YIFAN GUO

Department of Computer and Data Sciences
Case Western Reserve University, 10900 Euclid Ave., Cleveland, Ohio 44106
Phone: (847)868-4720 Email: yxg383@case.edu Web: yifan-guo.com

EDUCATION

- **Ph.D.** in Computing and Information Science — Anticipated 08/2022
  Case Western Reserve University (CWRU), Cleveland, OH, USA
  Advisor: Prof. Pan Li
- **M.S.** in Computer Science — 12/2015
  Northwestern University, Evanston, IL, USA
  Advisor: Prof. Seda Ogrenci-Memik
- **B.S.** in Information and Computing Sciences — 07/2013
  Beijing University of Posts and Telecommunications (BUPT), Beijing, China
  Advisor: Prof. Wenbao Ai

RESEARCH INTERESTS

- Intelligent 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 against different kinds of malicious attacks, such as adversarial attacks, backdoor attacks, and Byzantine attacks, with its related applications in IoT, CPS, computer vision, smart health, and wireless communications.

PUBLICATIONS

Conferences Papers

1. **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.
2. Tianxi Ji, Changqing Luo, **Yifan Guo**, Qianlong Wang, 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.
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. 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.

5. 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.

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

7. **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%)

8. 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," IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 2231-2242, Oct. 2020.

2. 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.

3. 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.

4. 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.

5. 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, June 2020.

6. 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.

7. 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.

8. 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.

9. 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." Smart Health, 5 (2018): 15-25.

Manuscripts in Preparation/Under Review

1. **Yifan Guo**, Qianlong Wang, Tianxi Ji, Xufei Wang, and Pan Li, "Resisting Distributed Backdoor Attacks in Federated Learning: A Dynamic Norm Clipping Approach," submitted to 2021 IEEE International Conference on Big Data (BigData'21).
2. **Yifan Guo**, Qianlong Wang, Xufei Wang, and Pan Li, "Efficient Defense against Adversarial Attacks: A Fast Quantized Adversarial Training Scheme," submitted to IEEE Transactions on Big Data.

TEACHING INTERESTS

Cybersecurity and privacy, machine learning, data mining, big data analytics, and data sciences and engineering.

TEACHING EXPERIENCES

- **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

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

HONORS AND AWARDS

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

PROFESSIONAL ACTIVITIES

- **Program Committee Member:**
  The AAAI Conference on Artificial Intelligence (AAAI'21'20)
  The International Conference on Big Data, Small Data, Linked Data and Open Data (ALLDATA'21)

- **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'20, BigData'20'19, MobiQuitous'20'19, ICCCN'20, AIIPCC'19, etc.