Scott Alfeld

salfeld@amherst.edu • http://www.scottalfeld.net

INTERESTS Adversarial methods in the contexts of artificial intelligence, machine learning, and data analysis.

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
- Master's Degree in Computer Science — Aug 2011 – Jun 2015

University of Southern California, Department of Computer Science

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

University of Utah, School of Computing

- Bachelor's of Science in Computer Science — Aug 2004 – Aug 2008

PUBLICATIONS

CONFERENCE PAPERS

- N. Marchant, B. I. P. Rubinstein, S. Alfeld — **AAAI '22**
  "Hard to Forget: Poisoning Attacks on Certified Machine Unlearning"
  in *Proceedings of the AAAI Conference on Artificial Intelligence*
- B. A. Miller, Z. Shafi, W. Ruml, Y. Vorobeychik, T. Eliassi-Rad, S. Alfeld — **ECML-PKDD '21**
  "PATHATTACK: Attacking Shortest Paths in Complex Networks"
  in *Proceedings of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases*
- D. Liu, Z. Shafi, W. Fleisher, T. Eliassi-Rad, S. Alfeld — **AIES '21**
  "RAWLSNET: Altering Bayesian Networks to Encode Rawlsian Fair Equality of Opportunity."
  in *Proceedings of the ACM conference on Artificial Intelligence, Ethics, and Society*
- S. Yu, L. Torres, S. Alfeld, T. Eliassi-Rad, Y. Vorobeychik — **SDM '21**
  "Optimizing Graph Structure for Targeted Diffusion"
  in *Proceedings of the Siam International Conference on Data Mining*
- S. Alfeld, A. Vartanian, L. Newman-Johnson, B. I. P. Rubinstein — **AAAI '19**
  "Attacking Data Transforming Learners at Training Time"
  in *Proceedings of the AAAI Conference on Artificial Intelligence*
- A. Sen, S. Alfeld, X. Zhang, A. Vartanian, Y. Ma, X. Zhu — **GameSec '18**
  "Training Set Camouflage"
  in *Proceedings of the Conference on Decision and Game Theory for Security*
- L. Tong, S. Yu, S. Alfeld, Y. Vorobeychik — **ICML '18**
  "Adversarial Regression with Multiple Learners"
  in *Proceedings of the International Conference on Machine Learning*
- S. Yu, Y. Vorobeychik, S. Alfeld — **AAMAS '18**
  "Adversarial Classification on Social Networks"
  in *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems*
- S. Alfeld, X. Zhu, P. Barford — **AAAI '17**
  "Explicit Defense Actions Against Test-Set Attacks"
  in *Proceedings of the AAAI Conference on Artificial Intelligence*
- A. Cahn, S. Alfeld, P. Barford, S. Muthukrishnan — **ASONAM '16**
  "What's in the Community Cookie Jar?"
  in *Proceedings of the IEEE/ACM Conference on Advances in Social Network Analysis and Mining*
- S. Alfeld, X. Zhu, P. Barford — **SoCS '16**
  "Machine Teaching as Search" (Short Paper)
  in *Proceedings of the Symposium on Combinatorial Search*

PUBLICATIONS CONT.

- S. Alfeld, X. Zhu, P. Barford **AAAI ’16**
  “Data Poisoning Attacks Against Autoregressive Models”
  in *Proceedings of the AAAI Conference on Artificial Intelligence*
- A. Cahn, S. Alfeld, P. Barford, S. Muthukrishnan **WWW ’16**
  “An Empirical Study of Web Cookies”
  in *Proceedings of the World Wide Web Conference*
- M. Malloy, S. Alfeld, P. Barford **ISIT ’15**
  “Contamination Estimation via Convex Relaxations”
  in *Proceedings of IEEE International Symposium on Information Theory*
- S. Alfeld, P. Barford **Energycon ’14**
  “Targeted Residual Analysis for Improving Electric Load Forecasting”
  in *Proceedings of IEEE Energy Conference*
- S. Alfeld, C. Barford, P. Barford **e-Energy ’12**
  “Toward an Analytic Framework for the Electrical Power Grid”
  in *Proceedings of the Third International Conference on Future Energy Systems*

ABSTRACTS AND WORKSHOP PAPERS

- B. A. Miller, Z. Shafi, W. Ruml, Y. Vorobeychik, T. Eliassi-Rad, S. Alfeld
  “ Defense Against Shortest Path Attacks”
  in *NETWORKS – A Joint Sunbelt and NetSci Conference ’22*
- B. A. Miller, Z. Shafi, W. Ruml, Y. Vorobeychik, T. Eliassi-Rad, S. Alfeld
  “Attacking the Shortest Path by Perturbing Edge Weights”
  in *NETWORKS – A Joint Sunbelt and NetSci Conference ’21*
- M. Stein, S. Alfeld,
  “GARFD: Gradient-based Autoregressive Forecaster Defense”
  in *Workshop on Dataset Curation and Security at NeurIPS ’20* 2020.
- X. Zhang, H. Ohannessian, A. Sen, S. Alfeld, X. Zhu
  “Optimal Teaching for Online Perceptrons”
  in *Constructive Machine Learning at NIPS ’16*
- S. Alfeld, P. Barford, X. Zhu
  “Optimal Defense Actions Against Test Set Attacks”
  in *ICML Workshop on Reliable Machine Learning in the Wild*
- 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 *AAMAS workshop on Multiagent Sequential Decision Making in Uncertain Domains*
- S. Alfeld, M.E. Taylor, P. Tandon, M. Tambe
  “Towards a Theoretic Understanding of DCEE”
  in *AAMAS Distributed Constraint Reasoning Workshop*

PATENT

- M. Malloy, S. Alfeld and P. Barford, 2020
  Fraudulent Traffic Detection and Estimation
  US10832280B2

SERVICE

- Advised teams in KPMG's Enterprise Innovation organization as a subject matter expert on AI 2022
- Invited Participant, *Northwestern University Machine Learning Impact Initiative Summit* 2021
- Invited Participant, *Northwestern University Machine Learning Impact Initiative Workshop* 2020
- Invited Panelist, *Panel on Adversarial Learning* at GameSec 2018 2018
- Book Reviewer for *Adversarial Machine Learning*, Morgan & Claypool 2018

CONFERENCES AND JOURNALS

- Regularly review for: AAAI,AAAI UC, EAAI, AIRE, ICML, NeurIPS 2016-Present
- AAAI Undergraduate Consortium Reviewer 2021
- AAAI 2020 SPC (Meta-Reviewer) 2020
- AIRE Reviewer 2019
- AISTATS 2017 Workflow Chair 2017
- Energycon 2014 Reviewer 2014

INVITED TALKS

- *On the Offensive: Attacking AI Systems* Apr 2022
  Talk at KPMG
- *Manipulating Learners at Training Time* Feb 2021
  Talk at MassMutual as part of the ECS:edu series
- *Attacking at Training Time: Complicated Attacks Against Simple Learners* Aug 2020
  Talk at Robustness of AI Systems Against Adversarial Attacks (RAISA3) 2020
- *Manipulating Learners: Machine Learning in the Presence of Adversarial Input* Mar 2019
  Talk at MIT Lincoln Labs, Lexington, Massachusetts
- *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

- *Physical Security Workshop, All Campus Makerspace, UMass, Amherst* 2020
- *UMass ECE Department's Circuits and Code* 2018, 2019
- *Recreational Lockpicking Workshop, UMass, Amherst* 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