Yihao Chen | Postdoctoral Researcher at CMU

+1 (510) 229 8681 • yihaoc@andrew.cmu.edu • Google Scholar • Homepage

Education

Ph.D. in Computer Science, Tsinghua University, Beijing, China — Sep. 2021 – Jun. 2026
Thesis: *Detection of Internet Inter-Domain Routing Anomalies*
Co-advisors: Prof. Jianping Wu and Prof. Qi Li

B.Eng. in Computer Science, Tsinghua University, Beijing, China — Sep. 2017 – Jun. 2021
Thesis: *BGP Anomaly Detection Based on Network Representation Learning*
Advisor: Prof. Qi Li

Publications

Peer-Reviewed Papers

ASRogue: Manipulating ASRank-Inferred AS Relationships — 2026
Yi Xu, **Yihao Chen**, Ke Xu, Qi Li, Jianping Wu
In proceedings of the *35th USENIX Security Symposium* (*Security'26*)

Understanding the Stealthy BGP Hijacking Risk in the ROV Era — 2026
Yihao Chen, Qi Li, Ke Xu, Zhuotao Liu, Jianping Wu
In proceedings of the *Network and Distributed System Security Symposium 2026* (*NDSS'26*)

Lightweight Consensus Mechanism Based on Source Address Validation — 2025
Yi Xu, **Yihao Chen**, Xiaoliang Wang, Ke Xu, Qi Li
Journal of Software (*ISSN 1000-9825; in Chinese*)

Learning with Semantics: Towards a Semantics-Aware Routing Anomaly Detection System — 2024
Yihao Chen, Qilei Yin, Qi Li, Zhuotao Liu, Ke Xu, Yi Xu, Mingwei Xu, Ziqian Liu, Jianping Wu
In proceedings of the *33rd USENIX Security Symposium* (*Security'24*)
Distinguished Paper Award 🏆 and Internet Defense Prize Winner 🏆

Low-Quality Training Data Only? A Robust Framework for Detecting Encrypted Malicious Network Traffic — 2024
Yuqi Qing, Qilei Yin, Xinhao Deng, **Yihao Chen**, Zhuotao Liu, Kun Sun, Ke Xu, Jia Zhang, Qi Li
In proceedings of the *Network and Distributed System Security Symposium 2024* (*NDSS'24*)

Generic and Robust Root Cause Localization for Multi-Dimensional Data in Online Service Systems — 2023
Zeyan Li, Junjie Chen, **Yihao Chen**, Chengyang Luo, Yiwei Zhao, Yongqian Sun, Kaixin Sui, ..., Dan Pei
Journal of Systems and Software 203 (2023): 111748

LogParse: Making Log Parsing Adaptive through Word Classification — 2020
Weibin Meng, Ying Liu, Federico Zaiter, Shenglin Zhang, **Yihao Chen**, Yuzhe Zhang, Yichen Zhu, ..., Dan Pei
In proceedings of the *29th International Conference on Computer Communications and Networks* (*ICCCN'20*)

LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs — 2019
Weibin Meng, Ying Liu, Yichen Zhu, Shenglin Zhang, Dan Pei, Yuqing Liu, **Yihao Chen**, ..., Rong Zhou
In proceedings of the *28th International Joint Conference on Artificial Intelligence* (*IJCAI'19*)

Preprints & Under Review

Exposing LLM User Privacy via Traffic Fingerprint Analysis: A Study of Privacy Risks in LLM Agent Interactions — 2025
Yixiang Zhang, Xinhao Deng, Zhongyi Gu, **Yihao Chen**, Ke Xu, Qi Li, Jianping Wu
arXiv preprint (*arXiv:2510.07176*)

Patents

Method for Efficient Inter-Domain Routing Simulation Using Matrix Operations — 2025
Qi Li, **Yihao Chen**, Ke Xu, Zhuotao Liu, Jianping Wu
Chinese patent application (CN121262137A)

Method for Detecting Stealthy Inter-Domain Routing Hijacks Using Cross-Vantage-Point Analysis — 2025
Qi Li, **Yihao Chen**, Ke Xu, Zhuotao Liu, Jianping Wu
Chinese patent application (CN121792142A)

Inter-Domain Routing Anomaly Detection Method Based on Network Representation Learning — 2024
Qi Li, **Yihao Chen**, Qilei Yin, Ke Xu, Zhuotao Liu, Yi Xu, Mingwei Xu, Ziqian Liu, Jianping Wu
Chinese patent application (CN118413373A), *US patent application* (US20250350631A1)

Standard Proposals

Structural Vulnerabilities in ASRank under Adversarial Conditions — 2026
Yi Xu, **Yihao Chen**, Ke Xu, Qi Li, Jianping Wu

IETF Internet Draft (draft-xu-sidrops-asrank-vulnerabilities, under review)

Risk of Stealthy BGP Hijacking under Incomplete Adoption of Route Origin Validation (ROV) 2025
Qi Li, **Yihao Chen**, Yi Xu, Ke Xu, Zhuotao Liu, Jianping Wu
IETF Internet Draft (draft-li-sidrops-stealthy-hijacking, under review)

