Computer Science & Engineering Dept.
Michigan State University
East Lansing, MI 48824, USA

Mobile: (+1)-315-744-6778
Email: liusiji5@msu.edu
Website: https://lsjxjtu.github.io/

PRIMARY RESEARCH AREAS

Trustworthy ML: Adversarial attack & defense, robustness certification, explainability, fairness
Scalable ML: Zeroth-order optimization, distributed learning, model compression, automated ML
Signal processing: Optimization for signal processing, graph signal processing, information fusion

WORK EXPERIENCE

Assistant Professor, CSE, Michigan State University Jan. 2021 – present

Research Staff Member, MIT-IBM Watson AI Lab, IBM Research Jan. 2018 – Dec. 2020

Postdoc Research Fellow, University of Michigan, Ann Arbor, MI July 2016 – Dec. 2017
Supervisors: Alfred Hero (EECS) and Indika Rajapakse (Computational Medicine & Bioinformatics)

Research Assistant, Syracuse University, Syracuse, NY June 2011 – Mar. 2016
Advisors: Pramod K. Varshney (EECS) and Makan Fardad (EECS)

EDUCATION

Ph.D. in Electrical and Computer Engineering, Syracuse University Aug. 2011– Mar. 2016
Thesis: "Resource management for distributed estimation via sparsity-promoting regularization"
(**All University Doctoral Prize**)

M.S. in Electrical Engineering, Xi'an Jiaotong University Aug. 2008– May 2011
Working on information fusion; Thesis: "Sensor registration for multi-target tracking"

B.S. in Electrical Engineering, Xi'an Jiaotong University Aug. 2004– May 2008
Major: Automation

HONORS AND RECOGNITION

- **IBM Outstanding Research Accomplishments**, 2019
  — *Trustworthy AI; Toward Automating the AI Lifecycle with AutoAI; Deep Learning on Graphs*
- **IBM Patent & Invention Plateau Award**, 2019
- **Winner of Best Student Paper Award (3rd place)**, the 42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017
- **Recipient of All University Doctoral Prize**, Syracuse University, 2016
- **Best Student Paper Nominee** (among the seven finalists) at Asilomar Conference on Signals, Systems, and Computers, CA, Pacific Grove, CA, 2013
- **Winner of Best Poster Award** at Nunan Poster Competition, Syracuse University, 2012
- **First Class Award in National Mathematics Olympiad**, 2004
  — *Exempted from National College Entrance Examination in China*

GRANT AWARDS

- **MSU co-PI**, *"Intelligent Diagnosis for Machine and Human-Centric Adversaries"*, DARPA AIE RED Award, 2020 – 2022, (with MSU PI Xiaoming Liu and NEU PI. Xue Lin)
- **IBM co-PI**, *"Toward Trustworthy AI: Efficient Algorithms for Building Provably Robust and Verifiable Neural Networks"*, MIT-IBM AI Challenge Award, 2018 – 2021 (MIT PI Luca Daniel)
- **IBM co-PI**, *"Instruction, Command Line or Script Malware Detection"*, MIT-IBM AI Challenge Award, 2019 – 2022 (MIT PI Una-May O'Reilly)
- **IBM co-PI**, *"Fast Learning of Neural Network Models with Provable Generalizability"*, RPI-IBM AI Challenge Award, 2020 – 2021 (RPI PI Meng Wang)

SELECTED PUBLICATIONS

Full **publications can be found at Google Scholar**

∗ denotes equal contribution, † denotes student authors under my supervision.

