Scott Alfeld

salfeld@amherst.edu • http://www.scottalfeld.net
CV Compiled January 2019

INTERESTS Statistical machine learning and data analysis in settings with multiple (possibly adversarial) agents.

POSITION

Assistant Professor of Computer Science, Amherst College — Jul 2017 – Present

EDUCATION

University of Wisconsin–Madison, Department of Computer Sciences

- Ph.D. in Computer Science (Minor: Mathematics) — Aug 2011 – May 2017
  - Co-Advisers: Paul Barford and Xiaojin (Jerry) Zhu
  - Thesis Title: Learning in the Presence of Adversaries
- Master's Degree in Computer Science — Aug 2011 – Jun 2015
  - Adviser: Paul Barford

University of Southern California, Department of Computer Science

- Ph.D. Program, no degree (Transferred to UW–Madison) — Aug 2009 – Aug 2011
  - Adviser: Fei Sha

University of Utah, School of Computing

- Bachelor's of Science in Computer Science — Aug 2004 – Aug 2008
  - Adviser: Hal Daumé III

STUDENTS

SUMMER RESEARCH

- *Digging into Fake News (SURF)*
  Annabelle Gary 20, Jason Greenfield 20, Samantha Rydzewski 21, Lesley Zheng 21
- *Gregory S. Call Fellowship*
  Lucas Newman-Johnson 19

SENIOR THESES

- *Title TBD*
  Lucas Newman-Johnson 19
- *Title TBD*
  Mackenzie Stein 19

EXTERNAL

- *Hampshire College Division 3*
  Nirman Dave 19

PUBLICATIONS

CONFERENCE PAPERS

- S. Alfeld, A. Vartanian, L. Newman-Johnson, B. I. P. Rubinstein "Attacking Data Transforming Learners at Training Time"
  in *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI '19)*, Feb 2019.
- A. Sen, S. Alfeld, X. Zhang, A. Vartanian, Y. Ma, X. Zhu "Training Set Camouflage"
  in *Proceedings of the Conference on Decision and Game Theory for Security (GameSec '18)*, Aug 2018.
- L. Tong, S. Yu, S. Alfeld, Y. Vorobeychik "Adversarial Regression with Multiple Learners"
  in *Proceedings of the International Conference on Machine Learning (ICML '18)*, Jul 2018.
- S. Yu, Y. Vorobeychik, S. Alfeld "Adversarial Classification on Social Networks"
  in *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS '18)*, Jul 2018.
- S. Alfeld, X. Zhu, P. Barford "Explicit Defense Actions Against Test-Set Attacks"
  in *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI '17)*, Feb 2017.
- A. Cahn, S. Alfeld, P. Barford, S. Muthukrishnan "What's in the Community Cookie Jar?"
  in *Proceedings of the IEEE/ACM Conference on Advances in Social Network Analysis and Mining (ASONAM '16)*, Aug 2016.
- S. Alfeld, X. Zhu, P. Barford "Machine Teaching as Search" (Short Paper)
  in *Proceedings of the Symposium on Combinatorial Search (SoCS '16)*, Jul 2016.
- S. Alfeld, X. Zhu, P. Barford "Data Poisoning Attacks Against Autoregressive Models"
  in *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI '16)*, Feb 2016.
- A. Cahn, S. Alfeld, P. Barford, S. Muthukrishnan "An Empirical Study of Web Cookies"
  in *Proceedings of the World Wide Web Conference (WWW '16)*, Apr 2016.
- M. Malloy, S. Alfeld, P. Barford "Contamination Estimation via Convex Relaxations"
  in *Proceedings of IEEE International Symposium on Information Theory (ISIT '15)*, Jun 2015.
- S. Alfeld, P. Barford "Targeted Residual Analysis for Improving Electric Load Forecasting"
  in *Proceedings of IEEE Energy Conference (Energycon '14)*, May 2015.
- S. Alfeld, C. Barford, P. Barford "Toward an Analytic Framework for the Electrical Power Grid"
  in *Proceedings of the Third International Conference on Future Energy Systems (e-Energy '12)*, May 2012.

WORKSHOP PAPERS

- X. Zhang, H. Ohannessian, A. Sen, S. Alfeld, X. Zhu "Optimal Teaching for Online Perceptrons"
  in *Constructive Machine Learning at NIPS 2016*, Feb 2017.
- S. Alfeld, P. Barford, X. Zhu "Optimal Defense Actions Against Test Set Attacks"
  in *ICML Workshop on Reliable Machine Learning in the Wild*, Jun 2016.
- S. Alfeld, K. Berkele, S. DeSalvo, T. Pham, D. Russo, L.J. Yan, M.E. Taylor "Reducing the Team Uncertainty Penalty: Empirical and Theoretical Approaches"
  in *Proceedings of the AAMAS workshop on Multiagent Sequential Decision Making in Uncertain Domains*, May 2011.
- S. Alfeld, M.E. Taylor, P. Tandon, M. Tambe "Towards a Theoretic Understanding of DCEE"
  in *Proceedings of the AAMAS Distributed Constraint Reasoning workshop*, May 2010.

