sensor Networks (MSN) 2006
- TPC member, IEEE GLOBECOM, 2006
- TPC member, ACM SIGCOMM Posters 2005, 2007
- TPC member, IADIS International Conference Applied Computing 2004, 2005
- NSF GENI panelist, 2008
- NSF CISE panelist for CAREER Program, 2008, 2009.
- NSF CISE panelist for CyberTrust Program, 2004, 2006, 2007, 2008, and 2009.
- Invited panelist for the Cyber Security Panel at the Transportation Center Advisory Board Committee meeting, Northwestern University, 2009
- Invited Reviewer for Qatar National Research Fund, 2011.
- Technology Reviewer for Hong Kong SAR Government ITS program proposals, 2009.
- Reviewer for AFOSR proposals, 2007, 2008, and 2009
- Reviewer for DOE SBIR/STTR proposals, 2006, 2007 and 2008
- Invited reviewer for the book “Internet Measurements” by Mark Crovella and Bala Krishnamurthy, John Wiley and Sons, Feb. 2005
- Invited reviewer for the book “Computer Networks and Data Communication” from Dr. Moshen Guizani, Wiley Publisher, Aug. 2004
- Referee for
 - IEEE Transaction on Mobile Computing 2009, ACM/IEEE Transaction on Networking (ToN) 2009, IEEE Transaction for Parallel and Distributed Systems 2010, ACM SIGCOMM CCR 2010, IEEE Transaction on Dependable and Secure Computing 2010.
 - Journal of Parallel and Distributed Computing 2008, IEEE Networks Special Issue on Implications and Control of Middleboxes in the Internet 2008, ACM/IEEE Transaction on Networking (ToN) 2008.
 - ACM Transaction on the Web (TWEB) 2007, ACM/IEEE Transaction on Networking (ToN) 2007.
 - IEEE Networking magazine 2006, ACM/IEEE Transaction on Networking 2006, IEEE ICNP 2006, USNEIX Security Symposium 2006, SIGCOMM IMC 2006, IEEE Journal on Selected Areas in Communications (J-SAC) 2006, IEEE INFOCOM 2006, USENIX Security Symposium 2006
 - IEEE Journal of Parallel and Distributed Systems 2005, IEEE Wireless Communications Magazine 2005, IEEE Journal of Computer Networks 2005, ACM/IEEE Transaction on Networking 2005, IEEE INFOCOM 2005
 - ACM SIGCOMM, ACM/USNEIX NSDI, IEEE INFOCOM, IEEE ICDCS, ACM SPAA, and many others (before 2005)

Teaching (All in Northwestern University)

- **EECS 213 Introduction to Computer Systems** (Fall 2006).
- **EECS 317 Data Management and Information Processing**, (Spring 2005).
- **EECS 340 Introduction to Computer Networking** (every other Winter, 2004-2010).

- **Developed EECS 350 Introduction to Computer Security** (for CS majors, Winter 2005 and Winter 2007).
- **Developed EECS 495/395 Basic Information Security: Technology Business and Laws** (with Prof. Andrea M. Matwyshyn of Law School, for non-CS majors, Fall 2005).
- **Developed EECS 354 Network Penetration and Security** (every Fall, 2007 - 2011).
- **Developed EECS 450 Internet Security** (Spring 2004, Spring 2005, Spring 2007, Winter 2009, and Spring 2010).
- **Developed EECS 395/495: Internet Measurement and its Reverse Engineering** (Spring 2006).
- **Developed MSIT 458: Information and Security Assurance** (for a professional MS program in IT, Spring 2007, Spring 2008, and Spring 2009, Winter 2010, Fall 2010, Fall 2011).

Current Research Staff and Graduate Students

- Prof. Bin Liu (visiting scholar from Tsinghua University, China)
- Yinzhi Cao (Ph.D. student)
- Kai Chen (Ph.D. student)
- Hongyu Gao (Ph.D. student)
- Vaibhav Rastogi (Ph.D. student)
- Xitao Wen (Ph.D. student)
- Xiang Pan (M.S. student)

