YONGSHENG MEI

+1 (571) 331-0829 ◇ 800 22nd St NW, Washington, DC 20052
ysmei@gwu.edu ◇ LinkedIn ◇ GitHub ◇ Homepage

SUMMARY

Final-year Ph.D. candidate with full-stack programming knowledge, research, and project experience in machine learning, including **Reinforcement Learning, Optimization, Generative AI (Foundation Models and Large Language Models)**.

SKILLS

Programming	Python, C, C++, Java, Go, MATLAB, SQL, R, Verilog
Libraries	PyTorch, TensorFlow, Keras, Scikit-Learn, NumPy, Pandas, Hugging Face, LangChain
Databases	MySQL, PostgreSQL, Microsoft SQL, MongoDB, ChromaDB
Tools	Git, Linux Bash, PySpark, Jupyter, LaTeX, Kubernetes, Docker, Tableau, AWS, GCP

EDUCATION

The George Washington University — Sept. 2019 – Dec. 2024
Doctor of Philosophy in Electrical Engineering — *Washington, DC, US*
Research Areas: Reinforcement Learning, Generative Models, Optimization, Network Security — GPA: 4.00

Huazhong University of Science and Technology — Sept. 2015 – June 2019
Bachelor of Engineering in Automation Engineering — *Wuhan, Hubei, China*
Relevant Courses: Pattern Recognition, Computer Vision, Control Theory, Computer Architecture — GPA: 3.81

EXPERIENCE

Research Assistant
Sept. 2019 - Present
The George Washington University — *Washington, DC, US*

Topic 1: Reinforcement Learning (RL)

- Developed an optimized **collective prioritized experience replay** scheme in off-policy multi-agent RL via the prioritization weights assignment. Experiments show that our rewards outperform baseline algorithms by up to 10%. This work has been published at **AAMAS 2023**.
- Applied system-algorithm co-design for RL acceleration, such as using the **data-reuse** strategy in conjunction with experience replay to accelerate the multi-agent RL, where the end-to-end training time reduction is 25.4% (for 32 agents), and exploiting a **virtual cache** to accelerate the sampling phase of the offline RL training, achieving 6× speed-ups.

Topic 2: Multimodal Learning

- Designed a multimodal image segmentation model for brain tumor MRI data. The framework can improve segmentation accuracy via **self-attention** with extracted correlated **common information microstructures** among modalities. The method achieves 92% accuracy for the whole tumor on the BraTS-2020 dataset. This work has been published in Machine Learning for Multimodal Healthcare Data workshop at **ICML 2023**.

Topic 3: Stochastic Modeling and Bayesian Optimization (BO)

- Developed a gradient-aware BO framework to **determine local optimal solutions** in multimodal unknown functions for hyperparameter tuning when using the optimal solution is not physically available.
- Proposed a BO model via Gaussian Cox process on discrete spatiotemporal data to **estimate arrival intensity** (outperforming baselines in 7 out of 9 settings) and **detect regions of interest** based on estimations. This work has been published at **ICLR 2024**.

Topic 4: Network Security

- Led the development of a reliable **self-synchronizing moving target defense** via customized network and Internet of Things protocols. The system can defend against common attacks, such as MITM and DoS.
- Introduced a **real-time network intrusion detection** model as a sequence of arriving packets using a causal decision transformer. This work has been accepted at the Artificial Intelligence for Cyber Security workshop at **AAAI 2024**.

Visiting Researcher
June 2023 – Aug. 2023
Purdue University — *West Lafayette, IN, US*

- Developed a **continual federated learning** model with time-variant input of each edge device, which leverages the **conditioned diffusion model** that is trained from scratch and fine-tuned from a pre-trained model to generate synthetic data to avoid the catastrophic forgetting problem.

Electronic Engineer Intern Feb. 2017 – Aug. 2017

HUST Electrical and Electronic Technology Innovation Center *Wuhan, Hubei, China*

- Led the printed circuit board design and FPGA programming for an adaptive signal filter and won the **Runner-Up Prize** in the 2017 National Undergraduate Electronic Design Contest.

