

Scott Alfeld

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

INTERESTS	Adversarial methods	
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
	• 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	

PUBLICATIONS

CONFERENCE PAPERS

- B. A. Miller, Z. Shafi, W. Ruml, Y. Vorobeychik, T. Eliassi-Rad, S. Alfeld “PATHATTACK: Attacking Shortest Paths in Complex Networks”
in *Proceedings The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD '21)* 2021.
- D. Liu, Z. Shafi, W. Fleisher, T. Eliassi-Rad, S. Alfeld “RAWLSNET: Altering Bayesian Networks to Encode Rawlsian Fair Equality of Opportunity.”
in *Proceedings of the ACM conference on Artificial Intelligence, Ethics, and Society (AIIES '21)*, 2021.
- S. Yu, L. Torres, S. Alfeld, T. Eliassi-Rad, Y. Vorobeychik “Optimizing Graph Structure for Targeted Diffusion”
in *Proceedings of the Siam International Conference on Data Mining (SDM '21)*, 2021.
- 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)*, 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)*, 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)*, 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)*, 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)*, 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)*, 2016.
- S. Alfeld, X. Zhu, P. Barford “Machine Teaching as Search” (Short Paper)
in *Proceedings of the Symposium on Combinatorial Search (SoCS '16)*, 2016.
- S. Alfeld, X. Zhu, P. Barford “Data Poisoning Attacks Against Autoregressive Models”
in *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI '16)*, 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)*, 2016.
- M. Malloy, S. Alfeld, P. Barford “Contamination Estimation via Convex Relaxations”
in *Proceedings of IEEE International Symposium on Information Theory (ISIT '15)*, 2015.
- S. Alfeld, P. Barford “Targeted Residual Analysis for Improving Electric Load Forecasting”
in *Proceedings of IEEE Energy Conference (Energycon '14)*, 2014.
- 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)*, 2012.

ABSTRACTS AND WORKSHOP PAPERS

- *Attacking the Shortest Path by Perturbing Edge Weights*
in *NETWORKS – A Joint Sunbelt and NetSci Conference '21*, 2021.
- M. Stein, S. Alfeld, “GARFD: Gradient-based Autoregressive Forecaster Defense”
in *Workshop on Dataset Curation and Security at NeurIPS '20*, 2020.
- X. Zhang, H. Ohanessian, A. Sen, S. Alfeld, X. Zhu “Optimal Teaching for Online Perceptrons”
in *Constructive Machine Learning at NIPS '16*, 2016.
- S. Alfeld, P. Barford, X. Zhu “Optimal Defense Actions Against Test Set Attacks”
in *ICML Workshop on Reliable Machine Learning in the Wild*, 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 *AAMAS workshop on Multiagent Sequential Decision Making in Uncertain Domains*, 2011.
- S. Alfeld, M.E. Taylor, P. Tandon, M. Tambe “Towards a Theoretic Understanding of DCEE”
in *AAMAS Distributed Constraint Reasoning Workshop*, 2010.

