MALHAR JERE

(+1)217-530-7679 ⋄ mjjere@ucsd.edu ⋄ malharj.github.io

EDUCATION

University of California San Diego *December 2019 - Present*
PhD student, Electrical and Computer Engineering Department
Specialization: Machine Learning and Data Science
Advisor: Farinaz Koushanfar

University of California San Diego *September 2017 - December 2019*
MS in Computer Engineering
Specialization: Machine Learning and Data Science

University of Illinois at Urbana Champaign *August 2013 - May 2017*
BS in Electrical Engineering.
Thesis: Laser and thermal annealing of single photon avalanche photodiodes in outer space

PROFESSIONAL EXPERIENCE

X, The Moonshot Factory (formerly Google X) ***Summer of 2020***
Software Engineering Intern *Mountain View, CA*
Machine Learning Research on early-stage undisclosed project.

Intuit ***Summer of 2019***
Data Scientist Intern *Mountain View, CA*
Generative neural networks for synthetic data generation.

Google X Development LLC ***Summer of 2018***
Hardware Engineering Intern *Mountain View, CA*

Motorola Solutions ***Summer of 2016***
Software Engineering Intern *Schaumburg, IL*
Custom functions for state-of-the-art Software defined radios.

PUBLICATIONS

1. **M Jere**, T Farnan, F Koushanfar. 'A Taxonomy of Attacks on Federated Learning'. **Accepted to the IEEE Magazine on Security and Privacy.**
2. P Neekhara, S Hussain, **M Jere**, F Koushanfar, J McAuley. "Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples". **Accepted to IEEE Winter Conference on Applications of Computer Vision (WACV) 2021**. **URL**: *arxiv.org/abs/1912.02316*.
3. C Ma, **Malhar Jere**, X Wang, S Mookherjea. "High CAR and low g(2)(0) of 1.55 μm entangled photon-pairs generated by a silicon microring resonator". Conference on Lasers and Electro-Optics (CLEO), 2018.
4. **M Jere**, RK Raman, L Varshney. "The Eurekometric Connectome: Discovering unexplored areas of neuroscience research". *Int. School Conf. Net. Science (NetSci)*, 2017.

WORKSHOP PAPERS

1. **M Jere**, S Herbig, C Lind, F Koushanfar. "Principal Component Properties of Adversarial Samples". *AAAI-20 Workshop on Engineering Dependable and Secure Machine Learning Systems (EDSMLS)*, 2020.

INVITED TALKS

1. **Security Auditing of Deep Neural Networks**.
   Semiconductor Research Company (SRC) Student Technology Conference (TechCON) 2020.
2. **Principal Component Properties of Adversarial Samples.**
   Intel Adversarial Machine Learning Research Group, 2020.

PREPRINTS

1. **M Jere**, B Hitaj, G Ciocarlie, F Koushanfar. "Scratch that! An Evolution-based Adversarial Attack against Neural Networks".
   URL: *arxiv.org/abs/1912.02316. (Under review)*

TEACHING EXPERIENCE

ECE 30: Introduction to Computer Engineering ***Fall 2019, Winter 2020***
Lead Teaching Assistant *La Jolla, CA*

PROFESSIONAL SERVICE

Reviewer

- USENIX 2020
- NDSS 2020
- DAC 2020
- ICCAD 2020
- ACM CCS 2020

Successful grants contributed to

- **Semiconductor Research Corporation**: Primary author of 300,000 USD grant to investigate research on neural network robustness and stability for autonomous vehicles.
- **DARPA: Techniques for Machine Vision Disruption**: Primary author of grant to develop universal adversarial samples for facial recognition systems.

SKILLS

Software	Python, C/C++, SQL, MATLAB, x86, ARM, Git, LTSpice
Frameworks	JAX, TensorFlow, Keras, PyTorch, MXNet, OpenCV, Google3, AWS SageMaker