PUBLICATIONS

1. **Yongsheng Mei**, Mahdi Imani, and Tian Lan, *Bayesian Optimization through Gaussian Cox Process Models for Spatio-temporal Data*, International Conference on Learning Representations (ICLR), May 2024. [PDF]
2. **Yongsheng Mei**, Hanhan Zhou, and Tian Lan, *Projection-Optimal Monotonic Value Function Factorization in Multi-Agent Reinforcement Learning*, International Conference on Autonomous Agents and Multiagent Systems (AAMAS), May 2024. [PDF]
3. Yurong Chen, **Yongsheng Mei**, Tian Lan, and Guru Venkataramani, *Exploring Effective Fuzzing Strategies to Analyze Communication Protocols*, ACM Digital Threats: Research and Practice, March 2024. [PDF]
4. Jingdi Chen, Hanhan Zhou, **Yongsheng Mei**, Gina Adam, Nathaniel Bastian, and Tian Lan. *Real-time Network Intrusion Detection via Decision Transformers*, AAAI workshop on Artificial Intelligence for Cyber Security (AICS), Feb. 2024. [PDF]
5. Jiayu Chen, Bhargav Ganguly, Yang Xu, **Yongsheng Mei**, Tian Lan, Vaneet Aggarwal, *Deep Generative Models for Offline Policy Learning: Tutorial, Survey, and Perspectives on Future Directions*, arXiv preprint, Feb. 2024 [PDF]
6. **Yongsheng Mei**, Tian Lan, Mahdi Imani, and Suresh Subramaniam, *A Bayesian Optimization Framework for Finding Local Optima in Expensive Multi-Modal Functions*, European Conference on Artificial Intelligence (ECAI), September 2023. [PDF]
7. **Yongsheng Mei**, Tian Lan, and Guru Venkataramani, *Exploiting Partial Common Information Microstructure for Multi-Modal Brain Tumor Segmentation*, ICML workshop on Machine Learning for Multimodal Healthcare Data (ML4MHD), July 2023. [PDF]
8. Kailash Gogineni, **Yongsheng Mei**, Peng Wei, Tian Lan, and Guru Venkataramani, *AccMER: Accelerating Multi-agent Experience Replay with Cache Locality-aware Prioritization*, IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), July 2023. [PDF]
9. **Yongsheng Mei**, Hanhan Zhou, Tian Lan, Guru Venkataramani, and Peng Wei, *MAC-PO: Multi-Agent Experience Replay via Collective Priority Optimization*, International Conference on Autonomous Agents and Multiagent Systems (AAMAS), June 2023. [PDF]
10. Kailash Gogineni, **Yongsheng Mei**, Guru Venkataramani, and Tian Lan, *Verify-Pro: A Framework for Server Authentication Using Communication Protocol Dialects*, IEEE Military Communications Conference (MILCOM), September 2022. [PDF]
11. **Yongsheng Mei**, Kailash Gogineni, Tian Lan, and Guru Venkataramani, *MPD: Moving Target Defense through Communication Protocol Dialects*, International Conference on Security and Privacy in Communication Networks (SecureComm), September 2021. [PDF]
12. Hongfa Xue, **Yongsheng Mei**, Kailash Gogineni, Guru Venkataramani, and Tian Lan, *Twin-Finder: Integrated Reasoning Engine for Pointer-related Code Clone Detection*, International Workshop on Software Clones (IWSC), February 2020. [PDF]

SIDE PROJECTS

Rental House Recommendations with LLM-based Chatbot

- Developed a prototype plug-in web chatbot for users to search rental house information based on their locations and preferences to find the matching houses from **MongoDB** stored data.
- Designed the LLM using LangChain for **retrieval augmented generation**, enabling real-time rental house recommendations by accessing the rental company database.
- **Instruction fine-tuned** a Flan-T5 model on AWS Sagemaker for the recommandation task that improved 10% performance to the original model on BookCrossing benchmark.
- Reduced the latent content toxicity using **RLHF** with PPO algorithm on Facebook's hate speech reward model.

Emotion Recognition from Multimodal Video Data

- Developed an end-to-end multimodal learning approach to recognize emotion from input video clips.
- Decoupled the audio and image sources from the video. Extracted the image features with the **vision transformer**. Converted the audio waves into Mel **Spectrogram** with Fourier transforms and extracted features via CNNs.
- Applied **late fusion** to extracted features for classification with cross-entropy and correlation losses, which increased 12% performance on audio-visual emotion dataset eNTERFACE'05.

PRESENTATIONS

GW SEAS 2024 R&D Showcase — April 2024, *Washington, DC, US*

GW 2024 Global Business & Policy Forum — April 2024, *Washington, DC, US*

ICML 2023 Machine Learning for Multimodal Healthcare Data workshop — July 2023, *Honolulu, HI, US*

Presenting to the Office of Naval Research on the protocol customization project — Feb. 2022, *online*

EAI 17th International Conference on Security and Privacy in Communication Networks — Sept. 2021, *online*

Hosting TPCP 2020 Software Security Summer School — Aug. 2020, *online*

IEEE 14th International Workshop on Software Clones — Feb. 2020, *London, Ontario, Canada*

AWARDS

2023 European Conference on Artificial Intelligence *Call to Arms* Award.

2020, 2021, 2022 GW University Fellowship

2019 HUST Outstanding Graduates

2019 HUST Best Undergraduate Thesis Nominee

2017 Runner-Up Prize in National Undergraduate Electronic Design Contest.

SERVICES

Journal Reviewer

- IEEE Transactions on Networking
- IEEE Micro
- IEEE Transactions on Aerospace and Electronic Systems
- Information Fusion

Conference Reviewer

- Conference on Neural Information Processing Systems (NeurIPS)
- International Conference on Machine Learning (ICML)
- IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)
- European Conference on Artificial Intelligence (ECAI)
- Chinese Conference on Pattern Recognition and Computer Vision (PRCV)

RECOMMENDATIONS

Dr. Tian Lan — Ph.D. Advisor, Professor
Department of Electrical and Computer Engineering, The George Washington University — *Washington, DC, US*
E-mail: tlan@gwu.edu — Website

Dr. Mahdi Imani — Assistant Professor
Department of Electrical and Computer Engineering, Northeastern University — *Boston, MA, US*
E-mail: m.imani@northeastern.edu — Website

Dr. Guru Prasadh Venkataramani — Professor
Department of Electrical and Computer Engineering, The George Washington University — *Washington, DC, US*
E-mail: guruv@gwu.edu — Website

Dr. Peng Wei — Associate Professor
Department of Mechanical and Aerospace Engineering, The George Washington University — *Washington, DC, US*
E-mail: pwei@gwu.edu — Website

Dr. Christopher G. Brinton — Associate Professor
Department of Electrical and Computer Engineering, Purdue University — *West Lafayette, IN, US*
E-mail: cgb@purdue.edu — Website