Wenbin Zhai

CONTACT

Email: wenbin.zhai@connect.polyu.hk
Homepage: Wenbin Zhai's Homepage
Google Scholar: Wenbin Zhai's Google Scholar
Address: Hong Kong Polytechnic University, 11 Yuk Choi Rd, Hung Hom, Hong Kong

PROFESSIONAL SUMMARY

Ph.D. student in the Department of Computing at The Hong Kong Polytechnic University.
My current research focuses on LLM agent security, especially tool-augmented LLM agents, agentic workflows, and external agent components such as tools, memory, and retrieval systems.
My broader research interests include cybersecurity, trustworthy AI, UAV/IoT networks, anomaly detection, and secure distributed systems.

EDUCATION

The Hong Kong Polytechnic University (PolyU), Hong Kong ***Sep. 2025 – Present***
Ph.D. in Computer Science and Technology, Department of Computing

Nanjing University of Aeronautics and Astronautics (NUAA), China ***Sep. 2020 – Apr. 2023***
M.Eng. in Computer Science and Technology, College of Computer Science and Technology

- **GPA:** 85.4/100, Ranking A (Top 15%)
- **Thesis Topic:** Research on Routing Protocol for Multi-hop Unmanned Aerial Vehicle Ad-hoc Networks **(Outstanding Postgraduate Thesis of Jiangsu Province and Outstanding Postgraduate Thesis of Jiangsu Computer Society)**

Nanjing University of Chinese Medicine (NJUCM), China ***Sep. 2016 – Jun. 2020***
B.Eng. in Computer Science and Technology, School of Artificial Intelligence and Information Technology

- **GPA:** 86/100, Ranking 8/61 (Professional GPA: 90.8/100, Ranking 2/61)
- **Thesis Topic:** Design and Implementation of a Method for the Safe Storage of Chinese Medicine Data based on Homomorphic Encryption **(Outstanding Undergraduate Thesis of Jiangsu Province)**

PUBLICATIONS

Journal Papers:

- **Wenbin Zhai**, Liang Liu, Youwei Ding, Shanshan Sun, and Ying Gu, "ETD: An Efficient Time Delay Attack Detection Framework for UAV Networks" in ***IEEE Transactions on Information Forensics and Security (TIFS)***. [**CORE A, CCF A, SCI-Q1**]
- **Wenbin Zhai**, Shanshan Sun, Liang Liu, Youwei Ding, and Wanying Lu, "HOTD: A Holistic Cross-Layer Time Delay Attack Detection Framework for UAV Networks" in ***Journal of Parallel and Distributed Computing (JPDC)***. [**CORE A, CCF B, SCI-Q1**]
- **Wenbin Zhai**, Feng Wang, Liang Liu, Youwei Ding, and Wanying Lu, "Federated Semi-Supervised and Semi-Asynchronous Learning for Anomaly Detection in IoT Networks" in ***IEEE Transactions on Network and Service Management (TNSM)***. [**CCF C, SCI-Q2**]
- Liang Liu*, **Wenbin Zhai***, Xin Li, Youwei Ding, Wanying Lu, and Ran Wang, "ESTA: An Efficient Spatial-Temporal Range Aggregation Query Processing Algorithm for UAV Networks" in ***IEEE Transactions on Network Science and Engineering (TNSE)***. [CCF C, SCI-Q1]
- Weichen Ding, **Wenbin Zhai**, Liang Liu, Ying Gu, and Hang Gao, "Detection of Packet Dropping Attack Based on Evidence Fusion in IoT Networks" in ***Security and Communication Networks (SCN)***. [CCF C, SCI-Q3]

- Kaibin Zhang, Liang Liu, **Wenbin Zhai**, Youwei Ding, and Jun Hu, "OSIS: Obstacle-Sensitive and Initial-Solution-First Path Planning" in ***Peer-to-Peer Networking and Applications (PPNA)***. [CCF C, SCI-Q2]
- Gongshun Min, Liang Liu, **Wenbin Zhai**, Zijie Wang, and Wanying Lu "An Efficient Data Collection Algorithm for Partitioned Wireless Sensor Networks" in ***Future Generation Computer Systems (FGCS)***. [CORE A, CCF C, SCI-Q1]
- Wenjie Zhao, Yu Wang, **Wenbin Zhai**, Liang Liu, and Yulei Liu, "Efficient Time-Delay Attack Detection Based on Node Pruning and Model Fusion in IoT Networks" in ***Peer-to-Peer Networking and Applications (PPNA)***. [CCF C, SCI-Q2]
- Yanlin Wang, Liang Liu, Mengqi Li, **Wenbin Zhai**, Weihua Ma, and Hang Gao, "Power Level Aware Charging Schedule in Wireless Rechargeable Sensor Network" in ***Peer-to-Peer Networking and Applications (PPNA)***. [CCF C, SCI-Q2]
- Yu Fan, Liang Liu, Xingxing Zhang, Huibin Shi, and **Wenbin Zhai**, "MAPP: An efficient multi-location task allocation framework with personalized location privacy-protecting in spatial crowdsourcing" in ***Information Sciences***, 2023, 619: 654-678. [**CORE A**, CCF B, SCI Q1]
- Jiancheng Song, Liang Liu, Yulei Liu, Jie Xi, and **Wenbin Zhai**, "Path Planning for Multi-Vehicle-Assisted Multi-UAVs in Mobile Crowdsensing" in ***Wireless Communications and Mobile Computing (WCMC)***, vol. 2022, 21 pages, 2022. [CCF C, SCI-Q3]

Conference Papers:

