Sujata Sinha

Durham Hall, Wireless@Virginia Tech
sujatasinha@vt.edu linkedin.com/in/sujatassinha/ github.com/sujatassinha

Research Interests

With over 5 years of experience in machine learning, I am broadly interested in the interplay between wireless communication systems and machine learning. In particular, my work focuses on understanding and fortifying the resilience of wireless networks against sophisticated and adaptive threats. My current work focuses on adversarial attacks and defenses, particularly in the context of varied and complex channel conditions and varying levels of knowledge available to the adversary.

Education

Virginia Tech **Blacksburg, VA**
PhD, Electrical & Computer Engineering *Aug. 2021 – Present*
- Advisor: Alkan Soysal

Auburn University **Auburn, AL**
MS (Thesis), Computer Science & Software Engineering *Aug. 2018 – Aug. 2021*
- Advisor: Jingyi Zheng

Dr. APJ Abdul Kalam University **Uttar Pradesh, India**
B.tech, Electronics & Communication Engineering *May. 2014 – June. 2018*
- Magna Cum Laude

Publications

Sujata Sinha and Alkan Soysal. **"Adversarial Attacks and Defenses for Wireless Signal Classifiers using CDI-aware GANs."** arXiv:2311.18820, Nov 2023.

Sujata Sinha and Alkan Soysal. **"Channel Aware Adversarial Attacks are Not Robust."** IEEE Military Communications Conference (MILCOM) Workshops, Nov 2023.

Jingyi Zheng, Mingli Liang, **Sujata Sinha,** Linqiang Ge, Wei Yu, Arne Ekstrom, and Fushing Hsieh. **"Time-Frequency Analysis of Scalp EEG With Hilbert-Huang Transform and Deep Learning."** IEEE Journal of Biomedical and Health Informatics, Sep 2021.

Sujata Sinha, Thomas Denney, Yang Zhou, and Jingyi Zheng. **"Automated Semantic Segmentation of Cardiac Magnetic Resonance Images with Deep Learning."** IEEE International Conference on Machine Learning and Applications (ICMLA), Dec 2020.

Research Experience

Wireless@VT **Virginia, VA**
Supervisor: Alkan Soysal *Aug. 2021 – Present*
- Developed a Channel Distribution Information (CDI)-aware generative network to address adversarial attacks in wireless communication systems, enhancing both attack and defense mechanisms.
- Proposed a dual discriminator model within the CDI-aware GAN, adept at generating realistic perturbations that effectively mimic Gaussian noise and adapt to complex channel effects, setting a new standard in generative model design.
- Investigate the dynamics of adversarial attacks in diverse wireless environments, including fading, shadowing, and path loss. Assessing the impact of various channel conditions and their influence on deep neural network-based modulation classifiers.

AU Stat Learning Lab in collaboration with MRI Research Center **Auburn, AL**
Supervisors: Jingyi Zheng and Thomas Denny *Aug. 2019 – Aug. 2021*
- Developed an end-to-end deep learning-based analytical pipeline for automated segmentation of short-axis cardiac magnetic resonance (CMR) imaging.
- Integrated advanced deep learning architectures, including modified U-Net, ResUNet, and FCN models for large-scale heterogeneous datasets to fully automate the CMR segmentation process, thereby significantly reducing the reliance on manual intervention and minimizing subjective errors.

AU Stat Learning Lab **Auburn, AL**

Supervisor: Jingyi Zheng *Aug. 2020 – Aug. 2021*

- Developed a data-driven method to derive subject-specific frequency bands for brain oscillations, addressing variability in neural responses.
- Demonstrated the application of two novel metrics as potential biomarkers in neuroscience, particularly in understanding the link between neural oscillations and cognition, and in EEG-based brain-computer interface (BCI) systems for improved user control.
- Automated feature engineering in inter- and intra- variability datasets using neural network architectures, noting the potential of deep learning models in large data scenarios despite their computational intensity and limited interpretability.

Graduate course projects

Trustworthy ML: Investigated evasion attacks (fast gradient method, Carlini-wagner, basic iterative method, momentum iterative method, and Madry et al.) aimed at fooling automatic modulation classifiers in whitebox and blackbox settings. The attacks are evaluated against Gaussian smoothing and adversarial training defenses.

Artificial Intelligence: Developed a deep learning framework for generating poetic language from images, leveraging convolutional neural networks (CNN) and LSTM models to seamlessly blend visual interpretation with creative text generation. The project showcased the ability of deep learning systems to translate visual imagery into corresponding poetic language.

Experimental Statistics: Demonstrated through mixed model ANOVA and validated by Kenward Roger and Bonferroni post-hoc tests, that temperature variations significantly alter meiotic recombination rates in Drosophila pseudoobscura. It offers critical insights into species adaptation under environmental stress and the broader ecological implications of climate change.

Technical Skills

Coding Languages: Python, MySQL, R/SAS, C
Machine Learning Tools: PyTorch, TensorFlow/Keras, OpenCV, Numpy, Scipy, Scikit-Learn, Pandas, Matplotlib, Seaborn.
Distribution and Deployment Tools: Docker, GitHub

Teaching Experience

Virginia Tech **Virginia, VA**

Advanced Machine Learning *Fall 2023, Spring 2023*

Auburn University **Auburn, AL**

Introduction to Engineering *Fall 2019*

Honors and Awards

Graduate Dean's Fellowship **2018**

Auburn Graduate School, Auburn University, USA

First Class Honors and Distinction **2018**

B.Tech, Dr. APJ Abdul Kalam University, India

Special recognition of Pulse Prognostics by Prime Minister of India **2018**

VG Start-Up Summit, India

Special recognition of Pulse Prognostics by Chief Minister of Uttar Pradesh **2017**

Kalam Research Center, India

Relevant Coursework

• Trustworthy Machine Learning • Nonlinearity and Prediction • Applied Bayesian Statistics • Machine Learning
• Stochastic Signals and Systems • Data Mining • Artificial Intelligence • Advanced Topics In Algorithms

Leadership / Extracurricular

Reviewer of ICMLA **2020**

Reviewed 2 papers in Deep Learning (Special Sessions)

Student Team Lead, Technical Events **2016**

Dr. APJ Abdul Kalam University

Co-founded Start-up, Pulse Prognostics **2015**

Designed a data-driven device to diagnose health conditions through the principles of traditional Chinese medicine