Arezoo Rajabi

● rajabia@oregonstate.edu ● http://rajabia.github.io ● www.linkedin.com/in/Arezoo-Rajabi

AREAS OF INTEREST

● **Machine Learning & Deep Learning**: Convolutional Neural Networks (CNNS), Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), Supervised and Unsupervised Learning, Anomaly Detection.
● **Data Science & Statistical Analysis**: Dimension Reduction, Regression, SVM, Feature Selection, Tree-Based Methods, Statistical Tests (T-test, Chi-Square test, One-Way ANOVA, A/B,.)
● **Data Privacy**: Image Privacy, Data Synthesization, Differential Privacy with GANs and VAEs
● **Complex Networks Analysis & Graph Mining**: Clustering, Topology Inference, Community Detection.
● **Cybersecurity**: False Data Tolerance Algorithms, Networks Security

SKILLS

Programming Languages: Python, Java, R, Matlab, C#
Machine Leatning and Data Science Tools: Tensorflow, MatConvNet, PyTorch, Keras, Scikit-Learn, SciPy, Spark, Matplot, ggplot, Panda, Rapid Miner, Weka
Other Tools: CVX (Convex Programming), Lindo (Optimization Solvers and Mathematical Programming Tools), MySQL, OPENET, Microsoft SQL, Amazon Web Services

EDUCATION

Ph.D. Candidate in Computer Science 2014 – Present
Oregon State University, Department of Electrical Engineering and Computer Science
Thesis: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations
Coursework: Convex Optimization, Estimation and Filtering, Machine & Deep Learning, Probabilistic Graphical Model, Bayesian Statistics, Distributed Systems, Sparse Signal Processing

M.Sc. in Computer Engineering (Software Engineering) 2011 – 2013
Sharif University of Technology, Department of Computer Engineering
Thesis: Local Community Detection in Social Networks
Coursework: Data Mining, Software Development Methodologies, Multi-media Networks

B.Sc. in Computer Science 2005 – 2010
Sharif University of Technology, Department of Computer Science
Thesis: Community Detection in Complex Networks

CERTIFICATES

Spark Fundamentals II, Cognitive Class (An IBM Initiative) 2019
Data Science Foundation - Level 2, Cognitive Class (An IBM Initiative) 2019

PUBLICATIONS

A. Rajabi , R. Bobba, M. Rosulek, C. Wright, W. Feng, On the (Im)Practicality of Adversarial Perturbation for Image Privacy, (Accepted in Privacy Enhancing Technology symposium (PETs) 2021).

M. abbasi, **A. Rajabi** , C. Shui, C. Gagné, R. Bobba , Toward Adversarial Robustness by Diversity in an Ensemble of Specialized Deep Neural Network, Canadian Conference on Artificial Intelligence, 2020.

M. abbasi, C. Shui, **A. Rajabi** , C. Gagné, R. Bobba , Toward Metrics for Differentiating Out-of-Distribution Sets, European Conference on Artificial Intelligence (ECAI), 2020.

A. Rajabi , R. Bobba, Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs , Dependable and Secure Machine Learning (DSML) 2019.

M. Salehi, H. R. Rabiee, and **A. Rajabi**. Sampling from complex networks with high community structures, Chaos: An Interdisciplinary Journal of Nonlinear Science,2012.

M. Ramezani, H.R. Rabiee, M. Tahani. and **A. Rajabi**. Dani: A fast diffusion aware network inference algorithm. rXiv:1706.00941, 2017.

M. Abbasi, **A. Rajabi**, A. S. Mozafari, R. B. Bobba, C. Gagne, Controlling Over-generalization and its Effect on Adversarial Examples Generation and Detection arXiv:1808.08282, 2018.

A. Rajabi and R. Bobba, False Data Detection in Distributed Oscillation Mode Estimation using Hierarchical K-means. IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2019.

A. Rajabi and R. Bobba, A Resilient Algorithm for Power System Mode Estimation using Synchrophasors. Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS), 2016.

A. Rajabi and R. Bobba, A Fully Distributed Resilient Algorithm for Power System Mode Estimation using Synchrophasors , (Under Revision of IEEE Transaction on Smart Grid).

HONORS AND AWARDS

First Place Winner at Grad showcase Research Poster Presentation 2018
Cyber Resilient Energy Delivery Consortium (CREDC) summer school student scholarship 2017
Student Travel Awards from Top Security Conferences (S&P, CCS , GREPSECIII , and ACSAC)

SELECTED PROJECTS

Academic Research Projects

- Image Privacy in Image Sharing Platforms 2019-Present
- Resilient Distributed Oscillations Mode Estimation in Power Systems 2016-2019
- Robust Deep Neural Networks 2017-2020
- Complex Networks Analysis 2010-2013

Industrial Research Project

- Data Anonymization and Synthesis (problem submitted by Desjardins in Tenth Montreal Industrial Problem Solving Workshop)

Coursework & Self-Practice Projects

- Dental Growth Rates Approximation (ST599).
- Knowledge Discovery in Relational Databases (CS540).
- Frequency Estimation in Single-Frequency Complex Tone Problem from Limited Number of Noisy Observations (ECE565).
- Practicing Seed Lab's Networks Security Problems and Solutions.

CERTIFICATES

Spark Fundamentals II, Cognitive Class (An IBM Initiative) 2019
Data Science Foundation - Level 2, Cognitive Class (An IBM Initiative) 2019
Cyber Resilient Energy Delivery Construction, Summer School Participation 2017

PROFESSIONAL EXPERIENCE

Research Assistant, Oregon State University 2014-Present

Research Assistant, Sharif University of Technology, Digital Media Lab 2011–2013

Teaching Assistant, Oregon State University 2014-Present
- Network Security • Advances System Security • Operating Systems (I)
- Analysis of Algorithms • Distributed Systems • Computer Applications

Teaching Assistant, Oregon State University 2011-2013
- Multi-media Networks • Complex Networks