- **Wenbin Zhai**, Liang Liu, Jianfei Peng, Youwei Ding, and Wanying Lu, "PAR: A Power-Aware Routing Algorithm for UAV Networks" in ***17th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2022)***, Dalian, China, November 24-26, 2022, Proceedings, Part III. Cham: Springer Nature Switzerland, 2022: 333-344. [**CCF C**]
- Yunfeng Cui, **Wenbin Zhai**, Liang Liu, Youwei Ding, and Wanying Lu, "A Framework for Moving Target Defense based on Federated Semi-Supervised Learning" in ***3rd International Conference on Emerging Information Security and Applications (EISA 2022)***, Wuhan, China, October 29-30, 2022, Proceedings. Cham: Springer Nature Switzerland, 2023: 209-224.
- Wanying Lu, **Wenbin Zhai**, Feng Wang, and Yu Fan, "Link Aware Aggregation Query with Privacy-Preserving Capability in Wireless Sensor Networks" in ***2023 International Conference on Electronics, Computers and Communication Technology (CECCT 2023)***, Guilin, China, November 17-19, 2023, Proceedings. Cham: Association for Computing Machinery, 2023: 245-250.
- Wanying Lu, Liang Liu, **Wenbin Zhai**, Haoyuan Chen, and Yulei Liu, "HBC: Combining Lossy and Lossless Hybrid Bilayer Compression Framework on Time-Series Data" in ***21st IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2023)***, Wuhan, China, December 21-24, 2023. [CCF C]
- Kaibin Zhang, Liang Liu, **Wenbin Zhai**, Youwei Ding, and Jun Hu, "OSIS: Obstacle-Sensitive and Initial-Solution-First Path Planning" in ***29th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2023)***, Hainan, China, December 17-21, 2023. [CCF C]
- Kun Guo, Liang Liu, **Wenbin Zhai**, and Youwei Ding, "EKR: An Efficient K-anycast Routing in UAV Networks" in ***9th International Conference on Computer and Communications (ICCC 2023)***, Chengdu, China, December 8-11, 2023.
- Zixiao Zhou, Liang Liu, **Wenbin Zhai**, Jiancheng Song, and Yulei Liu, "Power-Aware Path Planning for Vehicle-Assisted Heterogeneous UAVs in Mobile Crowd Sensing" in ***2023 International Conference on Data, Information and Computing Science (CDICS 2023)***, Singapore, December 8-10, 2023.
- Keyue Yang, Liang Liu, Shijie Li, **Wenbin Zhai**, Wenjing Wang, Ziyi Zheng, and Jinan Wang, "DDC: Efficient Dynamic-Dictionary-Based Compression on Floating Time Series Data" in ***23rd IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2025)***, Shenyang, China, October 10-12, 2025. [CCF C]

- Lingling Hu, Liang Liu, Yulei Liu, **Wenbin Zhai**, and Xinmeng Wang, "A Robust Fixed Path-Based Routing Scheme for Protecting Source Location Privacy in WSNs" in ***17th International Conference on Mobility, Sensing and Networking (MSN 2021)***, Exeter, UK, December 13-15, 2021, IEEE, 2021: 48-55. [CCF C]

* Equal contribution / co-first authors.

SELECTED AWARDS AND HONORS

- PolyU Research Postgraduate Scholarship (2025) ***May. 2025***
- Outstanding Postgraduate Thesis of Jiangsu Province (2023) ***Dec. 2024***
- Outstanding Postgraduate Thesis of Jiangsu Computer Society (2023) ***Dec. 2024***
- Tuition Fee Scholarship of UNSW Sydney (2023) ***Dec. 2023***
- Provincial Merit Student of Jiangsu Province (2022-2023) ***Apr. 2023***
- Outstanding Graduate of NUAA (2023) ***Apr. 2023***
- Merit Student of NUAA (2021-2022) ***Dec. 2022***
- Advanced Individual in Research and Innovation of NUAA (2021-2022) ***Dec. 2022***
- Second Class Scholarship for Postgraduates of NUAA (2020-2023) (CNY 8,000/year) ***Sep. 2020 – Sep. 2022***
- Outstanding Undergraduate Thesis of Jiangsu Province (2020) ***Oct. 2021***
- Outstanding Graduate of NJUCM (2020) ***Jun. 2020***
- Merit Student of NJUCM (2018-2019) ***Dec. 2019***
- Ruihua Soaring Scholarship (2018-2019) (CNY 8,000) ***Sep. 2019***
- National Encouragement Scholarship in China (2017-2019) (CNY 5,000/year) ***Dec. 2018 – Dec. 2019***
- First Class Scholarship for Undergraduates of NJUCM (2017-2019) (CNY 2,500/year) ***Dec. 2018 – Dec. 2019***
- Principal's Special Award of NJUCM (2017-2018) (CNY 10,000) ***Dec. 2018***
- Fei Xiaotong Virtue Scholarship (2017-2018) (CNY 6,000) ***Dec. 2018***

PROFESSIONAL ACTIVITIES

Conference Reviewer:

- The Fourteenth International Conference on Learning Representations (**ICLR 2026**) [CCF A]
- The IEEE/CVF Conference on Computer Vision and Pattern Recognition 2026 (**CVPR 2026**) [CCF A]
- The Forty-Third International Conference on Machine Learning (**ICML 2026**) [CCF A]

Journal Reviewer:

- IEEE Transactions on Information Forensics and Security (**TIFS**) [CORE A, CCF A, SCI-Q1]
- The Journal of Supercomputing (**TJSC**) [CCF C, SCI-Q2]
- Frontiers of Information Technology & Electronic Engineering (**FITEE**) [CCF C, SCI-Q2]