YIFAN GUO

332 Stevenson Lane APT C3, Towson, MD 21204

Phone: 847-868-4720 Email: yguo@towson.edu Web: yifan-guo.com

EMPLOYMENTS

- Assistant Professor at Towson University From 08/22/2022
  Address: 7800 York Rd, Towson, MD 21252, USA.
  Supervisor: Dr. Michael McGuire
  Responsibilities:
  - ◇ Teach undergraduate and graduate courses in the Department of Computer & Information Sciences.
  - ◇ Develop strong research programs, collaborate with faculty inside or/and outside the department on writing research papers and publish research results in top-tier peer-reviewed conferences or/and journals.
  - ◇ Mentor undergraduate and graduate students in their thesis and individual projects.
  - ◇ Apply for external funding from many government agencies, such as National Science Foundation (NSF), National Institutes of Health (NIH), Department of Defense (DoD), etc., and collaborate with faculty inside or/and outside the department on writing research proposals.
  - ◇ Participate in department activities, and attend the regular faculty meetings.
  - ◇ Provide service excellence through courteous, informed, accessible and professional engagement.
- Research Assistant at Case Western Reserve University 08/29/2016 - 07/29/2022
  Address: 2101 Martin Luther King Jr Dr, Cleveland, OH 44106, USA.
  Supervisor: Dr. Pan Li
  Responsibilities:
  - ◇ Conduct self-motivated research under the general research direction of my supervisor; Collect and log experimental data; Prepare graphs and spreadsheets to portray results; Write academic papers and publish them in top-tier peer-reviewed conferences or/and journals.
  - ◇ Monitor laboratory and/or other supplies to ensure sufficient inventory to support research projects and ensures quality of reagents or other supplies.
  - ◇ Assist my supervisor in writing research proposals, including collecting literature on related topics, implementing experiments for hypothesis justification, and summarizing primary results.

EDUCATION

- **Ph.D.** in Computing and Information Science
  Case Western Reserve University (CWRU), Cleveland, OH, USA
  Date of completion: 06/10/2022; Date of degree received: 08/19/2022
  Advisor: Prof. Pan Li
- **M.S.** in Computer Science
  Northwestern University, Evanston, IL, USA

Date of completion: 12/18/2015; Date of degree received: 02/15/2016
Advisor: Prof. Seda Ogrenci-Memik

- **B.S.** in Information and Computing Sciences
Beijing University of Posts and Telecommunications (BUPT), Beijing, China
Date of completion: 06/27/2013; Date of degree received: 06/27/2013
Advisor: Prof. Wenbao Ai

RESEARCH INTERESTS

- Deep learning schemes for anomaly detection in the Internet of Things (IoT) and cyber-physical systems (CPS).
- Algorithm optimization and practical system design in robust deep learning systems against adversarial attacks.
- Robust and trustworthy federated learning frameworks against various malicious attacks, such as backdoor attacks and Byzantine attacks, with the related applications in IoT, CPS, smart health, and wireless communications.

PUBLICATIONS

Conferences Papers

1. **Yifan Guo**, Qianlong Wang, Tianxi Ji, Xufei Wang, and Pan Li, "Resisting Distributed Backdoor Attacks in Federated Learning: A Dynamic Norm Clipping Approach," the 2021 IEEE International Conference on Big Data (BigData'21), December 15-18, 2021. (Acceptance Ratio = 97/486 = 19.9%)

2. **Yifan Guo**, Lixing Yu, Qianlong Wang, Tianxi Ji, Yuguang Fang, Jin Wei-Kocsis, and Pan Li, "Weak Signal Detection in 5G Cellular System: A Distributed Deep Learning Framework," the Twenty-Second ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc'21), Shanghai, China, July 26-29, 2021. (Acceptance Ratio = 28/139 = 20.1%)

3. **Yifan Guo**, Tianxi Ji, Qianlong Wang, Lixing Yu, and Pan Li, "Quantized Adversarial Training: An Iterative Quantized Local Search Approach," the 18th IEEE International Conference on Data Mining (ICDM'19), Beijing, China, November 8-11, 2019. (Acceptance Ratio = 184/1046 = 18.5%)

4. **Yifan Guo**, Weixian Liao, Qianlong Wang, Lixing Yu, Tianxi Ji, and Pan Li, "Multidimensional Time Series Anomaly Detection: A GRU-based Gaussian Mixture Variational Autoencoder Approach," the 10th Asian Conference on Machine Learning (ACML'18), Beijing, China, November 14-16, 2018. (Acceptance Ratio = 57/230 = 24.8%)

5. Tianxi Ji, Changqing Luo, **Yifan Guo**, Jinlong Ji, Weixian Liao, and Pan Li, "Differentially Private Community Detection in Attributed Social Networks," the 11th Asian Conference on Machine Learning (ACML'19), Nagoya, Japan, November 17-19, 2019.

6. Lixing Yu, Jinlong Ji, **Yifan Guo**, Qianlong Wang, Tianxi Ji, and Pan Li, "Smart Communications in Heterogeneous Spacecraft Networks: A Blockchain Based Secure Auction Approach," IEEE Cognitive Communications for Aerospace Applications Workshop, Cleveland, OH, June 25-26, 2019.

7. Xufei Wang, Weixian Liao, **Yifan Guo**, Lixing Yu, Qianlong Wang, Miao Pan, and Pan Li, "PerRNN: Personalized Recurrent Neural Networks for Acceleration-based Human Activity Recognition," IEEE International Conference on Communications (ICC'19), Shanghai, China, May 20-24, 2019.

