Junjie Liang

Security Research Engineer @ ByteDance
E-mail: jokitlueng@hotmail.com webpage: https://junjieliang672.github.io/

Research Interests

- **Longitudinal data analysis**. Machine learning for data with complex, unknown correlation structure (non-i.i.d. data).
- **Information Retrieval**. Retrieval Augmented Generation.
- **LLM Security**. Detection of privacy leakage. Prompt Injection and Jailbreaking Mitigation. Adversarial Attack and Robustness.

Education

2017-2022 The Pennsylvania State University (PSU)
Ph.D. in Informatics; Advisor: Vasant Honavar

2014-2017 South China University of Technology (SCUT)
M.S. in Computer Science and Engineering; Advisor: Jinlong Hu

2009-2013 Guangdong University of Technology (GDUT)
B.E. in Information Management and System; Advisor: Jie Zhao

Professional Experience

▷ Mar. 2025-Present | **Security Research Engineer** at ByteDance Inc.

- Applied Security Research on LLM Related Products and Services.

▷ Jun. 2022-Mar. 2025 | **Senior AI Research Engineer** at Bloomberg L.P.

- Agentic RAG for Large-scale Financial System.
- Lead the Design for Continuous Training and Continuous Annotation Framework for Federated Search System.
- Machine Learning and Ranking Evaluation for Document Search System.

▷ Jun.-Aug. 2021 | **Quant Associate Intern** at JPMorgan Chase & Co.
Mentor: Ping Liu, Lei Xu

- Project: Causal Inference for Auto Loan Pricing Business
  - Causal graphical model for Auto Loan pricing data: Identifying confounders, designing model to combine observational and experimental data, model evaluation.
  - *Techniques*: Structural equation estimation, causal effects estimation.

▷ May-Aug. 2020 | **Security Research Intern** at JD.com
Mentor: Xinyu Xing

- Project: Causal Reinforcement Learning in Imperfect Information Games
  - Causal graphical model for card games.
  - *Techniques*: Structural equation estimation, Proximal policy optimization (PPO)

▷ May-Aug. 2019 | **Security Research Intern** at JD.com
Mentor: Xinyu Xing

- Project: Semi-supervised learning with low-quality labels
  - Proposed a semi-supervised ensemble clustering model to predict the fine-grained classes using low-quality labeled data (i.e., labels are subject to wrong labeling, missing classes and coarse-grained labeling).
  - *Techniques*: (Deep) Clustering models, Metric learning.
  - *Publication*: NDSS 2021

▷ May-Aug. 2018 | **Data Scientist Intern** at Conversant
Mentor: Farooq Ali

- Project: Large scale recommendation system design
  - Designed and implemented a recommendation system algorithm on Spark platform.
  - Exploit and optimize computational parallelism.

Academic Research Experience

▷ 2017-present | **Research Assistant** at Penn State University, University Park
Advisor: Vasant Honavar

- Project: Machine learning for longitudinal data with complex, unknown correlations
  - *Goal*: Adapt and extend existing machine learning approaches to handle longitudinal (non-i.i.d.) data. Making efficient, accurate prediction while enabling automatic data correlation discovery.
  - *Directions*: Mixed effects models, latent factor models, Gaussian process, representation learning, variable selection.
  - *Publications*: AAAI 2021, WWW 2021, AAAI 2020
- Project: Causal Inference for longitudinal data
  - *Goal*: Causal effect estimations for longitudinal data with irregularly observed data, multiple time-varying treatments.
  - *Directions*: probabilistic graphical models, latent variable models, state transition models.

▷ 2015-2018 | **Research Assistant** at South China University of Technology
Advisor: Jinlong Hu

- Project: Collaborative Filtering approaches for recommendation system.
  - *Goal*: Design efficient collaborative filtering approaches for ranking-based recommendation systems
  - *Directions*: Neighborhood models, clustering, learning to rank, factorization machines
  - *Publications*: BigData 2018, ESWA 2018.

