MILIN ZHANG

◇ **Email**: zhang.mil@northeastern.edu ◇ **Phone**: (+1) 207-409-4421
◇ **LinkedIn**: milin-zhang-b82454204 ◇ **Github**: milinzhang

EDUCATION

Northeastern University Boston, MA
Ph.D Candidate Jan 2022 - Present
Computer Engineering

Syracuse University Syracuse, NY
M.Sci Jan 2020 - Dec 2021
Electrical Engineering

University of Electronic Science and Technology of China Sichuan, China
B.Sci Aug 2013 - June 2018
Electronic Engineering

RESEARCH INTEREST

- Trustworthy Machine Learning
- AI-driven Wireless Network
- Integrated Sensing and Communication

PUBLICATIONS

Ongoing

- **Milin Zhang** and Francesco Restuccia. "Model Protection in Distributed Neural Networks"
- Ildi Alla, **Milin Zhang** and Francesco Restuccia. "Wide-band WiFi RF-Fingerprint"
- **Milin Zhang**, Michael De Lucia, Ananthram Swami, and Francesco Restuccia. "Adversarial Machine Learning for Network Intrusion Detection Systems"
- Khandaker Foysal Haque, **Milin Zhang**, Francesca Meneghello, and Francesco Restuccia. "Si-FI: Learning the Beamforming Feedback for Simultaneous Multi-Subject Sensing"

Preprint

- Sayyed Sazzad, **Milin Zhang**, Shahriar Rifat, Ananthram Swami, Michael De Lucia, and Francesco Restuccia. "Resilience and Security of Deep Neural Networks Against Intentional and Unintentional Perturbations: Survey and Research Challenges." *arXiv preprint arXiv:2408.00193 (2024).*
- **Milin Zhang**, Mohammad Abdi, and Francesco Restuccia. "Adversarial Machine Learning in Latent Representations of Neural Networks." *arXiv preprint arXiv:2309.17401 (2023).*
- Khandaker Foysal Haque, **Milin Zhang**, Francesca Meneghello, and Francesco Restuccia, "BeamSense: Rethinking Wireless Sensing with MU-MIMO Wi-Fi Beamforming Feedback." *arXiv preprint arXiv:2303.09687 (2023).*

Journal

- Ankit Mittal, **Milin Zhang**, Thomas Gourousis, Ziyue Zhang, Yunsi Fei, Marvin Onabajo, Francesco Restuccia, and Aatmesh Shrivastava, "Sub-6 GHz Energy Detection-based Fast On-Chip Analog Spectrum Sensing with Learning-driven Signal Classification." *IEEE Internet of Things Journal (2024).*

Conference

- **Milin Zhang**, Mohammad Abdi, Shahriar Rifat, and Francesco Restuccia. "Resilience of Entropy Model to Intentional and Unintentional Interference in Distributed Deep Neural Networks." *in Proc. of the 18th European Conference on Computer Vision (**ECCV**), 2024.*
- **Milin Zhang**, Michael De Lucia, Ananthram Swami, Jonathan Ashdown, Kurt Turck and Francesco Restuccia. "HyperAdv: Dynamic Defense Against Adversarial Radio Frequency Machine Learning Systems" *in Proc. of IEEE Military Communications Conference (MILCOM), 2024*
- Daniel Uvaydov*, **Milin Zhang***, Clifton Paul Robinson, Salvatore D'Oro, Tommaso Melodia and Francesco Restuccia. "Stitching the Spectrum: Semantic Spectrum Segmentation with Wideband Signal Stitching." *in Proc. of IEEE Conference on Computer Communications (**INFOCOM**), 2024.*
- Thomas Gourousis, Ziyue Zhang, Mengting Yan, **Millin Zhang**, Ankit Mittal, Francesco Restuccia, Aatmesh Shrivastava, Yunsi Fei, Marvin Onabajo "Identification of Stealthy Hardware Trojans through On-Chip Temperature Sensing and an Autoencoder-Based Machine Learning Algorithm" *in Proc. of the IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS), 2023.*
- Khandaker Foysal Haque, **Milin Zhang**, Francesco Restuccia, "SiMWiSense: Simultaneous Multi-Subject Activity Classification Through Wi-Fi Signals." *in Proc. of the IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2023.*

SERVICE

Peer Reviewer

- Journal

  Elsevier Computer Network

  IEEE Journal of Selected Topics in Signal Processing

  IEEE Transactions on Communication

  IEEE Transactions on Cognitive Communication and Networking

  IEEE Transactions on Wireless Communication

- Conference

  IEEE International Conference on Communications

  IEEE Global Communications Conference

  IEEE International Conference on Sensing, Communication, and Networking

  IEEE International Symposium on World of Wireless Mobile and Multimedia Networks

  IEEE Military Communications Conference

SKILLS

- Convex Optimization, Information Theory, Statistic Learning, Wireless Communication, Digital Signal Processing
- C/C++, CUDA, Matlab, Python