

# FATEMEH SHEIKHOESLAMI

(+1) 612 999 8239 ◊ sheik081@umn.edu

460 Walter Library, Pleasant St. SE, Minneapolis, MN. 55455

Website:<https://fatemehsheikholeslami.github.io/>

## EDUCATION

---

### University of Minnesota, MN, USA

*Sept. 2013 - 2019 (expected)*

PhD. Electrical Engineering- Machine Learning

Overall GPA: 3.97 /4

Thesis: Scalable Kernel Learning, Tensors in Community Identification,  
and Robust Adversary Detection in Deep Neural Networks

Advisor: Prof. Georgios G. B. Giannakis

### Sharif University of Technology, Tehran, Iran

*Sept. 2010-Aug. 2012*

M.Sc. Electrical Engineering- Systems

Overall GPA: 17.44 /20

Advisor: Prof. Masoumeh Nasiri-Kenari

### University of Tehran, Tehran, Iran

*Sept. 2006-Sept. 2010*

B.Sc. Electrical Engineering

Overall GPA: 17.13 / 20

Advisor: Prof. Said Nader-Esfahani

## RESEARCH AND INTERNSHIP EXPERIENCE

---

### AI Research Intern, Technicolor AI Lab, Palo Alto, CA, USA

June 2018 - Aug. 2018

- **Adversarial learning in image classification via convolutional neural networks**

- Investigation on the fragility of CNN-based image classification in the presence of adversarial perturbations and characteristics of decision boundaries in high dimensional spaces
- Development of randomization-based algorithms for improved robustness in adversarial settings with structured and efficient matricized-variance-minimization (MVM) sampling in hidden layers for uncertainty minimization and attack detection

### Research Assistance, University of Minnesota, MN, USA

Sept. 2013 - present

*Signal Processing in Networking and Communications group (SPiNCOM) - with G. B. Giannakis*

- **Adversarial learning in image classification via convolutional neural networks**

- Proposing a general attack detection framework in deep neural networks, subsuming and explaining state-of-the-art alternatives
- Casting the problem of attack detection as a Bayesian hypothesis test by uncertainty minimizing for reduced probability of false alarm
- Analysis of the proposed Variance Minimization defense scheme as a layer-wise low-complexity and efficient uncertainty-minimization defense mechanism for detection of adversarial/malicious images with improved ROC-curve against state-of-the-art alternatives

- **Node embedding techniques and supervised learning over networks**

- Development of node embedding algorithms based on sparse tensor decomposition, non-convex optimization and different regularization techniques over large networks such as social media

- Application of supervised techniques such as logistic regression, SVMs, decision trees, neural networks and ensemble learning for classification/regression over nodes in network via the embedded features
- **Unveiling of overlapping communities over large networks using tensors**
  - Introduction of an egonet-based graph representation using tensors for a more robust capturing of intrinsic characteristics and higher-order connectivity structures in real-world networks
  - Development of overlapping community detection algorithms for large-scale networks using structured tensor decomposition
  - Exploitation of random-walks for smart sampling of the egonet tensor for a more scalable tensor decomposition with application over extremely-large networks
- **Scalable kernel-based learning and feature extraction**
  - Development of online and scalable kernel-based non-linear feature extraction schemes for application on large-scale datasets
  - Incorporation of non-smooth non-convex optimization techniques for sparsity-inducing nonlinear feature extraction
  - Utilization of the extracted features for fast linear classification and regression tasks
- **Reinforcement learning(RL)-enabled caching for next generation networks**
  - Development of a novel reinforcement-learning framework for caching in wireless networks, enabled with dimensionality reduction for applications on large networks

**Research Assistance, Sharif University of Technology, Iran**  
*Wireless Research Laboratory (WRL) - with M. Nasiri-Kenari*

Aug. 2010 - Aug 2012

- **Spectrum mobility analysis in cognitive radio networks**
  - Development of optimal sequencing schemes for reactive and proactive spectrum handoff policies for minimizing secondary-user service time (overhead) in discrete and continuous-time cognitive radio networks from a queuing-theory point of view

## PUBLICATIONS

---

### Pending Publications

1. **F. Sheikholeslami**, S. Jain, and G. B. Giannakis, “Minimum Uncertainty based Detection of Adversaries in Deep Neural Networks,” *IEEE Trans. on Pattern Analysis and Machine Intelligence* (under review).
2. A. Sadeghi, **F. Sheikholeslami**, A. Marques, and G. B. Giannakis, “Reinforcement Learning for Adaptive Caching with Dynamic Storage Pricing”, *IEEE Journal on Selected Areas in Communications* (under review).

## Refereed Journal Publications

3. **F. Sheikholeslami** and G. B. Giannakis, "Identification of overlapping communities via constrained egonet tensor decomposition," *IEEE Transactions on Signal Processing*, vol. 66, no. 21, pp. 5730-5745, November 2018.
4. **F. Sheikholeslami**, D. K. Berberidis, and G. B. Giannakis, "Large-scale kernel-based feature extraction via budgeted nonlinear subspace tracking," *IEEE Transactions on Signal Processing*, vol. 66, no. 8, pp. 1967-1981, April 2018.
5. A. Sadeghi, **F. Sheikholeslami**, and G. B. Giannakis, "Optimal and scalable caching for 5G using reinforcement learning of space-time popularities," *IEEE Journal on Special Topics in Signal Processing*, vol. 12, no. 1, pp. 180-190, February 2018.
6. **F. Sheikholeslami**, M. Nasiri-Kenari and F. Ashtiani, "Joint optimization of probabilistic initial and target channel selection for handoff in Cognitive radio networks," *IEEE Transaction on Wireless Communications*, vol. 14, no. 1, 2015.
7. H. Shokri Ghadikolaei, **F. Sheikholeslami**, M. Nasiri-Kenari, "Distributed multiuser sequential channel sensing schemes in multichannel cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, 2013.

