MILIN ZHANG

✉ zhang.mil@northeastern.edu | 🏠 milinzhang.github.io | ☎ (+1) 207-409-4421

Education

Northeastern University Boston, MA
Ph.D Candidate in Computer Engineering Apr 2026 (tentative)
Advisor: Prof. Francesco Restuccia

Syracuse University Syracuse, NY
M.Sci in Electrical Engineering Dec 2021

University of Electronic Science and Technology of China Sichuan, China
B.Eng in Electronic Engineering June 2018

Research Interest

I am broadly interested in the intersection between artificial intelligence and wireless communication. My PhD research spans:

- **AI Security**: adversarial robustness, out-of-distribution detection, on-device model protection
- **Efficient AI in Distributed Systems**: split computing, semantic communication
- **AI-Driven Wireless**: spectrum sensing, RF fingerprinting, integrated sensing and communication

Skills

Domain Expertise: Statistical Learning, Deep Learning, Wireless Communication, Digital Signal Processing, Convex Optimization, Information Theory

Coding: Python, C/C++, Matlab, CUDA

Language: Chinese (Mandarin, Cantonese), English (TOEFL 108/120), Japanese (JLPT N1)

Publications

Conference

(*) indicates equal contribution

- **Milin Zhang**, Michael De Lucia, Jonathan Ashdown, Nathaniel D. Bastian, Ananthram Swami, and Francesco Restuccia. “NI-Diff: Zero-Day and Adversarial Network Intrusion Detection with Diffusion Models” *in Proc. of IEEE Military Communications Conference (MILCOM), 2025*
- **Milin Zhang**, Mohammad Abdi, Shahriar Rifat, and Francesco Restuccia. “Resilience of Entropy Model in Distributed Neural Networks.” *in Proc. of the 18th European Conference on Computer Vision (**ECCV**), 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.*
- **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*

- 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 World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2023.*
- Thomas Gourousis, Ziyue Zhang, Mengting Yan, **Milin Zhang**, Ankit Mittal, Aatmesh Shrivastava, Francesco Restuccia, Yunsi Fei, and 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.*

Journal

- **Milin Zhang**, Mohammad Abdi, Jonathan Ashdown, and Francesco Restuccia, "Adversarial Attacks to Latent Representations of Distributed Neural Networks in Split Computing." *Computer Networks (2025).*
- **Milin Zhang***, Mohammad Abdi*, Venkat R. Dasari and Francesco Restuccia, "Semantic Edge Computing and Semantic Communications in 6G Networks: A Unifying Survey and Research Challenges" *Computer Networks (2025).*
- Khandaker Foysal Haque, **Milin Zhang**, Francesca Meneghello, and Francesco Restuccia, "BeamSense: Rethinking Wireless Sensing with MU-MIMO Wi-Fi Beamforming Feedback." *Computer Networks (2025).*
- Junyi Yang, Thomas Gourousis, Mengting Yan, Ruyi Ding, Ankit Mittal, **Milin Zhang**, Francesco Restuccia, Aatmesh Shrivastava, Yunsi Fei, and Marvin Onabajo. "A Low-Power Differential Temperature Sensor with Chopped Cascode Transistors and Switched-Capacitor Integration." *Electronics (2025).*
- 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).*

In Preparation

- **Milin Zhang***, Tanzil Hassan*, Mohammad Abdi, Venkat R. Dasari and Francesco Restuccia. "MIND: Multi-Device INference in Distributed Systems for Heterogeneous Edge Environments"
- **Milin Zhang** and Francesco Restuccia. "T-MUX: Securing Neural Networks with Task Multiplexing"
- Khandaker Foysal Haque, **Milin Zhang**, Francesca Meneghello, and Francesco Restuccia. "Si-FI: Learning the Beamforming Feedback for Simultaneous Multi-Subject Sensing"

Preprint

- Ildi Alla, **Milin Zhang**, Jonathan Ashdown, Valeria Loscri and Francesco Restuccia. "Finding a Needle in a (Spectrum) Haystack: Passwordless Wireless Authentication Through Multi-Band Multi-Device Radio Fingerprinting" (2025).
- Sayyed Sazzad, Shahriar Rifat, **Milin Zhang**, Ananthram Swami, Michael De Lucia, Nathaniel D. Bastian, and Francesco Restuccia. "Out-of-Distribution Detection in Computer Vision: A Comprehensive Survey and Research Challenges." (2025).
- 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).*

Patent

- Daniel Uvaydov, **Milin Zhang**, Salvatore D'Oro, Tommaso Melodia, Francesco Restuccia, and Clifton Paul Robinson. "Methods for Real-Time Wideband RF Waveform and Emission Classification." U.S. Patent Application 18/620,310, filed October 3, 2024.
- Francesco Restuccia, Khandaker Foysal Haque, and **Milin Zhang**. "Simultaneous Multi-Subject Activity Classification Through Wi-Fi Signals." U.S. Patent Application 18/489,570, filed June 6, 2024.
- Francesco Restuccia, Khandaker Foysal Haque, and **Milin Zhang**. "Method and Apparatus for Wi-Fi Sensing Through MU-MIMO Beamforming Feedback Learning." WO 2024/049970, filed August 31, 2023.

Service

Journal Reviewer

- IEEE Journal of Selected Topics in Signal Processing (2 reviews)
- IEEE Transactions on Communication (1 reviews)
- IEEE Transactions on Cognitive Communication and Networking (8 reviews)
- IEEE Transactions on Wireless Communication (3 reviews)
- IEEE Transactions on Mobile Computing (3 reviews)
- Elsevier Computer Networks (11 reviews)

Conference Reviewer

- (2022) IEEE International Conference on Communications
- (2023) IEEE Global Communications Conference
- (2023) IEEE International Conference on Sensing, Communication, and Networking
- (2024) IEEE International Symposium on World of Wireless Mobile and Multimedia Networks
- (2023, 2024, 2025) IEEE Military Communications Conference
- (2025) IEEE/CVF International Conference on Computer Vision
- (2025) AAAI Conference on Artificial Intelligence

Open-Source Contributor

- Adversarial Split Computing: `https://github.com/Restuccia-Group/AdvLatent`
- Dynamic Defense to Adversarial RFMLS: `https://github.com/Restuccia-Group/HyperAdv`
- Robustness of Entropy Model: `https://github.com/Restuccia-Group/EntropyR`
- Spectrum Segmentation: `https://github.com/uvaydovd/spectrum_sensing_stitching`

Presentation

- Poster Presentation: "Resilient and Real-Time Artificial Intelligence in 6G Networks", in 2nd Annual WIoT Forum: Toward Open 6G Networks, Feb 5th, 2025.