Hadi Givehchian

Email: hgivehch@ucsd.edu

Google Scholar
Linkedin

Education

- **Ph.D. & M.S. in Computer Science** Sept 2018 - Now
  University of California, San Diego
  GPA: 4/4 via 40 credits
  Thesis: ”Enhancing Security and Privacy of Wireless Systems with Machine Learning Based Wireless Sensing”
  Advisors: Dinesh Bharadia & Aaron Schulman
- **B.S. in Electrical Engineering (Communications), Minor in Computer Science** Sept 2013 - June 2018
  Sharif University of Technology, Tehran, Iran
  Thesis: ”Network Coding Algorithms for Memory Management in Distributed Systems”
  Advisors: M.A. Maddah-Ali & B.H. Khalaj

Selected Courses

- **Graduate**: Advanced Computer Vision (A+), Computer Vision (A+), Deep Learning & Applications (A+), Big Data Analytics (A+), Learning Algorithms (A+), Probabilistic Reasoning & Decision Making (A), Statistical Learning (A), Bayesian Machine Perception (A), Design and Analysis of Algorithms (A), Modern Communication Networks (S)
- **Undergraduate**: Digital Signal Processing, Data Structure, Databases, Probability & Statistics, Digital Communications, Signals & Systems, Network Coding, Linear Algebra

Computer & Technical Skills

- **Software & Tools:**: PyTorch, Python, Rust, MATLAB, Keras, PySpark, TorchServe, SQL, ZeroMQ, Docker, Software Defined Radios, GNU Radio, Linux, Bash, LaTeX, System Integration and Testing
- **Technical Knowledge:**: AI/ML algorithms and models, Communication Theory and Systems, Signal Processing, System Design, Random Processes, Information Theory, Optimization, Algorithm Design

Employement

- **Intern at Qualcomm Technologies, Inc.** June 2021 - Sept 2021
  Human Gait and Shape Recognition Using RF Sensing and Deep Learning
- **Intern at Qualcomm Technologies, Inc.** June 2020 - Sept 2020
  Indoor Map Generation Using RF Sensing and Deep Learning

Patents

- **Generating Indoor Maps Based on Radio Frequency Sensing**
  Hadi Givehchian , Xiaoxin Zhang, Peyman Siyari
- **RF Sensing Based Human Identification Using Combined Gait and Shape Recognition**, Pending
  Hadi Givehchian , Xiaoxin Zhang, Peyman Siyari

Publications

- **Practical Obfuscation of BLE Physical-Layer Fingerprints on Mobile Devices**
  Hadi Givehchian, Nishant Bhaskar, Alexander Redding, Han Zhao, Aaron Schulman, Dinesh Bharadia
  IEEE Symposium on Security and Privacy (SP) 2024. Acceptance rate 17.8%
- **Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices**
  Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez, Héctor Lópéz, Christian Dameff, Dinesh Bharadia, Aaron Schulman
  IEEE Symposium on Security and Privacy (SP) 2022. Acceptance rate 14.7%
- **Spoofing Attack Detection in the Physical Layer with Commutative Neural Networks**
  Daniel Romero, Peter Gerstoft, **Hadi Givehchian**, Dinesh Bharadia
  Arxiv 2022
- **Protecting Bluetooth User Privacy through Obfuscation of Carrier Frequency Offset**
  Ali Nikoofard, **Hadi Givehchian**, Nishant Bhaskar, Aaron Schulman, Dinesh Bharadia, Patrick Mercier
  IEEE Transactions on Circuits and Systems II 2022
- **Revealing Concealed IoT Devices through Passive Detection, Fingerprinting, and Localization**
  Wei Sun, **Hadi Givehchian**, Dinesh Bharadia
  Under Review

Honors & Awards

- Qualcomm Innovation Fellowship Winner (**$100,000**)
- UC San Diego Ph.D. Fellowship
- Member of Iranian National Elites Foundation
- Ranked 90th among more than 250,000 participants in the Iranian Nationwide University Entrance exam for B.Sc.

Selected Projects

- **Smart Radio System for Detection and Characterization of RF Anomalies** 2022 - Now
  ***Keywords**: Spectrum Sensing, Signal Detection, Anomaly Detection, Matrix Factorization, Cyclostationary Signal Processing, Software Defined Radios*
  - Data security is a vital and challenging task, specifically in the environments where the data owner does not have much control over. One possible indicator of breach or compromise of data is unexpected radio frequency (RF) transmissions. In this project, we design and implement a system that automatically detects and characterizes anomalous signals across the 6 GHz RF spectrum. To detect signals, we represent the problem as a non-negative matrix factorization problem and decompose the power spectral density (PSD) to base patterns representing different arbitrary activities in the RF spectrum. We use the reconstruction error as a metric to indicate presence of potential new anomalous signals, and we use cosine similarity to compare PSD patterns and detect new activities. To characterize signals, we apply cyclo-stationary signal processing algorithms (e.g., spectral correlation density) to the complex RF signal and feed the resulting image as the input to a neural network. We use a transformer network trained with metric learning (SoftTriple loss) to infer the characteristics of the signal such as modality and modulation. To satisfy the low latency and high throughput requirements of the system required for keeping up with several gigabytes of data per second, we implemented the system in Rust.