## Refereed Conference Publications

8. **F. Sheikholeslami**, and G. B. Giannakis, "Overlapping community detection via constrained PARAFAC: A divide and conquer approach," *IEEE Intl. Conf. on Data Mining (ICDM)*, New Orleans, USA, 2017 (Regular paper- Acceptance rate: 9.25%).
9. **F. Sheikholeslami**, S. Jain, and G. B. Giannakis, "Randomized Defenses against Adversarial Images in Convolutional Neural Networks", *IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, Brighton, UK, May 2019.
10. A. Sadeghi, **F. Sheikholeslami**, A. Marques, and G. B. Giannakis, "Reinforcement learning for 5G caching with dynamic costs," *Proc. of IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, Calgary, CA, April 2018.
11. A. Sadeghi, **F. Sheikholeslami**, and G. B. Giannakis, "Dynamic Proactive Caching via Reinforcement Learning," *IEEE Proc. of SPAWC*, Greece, July, 2018.
12. **F. Sheikholeslami**, and G. B. Giannakis, "Scalable Kernel-based Learning via Low-rank Approximation of Lifted Data," *Proc. of Allerton Conf. on Comm., Control, and Computing*, Urbana, IL, Oct. 4-6, 2017.
13. **F. Sheikholeslami**, D. K. Berberidis, and G. B. Giannakis, "Memory efficient low-rank non-linear subspace tracking," *Proc. of CAMSAP Conf.*, Curacao, Dutch Antilles, Dec. 10-13, 2017.
14. **F. Sheikholeslami** and G. B. Giannakis, "Soft Unveiling of Communities via Egonet Tensors," *Proc. of Asilomar Conf.*, Pacific Grove, CA, Oct. 29 - Nov. 1, 2017.
15. **F. Sheikholeslami**, B. Baingana, G. B. Giannakis, and N. D. Sidiropoulos, "Egonet tensor decomposition for community identification," *Proc. of Globalsip*, Washington, DC, Dec. 7-9, 2016.
16. **F. Sheikholeslami**, D. K. Berberidis, and G. B. Giannakis, "Kernel-based Low-rank Feature Extraction on a Budget for Big Data Streams," *Proc. of Globalsip Conf.*, Orlando, FL, Dec., 2015.
17. **F. Sheikholeslami** and G. B. Giannakis, "Online Subspace Learning and Nonlinear Classification of Big Data with Misses," *Proc. of 49th Conf. on Info. Sciences and Systems*, Johns Hopkins Univ., Baltimore, MD, March 18-20, 2015.

18. **F. Sheikholeslami**, M. Mardani, and G. B. Giannakis, “Classification of Streaming Big Data with Misses,” *Proc. of Asilomar Conf. on Signals, Systems, and Computers*, CA, Nov. 2014.

## RESEARCH INTERESTS

---

Experience and background includes algorithms, analysis, optimization and application of machine learning, statistical signal processing, and optimization tools in data/network sciences. On-going research focuses on the following topics.

- Robustification of deep neural networks in adversarial settings
- Sparse tensor-based optimization for community/anomaly detection in static/dynamic networks
- Node embedding over large networks for enabling (semi-)supervised learning such as SVMs, logistic regression, deep neural networks, and ensemble learning
- Development of machine-learning-based algorithms such as reinforcement-learning and dynamic programming with applications on next generation networks

## PROGRAMMING, SCRIPTING AND TOOLBOXES

---

**Python:** Tensorflow, Keras, Networkx, iGraph, Scikit-learn, Matplotlib

**Graph visualization:** Gephi, CytoSpec, R

**Tensor toolboxes:** SPLATT, Tensorlab, N-way Toolbox

**MATLAB:** LIBLINEAR, LIBSVM, cvx, signal processing toolbox

## HONORS AND AWARDS

---

NSF Student Travel Grant Award- 2016

ADC/DTC Fellowship University of Minnesota, USA- Fall 2013-spring 2014

Ranked 7th in the nation-wide PhD entrance exam in electrical engineering, spring 2012

Honorary admission for Master Degree studies in University of Tehran- 2010

Iran Telecommunications Research Center Fellowship in M.Sc. studies- 2010

Won University of Tehran Scholarship Award and Exceptional Talent Student- 2010

## SERVICES

---

### Mentoring

- Alireza Sadeghi, junior Ph.D. student, accomplished the project “Reinforcement Learning for Next-Generation Caching”, published in [3], [7], [8], and [17].

### Teaching Assistance

- Detection and Estimation (Spring ‘18) University of Minnesota
- Signals and systems (Fall ‘17) University of Minnesota
- Probability and statistics (Fall ‘11) Sharif University of Technology
- Signals and systems (Fall ‘10) Sharif University of Technology

## REFERENCES

---

Available upon request