Research Experience

Network & Information Security Lab, Tsinghua University Sep. 2020 – Aug. 2026
Student Researcher, co-advised by Prof. Jianping Wu and Prof. Qi Li.
Research keywords: Internet routing security, AI for security, network measurement, anomaly detection, traffic analysis

- Led the development and deployment of a BGP routing anomaly detection system at China Telecom, based on a novel network representation learning model that captures intrinsic AS routing policies in a semantics-rich vector space.
- Led the first systematic study of the emerging stealthy BGP hijacking threat under partial ROV deployment, establishing an online monitoring service, the first real-world incident dataset, and a comprehensive risk assessment framework.
- Leading an ongoing study to build an AI agent framework that reasons over open-source intelligence to uncover hidden relationships when domain-specific data falls short, and to distinguish malicious attacks of interest from benign events.
- Leading an ongoing study to uncover adversarial manipulation risks in common AS relationship inference pipelines, demonstrating a practical attack that can manipulate ASRank results by injecting carefully crafted BGP routes.
- Developed a lightweight consensus framework tailored for decentralized network-layer security, and developed an encrypted malicious traffic detection framework dedicated to handle low-quality, insufficient training data.

NetMan Lab, Tsinghua University Sep. 2018 – Aug. 2020
Student Research Intern, advised by Prof. Dan Pei.
Research keywords: AI for operations, root cause localization, anomaly detection, log analysis

- Designed and evaluated a generalized root cause localization approach for multi-dimensional data from online services, achieving over 30% F1-score improvements and identification of external faults.
- Developed and evaluated a semantics-aware unsupervised log anomaly detection framework that enables joint detection of sequential and quantitative anomalies, and developed an adaptive log parsing system tailored for log compression.

Invited Talks

Adversarial Manipulation Risks in Internet Measurement: A Case Study of ASRank
CAIDA AIMS-19 Workshop in San Diego, USA 2026

Understanding the Stealthy BGP Hijacking Risk in the ROV Era
The 60th Asia Pacific Network Information Center Conference (*APNIC'60*) in Da Nang, Vietnam 2025

Learning with Semantics: Towards a Semantics-Aware Routing Anomaly Detection System
2025 Asia Pacific Regional Internet Conference on Operational Technologies (*APRICOT'25*) in Petaling Jaya, Malaysia 2025
2025 International Forum for Security Research (*InForSec'25*) in Beijing, China 2025
The 8th Westlake International Forum on Cyber Security Research in Hangzhou, China 2025
2024 Annual Conference of Chinese Association for Cryptologic Research (*ChinaCrypt'24*) in Hangzhou, China 2024
The 33rd USENIX Security Symposium (*Security'24*) in Philadelphia, USA 2024

Honors & Awards

CBI Fellowship, Carnegie Bosch Institute 2026
Outstanding Doctoral Dissertation, Tsinghua University 2026
Outstanding Graduate (Beijing), Beijing Municipal Commission of Education 2026
National Scholarship (Doctorate), 30000 CNY, Ministry of Education of the P. R. China 2025
Internet Defense Prize (1/2276, top 0.04%), 50000 USD, the 33rd USENIX Security Symposium 2024
Distinguished Paper Award (15/2276, top 0.7%), the 33rd USENIX Security Symposium 2024
Best Poster Award (1/52, top 1.9%), the 8th Westlake International Forum on Cyber Security Research 2024
Deng Feng Fund for International Conference Travel, 15000 CNY, Tsinghua University 2024, 2025
Comprehensive Excellence Scholarship (First-Tier), 10000 CNY, Tsinghua University 2023, 2024
Outstanding Social Service Scholarship, 1000 CNY, Tsinghua University 2023
Outstanding Graduate, Department of Computer Science and Technology, Tsinghua University 2021, 2026
Tsinghua-Sohu R&D Scholarship, 10000 CNY, Tsinghua University and Sohu, Inc. 2020

Academic Services

Teaching Assistant

Foundations and Frontiers of Cyberspace Security (74120023-0, Tsinghua) Fall 2022, Fall 2023, Fall 2024, Fall 2025
Core graduate-level CS course (~80 students)
I redesigned grading guidelines beyond regular TA work

Internet Architecture and Security Foundation (74120013-0, Tsinghua) Fall 2023, Fall 2024, Fall 2025
Graduate-level CS course (~20 students)
I prepared and led one session on BGP routing security beyond regular TA work

Next Generation Internet (00240112-90, Tsinghua) Spring 2023, Spring 2024
Undergraduate-level CS course (~15 students)
I designed and led one lab session on network measurement beyond regular TA work

Peer Reviewer

Journal Reviewer: IEEE TDSC

External Reviewer: USENIX Security 2022/2023, ISOC NDSS 2022/2023/2024/2025/2026, ACM CCS 2022/2023/2024/2025, ACM WWW 2025, IEEE ICNP 2025, ACM ASIACCS 2022/2024