Graduated Students

- Zhichun Li (Ph.D. 2009. Now a Researcher at NEC Labs America)
 - Thesis title: Router-based Anomaly/Intrusion Detection and Mitigation Systems
- Yao Zhao (Ph. D., 2009. Now a Researcher at Bell Labs)
 - Thesis title: Internet Networking and Application Troubleshooting.
 - Won the EECS Best Dissertation Award in Northwestern University
- Guohan Lu (Ph. D. of Tsinghua University China, 2008, co-advised with Prof. Xing Li at Tsinghua. Now Associate Researcher at Microsoft Research Asia.)
 - Thesis title: Measurement-based Inference Techniques for TCP Throughput Diagnosis and Packet Forwarding Priority Discovery.
- Clint Sbisa (M.S., 2011, first employer: Amazon)
- Kenny Tay (M. S., 2011, first employer: Microsoft)
- Rahul Potharaju (M.S. 2009, now at Purdue University)
 - Thesis title: Exploring More Complete AS Topologies for Internet Emergency Recovery
- Zhaosheng Zhu (M.S. 2009, now at Data Domain Inc.)
 - Thesis title: Using Failure Information Analysis to Detect Enterprise Zombies and Network Anomalies.
- Anup Goyal (M. S. 2009, now at Yahoo! Inc.)
 - Thesis title: Rake: Semantics Assisted Network-based Large Distributed System Diagnosis
- Jiazhen Chen (M. S. 2009, now at Morningstar Inc.)
 - Thesis title: Discovery and Countermeasures for Exception Triggered Attacks on Wireless Networks.
- Sagar Vemuri (M. S. 2008, now at Riverbed Technology.)
 - Thesis title: Error Message Based DoS Attacks on Wireless Networks
- Prasad Narayana (M. S. 2007, now at Nextwave Broadband Inc.)
 - Thesis title: Vulnerability Analysis of Wireless Network Protocols
- Yan Gao (M. S. 2007)

- Thesis title: Online Scalable Intrusion Detection Systems for High-speed Networks
- Leon Zhao (M. S. 2006, now at Vibes Inc.)
 - Thesis title: Anomaly/Intrusion Detection on Wireless Networks.

Past visiting PhD students.

- Jun Hu (from Huazhang University of Science and Technology, China), 2009-2011.
- Jin Yuan (from Tsinghua University, China) 2009-2010.
- Yi Tang (from Tsinghua University, China) 2008-2009.
- Chengchen Hu (from Tsinghua University, China), 2007.
- Gao Xia (from Tsinghua University, China), 2007.
- Ying He (from the Beihang University China), 2007-2008.
- Lanjia Wang (from Tsinghua University, China), 2006.
- Yanmei Zhang (from China University of Mining & Technology), 2006-2007.

Invited Talks

- “Intrusion Detection and Prevention for Emerging and Challenging Network Environments”, invited talk at the Hong Kong Polytechnic University, National University of Defense Technology, and Xi’an Jiaotong University in China, July-August 2011.
- “NetShield: Massive Semantics-based Vulnerability Signature Matching for High-speed Networks”, invited talk at Tsinghua Information Forum, Tsinghua University, China, March 2011.
- “Detecting and Characterizing Social Spam Campaigns”, invited talk at Toronto Networking Seminar Series, University of Toronto, Canada, February, 2011.
- “Configuring, Diagnosing, and Securing Data Center Networks and Systems”, invited talk at the Institute of Computing Technology, Chinese Academy of Sciences, January, 2011.
- “NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense”, invited talk at DIMACS Workshop on Network Data Streaming and Compressive Sensing, October 2010.
- “NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense”, invited talk at Shanghai Jiaotong University, China, June 2010.
- “NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense”, invited talk at University of Toronto Networking Seminar, October 2009.
- “NetShield: Matching with a Large Vulnerability Signature Ruleset for High Performance Network Defense”, invited talk at Juniper Networks Inc., July 2008.
- “Anomaly/Intrusion Detection and Prevention in Challenging Network Environments”, Distinguished Lecture at Intelligent Automation, Inc., one of the top technology incubator company with over 10 million dollar annual grant from federal agencies, June 2008.
- “P2P Doctor: Measurement and Diagnosis of Misconfigured Peer-to-Peer Traffic”, University of Toronto, January 2008.
- “P2P Doctor: Measurement and Diagnosis of Misconfigured Peer-to-Peer Traffic”, TSS seminar at the Information Trust Institute, UIUC, December 2007.
- “Network-based Intrusion Detection, Prevention and Forensics System”, Tsinghua University and Peking University, China, August 2007.
- “Vulnerability Analysis for WiMAX Networks”, Microsoft Research Asia, August 2007.
- “Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience”, the School of Computer Science, Telecommunications and Information Systems, DePaul University, Jul. 2006.
- “IRC-based Botnet Detection on Routers”, invited talk at ARO-DARPA-DHS workshop on Botnets, June 2006.