8. Weixian Liao, **Yifan Guo**, Xuhui Chen, and Pan Li, "A Unified Unsupervised Gaussian Mixture Variational Autoencoder for High Dimensional Outlier Detection," the 2018 IEEE International Conference on Big Data (BigData'18), Seattle, WA, December, 2018. (Acceptance Ratio = 99/518 = 19.1%)

9. Lixing Yu, Qianlong Wang, **Yifan Guo**, and Pan Li, "Spectrum Availability Prediction for Cognitive Aerospace Communications: A Deep Learning Perspective," IEEE Cognitive Communications for Aerospace Applications Workshop, Cleveland, OH, June 27-28, 2017.

Journals Papers

1. **Yifan Guo**, Tianxi Ji, Qianlong Wang, Lixing Yu, Geyong Min, and Pan Li, "Unsupervised Anomaly Detection in IoT Systems for Smart Cities," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 2231-2242, Oct. 2020.

2. Tianxi Ji, **Yifan Guo**, Qianlong Wang, Xufei Wang, and Pan Li. "ECONOMY: Point Clouds-based Energy-efficient Autonomous Navigation for UAVs," to appear in IEEE Transactions on Network Science and Engineering.

3. Qianlong Wang, **Yifan Guo**, Lixing Yu, Xuhui Chen, and Pan Li, "Deep Q-Network-Based Feature Selection for Multisourced Data Cleaning," to appear in IEEE Internet of Things Journal.

4. Lixing Yu, Ming Li, Wenqiang Jin, **Yifan Guo**, Qianlong Wang, Feng Yan, and Pan Li, "STEP: A Spatio-Temporal Fine-Granular User Traffic Prediction System for Cellular Networks," to appear in IEEE Transactions on Mobile Computing.

5. Qianlong Wang, **Yifan Guo**, Xufei Wang, Tianxi Ji, Lixing Yu, and Pan Li, "AI at the Edge: Blockchain-Empowered Secure Multiparty Learning with Heterogeneous Models," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9600-9610, Oct. 2020.

6. Lixing Yu, **Yifan Guo**, Qianlong Wang, Changqing Luo, Ming Li, Weixian Liao, and Pan Li, "Spectrum Availability Prediction for Cognitive Radio Communications: A DCG Approach," in IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 2, pp. 476-485, Jun. 2020.

7. Qianlong Wang, Tianxi Ji, **Yifan Guo**, Lixing Yu, Xuhui Chen, and Pan Li, "TrafficChain: A Blockchain based Secure and Privacy-Preserving Traffic Map," in IEEE Access, vol. 8, pp. 60598-60612, 2020.

8. Qianlong Wang, **Yifan Guo**, Lixing Yu, and Pan Li, "Earthquake Prediction based on Spatio-temporal Data Mining: An LSTM Network Approach." in IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 1, pp. 148-158, March 2020.

9. Tianxi Ji, Changqing Luo, **Yifan Guo**, Qianlong Wang, Lixing Yu, and Pan Li, "Community Detection in Online Social Networks: A Differentially Private and Parsimonious Approach," in IEEE Transactions on Computational Social Systems, vol. 7, no. 1, pp. 151-163, Feb. 2020.

10. Yi Cai, **Yifan Guo**, Haotian Jiang, and Ming-Chun Huang, "Machine-learning Approaches for Recognizing Muscle Activities Involved in Facial Expressions Captured by Multi-channels Surface Electromyogram." in Smart Health, 5 (2018): 15-25.

Manuscripts in Preparation/Under Review

1. **Yifan Guo**, Tianxi Ji, Xufei Wang, Qianlong Wang, Miao Pan, Ying Ma, and Pan Li, "Efficient Defense against Adversarial Attacks: A Fast Quantized Adversarial Training Scheme," submitted to IEEE Transactions on Big Data.

2. **Yifan Guo**, Tianxi Ji, Xufei Wang, and Pan Li, "Federated Defense Against Backdoor Attacks for Edge Intelligent IIoT Applications", under preparation.

TEACHING INTERESTS

Information security, computer security, data mining, big data analytics, deep learning, and data sciences for engineering.

TEACHING EXPERIENCES

- **Instructor**, Towson University
  COSC 336 Data Structures and Algorithm Analysis — Fall 2022
  COSC 350 Data Communications and Networking — Fall 2022

- **Guest Lecturer**, Case Western Reserve University
  DSCI 133 Introduction to Data Science and Engineering — Spring 2019

- **Teaching Assistant**, Case Western Reserve University
  EECS 302 Discrete Mathematics — Fall 2016, Spring 2017, Spring 2019
  EECS 341 Introduction to Database Systems — Fall 2017
  EECS 414 Wireless Communication — Fall 2018, Fall 2020

- **Peer Mentor**, Northwestern University
  EECS 317 Data Management and Information Processing — Fall 2015

HONORS AND AWARDS

- Student travel award, BigData'21 — 2021
- Bridge funding scholarship, CWRU — 2019
- Student travel award, ACML'18 — 2018
- Certificate of the CWRU future faculty preparation, CWRU — 2017
- Honorable mention (top 15%), MCM/ICM by COMAP — 2012
- First-class scholarship of BUPT (top 5%), BUPT — 2011, 2012

PROFESSIONAL ACTIVITIES

- **Program Committee Member:**
  The AAAI Conference on Artificial Intelligence (AAAI'22'21)
  The International Conference on Big Data, Small Data, Linked Data and Open Data (ALLDATA'21)
  Mobile and Wireless Networks Symposium of IEEE Global Communications Conference (GLOBECOM MWN Symposium'22)

- **Reviewer for journals:**
  IEEE Internet of Things Journal, IEEE Transactions on Neural Networks and Learning Systems, IEEE Access, Information Sciences, etc.
- **Reviewer for conferences:**
  IJCAI'20, Infocom'21'20, BigData'21'20'19, MobiQuitous'20'19, ICCCN'20, AIIPCC'19, etc.