Teaching Experience

DS 497, Spring 2019 | Principles of Artificial Intelligence
Penn State University, College of Inforamtion Sciences and Technology
Instructor: Vasant Honavar

Publications

1. **Liang, J.**, Ren, W., Sahar, H., Honavar, V. (2024). Inducing Clusters Deep Kernel Gaussian Process for Longitudinal Data. In: Proceddings of the AAAI International Conference on Artificial Intelligence (**AAAI 2024**).
2. **Liang, J.**, Wu, Y., Xu, D., Honavar, V. (2021). Longitudinal Deep Kernel Gaussian Process Regression. In: Proceddings of the 35th AAAI International Conference on Artificial Intelligence (**AAAI 2021**).
3. **Liang, J.**, Guo, W., Luo, T., Honavar, V., Wang, G., Xing, X. (2021). FARE: Enabling Fine-grained Attack Categorization under Low-quality Labeled Data. *In Proceedings of the 28th Annual Network and Distributed System Security Symposium* (**NDSS 2021**).
4. Xu, D., **Liang, J.**, Cheng, W., Wei, H., Chen, H., Zhang, X. (2021). Transformer-Style Relational Reasoning with Dynamic Memory Updating for Temporal Network Modeling. *In: Proceddings of the 35th AAAI International Conference on Artificial Intelligence* (**AAAI 2021**).
5. Wei, H., Xu, D., **Liang, J.**, Li, Z. (2021). How Do We Move: Modeling Human Movement with System Dynamics. *In: Proceddings of the 35th AAAI International Conference on Artificial Intelligence* (**AAAI 2021**).
6. Chen, C., **Liang J.**, Ma, F., Glass, L., Sun, J., Xiao, C. (2021). UNITE: Uncertainty-based Health Risk Prediction Leveraging Multi-sourced Data. *In: Proceddings of The Web Conference 2021* (**WWW 2021**).
7. **Liang, J.**, Xu, D., Honavar, V. (2020). LMLFM: Longitudinal Multi-Level Factorization Machines. In: Proceddings of the 34th AAAI International Conference on Artificial Intelligence (**AAAI 2020**).
8. **Liang, J.**, Hu, J., Dong, S., & Honavar, V. (2018). Top-N-Rank: A Scalable List-wise Ranking Method for Recommender Systems. In: Proceedings of the IEEE International Conference on Big Data (**BigData 2018**).
9. Hu, J., **Liang, J.**, Kuang, Y., & Honavar, V. (2018). A User Similarity-based Top-N Recommendation Approach for Mobile In-application Advertising. Expert Systems with Applications, vol. 111, pp. 51-60. DOI: 10.1016/j.eswa.2018.02.012 (**ESWA 2018**).
10. Hu, J., **Liang, J.**, & Dong, S. (2017). iBGP: A Bipartite Graph Propagation Approach for Mobile Advertising Fraud Detection. Mobile Information Systems, Volume 2017. DOI: 10.1155/2017/6412521
11. Zhao, J., **Liang, J.**, Dong, Z., Chen, X., & Tang, D. (2015). Global Positive Region Inconsistency Based Attributes Core Computation. Computer Science, 42(8): 259-264. (In Chinese)
12. Zhao, J., **Liang, J.**, Dong, Z., & Tang, D. (2015). Rough Set Attribute Reduction Algorithm Using Bit Arithmetic and Core Attributes Quick Identification. Journal of Chinese Mini-Micro Computer Systems, 36(2): 316-321. (In Chinese)

Patents

1. Characterizing network scanners by clustering scanning profiles. Publication number: WO2023287921A1. Jan. 19, 2023.
2. Quantitative scoring method for implicit feedback of user. Publication number: CN107025277A. Aug. 8, 2017.
3. Large-scale on-line recommendation method based on mobile context. Publication number: CN106951436A. Jul. 14, 2017.

Professional Services

Journal Reviewer

1. Expert Systems with Applications (ESWA)
2. The ACM Transactions on Knowledge Discovery from Data (TKDD)

Conference Reviewer

1. 2025 International Workshop on Resource-Efficient Learning for the Web (RelWeb) 2025
2. International Workshop on Resource-Efficient Learning for Knowledge Discovery (RelKD) 2023
3. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD) 2023
4. Association for Computational Linguistics (ACL) 2023
5. AAAI Conference on Artificial Intelligence (AAAI) 2021, 2020
6. Neural Information Processing Systems (NeurIPS) 2021, 2020
7. International Joint Conferences on Artificial Intelligence (IJCAI) 2021, 2020
8. ACM International Conference on Web Search and Data Mining (WSDM) 2020

Awards

2024	AI-related Dissertation Contest Finalists
2020	AAAI Student Scholarship
2020	IST Travel Award
2019	IST Travel Award
06/2013	Top-ten Distinguished Graduating Students' Price
06/2013	Best Thesis Award
2009-2010	National Scholarship