ADDITIONAL POSTERS

- *Machine Learning in the Presence of an Adversary* 2016
  Greater Chicago Area Systems Research Workshop (GCASR)
- *Improving Energy Efficiency: A Data-Driven Approach* 2013
  ACM SIGKDD Conference on Knowledge Discovery and Data Mining
- *Understanding and Improving the Electric Grid* 2012
  Wisconsin Institute on Software-Defined Datacenters Of Madison (WISDOM)

AWARDS

- Cisco Distinguished Graduate Fellowship 2016-2017
  One of two annual awards for graduate students in UW's CS department.
  Provides tuition and a stipend for 9 months.
  Based on "academic merit, creativity, research accomplishments and commitment to research."
- Student Travel Grant, SoCS '16 2016
  Award covering airfare. Application open to US-citizen students attending the conference.
- Student-voted Favorite Talk for UW's *Estimating Functions From Data* 2012
  Talk Title: *Maximum Covariance Unfolding*
  A $200 award determined by vote amongst UW's STAT 838 Students.
- Center for Risk and Economic Analysis of Terrorism Events (CREATE) Fellowship 2010–2011
  Part of the DHS Career Development Student Fellowship Program.
  Provides tuition and a stipend for 12 months.
  Award based on "student's academic record and submitted test scores, recommendation letters, and essay."
- University of Utah *School of Computing Outstanding Teaching Assistant* Award 2008 – 2009
  An annual award to up to two teaching assistants in the School of Computing.

ACADEMIC SERVICE

- Book Reviewer for *Adversarial Machine Learning*, Morgan & Claypool 2018
- Invited Panelist, *Panel on Adversarial Learning* at GameSec 2018 2018

CONFERENCES

- NIPS 2018 PC Member (Reviewer) 2018
- ICML 2018 PC Member (Reviewer) 2018
- AAAI 2018 PC Member (Reviewer) 2018
- EAAI 2018 Project Reviewer 2018
- AAAI 2017 PC Member (Reviewer) 2017
- WWW 2017 PC Member (Reviewer) 2017
- AISTATS 2017 Workflow Chair 2016
- ICML Student Volunteer 2016
- Energycon 2014 Reviewer 2014

LOCAL

- SURF Ethics Luncheon Panelist 2018
- Amherst College Marker Faire Table 2018
- Five-College Data Science Committee 2017 – Present
- LUCID (https://lucid.wisc.edu) Senior Graduate Mentor 2016 – 2017
- Head coordinator of the Artificial Intelligence Reading Group, UW–Madison 2014 – 2017
- Co-coordinator of the Time Series Analysis Reading Group, UW–Madison 2015

INVITED TALKS

- *Hacking Machine Learning* Aug 2018
  Talk at University of Melbourne, Melbourne
- *Attacking and Defending Forecasters* Jul 2017
  Talk at Vanderbilt University, Nashville, Tennessee
- *Deep Security – How to Pick a Lock* Jan 2017
  Lecture on Physical Security at Google, Madison
- *Time Series Forecasting in the Presence of an Adversary* Nov 2015
  Lecture for the Human, Animal, and Machine Learning: Experiment and Theory (HAMLET) organization
- *Improving Load Forecasting by Augmenting the MISO Model* Sep 2012
  Presentation to the Load Forecasting Team of Midwest ISO (MISO)
- *Analyzing the Grid via Wholesale Electricity Markets* Feb 2012
  Presentation to the BACTER Institute at UW–Madison

VOLUNTEER WORK

- *Recreational Lockpicking Workshop, UMass, Amherst* 2018
- *UMass ECE Department's Circuits and Code* 2018
- *LockDown* IT Security event 2017
- *Wisconsin Science Festival* 2016
- *LockDown* IT Security event 2015
- 2014 Milwaukee Maker Faire 2014
- American Player's Society, Madison, WI 2011
- Hi-GEAR High School Girl's Outreach Program, Salt Lake City 2008
- University of Utah School of Computing High School Programming Competition 2007
- National Forensics League National Tournament, Salt Lake City 2004

PATENT

- M. Malloy, S. Alfeld and P. Barford, "Creative Impression and Pageview Fraud Detection and Estimation", US patent pending 2015

SELECTED SOFTWARE PROJECTS

- TEDUSearch: Machine Teaching as Search, Python 2016 – 2018
- Quokka: A General Purpose Machine Learning Toolkit, Python 2010 – 2014
- Numerical Stability of Linear Methods in Machine Learning, an Empirical Study 2013 – 2014
- Exploration of Dimensionality Reduction Techniques, Python 2011
- Conflicting Visual Cues in Human Visual System, C++/Python 2010
- Sokuban AI, C++ 2008
- Semantic Net Implementation, C++ 2008
- Sugar Glider 3D Model, Maya 2008
- Halting Problem in HOL-4 (With Prof. Konrad Slind) 2008
- Authorship Identification System, C++/Perl 2007
- Propositional Logic Inference Program, C++ 2006
- Information Retrieval System for Disease Outbreaks, Java 2006