AI/Machine learning

[1] T. Chen, J. Frankle, S. Chang, **S. Liu**, Y. Zhang, M. Carbin, Z. Wang, "The Lottery Tickets Hypothesis for Supervised and Self-supervised Pre-training in Computer Vision Models", CVPR'21

[2] J. Mohapatra, C.-Y. Ko, L. Weng, P.-Y. Chen, **S. Liu**, L. Daniel, "Hidden Cost of Randomized Smoothing", AISTATS'21

[3] Z. Li†, P.-Y. Chen*, **S. Liu***, S. Lu*, Y. Xu*, "Rate-Improved Inexact Augmented Lagrangian Method for Constrained Nonconvex Optimization", AISTATS'21

[4] R. Wang†, K. Xu†, **S. Liu**, P.-Y. Chen, T.-W. Weng, C. Gan, M. Wang, "On Fast Adversarial Robustness Adaptation in Model-Agnostic Meta-Learning", ICLR'21

[5] T. Chen*,†, Z. Zhang*, **S. Liu**, S. Chang, Z. Wang, "Robust Overfitting May be Mitigated by Properly Learned Smoothening", ICLR'21

[6] T. Chen*,†, Z. Zhang*, **S. Liu**, S. Chang, Z. Wang, "Long Live the Lottery: The Existence of Winning Tickets in Lifelong Learning", ICLR'21

[7] S. Srikant†, **S. Liu**, T. Mitrovska, S. Chang, Q. Fan, G. Zhang, U.-M. O'Reilly, "Generating Adversarial Computer Programs using Optimized Obfuscations", ICLR'21

[8] A. Boopathy†, L. Weng, **S. Liu**, P.-Y. Chen, G. Zhang, L. Daniel, "Fast Training of Provably Robust Neural Networks by SingleProp", AAAI'21

[9] M. Cheng†, P.-Y. Chen, **S. Liu**, S. Chang, C.-J. Hsieh, P. Das, "Self-Progressing Robust Training", AAAI'21

[10] T. Chen, J. Frankle, S. Chang, **S. Liu**, Y. Zhang, Z. Wang, M. Carbin, "The Lottery Ticket Hypothesis for the Pre-trained BERT Networks", NeurIPS'20

[11] T. Chen, W. Zhang, J. Zhou, S. Chang, **S. Liu**, L. Amini, Z. Wang, "Training Stronger Baselines for Learning to Optimize", NeurIPS'20 (spotlight)

[12] J. Mohapatra, C.-Y. Ko, L. Weng, P.-Y. Chen, **S. Liu**, L. Daniel, "Higher-Order Certification For Randomized Smoothing", NeurIPS'20 (spotlight)

[13] K. Xu†, G. Zhang†, **S. Liu**, Q. Fan, M. Sun, H. Chen, P.-Y. Chen, Y. Wang, X. Lin, "Adversarial T-shirt! Evading Person Detectors in A Physical World", ECCV'20 (spotlight)

[14] R. Wang†, G. Zhang†, **S. Liu**, P.-Y. Chen, J. Xiong, M. Wang, "Practical Detection of Trojan Neural Networks: Data-Limited and Data-Free Cases", ECCV'20

[15] **S. Liu**, P.-Y. Chen, B. Kailkhura, G. Zhang, A. O. Hero III and P. K. Varshney, "A Primer on Zeroth-Order Optimization in Signal Processing and Machine Learning: Principals, Recent Advances, and Applications", IEEE Signal Processing Magazine, 2020

[16] A. Boopathy†, **S. Liu**, G. Zhang, P.-Y. Chen, S. Chang, and L. Daniel, "Proper Network Interpretability Helps Adversarial Robustness in Classification", ICML'20

[17] **S. Liu***, S. Lu*, X. Chen*, Y. Feng*, K. Xu*, A. Al-Dujaili*, M. Hong, and U.-M. Obelilly, "Min-Max Optimization without Gradients: Convergence and Applications to Adversarial ML", ICML'20

[18] T. Chen†, **S. Liu**, S. Chang, Y. Cheng, L. Amini, and Z. Wang "Adversarial Robustness: From Self-Supervised Pretraining to Fine-Tuning", CVPR'20

[19] J. Mohapatra, L. Weng, P.-Y. Chen, **S. Liu**, L. Daniel “Towards Verifying Robustness of Neural Networks against Semantic Perturbations”, CVPR'20

