Arezoo Rajabi

Postdoctoral Scholar

Email: rajabia@uw.edu
Linkedin: www.linkedin.com/in/arezoo-rajabi
Homepage: http://rajabia.github.io

NSL Lab
University of Washington
Seattle, USA

EDUCATION

Ph.D. in Computer Science 2014 – 2021
Oregon State University, Corvallis, Oregon, USA
Thesis: Two Sides of a Coin: Adversarial-Based Image Privacy and Defending Against Adversarial Perturbations for Robust CNNs

M.Sc. in Computer Engineering (Software Engineering) 2011 – 2013
Sharif University of Technology, Tehran, Iran
Thesis: Local Community Detection in Social Networks

B.Sc. in Computer Science 2005 – 2011
Sharif University of Technology, Tehran, Iran
Thesis: Community Detection in Complex Networks

RESEARCH AREAS

Robustness in Deep Neural Networks: Exploring the vulnerabilities of deep neural networks and developing defenses to mitigate them
Differential Privacy: developing differential privacy solutions and defenses against membership inference attacks
Cyber-security: developing fault tolerance algorithms in distributed learning methods

RESEARCH EXPERIENCE

Postdoctoral Scholar, 2021-Present
NSL Lab, University of Washington, WA, USA

- Developing a differential private method for RL algorithm with risk-neutral decision making approach and a defense for membership inference attacks for pre-trained deep neural network
- Developing new attacks for injecting backdoors in deep neural network

Graduate Research Assistant, 2015-2020
Oregon State University, Corvallis, Oregon, USA

- Developing image privacy methods based on adversarial learning methods against automated face detection methods
- Developing two fault tolerance approaches for outliers in distributed smart grid power systems

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

- Proposed a sampling method for unknown complex networks with high community structure

VOLUNTEER EXPERIENCE

Student Researcher
Industrial Problem Solving Workshop (IPSW), Montreal, Canada
Worked on data anonymization and synthesis project which was submitted by Desjardin and Bank of Canada

PUBLICATIONS AND MANUSCRIPTS

1. **A. Rajabi**, B. Ramasubramanian, A. Marruf, R. Poovendran, Privacy Preserving Reinforcement Learning Beyond Expectation, Accepted in 61st IEEE Conference on Decision and Control, 2022.(https://arxiv.org/pdf/2203.10165.pdf).

2. **A. Rajabi**, M. Abbasi, R. B. Bobba, K. Tajik, Adversarial Images Against Super-Resolution Convolutional Neural Networks for Free, Privacy Enhancing Technology Symposium (PETS), 2022.

3. **A. Rajabi**, R. B. Bobba, Resilience Against Data Manipulation in Distributed Synchrophasor-Based Mode Estimation, IEEE Transaction on Smart Grid, 2021.

4. **A. Rajabi**, R. B. Bobba, M. Rosulek, C. Wright, W. Feng, On the (Im)Practicality of Adversarial Perturbation for Image Privacy, Privacy Enhancing Technology Symposium (PETS), 2021.

5. M. Abbasi, **A. Rajabi**, C. Shui, C. Gagné, R. B. Bobba, Toward Adversarial Robustness by Diversity in an Ensemble of Specialized Deep Neural Network, Canadian Conference on Artificial Intelligence (Canadian AI), 2020. (Best Paper Award)

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

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

8. **A. Rajabi**, R. B. 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.

9. **A. Rajabi**, M. Abbasi, C. Gagné, R. B. Bobba, Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning, DSN workshop on Dependable and Secure Machine Learning (DSML), 2018.

10. 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.

11. M. Ramezani, H.R. Rabiee, M. Tahani, **A. Rajabi**, Dani: A Fast Diffusion Aware Network Inference Algorithm, arXiv:1706.00941, 2017.

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

13. M. Salehi, H. R. Rabiee, **A. Rajabi**, Sampling from Complex Networks with High Community Structures, Chaos: An Interdisciplinary Journal of Nonlinear Science, 2012.

14. **A. Rajabi**, B. Ramasubramanian, A. Marruf, R. Poovendran, Train the Trojan Horse: Breaking Defenses against Backdoor Attacks, https://arxiv.org/pdf/2203.15506.pdf.

15. D. Sahabandu, **A. Rajabi**,L. Niu, B. Li, B. Ramasubramanian, R. Poovendran, Game of Trojans: A Submodular Byzantine Approach, https://arxiv.org/pdf/2207.05937.pdf.

PRESENTATIONS

Paper Presentation at DSN workshop on Dependable and Secure Machine Learning Workshop for *”Adversarial Profile: Detecting Out-distribution Samples and Adversarial Examples for Pre-trained CNNs”* 2019

Paper and Poster Presentation at 2nd Annual Industrial Control System Security Workshop (ICSS) for *”A Resilient Algorithm for Power System Mode Estimation using Synchrophasors”* 2016

Poster Presentation at Graduate Research Showcase, School of Engineering, Oregon State University for *”Towards Dependable Deep Convolutional Neural Networks (CNNs) with Out-distribution Learning”* 2018

TEACHING EXPERIENCE

Teaching Assistant 2014-2020
Oregon State University, Corvallis, Oregon, USA
Courses: Network Security, Advanced System Security, Operating Systems (I), Analysis of Algorithms, Distributed Systems, Computer Applications

Teaching Assistant 2011-2013
Sharif University of Technology, Tehran, Iran
Courses: Multi-media Networks, Complex Networks

SELECTED PROJECTED

Machine Learning Projects:

- *Frequency estimation in single-frequency complex tone problem from limited Number of noisy observations(Estimation, Detection and Filtering Course)*: Using two different estimators of (i) Maximum Likelihood and Method of Moments Estimators and (ii) derived the Carmer-Rao lower bounds.
- *Knowledge Discovery in Relational Databases(Advanced Database):* using three relational machine learning algorithms of (i) First Order Inductive Logic (FOIL) , (ii) Top-Down Inductive Decision Tree (TILDE) and (iii) Mixture Model Membership
- *Hierarchical linear Bayesian model for dental growth rates approximation (Bayesian Statistics Project)*

Network and Security Projects:

- *Implementing a two-layer Map-Reduce to sort the words in given several text files using Hadoop*
- *Implementing robust PCA via outlier pursuit:* using a convex optimization-based outlier pursuit to localize the corrupted points and recover optimal low-dimensional subspace.
- Evaluating the performance of l_1 minimization, Matching Pursuit, and Orthogonal Matching Pursuit (OMP).

AWARDS

First Place Winner at Graduate Research Showcase for Poster Presentation 2018

Cyber Resilient Energy Delivery Consortium (CREDC) Summer School Student Scholarship 2017

Student Travel Awards from Top Security Conferences (S&P, CCS, GREPSEC, and ACSAC)

TECHNICAL SKILLS

Programming Languages: Python, Java, R, Matlab, C#
Machine/Deep Learning Tools: PyTorch, Opacus, Keras, Tensorflow, MatConvNet, Scikit-Learn, ggplot, SciPy, Robustness, Hugging Face
Other Tools: SQL, Hadoop, Amazon Web Services