- **Deep Learning Framework for RF Fingerprinting** 2022 - Now
  ***Keywords**: RF Fingerprinting, Metric Learning, Open Set Recognition, Domain Adaptation*
  - Hardware imperfections caused by manufacturing process leave a unique fingerprint in the signal sent by IoT devices, making it possible to identify devices even from the same make and model. However, different wireless signals (Wi-Fi, BLE, ZigBee, etc.) demand different algorithms to estimate such imperfection from the received signal. In addition, these imperfections are usually minuscule, and hard to measure accurately and fine enough to identify a large number of devices. In this project, we develop a deep learning framework that can be trained on an arbitrary wireless technology, and extract distinguishable fingerprints from these signals to uniquely identify and/or verify a large number of transmitter devices. We use deep metric learning (e.g. LMCL and SoftTriple loss) to learn feature embeddings with low within-class and high inter-class variance, so that we can distinguish a large number of devices. Once the network is trained on a set of devices, it can be transferred as the feature extractor to new un-seen devices. Further, we use data augmentation and ensemble of signal slices to make the embeddings robust to wireless channel conditions and packet contents, and use domain adaptation to transfer learned embeddings across different receivers. We also use the perfect signal (without hardware imperfections) as the input during training so that the network can learn the hardware imperfection embeddings easier for any type of modulation and wireless protocol. The intuition is that the distortion caused by hardware imperfections can be modeled as a function applied to the perfect signal. The network can be trained to approximate this function and estimate the hardware imperfection embeddings.

- **TS4: Tensorized Structured State Space Sequence Neural Networks** 2023 - Now
  ***Keywords**: Sequence Modelling, Transformers, State Space Models, Tensorization*
  - Recently, structured state space sequence (S4) models have generated considerable interest due to their simplicity and favorable performance compared to the transformer architecture in certain sequence modelling tasks. A very important property that distinguishes these models from traditional gated RNNs is the linear dependence of the model output on the latent space vector at each time step, even when an input dependent selection mechanism is incorporated. This means that the computation underlying inference and sequence mapping in these models involves linear time evolution of the latent space vector. Inspired by long standing studies of time evolution of matrix product states in quantum mechanics, we study the problem of compressing the latent space of sequence models using tensorization methods. We name such Tensorized Structured State Space Sequence models (TS4). Various novel structures on the parameters of S4 models within the tensorization setting are imposed to derive new classes of structured sequence models. We evaluate the performance of each such class on common datasets and tasks related to sequence processing.

- **Obfuscation of Physical-Layer Hardware Imperfection Fingerprints on Mobile Devices** 2021 - 2023
  ***Keywords**: Bluetooth/WiFi, Security & Privacy, RF Impairments, Obfuscation, Bayes Risk*
  - Radios used in personal electronic devices such as BLE or WiFi chipsets in smartphones have manufacturing imperfections that can be used as a fingerprint to distinguish them from each other. This can be misused by an attacker to identify the presence of the device owner within a few seconds, and track a target by sniffing their wireless signals. To mitigate this privacy threat, we proposed a method to obfuscate the hardware imperfection fingerprints by randomizing the hardware imperfections that the radios generate. The obfuscation mechanism tries to maximize the conditional entropy and minimize the success rate (increase the Bayes risk) of an optimal attacker in identifying the transmitter device. By taking advantage of a hierarchy of distributions, we design an algorithm that prevents the optimal attacker from identifying the device even if they continuously observe the target device for many hours.

- **Physical-Layer BLE Fingerprinting and Tracking Attacks on Mobile Devices** 2019 - 2021
  ***Keywords**: Bluetooth, Security & Privacy, RF Impairments, Non-Convex Optimization*
  - Periodic transmissions of Bluetooth Low Energy (BLE) advertisements are becoming popular in personal electronic devices. These transmissions are continuous: many personal devices, including iPhones and FitBits, transmit at least one advertisement per second, during the entire time that the device is powered on. The frequent transmission of these advertisements may make it possible to track the location of personal devices by passively listening for nearby

advertisements messages. This has not been feasible today, because BLE transmitters hide their identity in these advertisements by randomizing their MAC address. In this work, we demonstrate the first physical-layer fingerprinting mechanism that can be used to identify BLE devices. We build a BLE tracking tool to accurately estimate hardware imperfection parameters by modeling the problem as an optimization problem, and create a profile for the target devices. We collect a large-scale dataset consisting of hundreds of uncontrolled devices in the wild to evaluate the feasibility of RF fingerprinting.

- **Network Coding Algorithms for Memory Management in Distributed Systems** 2016 – 2018
  Keywords: *Distributed Systems, Memory Management, Coding Theory*
  - Big Data frameworks such as Apache Spark in which computations are scheduled according to a DAG, suffer from memory management schemes that can potentially have a poor performance in server failure scenarios. We set out to define a mathematical model for distributed systems that incorporates the stochastic aspects of the system introduced by server failures. Our goal was to develop an approximately optimal algorithm for memory sharing in such systems using information theoretic approaches and network coding techniques to handle server failures.

Teaching Assistant Experience

- Computer Networks
- Digital Signal Processing
- Signals & Systems
- Data Structures
- Probability & Statistics

Mentorship

- Pratik Ratadiya (Graduate Student, UCSD)
- Omm Prakash Sahoo (Graduate Student, IIT BHU)
- Wangdong Xu (Graduate Student, UCSD)
- Eliana Rodriguez (Undergraduate Student, UCSD)