[20] M. Cheng, S. Singh, P.-Y. Chen, **S. Liu**, and C.-J. Hsieh, “Sign-OPT: A Query-Efficient Hard-label Adversarial Attack ”, ICLR'20

[21] **S. Liu***, P. Ram*, D. Vijaykeerthy, D. Bouneffouf, G. Bramble, H. Samulowitz, D. Wang, A. R. Conn, and A. Gray “An ADMM Based Framework for AutoML Pipeline Configuration”, AAAI'20

[22] P. Zhao*†, L. Weng*, **S. Liu**, P.-Y. Chen, X. Lin, and L. Daniel, “Towards Certificated Model Robustness Against Weight Perturbations”, AAAI'20

[23] **S. Liu***, X. Chen*†, K. Xu*†, X. Li*, X. Lin, M. Hong, and D. Cox, “ZO-AdaMM: Zeroth-Order Adaptive Momentum Method for Black-Box Optimization”, NeurIPS'19

[24] K. Xu*†, H. Chen*†, **S. Liu**, P.-Y. Chen, T.-W. Wen, M. Hong, and X. Lin, “Topology Attack and Defense for Graph Neural Networks: An Optimization Perspective”, IJCAI'19

[25] P. Zhao†, **S. Liu**, P.-Y. Chen, N. Hoang, K. Xu, S. Wang, Y. Wang, and X. Lin, “On the Design of Black-box Adversarial Examples by Leveraging Gradient-free Optimization and Operator Splitting Method”, ICCV'19

[26] S. Ye*†, K. Xu*†, **S. Liu**, H. Cheng, J.-H. Lambrechts, H. Zhang, A. Zhou, K. Ma, Y. Wang, and X. Lin, “Adversarial Robustness vs. Model Compression, or Both?”, ICCV'19

[27] T. Zhang†, **S. Liu**, Y. Wang, and M. Fardad, “Generation of Low Distortion Adversarial Attacks via Convex Programming", ICDM'19

[28] P.-Y. Chen, L. Wu, **S. Liu**, I. Rajapakse, “Fast Incremental von Neumann Graph Entropy Computation: Theory, Algorithm, and Applications", ICML'19

[29] **S. Liu**, P.-Y. Chen, X. Chen, M. Hong, “signSGD via Zeroth-Order Oracle”, ICLR'19

[30] **S. Liu***, K. Xu*†, P. Zhao, P.-Y. Chen, H. Zhang, Q. Fan, D. Erdogmus, Y. Wang, and X. Lin “Structured Adversarial Attack: Towards General Implementation and Better Interpretability”, ICLR'19

[31] X. Chen†, **S. Liu**, R. Sun, and M. Hong. “On the Convergence of A Class of Adam-Type Algorithms for Non-Convex Optimization”, ICLR'19

[32] A. Boopathy†, L. Weng, P.-Y. Chen, **S. Liu**, and L. Daniel, “CNN-Cert: An Efficient Framework for Certifying Robustness of Convolutional Neural Networks”, AAAI'19

[33] C.-C. Tu*, P.-S. Ting*, P.-Y. Chen*, **S. Liu**, H. Zhang, J. Yi, C.-J. Hsieh, and S.-M. Chen, “AutoZOOM: Autoencoder-based Zeroth Order Optimization Method for Attacking Black-box Neural Networks”, AAAI'19

[34] **S. Liu**, B. Kailkhura, P.-Y. Chen, P. Ting, S. Chang and L. Amini, “Zeroth-Order Stochastic Variance Reduction for Nonconvex Optimization”, NeurIPS'18

[35] P. Zhao†, **S. Liu**, Y. Wang, X. Lin, “An ADMM-Based Universal Framework for Adversarial Attacks on Deep Neural Networks”, ACMMM'18

[36] **S. Liu**, J. Chen, P.-Y. Chen and A. O. Hero, “Zeroth-Order Online Alternating Direction Method of Multipliers: Convergence Analysis and Applications”, AISTATS'18

