Jiadong Lou

Email: loujd@udel.edu
Address: 312 Wharton Dr., Newark, DE, 19711
Tel: (337)-414-0845
Website: https://jiadong-lou.github.io/

EDUCATION

Ph.D. candidate in Computer Science — Sept. 2023 - Present
University of Delaware, Newark, DE
Advisor: **Prof. Xu Yuan**

M.S. in Computer Science — August 2018 - August 2023
University of Louisiana at Lafayette, Lafayette, LA
Advisor: **Prof. Xu Yuan**

B.S. in Internet of Things — Sept. 2014 - May 2018
Harbin Institute of Technology, Harbin, China

RESEARCH INTERESTS

Cybersecurity, data privacy, machine learning, AI for science, wireless communications, and Cyber-physical system

AWARDS

- IEEE/IFIP DSN 2023, Distinguished Paper Award
- IEEE/IFIP DSN 2023, Best Paper Award
- IEEE CNS 2024, Best Paper Runner-up Award

PUBLICATIONS

First-authored Papers

1. [**Submitted to TGRS**] **Jiadong Lou**, Xu Yuan, and Bingqing Liu, "Hyperspectral retrievals of phytoplankton absorption and chlorophyll-a via VAE," submitted to *IEEE Transactions on Geoscience and Remote Sensing*, 2024.

2. [**IEEE S&P'25**] **Jiadong Lou**, Xu Yuan, Xingliang Yuan, Neil Zhenqiang Gong, and Nian-Feng Tzeng, "GRID: Protecting training graph from link stealing attacks on GNN models," accepted by *IEEE Symposium on Security and Privacy*, 2025.

3. [**IEEE CNS'24**] **Jiadong Lou**, and Xu Yuan, "Membership inference via self-comparison," accepted by *IEEE Conference on Communications and Network Security (CNS)*, 2024. **Best Paper Runner-up Award**

4. [**IEEE/IFIP DSN'23**] **Jiadong Lou**, Xu Yuan, and Ning Zhang, "Devils in Your Apps: Vulnerabilities and user privacy exposure in mobile notification systems," in Proc. of *IEEE/IFIP International Conference on Dependable Systems and Network*, 2023. **Best Paper Award and Distinguished Paper Award**

5. [**ACM AsiaCCS'23**] **Jiadong Lou**, Xu Yuan, Miao Pan, Hao Wang, and Nian-Feng Tzeng, "Data privacy examination against semi-supervised learning," in Proc. of *ACM ASIA Conference on Computer and Communications Security*, 2023.

6. [**IEEE TMC**] **Jiadong Lou**, Xu Yuan, Purushottam Sigdel, Xiaoqi Qin, Sastry Kompella, Nian-Feng Tzeng, "Age of information optimization in multi-channel based multi-hop wireless networks," *IEEE Transactions on Mobile Computing*, 2022.

7. [**USENIX Security'21**] **Jiadong Lou**, Xu Yuan, Ning Zhang, "Messy States of Wiring: Vulnerabilities in emerging personal payment Systems," in Proc. of *USENIX Security Symposium*, 2021.

8. [**IEEE/ACM ToN**] **Jiadong Lou**, Xu Yuan, Sastry Kompella, Nian-Feng Tzeng, "Boosting or hindering: AoI and throughput interrelation in routing-aware multi-hop wireless networks," *IEEE/ACM Transactions on Networking*, 2021.

9. [**IEEE INFOCOM'20**] **Jiadong Lou**, Xu Yuan, Sastry Kompella, and Nian-Feng Tzeng. "AoI and throughput tradeoffs in routing-aware multi-hop wireless networks," in Proc. of *IEEE International Conference on Computer Communication*, 2020.

10. [**IEEE SECON'20**] **Jiadong Lou**, Xu Yuan, Nian-Feng Tzeng, "Instant AoI optimization in IoT networks with packet combination," in Proc. of *IEEE International Conference on Sensing, Communication, and Networking*, 2020.

Co-Authored Papers

13. [**ACM CIKM'24**] Fudong Lin, Xu Yuan, **Jiadong Lou**, and Nian-Feng Tzeng, "Towards robust vision transformer via masked adaptive ensemble," accepted by *ACM International Conference on Information and Knowledge Management*, 2024.

14. [**ACM ToSN**] Jie Lian, Xu Yuan, **Jiadong Lou**, Li Chen, Hao Wang, Nian-Feng Tzeng, "Room-Scale location trace tracking via continuous acoustic waves," *ACM Transactions on Sensor Networks*, 2024.

15. [**ACM ToSN**] Jie Lian, Changlai Du, **Jiadong Lou**, Li Chen, Xu Yuan, "EchoSensor: Fine-Grained ultrasonic sensing for smart home intrusion detection," *ACM Transactions on Sensor Networks*, 2023.

16. [**ACM CCS'21**] Yihe Zhang, Xu Yuan, Jin Li, **Jiadong Lou**, Li Chen, and Nian-Feng Tzeng. "Reverse Attack: Black-box Attacks on Collaborative Recommendation," in Proc. of *ACM SIGSAC Conference on Computer and Communications Security*, 2021.

17. [**ACM Ubicomp/IMWUT'21**] Jie Lian, **Jiadong Lou**, Li Chen, and Xu Yuan. "Echospot: Spotting your locations via acoustic sensing." in Proc. of *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, pp. 1-21, 2021.

18. [**ESORICS'20**] Yihe Zhang, **Jiadong Lou**, Li Chen, Xu Yuan, Jin Li, Tom Johnsten, and Nian-Feng Tzeng. "Towards poisoning the neural collaborative filtering-based recommender systems," In Proc. of *European Symposium on Research in Computer Security*, 2020.

GRANTS WRITING EXPERIENCES

1. **National Science Foundation**, "CAREER: Holistic Framework for Constructing Dynamic Malicious Knowledge Bases in Social Networks," Award Number: 2348452. Total Award Amount: $500,000. My Role: Main Technical Contributor

2. **National Science Foundation**, "Collaborative Research: SaTC: CORE: Small: Critical Learning Periods Augmented Robust Federated Learning," Award Number: 2315613. Total Award Amount: $500,000. My Role: Main Technical Contributor

3. **National Science Foundation**, "Collaborative Research: CAIG: Empowering Artificial Intelligence to Reveal Phytoplankton Community Dynamics in Coastal Oceans," Award Number: 2425812. Total Award Amount: $849,636. My Role: Main Technical Contributor

TEACHING EXPERIENCES

Instructor

University of Louisiana at Lafayette

- Machine Learning: Applications and Practices, and Introduction to Meteorology   June 2023 - August 2023

Louisiana State University, IBM

- TigerAI Bootcamp   May 2024

Teaching Assistant

University of Louisiana at Lafayette   Jan. 2019 - May 2023

- Programming Languages
- Principle of Operating System Theory
- Computer Communication & Networks
- Principles of Computer Architecture

ACADEMIC SERVICES

Journal Reviews   16

- IEEE Transaction on Mobile Computing   5
- IEEE Internet of Things Journal   3
- IEEE Communications Letters   1
- IEEE Transactions on Vehicular Technology   1
- IEEE Transactions on Network Science and Engineering   1
- IEEE Transactions on Dependable and Secure Computing   2
- Security and Communication Networks   2
- Computers & Security   1

TPC Member

IEEE International Conference on Mobility, Sensing and Networking (**MSN**), 2024

Student Volunteer

IEEE International Conference on Computer Communications (**IEEE INFOCOM**), 2022