Mridul Gupta

Yardi School of Artificial Intelligence
Indian Institute of Technology, Delhi

Email: Mridul.Gupta@scai.iitd.ac.in

	Institute	Year	GPA
Ph.D.	IIT Delhi	2021–	8.00/10.00
M.Tech.	MNIT Jaipur	2019–2021	8.54/10.00
B.Tech.	NIT Raipur	2013–2017	7.54/10.00

Projects

- **Graph Distillation with Explainable Tree Selection** (Dec'23 –)
  – under the guidance of **Dr. Sayan Ranu** and **Dr. Hariprasad Kodamana**, ScAI, IIT Delhi

  We are planning to augment the work done in Mirage with explainable tree selections by making use of Shapley values of node neighborhoods in the graphs.

- **Mirage: Model-agnostic Graph Distillation for Graph Classification** (Mar'23 – Nov'23)
  – under the guidance of **Dr. Sayan Ranu** and **Dr. Hariprasad Kodamana**, ScAI, IIT Delhi
  Accepted in ICLR'24

  We develop a novel technique for reducing graph dataset size while still maintaining the performance close to optimum in a way that is independent of the model that this dataset will be used on, unlike previous work.

- **Frigate: Frugal Spatio-temporal Forecasting on Road Networks** (Jan'22 – Feb'23)
  – under the guidance of **Dr. Sayan Ranu** and **Dr. Hariprasad Kodamana**, ScAI, IIT Delhi
  Accepted in ACM SIGKDD'23

  We develop a novel graph convolution layer designed specifically for traffic prediction that provides a very informative prior thus improving the performance. Also, we create the model with generalisation to missing nodes in mind given that deploying a sensor at every location in a city might not be economically feasible. The model couples this new graph convolution layer along with an LSTM based encoder-decoder style sequence to sequence model to solve the regression task of traffic prediction on realistic power-law distributed traffic datasets.

- **Defending against website fingerprinting using adversarial attacks for Tor browser with optimal overhead** (May'20 – May'21)
  – under the guidance of **Dr. Pilli Emmanuel Shubhakar**, CSE, MNIT Jaipur

  We develop a proof of concept that adversarial attacks can be used as a defense against website fingerprinting. Website fingerprinting is done using time series classification models that classify the encrypted packet exchange between a client and server just based on the frequency and packet sizes being transmitted. This poses a threat to privacy and we try to extend black box adversarial attacks from image domain to time series domain to figure out optimal dummy packet placements to mask the

web browsing pattern.

Notable Academic Projects

- Finetuning XLM-RoBERTa for cross lingual natural language inference task as part of natural language processing coursework.
- Creating a model that identifies multi-oriented multi-font text from images with possible natural image background and converts it to text as part of machine learning coursework.
- Used particle swarm optimization to calculate optimal routing in wireless sensor networks as course project as part of requirement for my bachelor's degree.

Deep Learning and Research Tools and Frameworks

- PyTorch, PyTorch Geometric, Huggingface, Python, Anaconda, LaTeX, Git, Linux