[37] **S. Liu**, Y. Wang, M. Fardad and P. K. Varshney, “A Memristor-Based Optimization Framework for Artificial Intelligence Applications”, IEEE Circuits and Systems Magazine, 2018

Computational biology

[38] **S. Liu**, H. Chen, S. Ronquist, L. Seaman, N. Ceglia, W. Meixner, L. A. Muir, P.-Y. Chen, G. Higgins, P. Baldi, S. Smale, A. O. Hero and I. Rajapakse, “Genome Architecture Mediates Transcriptional Control of Human Myogenic Reprogramming,” iScience, Cell, 2018

[39] H. Chen, L. Seaman, **S. Liu**, T. Ried, and I. Rajapakse, "Chromosome conformation and gene expression patterns differ profoundly in human fibroblasts grown in spheroids versus monolayers," `Nucleus`, 2017

[40] H. T. Ali†, **S. Liu**, Y. Yilmaz, R. Couillet, I. Rajapakse, A. Hero, "Latent Heterogeneous Multilayer Community Detection", `ICASSP'19`

Signal processing

[41] S. Zhang†, **S. Liu**, V. Sharma and P. K. Varshney, "Optimal Sensor Collaboration for Parameter Tracking Using Energy Harvesting Sensors", `IEEE Trans. Signal Process.`, 2018

[42] **S. Liu**, P.-Y. Chen and A. O. Hero, "Accelerated Distributed Optimization for Evolving Networks of Growing Connectivity", `IEEE Trans. Signal Process.`, 2017

[43] **S. Liu**, S. Kar, M. Fardad and P. K. Varshney, "Optimized Sensor Collaboration for Estimation of Temporally Correlated Parameters", `IEEE Trans. Signal Process.`, 2016

[44] **S. Liu**, S. P. Chepuri, M. Fardad, E. Masazade, G. Leus and P. K. Varshney, "Sensor Selection for Estimation with Correlated Measurement Noise", `IEEE Trans. Signal Process.`, 2016

[45] B. Kailkhura, **S. Liu**, T. Wimalajeewa and P. K. Varshney, "Measurement Matrix Design for Compressive Detection with Secrecy Guarantees", `IEEE Wireless Commun. Lett.`, 2016

[46] **S. Liu**, S. Kar, M. Fardad and P. K. Varshney, "Sparsity-Aware Sensor Collaboration for Linear Coherent Estimation", `IEEE Trans. Signal Process.`, 2015

[47] **S. Liu**, A. Vempaty, M. Fardad, E. Masazade and P. K. Varshney, "Energy-Aware Sensor Selection in Field Reconstruction", `IEEE Signal Process. Lett.`, 2014

[48] X. Shen, **S. Liu** and P. K. Varshney, "Sensor Selection for Nonlinear Systems in Large Sensor Networks", `IEEE Trans. Aerosp. Electron. Syst.`, 2014

[49] **S. Liu**, M. Fardad, E. Masazade and P. K. Varshney, "Optimal Periodic Sensor Scheduling in Large-Scale Dynamical Networks", `IEEE Trans. Signal Process.`, 2014

[50] P.-Y. Chen and **S. Liu**, "Bias-Variance Tradeoff of Graph Laplacian Smoothing Regularizer", `IEEE Signal Process. Lett.`, 2017

[51] **S. Liu**, A. Ren†, Y. Wang and P. K. Varshney, "Ultra-Fast Robust Compressive Sensing Based on Memristor Crossbars," `ICASSP'17` (Winner of Best Student Paper Award, 3rd place)

[52] **S. Liu**, **S. Liu**, E. Masazade, X. Shen and P. K. Varshney, "Adaptive Non-Myopic Quantizer Design for Target Tracking in Wireless Sensor Networks," `Asilomar'13` (Best Student Paper Award Finalist)

PRESS COVERAGE

- **MIT News:** *Shrinking massive neural networks used to model language* December 2020
- **VentureBeat:** *Researchers foil people-detecting AI with an 'adversarial' T-shirt* October 2019
- **IBM Research Blog:** *Making Neural Networks Robust with New Perspectives* August 2019
- **Medium:** *AI Safety - How Do you Prevent Adversarial Attacks?* August 2019
- **IBM Research Blog:** *Will Adam Algorithms Work for Me?* May 2019
- **Medium:** *CNN-Cert: A Certified Measure of Robustness for Convolutional Neural Networks* January 2019

PATENT

10 patents have been filed since 2015.

