Xiaowen Li

Tampa, Florida | li33@usf.edu | 832 740 2091 | linkedin.com/in/xiaowen-lee-li/ | github.com/LeeeeeLy

Education

University of South Florida(USF), Tampa, FL — Aug 2021 – Present
Ph.D. in Computer Science — GPA: 3.93/4.0
University of Kansas(KU), Lawrence, KS — Aug 2018 – May 2021
MA in Mathematics — GPA: 3.33/4.0
Baylor University(BU), Waco, TX — Aug 2015 – May 2018
BS in Mathematics — GPA: 3.62/4.0

Expertise

- Adversarial Machine Learning (Human-ML Perception Gap, Robustness training, Privacy)
- Efficient & Scalable Learning (Optimization, efficient/low-resource training, compression & sparsity)
- Parameter-Efficient Transfer (Adapters/LoRA, multi-task & continual adaptation)

Skills

Languages: Python, Matlab, C++, C, Bash, Lua, R language
Technologies: PyTorch, TensorFlow; Hugging Face (Transformers, PEFT, Accelerate); Git, SVN, Linux

Research Experience

Human-Centric Adversarial Machine Learning[1] — 2023 – present

- Addressed the **Human-AI alignment gap** by conducting a large-scale human study to quantify how traditional l_p metrics fail to capture visual degradation in adversarial examples.
- Engineered the **Perceptual Quality Predictor (PQP)**, a machine learning metric trained on human perceptual data to guide attack generation.
- Developed **PGLP attacks** that exploit fixed-norm defense vulnerabilities, achieving significant success rates by maximizing adversarial distance while maintaining high visual fidelity.

Parameter-Efficient Fine-Tuning (PEFT) for Robustness [2] — 2025

- Tackled the **Robustness-Accuracy trade-off** in deep learning by applying modular **Adapter** architectures to adversarial training.
- Developed **Adapter-AT**, a framework that freezes the backbone model to preserve "clean" performance while training lightweight modules for defense.
- Optimized for **low-resource environments**, reducing trainable parameters by 97% and GPU memory usage by 73% without sacrificing model security.

Scalable AI: Dynamic Sparse Defense Updating [3] — 2025

- Investigated **Model Sparsity** to identify robustness-critical subnetworks within dense neural networks.
- Designed a dynamic pruning-and-updating strategy using **gradient magnitude analysis** to focus training energy on the most impactful parameters.
- Enhanced computational efficiency by 30%, demonstrating that adversarial robustness can be achieved through strategic sparse optimization rather than brute-force dense training.

AI Privacy & Intellectual Property Protection [4] — 2025

- Researched defenses against **Model Stealing (Extraction) attacks** that threaten proprietary MLaaS (Machine Learning as a Service) APIs.
- Developed **Consistency-Preserving Logit Shaping**, a defense that applies input-dependent, class-orthogonal noise to model outputs.
- Mathematically ensured the defense is **argmax-invariant**, meaning it protects the model's internal logic without changing the final prediction for the user.

Signal Security: Spectrum Sensing Defense [6] — 2021 – 2022

- Developed a security framework for **Cognitive Radio Networks** using Distance to Decision Boundary (DDB)

statistics.

- Created a high-speed detection algorithm to identify malicious "Spectrum Attacks" in real-time by monitoring shifts in the model's feature space distribution.

Numerical Linear Algebra & Randomized Algorithms [7] 2018 – 2021

- Researched **Randomized Numerical Linear Algebra (RandNLA)** to accelerate large-scale Singular Value Decomposition (SVD) for high-dimensional data.
- Developed a specialized **Matlab Toolbox** to implement randomized algorithms, providing a 10x speedup in computing low-rank approximations compared to deterministic methods.

Teaching Experience

Graduate Teaching Assistant, University of South Florida 2021 – Present

- **COT 4521 - Computational Geometry/ CNT 6410 - Network Security/ COT 4400 - Analysis of Algorithms**

Graduate Instructor & TA, University of Kansas 2018 – 2021

- **MATH 115/125 - Calculus I/ MATH 101 - College Algebra**

Professional Service

- **Reviewer:**
  - **Reviewer:** IEEE INFOCOM, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE/ACM Transactions on Networking (ToN), IEEE Transactions on Cognitive Communications and Networking (TCCN), IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP).
  - **Secondary Reviewer:** USENIX Security, ACM Conference on Computer and Communications Security (CCS), Annual Computer Security Applications Conference (ACSAC), IEEE Symposium on Security and Privacy (S&P), IEEE Conference on Communications and Network Security (CNS), ACM HotMobile.
- **National Patent:** First inventor and applicant of "Ammonium chloride decomposition test tube for experimental teaching" [CN203108560 (U)], 2013.
- **Provost's Gold Scholarship:** Merit-based academic scholarship, Baylor University, 2015–2018.
- **Society:** IEEE Graduate Student Member (2023 – Present)/ American Mathematical Society(AMS) Sponsored Student Member (2018 – 2021)/ Association for Women in Mathematics(AWM) Sponsored Student Member (2018 – 2021)

Publications

[1] **X. Li**, W. Zhao, R. Duan, Y. Liu, and Z. Lu, "Perception-Guided Large Perturbation Attacks against Adversarial Training of Neural Networks." Submitted to: *IEEE Transactions on Dependable and Secure Computing (TDSC)* (Under Review).

[2] **X. Li**, W. Zhao, Y. Liu, and Z. Lu, "Adapter-Based Parameter-Efficient Adversarial Training for Enhanced Clean Accuracy." Submitted to: *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)* 2026 (Under Review).

[3] **X. Li**, W. Zhao, Y. Liu, and Z. Lu, "Dynamic Sparse Defense Updating: Discovering Robustness-Critical Subnetworks." Submitted to: *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)* 2026 (Under Review).

[4] **X. Li**, W. Zhao, Y. Liu, and Z. Lu, "Consistency-Preserving Logit Shaping for Robust Model Stealing Defense." Submitted to: *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)* 2026 (Under Review).

[5] W. Zhao, Y. Peng, **X. Li**, J. Xu, Y. Liu, and Z. Lu, "Malicious Forgetting: Backdoor Injection in Active Federated Unlearning and Countermeasure Design." *IEEE INFOCOM 2026, Tokyo, Japan, 2026*

[6] W. Zhao, **X. Li**, S. Zhao, J. Xu, Y. Liu and Z. Lu, "Detecting Adversarial Spectrum Attacks via Distance to Decision Boundary Statistics," *IEEE INFOCOM 2024*, Vancouver, BC, Canada, 2024, pp. 691-700, doi: 10.1109/INFOCOM52122.2024.10621153.

[7] **X. Li**, "Randomized Algorithms for Solving Singular Value Decomposition Problems with Matlab Toolbox", *Master's thesis, Dept. Math., Univ. Kansas, Lawrence, KS, USA, 2021. [Online]. Available: KU ScholarWorks*.