- “High-Performance Network Anomaly/Intrusion Detection and Mitigation Systems (HPNAIDM)”, Honeywell, Mar. 2006.
- “Efficient HopID based Routing for Sparse Ad Hoc Networks”, Honeywell, Mar. 2006.
- “Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience”, the Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, Feb. 2006.
- “Scalable and deterministic overlay network diagnosis”, School of Computing, Georgia Institute of Technology, June, 2005.
- “Network Intrusion Detection and Mitigation”, Motorola Labs, Schaumburg, IL, Feb. 2005.
- “Tomography-based Overlay Network Monitoring”, ICIR (The ICSI Center for Internet Research), Berkeley, California, Sep. 2003.
- “Clustering Web Content for Efficient Replication”, University of California at Davis, Dec. 2002.
- “SCAN: a Dynamic Scalable and Efficient Content Distribution Network”, AT&T Labs - Research, Florham Park, NJ, Aug. 2002.
- “Wide-Area Network Measurement and Monitoring Services”, Cisco Inc., Mountain View, California, Jul. 2001.
- “Wide-Area Network Measurement and Monitoring Services”, Ericsson Research Lab at Berkeley, California, Jan. 2002.
- “Dynamic Replica Placement for Scalable Content Delivery”, Ericsson Research Lab, Stockholm, Sweden, Jun. 2001.

Media Coverage

- My joint work with UCSB resulted with the paper "*Detecting and Characterizing Social Spam Campaigns*", was featured in the Wall Street Journal, [INTERNET: Dissecting Facebook Spam](#), and MIT Technology Review, "[Scrutinizing Facebook Spam](#)", and [ACM Tech News](#).
- Interviewed and featured in the article entitled “AFOSR-Supported YIP Research Leads to Algorithms That Deflect Network Attackers”, in Air Force Print News, October 18, 2010. <http://www.wpafb.af.mil/news/story.asp?id=123226799>
Further selected in ACM TechNews, Oct. 25, 2010 (see the link below)
<http://technews.acm.org/archives.cfm?fo=2010-10-oct/oct-25-2010.html#488908>
- Interviewed by Towers Productions, Inc. for an episode of *Investigative Reports* on the A&E Network, 2007. The program is about cybercrime/ computer security.
- “Getting their hands dirty – McCormick students find real solutions to today’s problems”, Fall 2005, McCormick By Design Magazine.

University Services

- Ph.D. Thesis Committee, Department of EECS:
 - Ionut Trestian, graduated in 2012
 - Amit Modal, Karl Deng, David Choffnes and Oliviu Ghica, graduated in 2010.
 - Zhichun Li and Yao Zhao (Chair of Committee), Robert Schwellerr, graduated in 2009.
 - Manan Sanghi, Ashish Gupta, Stefan Birrer, graduated in 2008.
 - Pin Ren, graduated in 2007.
 - Dong Lu, graduated in 2005.
- Qualification Exam Committee, Department of EECS:
 - Yinzhi Cao and Hongyu Gao (Chair of Committee), 2011
 - Kai Chen (Chair of Committee), 2010
 - David Choffnes, 2008
 - Karl Deng, Amit Modal and Ao-Jan Su, 2007.
 - Zhichun Li (Chair), and Yao Zhao (Chair), 2006.

- Joseph Paris, 2005
- Bin Lin, Ashish Gupta, Yi Qiao and Stefan Birrer, Manan Sanghi and Robbie Schwellerr, 2004.
- Director of Computer Science program for Weinberg School of Arts and Sciences, Member of the Computer Science Undergraduate Curriculum Committee, AY 2011-2012.
- Chair of Computer Science Undergraduate Curriculum Committee, Member of Computing Facilities Committee, and Member of Computer Engineering Undergraduate Curriculum Committee for AY 09, Department of Electrical Engineering and Computer Science.
- Department representative to attend the Weinberg Undergraduate Convocation, 2009
- Chair of Computer Science Undergraduate Curriculum Committee, Member of Computing Facilities Committee, and Member of Computer Engineering Undergraduate Curriculum Committee for AY 08, Department of Electrical Engineering and Computer Science.
- Ph.D. Thesis Committee of Taghrid Samak (invited external member), Department of Computer Science, DePaul University, April. 2009.
- Department representative to attend the McCormick Undergraduate Convocation, 2008
- Member of the Graduate Committee, Member of the Computer Science Undergraduate Curriculum Committee and Member of Faculty Search Committee for AY 2007, Department of Electrical Engineering and Computer Science.
- Attend the demo and help evaluate a security product from Elemental Security for the Dean's office, July 2006.
- Member of the Graduate Committee and Member of the Computer Science Undergraduate Curriculum Committee for AY 2006, Department of Electrical Engineering and Computer Science
- Attend the meeting with NUIT and Dean Jay Walsh to evaluate a NUIT-proposed security measures as well as its impact, July 2005.
- Chair of the Departmental Colloquia and Member of the Curriculum Committee for Academic Year 2005, Department of Computer Science
- Member of the Graduate Student Admission Committee and Member of the Curriculum Committee for Academic Year 2004, Department of Computer Science