SELECTED TALKS

[1] Zeroth Order Optimization: Theory and Applications to Deep Learning, *CVPR'20* (tutorial talk)

[2] Zeroth-order optimization and applications to adversarial robustness, *KDD'19* (tutorial talk)

[3] Towards deeper understandings of adversarial examples in deep learning, *Khoury College of Computer Sciences, Northeastern University*, Feb. 2019 (invited talk)

[4] Black-box adversarial attack meets zeroth-order optimization, *ALFA-MIT*, Dec. 2018

[5] Recent progress in zeroth order optimization and its applications to adversarial robustness in deep learning, *IEEE Big Data'18* (tutorial talk)

[6] Zeroth-order optimization: Theory and applications, *Texas State University, Austin*, Oct. 2018 (invited talk)

[7] Zeroth-order online learning and bifurcation detection in cell reprogramming, *IBM T. J. Waston Research Center*, Oct. 2017 (invited talk)

[8] Zeroth-order online ADMM, *University of Michigan, Ann Arbor*, June 2017 (invited talk)

[9] Data-enabled graphical model to build chemical reaction mechanisms, *The Michigan Institute for Computational Discovery and Engineering Symposium*, Ann Arbor, April 2017 (invited talk)

[10] An algorithm for cellular reprogramming, *Carnegie Mellon University*, April 2017 (invited talk)

TEACHING EXPERIENCE

- Instructor for *Adversarial Machine learning (CSE 891)*, Michigan State University, Spring 2021
- Guest Lecturer for *Adaptive Learning (ELE 853)*, Syracuse University, Fall 2015
- Guest Lecturer for *Advanced Numerical Methods II (MAT 781)*, Syracuse University, Fall 2014
- Guest Lecturer for *Optimal Control Systems (ELE 712)*, Syracuse University, Fall 2013

SERVICE

- **Co-chair** of IBM AI Research Week Workshop *Foundations of Safe Learning*, 2019-2020
- **Co-chair** of KDD Workshop *Adversarial Learning Methods for Machine Learning and Data Mining*, 2019-2020
- **Co-chair** of IEEE GlobalSIP Workshop *Signal Processing for Adversarial Machine Learning*, 2018
- **Co-chair** of ICME workshop *Machine Learning and Artificial Intelligence for Multimedia Creation*, 2018
- **Guest editor**, *IEEE Internet of Things Journal special issue on AI Enabled Cognitive Communications and Networking for IoT*, 2018
- **Vice-chair** of *IEEE ComSoc SIG on AI Embedded Cognitive Networks*, 2017-present
- **Referee for journals**: *Journal of Machine Learning Research, IEEE Transactions on Information Theory, IEEE Transactions on Signal Processing, IEEE Transactions on Wireless Communications, IEEE Transactions on Automatic Control, Proceedings of the IEEE*
- **Program committee member for conferences**: *NeurIPS, ICML, ICLR, AAAI, CVPR, ICCV, ECCV, UAI, IJCAI, ACMMMM, ICASSP*

MISCELLANEOUS ACTIVITIES

- Judge for class project competition 'Modeling & Simulation of Complex & Multi-Disciplinary Dynamical Systems', invited by Prof. Luca Daniel, MIT, Dec. 2018
- Mentor for HackMIT 2018, MIT, Sept. 2018
- Judge for UofM Engineering Graduate Symposium, University of Michigan, Nov. 2017