

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 08/2021
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 Ogresci-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).
- Secure deep learning against adversarial attacks, and robust and trustworthy federated learning.
- Security and privacy issues in both distributed and decentralized systems, and related applications in IoT, CPS, computer vision, smart city, smart health, and wireless communications.

PUBLICATIONS

Manuscripts in Preparation/Under Review

1. **Yifan Guo**, Qianlong Wang, Tianxi Ji, and Pan Li, "United As One: Defense against Collusive Backdoor Attacks in Federated Learning," under submission, 2020.
2. **Yifan Guo**, Qianlong Wang, Xuwei Wang, and Pan Li, "Efficient Defense against Adversarial Attacks: A Fast Quantized Adversarial Training Scheme," submitted to IEEE Transactions on Big Data.
3. **Yifan Guo**, Ming Li, Lixing Yu, Qianlong Wang, Tianxi Ji, Jin Wei-Kocsis, and Pan Li, "Weak Signal Detection in 5G Cellular System: A Distributed Deep Learning Framework," submitted to ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc' 21).

Papers in Refereed Journals

1. **Yifan Guo**, Tianxi Ji, Qianlong Wang, Lixing Yu, Geyong Min, and Pan Li, "Unsupervised Anomaly Detection in IoT Systems for Smart Cities," to appear in IEEE Transactions on Network Science and Engineering.
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.
10. **Yifan Guo**, Teng Li, and Yu-Cui Guo, "Trust Management Model based on Value-at-risk Evaluation with Changing Time in P2P Network." Journal of Computer Applications (ISSN: 1001-9081. CN: 51-1307), no. 9 (2012): 2613-2616.

Papers in Refereed Conferences

1. 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.
2. **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 = $184/1046 = 18.5\%$)
3. 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.
4. 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.
5. 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 = $99/518 = 19.1\%$)
6. **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 = $57/230 = 24.8\%$)

7. 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.

TEACHING INTERESTS

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

TEACHING EXPERIENCES

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

HONORS AND AWARDS

- Bridge funding scholarship, Case Western Reserve University 2018
- Student travel awards, ACML'18 2018
- Certificate of the CWRU Future Faculty Preparation 2017
- Honorable Mention, MCM/ICM by COMAP (top 15%) 2012
- First-class scholarship of BUPT (top 5%), BUPT 2011, 2012

PROFESSIONAL ACTIVITIES

- **Conference TPC member:**
The 35th AAAI Conference on Artificial Intelligence (AAAI'21)
The 29th International Joint Conference on Artificial Intelligence and the 17th Pacific Rim International Conference on Artificial Intelligence (IJCAI-PRICAI'20)
- **Reviewer for journals:**
IEEE Internet of Things Journal, IEEE Access, Information Sciences, etc.
- **Reviewer for conferences:**
Infocom'20, BigData'20'19, MobiQuitous'20'19, ICCCN'20, AIIPCC'19, etc.