ADDITIONAL POSTERS	▪ <i>PATHATTACK: Attacking Shortest Paths in Complex Networks</i>	2021
	GraphEx	
	▪ <i>POTION: Optimizing Graph Structure for Targeted Diffusion</i>	2021
	NETWORKS – A Joint Sunbelt and NetSci Conference '21	
	▪ <i>Machine Learning in the Presence of an Adversary</i>	2016
Greater Chicago Area Systems Research Workshop (GCASR)		
▪ <i>Improving Energy Efficiency: A Data-Driven Approach</i>	2013	
ACM SIGKDD Conference on Knowledge Discovery and Data Mining		
▪ <i>Understanding and Improving the Electric Grid</i>	2012	
Wisconsin Institute on Software-Defined Datacenters Of Madison (WISDOM)		
ACADEMIC SERVICE	▪ Invited Participant, <i>Northwestern University Machine Learning Impact Initiative Summit</i>	2021
	▪ Invited Participant, <i>Northwestern University Machine Learning Impact Initiative Workshop</i>	2020
	▪ Invited Panelist, <i>Panel on Adversarial Learning</i> at GameSec 2018	2018
	▪ Book Reviewer for <i>Adversarial Machine Learning</i> , Morgan & Claypool	2018
CONFERENCES AND JOURNALS		
▪ EAAI 2021 PC Member (Reviewer)	2021	
▪ AAAI Undergraduate Consortium Reviewer	2021	
▪ NeurIPS 2020 Reviewer	2020	
▪ AAAI 2020 SPC (Meta-Reviewer)	2020	
▪ AIRE Reviewer	2019	
▪ EAAI 2020 PC Member (Reviewer)	2019	
▪ 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		
▪ <i>Attack, Defend, Steal:</i>	2020	
<i>Student-Led Research Projects in Adversarial Machine Learning at Amherst College</i>		
Invited Talk to Amherst College Alumni, Zoom		
▪ <i>The Intersection of Machine Learning and Security</i>		
Invited Talk to Amherst College Alumni at “An Evening with Professor Scott Alfeld”, NYC	2020	
▪ <i>When Hackers Meet Data</i>		
Invited Talk as part of the STEM Incubator Colloquium Series	2020	
▪ <i>Adversarial Machine Learning</i>		
Invited Talk at Amherst College 2019 Reunion	2019	
▪ Instruction Weekend Science Center Panel	2019	
▪ Amherst Promise Campaign Data Science Panel, NYC	2019	
▪ 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	▪ <i>Manipulating Learners at Training Time</i>	Feb 2021
	Talk at MassMutual as part of the ECS:edu series.	
	▪ <i>Attacking at Training Time: Complicated Attacks Against Simple Learners</i>	Aug 2020
	Talk at Robustness of AI Systems Against Adversarial Attacks (RAISA3) 2020	
	▪ <i>Manipulating Learners: Machine Learning in the Presence of Adversarial Input</i>	Mar 2019
	Talk at MIT Lincoln Labs, Lexington, Massachusetts	
	▪ <i>Hacking Machine Learning</i>	Aug 2018
	Talk at University of Melbourne, Melbourne	
	▪ <i>Attacking and Defending Forecasters</i>	Jul 2017
	Talk at Vanderbilt University, Nashville, Tennessee	
▪ <i>Deep Security – How to Pick a Lock</i>	Jan 2017	
Lecture on Physical Security at Google, Madison		
▪ <i>Time Series Forecasting in the Presence of an Adversary</i>	Nov 2015	
Lecture for the Human, Animal, and Machine Learning: Experiment and Theory (HAMLET) organization		
▪ <i>Improving Load Forecasting by Augmenting the MISO Model</i>	Sep 2012	
Presentation to the Load Forecasting Team of Midwest ISO (MISO)		
▪ <i>Analyzing the Grid via Wholesale Electricity Markets</i>	Feb 2012	
Presentation to the BACTER Institute at UW–Madison		
VOLUNTEER WORK	▪ <i>Physical Security Workshop, All Campus Makerspace, UMass, Amherst</i>	2020
	▪ <i>UMass ECE Department’s Circuits and Code</i>	2018, 2019
	▪ <i>Recreational Lockpicking Workshop, UMass, Amherst</i>	2018
	▪ <i>LockDown IT Security event</i>	2017
	▪ <i>Wisconsin Science Festival</i>	2016
	▪ <i>LockDown IT Security event</i>	2015
	▪ <i>2014 Milwaukee Maker Faire</i>	2014
	▪ <i>American Player’s Society, Madison, WI</i>	2011
	▪ <i>Hi-GEAR High School Girl’s Outreach Program, Salt Lake City</i>	2008
	▪ <i>University of Utah School of Computing High School Programming Competition</i>	2007
▪ <i>National Forensics League National Tournament, Salt Lake City</i>	2004	
PATENT	▪ M. Malloy, <u>S. Alfeld</u> and P. Barford, Fraudulent Traffic Detection and Estimation US10832280B2	2020